



SECTOR RISK ASSESSMENT

**Money Laundering and Terrorist
Financing Through Virtual Assets and
Virtual Asset Service Providers 2023**

**BANK OF PAPUA NEW GUINEA'S
FINANCIAL ANALYSIS AND SUPERVISION UNIT**

ACKNOWLEDGEMENTS

The Bank of Papua New Guinea through the Financial Analysis and Supervision Unit compiles the development of this Sector Risk Assessment on Money Laundering and Terrorist Financing through virtual assets and Virtual Assets Service Providers. FASU acknowledge the support of the financial institutions and Designated Non-Financial Businesses or Professions, National Coordinating Committee member agencies and individuals who participated in the related survey. Their contribution enabled the development of this Sectoral Risk Assessment.

DISCLAIMER

The publication remains the property of the Bank of Papua New Guinea through FASU based on the information available and responses obtained at the time of the publication. Its officers will not be held liable for any loss incurred as a result of this publication.

This publication is pursuant to Section 72 (2) (b) of the *Anti-Money Laundering and Counter Terrorist Financing Act 2015*. Permission is required from FASU in order to reproduce, or copy any or part of this publication.

Contact fasu@bankpng.gov.pg or PDCD@bankpng.gov.pg for any queries relating to this publication.

CONTENTS

ABBREVIATIONS	3
EXECUTIVE SUMMARY	4
FOREWORD	6
1. CHANGES TO THE FATF STANDARDS	7
2. UNDERSTANDING VIRTUAL ASSETS.....	7
3. RISKS ASSOCIATED WITH VIRTUAL ASSETS	12
4. METHODOLOGY and FINDINGS	12
4.1. Risk Assessment Methodology	12
4.2. Review of Major VASPs Globally	13
4.3. Findings of the Survey on Virtual Assets and VASPs in PNG	15
4.4. Analysis of Survey Results.....	16
5. LIMITATIONS	17
6. RECOMMENDATIONS AND CONCLUSION.....	23
7. INDICATORS TO IDENTIFY TRANSACTIONS RELATED TO VIRTUAL ASSETS	24
8. APPENDICES	26
8.1. Appendix 1 – Sources of External Information	26
8.2. Appendix 2 – Survey Questionnaire.....	27
8.3. Appendix 3 – Survey Questionnaire Responses.....	31

ABBREVIATIONS

AML/CTF/CPF	Anti-Money Laundering, Counter Terrorist Financing and Counter Proliferation Financing
ATM	Automated Teller Machine
BPNG	Bank of Papua New Guinea
CDD	Customer Due Diligence
DNFBP	Designated Non-Financial Business or Profession
FASU	Financial Analysis and Supervision Unit
FATF	Financial Action Task Force
FI	Financial Institution
FIU	Financial Intelligence Unit
KYC	Know Your Customer
ME	Mutual Evaluation
ML/TF/PF	Money Laundering, Terrorist Financing and Proliferation Financing
MVTS	Money or Value Transfer Service Providers
P2P	Peer-to-Peer
PNG	Papua New Guinea
RBA	Risk Based Approach
SRA	Sector Risk Assessment
VA	Virtual Asset
VASP	Virtual Asset Service Provider

EXECUTIVE SUMMARY

The Financial Action Task Force (FATF) is the international standard-setting body that aims to Combat Money Laundering, Terrorist Financing and Proliferation Financing (ML/TF/PF). At its core, the Standards require countries to identify, assess, and understand the risks of ML/TF/PF they face to ensure adequate mitigating measures are established at a national level. Papua New Guinea (PNG) undertook a National Risk Assessment in 2017 and has subsequently undertaken sector risk assessment on Virtual Assets and Virtual Assets Service Providers to understand their presence in the country.

In 2018-2019, the FATF adopted amendments to its Standards to clarify how its Anti-Money Laundering, Counter Terrorist Financing and Counter Proliferation Financing (AML/CTF/CPF) requirements apply in the context of virtual assets and virtual asset service providers (VASPs). This is PNG's first Sector Risk Assessment (SRA) on Money Laundering and Terrorist Financing (ML/TF) through virtual assets and VASPs, and it forms a key component of the country's implementation of the revised Standards, particularly Recommendation 15, where *'countries and financial institutions (FIs) are required to identify and assess the ML/TF risks that may arise in relation to (a) the development of new products and new business practices, including new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products[...]*'. This ML/TF SRA of virtual assets and VASPs suggests the following findings:

- The risk of ML/TF through virtual assets and VASPs in PNG is considered **medium** considering that PNG has not established a legal framework to regulate the trading of virtual assets and VASPs. It appears that key authorities lack tools and technical knowledge on virtual asset eco system to properly supervise this sector;
- There is no evidence of foreign or domestic-sourced funds or virtual assets being laundered in or through PNG using existing structures or channels such as VASPs;
- There is no evidence of TF through virtual assets or VASPs in PNG;
- There is no evidence of VASPs being domiciled in PNG. However, Papua New Guineans do have access to VASPs domiciled elsewhere, via the internet;
- The main risk of ML/TF associated with virtual assets relates to PNG citizens accessing virtual assets over the internet. However, there are no cases of ML/TF through VA/VASP being reported, detected or identified to-date; and

- PNG should continue to remain vigilant to the evolving risks relating to virtual assets and VASPs, and should continue to strengthen its defences against potential risks.

FASU has pro-actively undertaken research, intelligence gathering and monitoring to detect any ML/TF that may be occurring using virtual assets and VASPs in PNG. This exercise has provided PNG with an unprecedented level of understanding of the ML/TF risks in this area, giving the country a firm foundation from which to monitor and mitigate emerging risks relating to new technologies on an ongoing basis.

FOREWORD

The Bank of Papua New Guinea (BPNG)'s Financial Analysis and Supervision Unit (FASU) is PNG's Financial Intelligence Unit (FIU) and AML/CTF S. As the AML/CTF supervisor, it is mandated to oversee, monitor, and enforce compliance with the *Anti-Money Laundering and Counter Terrorist Financing Act 2015* (the Act). Part of FASU's compliance function is to ensure that reporting entities¹ implement adequate measures to enable them to deter, detect, and report ML/TF related activities.

FASU commenced the development of this SRA² on virtual assets and VASPs in 2020 to understand the associated risk or impact these high-tech advancement may have on reporting entities in the country. This was conducted in a manner that complies with the updated FATF Recommendation 15 and international standards that related to ML /TF risks using virtual assets and VASPs in PNG.

Despite the limitations and challenges encountered or identified through this risk assessment, the findings are based on sufficient data to adequately support the financial sector, regulators, law enforcement agencies and other stakeholders in the development of processes and frameworks to manage the ML/TF risks associated with virtual assets and VASPs.

¹ Reporting entities are financial institutions and designated non-financial business or profession defined by Section 5 of the Act.

² Pursuant to its function under Section 72 (2)(b) of the Act to develop risk assessments.

1. CHANGES TO THE FATF STANDARDS

FATF Recommendation 1 requires countries to identify, assess, and understand the ML/TF/PF risks within their jurisdiction, and to implement measures to mitigate those risks.

In October 2018, the FATF adopted a revised Recommendation 15 on new technologies. Prior to the 2018 amendment, Recommendation 15 already required countries and financial institutions to identify and assess the ML/TF risks that may arise in relation to new technologies. The 2018 revision of Recommendation 15 formally incorporated virtual assets and VASPs into the FATF standards. In particular, Recommendation 15 requires VASPs to be regulated for AML/CTF purposes, and licensed or registered, and subject to effective systems for monitoring and supervision to ensure compliance with the relevant measures called for in the FATF Recommendations.

In June 2019, the FATF adopted a new interpretive note to Recommendation 15. The interpretive note provides clarity on various aspects of how the FATF requirements apply in relation to virtual assets and VASPs. Regarding risk assessment, the interpretive note states: *In accordance with Recommendation 1, countries should identify, assess, and understand the money laundering, terrorist financing and proliferation financing risks emerging from virtual asset activities and the activities or operations of VASPs.* The interpretive note also covers: the application of the risk based approach (RBA); licensing and registration; regulation, supervision and monitoring; sanctions for non-compliance by VASPs; and preventative measures such as Customer Due Diligence (CDD), record keeping, suspicious matter reporting, sanctions screening and monitoring; and international cooperation.

The FATF also published guidance to assist countries and entities in applying a RBA to virtual assets and VASPs, and has issued interpretive notes in other key related areas, in particular Recommendation 16 on wire transfers.

2. UNDERSTANDING VIRTUAL ASSETS

The FATF uses the term ‘virtual asset’³ to refer to digital representations of value that can be digitally traded or transferred and can be used for payment or investment purposes. These includes digital representations of value that function as a medium of exchange, a unit of

³ <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf>

account, and/or a store of value. The FATF emphasises that virtual assets do not include digital representation of fiat currency (a.k.a. “real currency,” “real money,” or “national currency”), which is the money of a country that is designated as its legal tender, securities, and other financial assets that are already covered elsewhere in the FATF Standards.

Virtual assets enable pseudo-anonymous transactions, fast cross-border value transfer and non-face-to-face business relationships. Those properties have the potential to improve multiple financial products and services such as trade financing, cross-border payments and financial instrument settlement. Criminal organisations, cybercriminals, human traffickers among others use virtual assets to move and launder the proceeds of crime. Virtual assets allow such groups to access cash anonymously and obscure the transaction trail. Some virtual assets, such as Monero, are designed as privacy coins to obfuscate the identities of the sender, the recipient, and the transaction itself which challenge customer due diligence (CDD) measures and therefore are particularly appealing to criminals.

The United Nations estimates that the amount of money laundered every year is around 2-5% of global GDP (\$800bn - \$2tn)⁴. Although virtual assets remain the asset of choice by criminals for certain unlawful activities⁵ in 2020, global virtual asset-related crime fell from \$21.4bn (2.1% of all virtual asset transaction volume in 2019), to \$10bn (0.34% of all virtual asset transaction volume in 2020)⁶

2.1. Difference between Virtual Assets and e-money or Virtual Currency

Virtual assets and e-money are both digital currencies where the value can be exchanged, stored and transferred electronically. The difference between them is that e-money is backed by a fiat currency (currency that has legal tender status in a country), and can be used as transfer mechanism for fiat currency. In contrast, virtual assets are not backed by any fiat currency.

2.2. The Virtual Assets Exchange Eco System

The following are the major participants of virtual asset exchange eco system:

⁴ <https://www.unodc.org/unodc/en/money-laundering/overview.html>

⁵ <https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021>

⁶ <https://go.chainalysis.com/rs/503-FAP-074/images/Chainalysis-Crypto-Crime-2021.pdf>

- a) **Administrator:** the person or entity, which issues centralized virtual assets, establishes the rules for its use; maintains a payment ledger; and has the authority to redeem the virtual assets.
- b) **Miner:** the person or entity that participates in a decentralized virtual assets network by running special software to solve complex algorithms in a distributed proof system used to validate transactions in the virtual asset exchange eco system.
- c) **Exchanger:** the person or entity engaged in business of virtual assets exchange for real currency, funds, or other forms of virtual assets for a commission. Exchangers typically accept a wide range of payments, such as cash, wire transfers, credit cards, and other virtual assets. Individuals typically use exchangers to deposit and withdraw money from virtual assets accounts. Some of the well-known exchangers are Bitfinex, Coinbase, Bitstamp, Poloniex, Coinmama, CEX.IO etc.
- d) **User:** a person/entity who obtains and uses the virtual assets. Users can obtain virtual assets in several ways. For example, they can purchase virtual assets, using fiat currency, from an exchanger or from an administrator or miner. Alternatively, a user can engage in specific activities that earn virtual assets as payment.
- e) **Virtual asset wallet:** the software application for holding, storing and transferring virtual assets.
- f) **Wallet provider/custodian:** an entity that provides a virtual asset wallet for holding, storing and transferring virtual assets. A wallet provider facilitates participation in a virtual asset exchange eco system by allowing users, exchangers, and merchants to more easily conduct the virtual assets transactions. The wallet provider maintains a customer's virtual assets balance and provides storage and transaction security. Some well-known wallet providers are Bitcoin Core protocol, Electrum, Exodus, Jaxx, Copay, Coinbase, Blockchain etc.

2.3. Classification of Virtual Assets

Based on the involvement of different participants in the virtual asset exchange eco system, virtual assets can be categorised as either centralized or decentralized virtual assets. Table one (1) shows the distinctive features of these categories.

Table 1. Features of centralised and decentralised virtual asset exchange eco system

Criterion	Centralized	Decentralized
Software Architecture	Centralized	Distributed (Blockchain)
Issuer	Administrator	Miner
Exchange Rate	Pegged	Floating
Convertibility	Exchanged for fiat currency	Exchanged for fiat currency
Participants	Administrator, Exchanger, User	Miner Exchanger, User
Examples	E-gold, Web Money, Linden Dollars	Bitcoin, Onecoin, Litecoin, Ripple

*Source: Pakistan Financial Intelligence Unit's 2019 Strategic Analysis – Virtual Assets
Emerging Risk of Money Laundering and Terrorism Financing*

Decentralized virtual assets may be more vulnerable to ML/TF abuse, due to the ease of convertibility and the distributed architecture upon which they are based. In some cases, this may provide anonymous transfer of funds without passing through a central authority.

2.4. The Transaction Cycle of Virtual Assets

The transactions of virtual assets relies on public and private keys (typically provided through a virtual assets wallet) to transfer value from one person to another. The safety, integrity and balance of virtual assets ledgers is provided by a network of mutually sceptical parties (miners) who protect the network in exchange for the opportunity to obtain a randomly distributed fee.

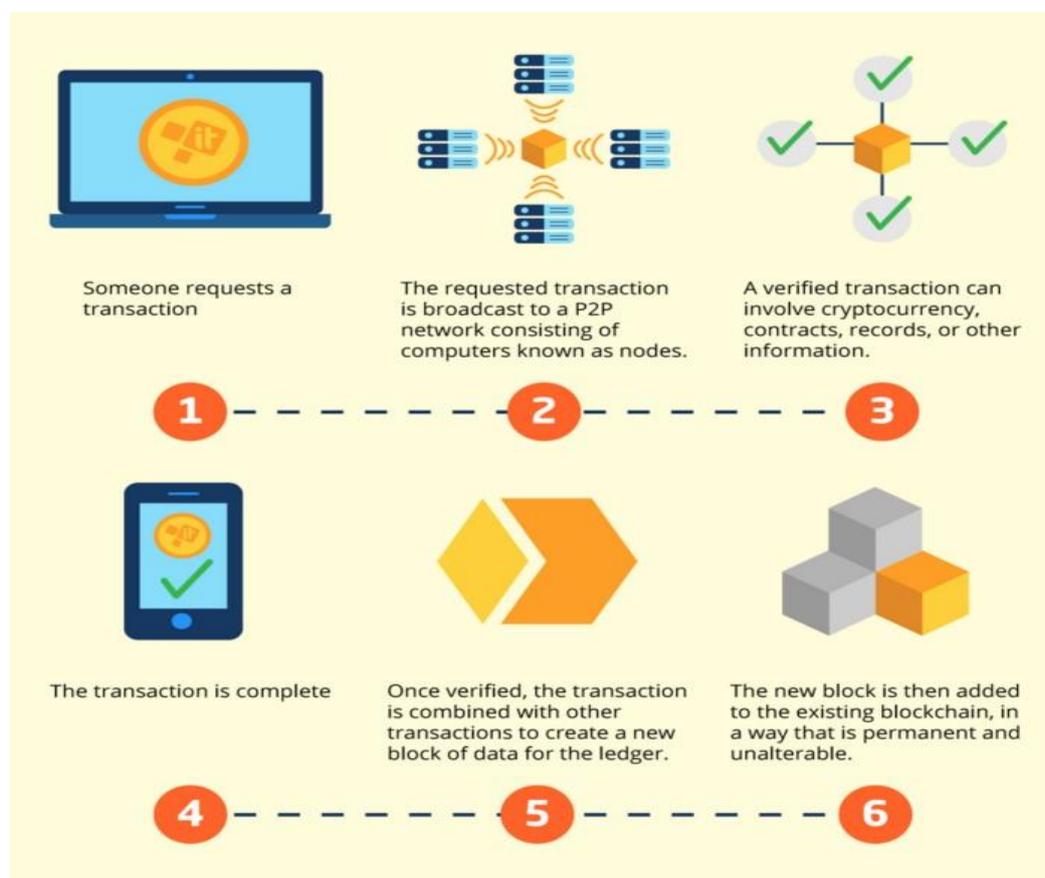
The general process of transferring virtual assets, such as bitcoin, from one person to another is:

- a) **Virtual asset wallets:** The individuals (sender and receiver) acquire virtual asset wallets for performing a transaction. A virtual asset wallet contains a public key and a private key.
- b) **Address creation:** The receiver randomly generates a new address (public key) for the sender using the wallet.
- c) **Payment submission:** The sender will enter the unique address (public key) shared by the receiver in the wallet along with the amount of virtual assets to be sent.
- d) **Signature:** The sender will digitally sign the transaction with a unique private key, which will prove the integrity of transaction.

- e) **Transmission and validation:** The transaction will go through the distributed network to nodes where verification checks are performed and the verified transaction is communicated to other peers in the network.
- f) **Creation of block:** After validation, miners include the transaction in the next block to mine.
- g) **Proof-of-work:** Miners will compete with each other to calculate a hash that will solve the Proof-of-Work. This process takes 10 minutes on average.
- h) **Confirmation of transaction:** Once the transaction is included in a block, the sender and receiver will receive a confirmation in their wallets that the transaction is complete.

Once the transaction gets included in a block, it cannot be reversed or altered. A set of virtual asset transactions creates a block. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data, thereby forming a chain - hence the term 'Blockchain'.

Figure 1. A graphical transaction cycle of a virtual asset, in which a Bitcoin transfer transaction is performed.



Picture Credit: *Vladimir Fedak* _ <https://towardsdatascience.com>

The complexity of the virtual asset exchange eco system require officers of regulatory and law enforcement agencies (LEAs) to have certain level of technical capability or proficiency to understand the mechanisms behind the creation, transactions and trading of virtual assets. There are several range of cross cutting considerations with respect to the assignment of the responsibility for AML/CTF/CPF supervision and enforcement for transactions related to virtual assets. Domestic key authorities and LEAs may face barriers to deal with VASPs that are located in foreign jurisdictions.

3. RISKS ASSOCIATED WITH VIRTUAL ASSETS

Like all businesses, VASPs are not immune from ML/TF risks. Information available online shows that supervision, monitoring and regulation of VASPs can be challenging. PNG have to find ways to deal with possible risks in this unregulated sector such as but not limited to “absence of virtual asset transaction analytical tools at the disposal of reporting entities for monitoring of virtual assets transactions”, “no government e-wallet to seize or confiscate virtual assets or cryptocurrencies after successful ML/TF conviction”, and “absence of supervisory tools” for regulators to monitor and enforce compliance in this sector. This also could suggests that lack of specialised resources and appropriate technological tools may be perceived as a major risk for the country to address in the nearest future on an ongoing basis. The lack of a regulatory framework for virtual assets and VASPs, at the time of developing this risk assessment may imply that PNG’s key authorities are yet to develop in-house capacity to build stronger understanding of the virtual asset exchange eco system and its impact on the economy.

4. METHODOLOGY and FINDINGS

4.1. Risk Assessment Methodology

The SRA developed by FASU is focused on highlighting the uncertainties around the conduct of virtual assets and VASPs in PNG, and whether or not they have a presence or establishment in country. In order to reach that conclusion, FASU undertook a two-step approach. First, FASU completed a literature review to better understand the state of play regionally and internationally with virtual assets and VASPs. This included a review of FATF publications, reports and documents on virtual assets and, AML/CTF regulations from other countries.

Second, based on the information and understanding developed from this literature review, a survey was conducted to gather quantitative and qualitative data.

The bulk of the selected survey participants were reporting entities that have registered with FASU in 2020 (i.e. total of 135 reporting entities, 60 financial institutions and 75 DNFBPs). The survey questionnaire was circulated to a targeted population of 37 organisations, which consisted of 18 financial institutions and 12 DNFBPs that were registered with FASU. The participants of the survey were:

- 10 out of 16 firms from the banking and finance sector;
- 4 out of 19 firms from the insurance sector;
- 2 out of 8 firms from superannuation sector;
- 2 out of 2 firms from the securities/stock exchange sector;
- 5 out of 32 firms from the legal sector;
- 4 out of 22 firms from accounting and auditing sector;
- 3 out of 13 firms from the real estate sector;
- 3 peer regulators responsible for the banking and finance sector, the superannuation, sector and general insurance sector; and
- 4 information and technology (IT) experts from IT companies including BPNG's IT and Communication Department's Consultant.

The selected survey population were mainly from the industries with high probability of being involved in, or exposed to, virtual asset transactions or VASPs. From the targeted population, managers and senior officers who are familiar with virtual assets and VASPs were encouraged to participate in the survey. From the FASU registered 135 reporting entities, the reporting entities that did not participate in the survey were moneychangers, savings and loans societies companies, life insurance companies, dealers in precious metals and stones and motor vehicle dealers. The FASU held registration information on these reporting entities that did not participate in the survey suggests that there may be less or no transactional activities relating to virtual assets and VASPs being conducted by these reporting entities.

4.2. Review of Major VASPs Globally

The development and advancement in technology has had a significant impact with the use of virtual assets prompting widespread public adoption. While people find it easier and cheaper to make payments by embracing change in the new technological arena, it also pose challenges for ML/TF/PF for countries.

Some jurisdictions accepted the use of virtual assets and have developed regulatory framework that is evolving rapidly and changing at a faster pace. Other jurisdictions have imposed an absolute ban on the use of virtual assets while others are in between and still deciding on best possible options.

PNG does not have existing or active domiciled VASPs and merchants that are operating or providing accessibility or trading platform for users of virtual assets. However, as part of the global community, PNG is not immune to the ML/TF/PF risks posed by virtual assets and VASPs. The Bank of PNG has made public statements⁷ advising the public *“cryptocurrencies are not currencies issued or regulated by PNG’s Central Bank. They do not have any legal tender status to be accepted as a currency in PNG. Investment in such digital currencies is considered very risky and speculative in nature. PNG’s Central Bank have however been researching into the potential use of block chain technology as a platform for promoting financial inclusion.”*

Domestic commercial banks take the risk associated with crypto currencies gravely where they have stopped the use of their VISA cards for cryptocurrency and similar type of transactions. The BSP Financial Group Limited (BSP) published on its website⁸ that *“due to concerns regarding the ability of BSP to have access to data relating to cryptocurrency transactions, and the authenticity of those transactions, BSP’s VISA cardholders will no longer be able to perform transactions using their BSP issued VISA card for cryptocurrency type transactions”*. Further, Kina Bank Limited published cryptocurrency information on its website⁹ pointing out that the bank *“does not recognise cryptocurrency, nor does it help facilitate in the trading of any cryptocurrency”*.

There are different channels/platforms that are used for virtual asset trading. The major channels for exchanging virtual assets globally are:

- www.fxpro.com
- www.localbitcoins.com
- www.cmcmarkets.com
- www.iqoptions.com
- www.playtika.com
- www.etoro.com
- www.mtlotcrypto.com
- www.coinmama.com

⁷ March 2023 - <https://studyinpng.com/2023/03/bank-of-papua-new-guinea-warning-against-fast-money-schemes-or-scams/>, July 2018 - <https://www.looppng.com/business/bpng-warns-against-cryptocurrencies-78050>, https://www.bankpng.gov.pg/wp-content/uploads/2018/07/Cryptocurrency_half-page-portrait-1.pdf
January 2022 - <https://news.pngfacts.com/2022/01/png-kina-bank-suspends-local-sme.html>,

⁸ <https://www.bsp.com.pg/about-us/bsp-publications/cryptocurrencies/>

⁹ <https://www.kinabank.com.pg/understanding-cryptocurrency-and-how-it-all-works/>

- www.coindirect.com
- www.bitsale.com
- www.bitlish.com
- www.24Option.com
- www.finq.com
- www.skrill.com
- www.moneypolo.com
- www.robokassa.ru
- [International Capital Market PTY limited, Australia](http://InternationalCapitalMarketPTYlimitedAustralia)
- www.instaforex.com
- www.cex.io
- www.mexbitcoin.com
- www.coinbase.com
- www.trade.com
- www.bitcoins.com
- www.fxpro.com
- www.plaster.co
- www.neteller.com
- www.axitrader.com

None of these channels is domiciled in PNG. However, there are uncertainties about PNG nationals accessing such online platforms to trade with virtual assets. Hence, the ML/TF risk remains at **medium** given that there is no cases and that there is no consequences.

4.3. Findings of the Survey on Virtual Assets and VASPs in PNG

The result of the survey demonstrate zero or minimal presence of virtual assets and VASPs in PNG. Further, responses from the survey suggest that there is no evidence of crowd participants in this sector:

- 96% of the respondents indicated that their business does not have any VASPs as customers;
- All of the respondents confirmed that their business does not provide exchange services for virtual assets (exchanging virtual assets to fiat currency or other assets);
- 96% of the respondents have not identified any of their customers using virtual assets;
- 98% of the respondents attested that their business does not make virtual assets accessible for their customers;
- 94% of the respondents were not aware of any events that could be characterized as ML/TF involving virtual assets in PNG;
- 77% of the respondents stated that they did not think that there are vulnerabilities in PNG's AML/CTF regime that might render PNG vulnerable to ML/TF involving virtual assets.

4.4. Analysis of Survey Results

Prima facie, the survey responses suggest there is a low risk of ML/TF relating to VA/VASPs in PNG. None of the respondents provides exchange services to move into fiat currency. Furthermore, close to 100% of respondents indicated zero VASP customers, do not have any customers using VASPs, do not make virtual assets accessible for customers and have not seen evidence of possible ML/TF events involving VASPs. The minority who responded positively to the survey questions noted occurrences of online scams none of which were information related to virtual asset trading nor possible occurrences of ML/TF through the virtual asset exchange eco system. These headline findings suggest zero or minimal presence of VA/VASPs in PNG.

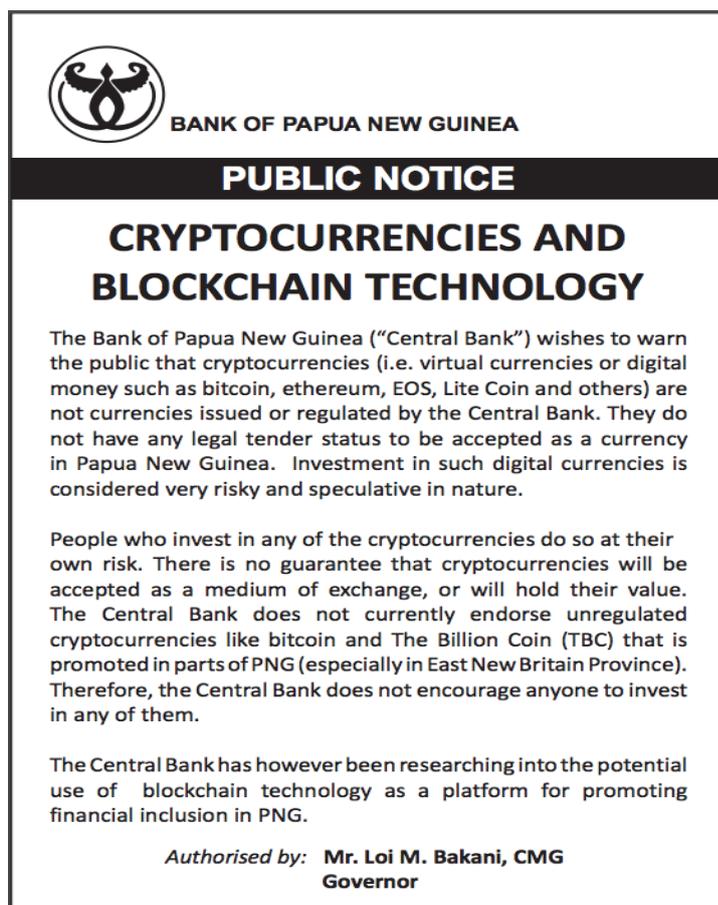
However, this conclusion would be hasty for several reasons. First, some of the responses might indicate a low level of understanding of VA/VASPs rather than a low level of risk. Second, bank reporting suggests that there are some bitcoin and crypto currency scams being conducted in PNG. Indeed, Papua New Guineans have been victims of online scam and fraud because most are unaware of how scammers operate¹⁰. Third, the borderless nature of VASPs suggest that while we may not identify any operating in PNG currently, the country is susceptible to the risks posed by VASPs external to PNG.

In considering the VA/VASP risk, it is also important to consider the wider risk environment i.e. the potential interaction between VA/VASPs and other ML/TF risk areas in PNG. In the future, PNG could build its understanding around possibilities of VAs that may be used to facilitate illegal activities such as fraud and forgery, smuggling and illegal trade in wildlife.

Regarding the vulnerability side of the risk assessment, over three-quarters of respondents did not think there are particular vulnerabilities. This could be related to the fact that the Bank of PNG does not recognize virtual assets as legal tender in PNG and discourages the public from trading in any type of virtual asset transactions, as demonstrated in Figure 2 below. That said, there is an absence of a legislative basis in PNG aimed at managing ML/TF risks relating to VA/VASPs. This likely increases PNG's vulnerability to ML/TF risk related to VA/VASPs and is potentially a driver behind the 23% of survey respondents that identified such vulnerabilities.

¹⁰ <https://www.postcourier.com.pg/pngx-warns-against-crypto-scams/>

Figure 2. Bank of PNG’s public notice cautioning the public that cryptocurrency is not recognised in PNG.



Picture Credit: <https://www.bankpng.gov.pg/news-events/cryptocurrencies-and-blockchain-technology/>

5. LIMITATIONS

The virtual asset exchange eco system is an emerging market, which evolved rapidly in the developed economies with the change in technology. In PNG, the application of virtual assets and VASPs appear to be minimal to none. However, thorough understanding of the virtual asset exchange eco system will position key authorities to develop appropriate AML/CTF policies and regulations related to virtual assets and VASPs that will eventually:

- Increase understanding of virtual asset exchange eco system and its players/actors.
- Increase understanding of ML/TF risks and vulnerabilities associated with trading of virtual assets;

- Increase understanding of different virtual assets' characteristics;
- Increase understanding of ways to safeguarding the financial sector from the risks posed by virtual assets and VASPs;
- Increase capabilities of key authorities to identify the financial sectors, products, delivery channels, and transactional pattern adopted by virtual asset traders for sale/purchase of different virtual assets; and
- Increase understanding on how to identify red flag indicators involved in virtual asset trading concerning customers, products, delivery channels and geographic areas.

It is important to note that, at the time of developing this risk assessment, the focus of the methodology was to determine the presence of VASPs in the country's financial sector. Therefore, it is suggested for PNG to take a whole of government approach to develop an enhanced, in-dept VA/VASP risk assessment in the near future using the World Bank's VA/VASP Methodology and Risk Assessment Tool.

A report¹¹ published by the Law Library of Congress, Global Legal Research Directorate of the United States in 2021 further covered the regulation of cryptocurrencies around the world. The report noted that regulatory framework surrounding cryptocurrencies, in particular the application of tax laws and AML/CTF laws to cryptocurrencies vary from one country.

Table 2. Virtual assets and VASPs regulatory framework of different countries

Jurisdiction	Ban on Cryptocurrencies?		Application of Tax Laws?	Application of AML/CTF Laws?	Citations
	Absolute?	Implicit?			
Australia	No	No	Yes	Yes	<p>Tax: <i>Tax Treatment of Cryptocurrencies</i>, Australian Taxation Office (ATO), https://perma.cc/QDX7-NQME; GST and Digital Currency, ATO, https://perma.cc/276V-HPY7 (GST does not apply unless carrying on a business).</p> <p>AML/CFT: Digital Currency Exchange Providers, AUSTRAC, https://perma.cc/SL99-8C75; AML/CFT Act 2006 (Cth) pt 6A, https://perma.cc/Y4JM-T3FB.</p>
Brunei	No	No	No Information	No Information	<p>Press Release, Autoriti Monetari Brunei Darussalam, Public to Exercise High Caution with Cryptocurrencies (Dec. 22, 2017), https://perma.cc/4N9M-AL26.</p>
Canada	No	No	Yes	Yes	<p>Tax: Virtual Currency, Canada Revenue Agency (CRA), https://perma.cc/YQ43-HDHB; Guide for Cryptocurrency Users and Tax Professionals, CRA, https://perma.cc/25YR-EFNH.</p>

¹¹ Link for the report published by the Law Library of Congress, Global Legal Research Directorate of the US <https://tile.loc.gov/storage-services/service/l1/llglrd/2021687419/2021687419.pdf>

					AML/CFT: Proceeds of Crime (Money Laundering) and Terrorist Financing Registration Regulations SOR/2007-121, https://perma.cc/64T9-J3U4 , (under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act, S.C. 2000, c. 17, https://perma.cc/KL6H-6JXQ); Money Laundering and Terrorist Financing Indicators—Virtual Currency Transactions, FINTRAC, https://perma.cc/LE2J-7HCS .
China	Yes	No	Unclear	Unclear	People’s Bank of China , Circular on Further Preventing and Disposing of Speculative Risks in Virtual Currency Trading (Sept. 15, 2021), § 1(2), https://perma.cc/DC7U-MSDF .
Hong Kong	No	No	Yes	Yes	Tax: Hong Kong Inland Revenue Department, Departmental Interpretation and Practice Notes No. 39 (Revised) (Mar. 2020), https://perma.cc/AXN9-CE3G .
					AML/CFT: Securities and Futures Commission, Position Paper: Regulation of Virtual Asset Trading Platforms (Nov. 6, 2019), para. 61, https://perma.cc/9ZEP-7B83 .
Indonesia	No	Yes	No	No	Cryptocurrencies—Indonesia’s Current Legal Climate on Crypto Assets, Bagus Enrico & Partners (Mar. 9, 2021), https://perma.cc/4N26-AXM9 ; Yihui Xie, Indonesian Regulators Play Catch-up as Crypto Investment Soars, Forkast (July 23, 2021), https://perma.cc/TY5H-3Q6T .
Japan	No	No	Yes	Yes	Tax: Tax Treatment of Cryptocurrencies, National Tax Agency, https://perma.cc/K64T-4AVE .
					AML/CFT: Act on Prevention of Transfer of Criminal Proceeds art. 2, para. 2, item 31, https://perma.cc/M9U6-PVJP (in Japanese).
Malaysia	No	No	Yes	Yes	Tax: Digital Business, Inland Revenue Board of Malaysia, https://perma.cc/7CCP-2BYV ; Inland Revenue Board of Malaysia, Guidelines on Electronic Commerce Transactions (May 2019), https://perma.cc/CL3U-74WS .

					AML/CFT: Bank Negara Malaysia, Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) — Digital Currencies (Sector 6) (Feb. 2018), https://perma.cc/69RQ-R4LM .
Philippines	No	No	No Information	Yes	AML/CFT: Bangko Sentral ng Pilipinas, Guidelines for Virtual Currency (VC) Exchanges, Circular No. 944 (Feb. 6, 2017), Subsec. 4512N.1 Scope, https://perma.cc/XY84-GQB8 ; Anti-Money Laundering Council, 2018 Implementing Rules and Regulations of Republic Act No. 9160, as amended, Rule 19-5.2, https://perma.cc/SH7Y-A93F .
Singapore	No	No	Yes	Yes	Tax: Inland Revenue Authority of Singapore, IRAS e-Tax Guide: Income Tax Treatment of Digital Tokens (Apr. 17, 2020, rev. Oct. 9, 2020), https://perma.cc/9S9Q-3MAR .
					AML/CFT: Monetary Authority of Singapore, A Guide to Digital Token Offerings (May 26, 2020), para. 3.1, https://perma.cc/6NNQ-3H76 .
South Korea	No	No	Yes (from 2022)	Yes	Tax: Income Tax Act art. 21, para. 1, sub-para. 27, https://perma.cc/KB96-BRAU (in Korean).
					AML/CFT: Act On Reporting And Using Specified Financial Transaction Information art. 2, para. 1, sub-para. n, https://perma.cc/P4BB-ASBA (in Korean).
Taiwan	No	No	Yes	Yes	Tax: Central Bank: 90% of Bitcoin Transactions Are Speculative Investments, with Payments Account for Only 1%,
					Overseas Community Affairs Council, Republic of China (Taiwan) (Nov. 2, 2021), https://perma.cc/AQL8-HQG9 .
					AML/CFT: Money Laundering Control Act (Nov. 7, 2018), art. 5, https://perma.cc/Z5GU-KNS4 ; Financial Supervisory Commission, Regulations Governing Anti-Money Laundering and Countering the Financing of Terrorism for Enterprises Handling Virtual Currency Platform or Transaction (June 30, 2021), https://perma.cc/M8ET-S8QL .
Thailand	No	No	Yes	Yes	Tax: Revenue Code sec. 40 (4) (h) & (i), https://perma.cc/AZ6M-5D6G .

					AML/CFT: Anti-Money Laundering Act B.E. 2542 (1999), https://perma.cc/5NF4-2YP6 (in Thai).
United States	No	No	Yes	Yes	Tax: I.R.S. Notice 2014-21, 2014-16 I.R.B. 938 (Apr. 14, 2014), https://perma.cc/GY3L-57JK ; Frequently Asked Questions on Virtual Currency Transactions, Internal Revenue Service (June 4, 2021), https://perma.cc/B85E-M37X .
					AML/CFT: Application of FinCEN’s Regulations to Certain Business Models Involving Convertible Virtual Currencies, Fin. Crimes Enft Network (May 9, 2019), https://perma.cc/JZ2C-TBRN . See also Anti-Money Laundering and Countering the Financing of Terrorism National Priorities, Fin. Crimes Enft Network (June 30, 2021), https://perma.cc/B3EL-93UB . (FinCEN intends to issue regulations specifying how financial institutions should incorporate “cybercrime, including relevant cybersecurity and virtual currency considerations, “among other priorities, into their AML programs.)
Vietnam	No	Yes	No	Yes	Ban: State Bank of Vietnam (SBV) Official Letter No. 5747/NHNN-PC dated July 21, 2017, https://perma.cc/W7E6-3K9B (cryptocurrencies are not legal currencies or a means of payment in Vietnam, and any issuance, supply, or use of them as currency or a means of payment is prohibited, and subject to administrative or even criminal sanctions).
					AML/CFT: Directive No: 10/CT-TTg on Improving the Management of Activities Related to Bitcoins and other Similar Virtual Currencies (Apr. 11, 2018), https://perma.cc/35TZ-8VPF .

Source: Law Library of Congress, Global Legal Research Directorate of the US, see website link in footnote⁸

6. RECOMMENDATIONS AND CONCLUSION

As identified in the survey, very few PNG nationals are participating in the trade of virtual assets. The scope and use of virtual assets inevitably will increase in PNG in the near future given the developing landscape in the use of technology. There is need for domestic regulatory framework for virtual assets and VASPs in place to comply with the international standards for combating ML/TF/PF.

A committee should be formed at the national level to develop legal and regulatory framework to govern the trading of virtual assets in PNG. This committee should comprise of Technical Working Group (TWG) officers from key government agencies with capacity to build and maintain VA/VASP legal and regulatory framework for PNG. Alternatively, the current National Coordinating Committee (NCC) on AML/CTF co-chaired by the Department of Justice and Attorney General (DJAG) and BPNG's FASU can be the interim platform to pursue and manage matters that relates to virtual assets and VASPs. PNG need to identify and empower a suitable authority to regulate the VA/VASP sector. Further, where applicable, reporting entities must carry out internal risk assessment of virtual assets to decrease the inherent risk posed by the trading of virtual assets.

PNG can consider the following suggestions when developing a legal and regulatory framework for virtual assets and VASPs: limited to:

- PNG's AML/CTF legal framework could be amended to incorporate virtual assets and VASPs so that there is visibility in terms of registration or licensing, preventative measures such as CDD, record keeping, suspicious matter reporting, sanctions, other enforcement matters and international cooperation.
- In line with FATF Recommendation 15, the role of regulator for virtual assets and VASPs should be clearly assigned to a domestic agency. An amendment of the current AML/CTF Act can enable FASU to be the sole supervisor for VASPs until such time when an appropriate regulator or agency is identified. However, it is upon the country to decide the 'Suitable Authority' to regulate the VASP sector whilst considering the experience of other countries.
- The Suitable Authority can also license and regulate the conversion of virtual assets to fiat currency, which in this case would be PNG Kina (PGK) and will require more awareness to ensure the related 'acceptable practice of exchange' is widely accepted and used.

- More technical capacity building programs are needed, more publicity or awareness, to ensure that the country is adequately resourced to take on the new challenge
- AML/CTF requirements for financial institutions and DNFBPs must be applied to VASPs as required by the FATF standards.

As evident in the report published by the Law Library of Congress, Global Legal Research Directorate of the United States, countries have setup laws and regulations for governing virtual assets and VASPs whether as exchanger, platform to ease payment system or as commodity and security.

It is important that PNG take a proactive approach in coming up with a legal and regulatory framework to cater for the emerging risks posed by virtual assets and VASPs. If PNG finds it too risky to regulate the trading of virtual assets, the country should simply put an **‘absolute ban’** on trading of such assets. However, as a developing economy, more research needs to be conducted in order to reach a conclusive decision as well as addressing FATF recommendations.

7. INDICATORS TO IDENTIFY TRANSACTIONS RELATED TO VIRTUAL ASSETS

This technological era makes virtual assets accessible to criminals wish to launder and conceal their proceeds of crimes. Criminals will do everything to avoid the detection of their illicit activity that generated these proceeds or linkage to themselves. Possible red flag indicators of transactions that may be related to ML/TF through virtual assets are but not limited to one or a combinations of the following scenarios:

- Utilising of bank accounts, credit cards, debit cards, branchless banking facilities for trading of virtual assets to avoid over-the-counter transactions;
- Bank accounts and credit/ debit cards with high inter-bank fund transfer limits relating to virtual assets;
- Transactions involving more than one type of virtual assets particularly those that provide enhanced anonymity despite additional transaction fees;
- Virtual assets moved from a public, transparent block-chain to a centralised exchange and then immediately traded for anonymity enhanced cryptocurrency or privacy coin;

- Customers that operate as an unlicensed virtual asset service provider on P2P exchange website;
- Abnormal transaction activity of virtual assets from P2P platform associated wallets with no logical business explanation;
- Virtual assets traded to or from wallets that indicated the use of mixing or tumbling services or P2P platforms;
- Transferring virtual assets immediately to multiple VASPs including those operating in other countries;
- Transactions involving multiple virtual, or multiple accounts, without a logical business explanation; and
- Customer utilises a virtual asset exchanger or foreign-located money or value transfer service provider in a high-risk country lacking, or known to have inadequate AML/CTF regulations for VASPs, including inadequate CDD/KYC measures.

Each of these indicators does not necessarily indicate or constitute criminal activities, but must be considered in context and lead to further monitoring and examination.

8. APPENDICES

8.1. Appendix 1 – Sources of External Information

- <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-andpotential-aml-cft-risks.pdf>
- <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf>
- <http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf>
- <https://publications.jrc.ec.europa.eu/repository/bitstream/JRC105207/lbna28386enn.pdf>
- <https://www.loc.gov/law/help/cryptocurrency/world-survey.php>

8.2. Appendix 2 – Survey Questionnaire

Survey Title: Money Laundering and Terrorist Financing through Virtual Assets and Virtual Asset Service Providers in Papua New Guinea

The Bank of Papua New Guinea’s Financial Analysis and Supervision Unit (FASU) purposely to implement Recommendation 15 of the Financial Action Task Force’s (FATF) relating to new technology conduct this survey.

The purpose of this survey is to determine the level of money laundering and terrorist financing (ML/TF) risks relating to Virtual Assets (VA) and Virtual Assets Service Providers (VASPs) in PNG and its impact on the society. The results of this survey will be used to develop a sector risk assessment (SRA) on VA and VASP.

Please answer all questions as well as you can and should you have questions or seek further clarifications, do not hesitate to contact FASU. *All responses will be kept confidential and used only for the purpose mentioned above.*

Virtual Asset refers to any digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies (i.e. real money or banknotes and coins that are in circulation as medium of exchange or accepted legal tender), securities and other financial assets that are already covered elsewhere in the FATF Recommendations. Examples of VAs include virtual currencies such as Bitcoin.

Virtual Asset Service Provider refers to any natural or legal person who is not covered elsewhere under the FATF Recommendations and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

- i. exchange between virtual assets and fiat currencies;
- ii. exchange between one or more forms of virtual assets;
- iii. transfer of virtual assets;
- iv. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and

- v. participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

Financial innovation has drastically changed the financial scenery, new technologies, services and products offer efficient alternatives to standard financial products. At the same time, the speed and anonymity of some of these innovative products can attract criminals and terrorists who wish to use them to launder the proceeds of their crimes and finance their illicit activities.

Your responses will provide an indication of PNG's level of risk relating to laundering of illicit proceeds and financing of illicit activities through VASPs. FASU greatly appreciates your participation.

Thank you!

Survey Questions

1. Does your business have any customers or clients that are Virtual Asset Service Providers?

Yes

No

2. Does your business provide exchange services for Virtual Assets (exchanging virtual assets to fiat currency or other assets)?

Yes

No

If yes, what sort? Or please explain? _____

3. Are you aware of any customers or clients of your business using Virtual Assets?

Yes

No

If yes, approximately how many customers or clients and list down the type of virtual assets they use. Please explain -

4. Does your business provide access for clients or customers to Virtual Assets?

Yes

No

If yes, what type? Please explain -

5. Are you aware of any events that could be characterised as money laundering or terrorist financing involving virtual assets in Papua New Guinea?

Yes

No

If yes, please provide a short explanation.

6. Are you aware of events that could be characterised as money laundering or terrorist financing involving virtual assets in Papua New Guinea?

Yes

No

If yes, please explain what could be done to prevent similar event occurring again

-

7. Are you aware of vulnerabilities in PNG's AML/CTF regime that might render PNG vulnerable to money laundering or terrorist financing involving virtual assets?

Yes

No

If yes, please provide a short explanation

8. In your opinion, what might PNG authorities do to detect money laundering or terrorist financing involving virtual assets in the future?

Thank you for participating.

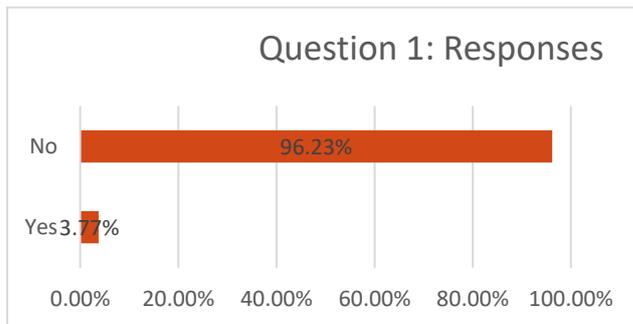
8.3. Appendix 3 – Survey Questionnaire Responses

Q1 Does your business have any customers or clients that are Virtual Asset Service Providers?

Answered: 53

Skipped: 0

Answer Choices	Responses
Yes	3.77%
No	96.23%
Yes	2
No	51
TOTAL	53



Q2 Does your business provide exchange services for Virtual Assets (exchanging virtual assets to fiat currency or other assets)?

Answered: 53

Skipped: 0

Answer Choices	Responses
Yes	0.00%
No	100.00%
Yes	0
No	53
TOTAL	53

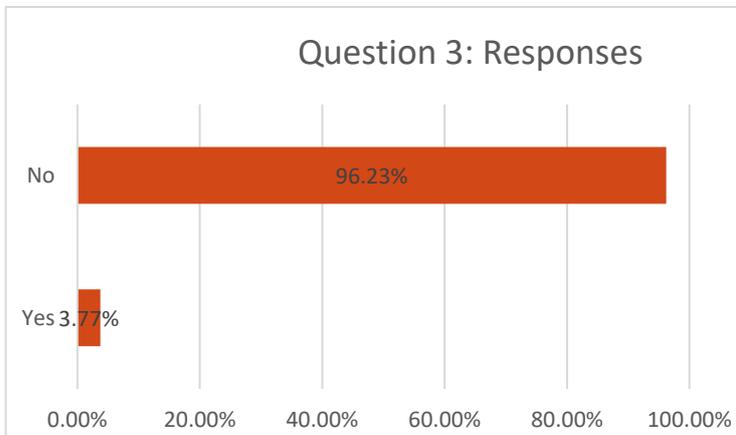
Q3

Are you aware of any customers or clients of your business using Virtual Assets?

Answered: 53

Skipped: 0

Answer Choices	Responses
Yes	3.77%
No	96.23%
Yes	2
No	51
TOTAL	53



If yes, approximately how many customers or clients and list down the type of virtual assets they use?

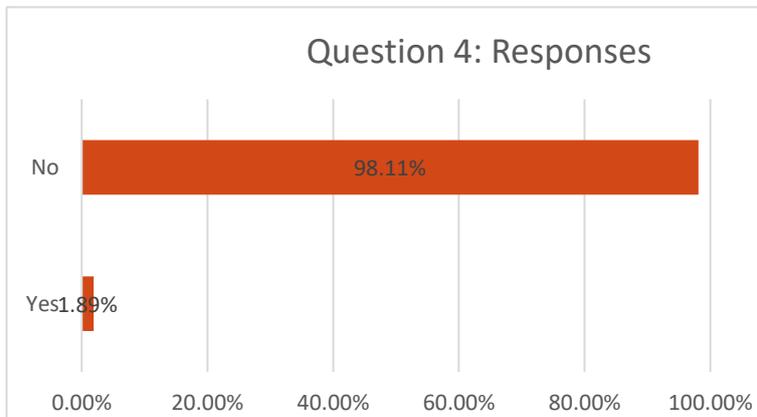
No.	Date/Time	Comments for Question 3
#1	6/24/2020 9:07 AM	200 Customers - Use high frequency trading of bitcoin, ethereum and other virtual assets as well as security token offerings

Q4**Does your business provide access for clients or customers to Virtual Assets?**

Answered: 53

Skipped: 0

Answer Choices	Responses
Yes	1.89%
No	98.11%
Yes	1
No	52
TOTAL	53

**If yes, what type?**

No.	Date/Time	Comments for Question 4
#1	6/24/2020 9:07 AM	Advisory on the best exchanges, security, investors, traders and custodial accounts in US and Europe

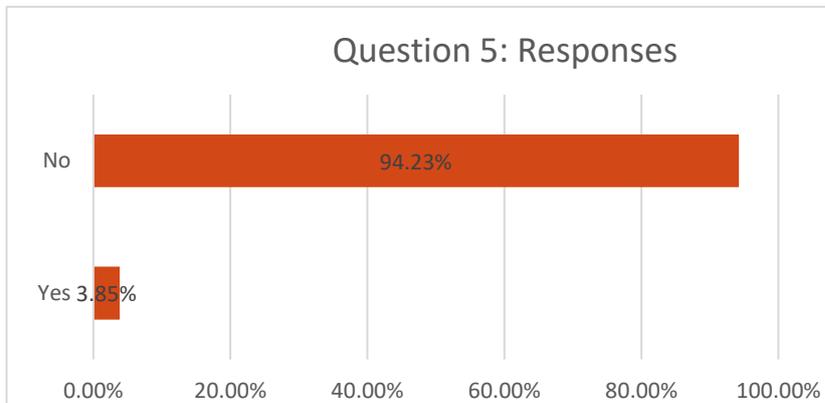
Q5

Are you aware of any events that could be characterized as money laundering or terrorist financing involving virtual assets in Papua New Guinea?

Answered: 52

Skipped: 1

Answer Choices	Responses
Yes	3.85%
No	94.23%
Yes	2
No	49
TOTAL	52



If yes, please provide a short explanation.

No.	Date/Time	Comments for Question 5
#1	7/17/2020 5:55 PM	There are virtual currency dealers or service dealers that operate on Facebook accounts promising FX gains through crypto-currency, etc. Unsuspecting people quite unaware of the pros & cons of such schemes have easily signed up at the pre-text of gaining huge profits.
#2	7/15/2020 9:39 PM	Chinese entities as well as some local PNG entities travel agencies selling tickets for non PNG routes and customers
#3	6/25/2020 11:04 AM	The use of bitcoin to purchase or sale securities online

Q6

If you are aware of events that could be characterized as money laundering or terrorist financing involving virtual assets in PNG, what could be done to prevent similar event occurring again in the future?

Answered: 31

Skipped: 22

No.	Date/Time	Comments for Question 6
#1	7/02/2020 12:10	Conduct Enhanced Due Diligence
#2	7/02/2020 15:22	Not applicable
#3	7/03/2020 11:29	No
#4	7/03/2020 12:54	Refer to the BPNG for guidance and advise.
#5	7/03/2020 13:57	I have no knowledge
#6	7/06/2020 9:47	Not applicable
#7	7/07/2020 13:55	File SMR, conduct ECDD and recommend customer to be exited and listed in the blacklist.
#8	7/07/2020 15:29	Enhance database registers and ensure quality data is available at all times.
#9	7/07/2020 15:45	Not aware of any.
#10	7/07/2020 16:05	Report any suspicious matter to the AML/CFT compliance officer to do further investigation
#11	7/07/2020 16:49	Awareness and Education of Virtual Assets to all Financial Institutions via a workshop to also enable sharing of information. This will then enable a common understanding and everyone is equipped with information on what it is and what to look out for.
#12	6/24/2020 9:07	BPNG and FASU can invest in a reserve of bitcoin and virtual assets to take these coins off the market and defend the PGK against future speculative attacks from cryptocurrency by using btc as a reserve in the fx baskets as well as a currency hedge. BPNG and FASU can license crypto exchanges to regulate the on and off ramps for these users. Users will have to eventually convert out of BTC into fiat and it is at this point, where regulation can be most useful.

#13	6/25/2020 11:04	The use of issuing directives to prevent an event occurring in the future should there be no legislation defining or stipulating the VA or VASP. However, legislation should be developed to govern and regulate VA and VASP.
#14	6/25/2020 11:11	More public education and awareness needed in this area. Yes, there are reports or activity suggesting money laundering but public is still financial illiterate. The way out is strengthen the role of Securities Commission of Papua New Guinea
#15	6/25/2020 4:00	Formulate dialogue with IXP in country to censor internet traffic relating to ALM/TF activities I guess.
#16	6/26/2020 9:01	Continuous educating through awareness
#17	6/26/2020 9:11	Carrying out awareness and campaigns in different regions in the country to educate everyone on the issues.
#18	6/26/2020 9:21	The one main reason to stop this is, is to make sure all clients use a bank account for all payment purposes and provide proof that they do so. Here at Moni Plus FX, our clients upon registering have to prove that they have a bank account and all payments or receipts are done direct to all clients' bank accounts.
#19	6/26/2020 9:45	Report to Bank Of Papua New Guinea and the Police immediately.
#20	6/29/2020 11:14	None
#21	6/29/2020 11:24	N/A
#22	6/29/2020 11:34	NIL
#23	6/29/2020 11:53	N/A
#24	6/29/2020 9:02	I am not aware of any money laundering or terrorist financing involving virtual assets in PNG.
#25	6/30/2020 4:51	Conduct enhanced due diligence, check adverse media
#26	7/14/2020 1:14	Firstly, if we, as an organisation becomes aware, a SMR report should immediately be lodged with FASU, discourage and advice individuals against investing in VAs and moreover there needs to be active awareness to the general public on the risks associated with VAs and VASPs
#27	7/15/2020 1:38	Do not know any

#28	7/15/2020 2:41	N/A
#29	7/16/2020 11:21	No
#30	7/17/2020 5:55	I guess if any organization, individual or non-individual is into virtual currency trading should be properly registered with BPNG. BPNG as the regulator then should ensure stricter controls are in place to allow for safer usage of the virtual currency service.
#31	7/20/2020 1:57	Strengthen controls in the ML/TF regime. Develop tools that can assist flag and monitor suspicious payments.

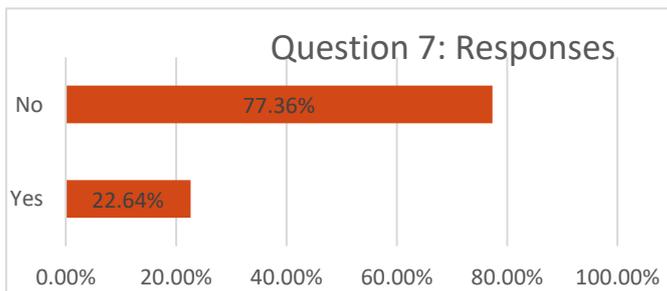
Q7

Are you aware of vulnerabilities in PNG's AML/CTF regime that might render PNG vulnerable to money laundering or terrorist financing involving virtual assets?

Answered: 53

Skipped: 0

Answer Choices	Responses
Yes	22.64%
No	77.36%
Yes	12
No	41
TOTAL	53



No.	Date/Time	Comments for Question 7
#1	7/02/2020 15:22	Lack of specific regulation of this sector in current regulation
#2	7/06/2020 9:47	Lack of specific regulation in this sector

#3	7/07/2020 15:29	the gap in connectivity between stakeholders i.e. IPA, IRC, Lands dept
#4	44081.46875	1. Obligations that apply to financial institutions and DNFBPs under the AML/CTF Act do not extend to Virtual Asset Service Providers; and 2. AML/CTF Act relies heavily on KYC and CIP related procedures that ensure customer identification and detection/monitoring of funding/wealth sources but such a legislative framework may be vulnerable to the anonymity risks associated with Virtual Asset Activities and Virtual Asset Service Providers.
#5	6/25/2020 11:04	FASU needs to be prepared in terms of policy and system enhancement to trace and identify the beneficial owners.
#6	6/25/2020 11:04	Black Wednesday- In 1992 George Soros launched a speculative attack on the Bank of England and broke the pound. One of if not the greatest currency trade in history. Look there.
#7	6/26/2020 9:11	Bitcoin
#8	6/26/2020 9:21	Yes, i believe one major gap is the annual limit to service payments out of PNG. For example client X sends 500,000 to his account in Philippines, he then goes to BSP and does the same and also to other FX providers like moni plus fx. He has already sent more than what is allowed above his annual limit and without paying for any tax certificate at IRC. BPNG still has not found a way to monitor this from a central database (from my understanding). Not just tax avoidance, but funding illicit activities overseas as well.
#9	6/29/2020 11:24	The AML/CTF Act 2015 as it is doesn't define "virtual assets/VASP's" hence the Act should be amended accordingly to take into consideration the FATF Recommendation 15.
#10	7/14/2020 1:14	Virtual currencies are growing in popularity and expanding across the globe. Their rapid development poses policy, legal, and enforcement challenges. Many jurisdictions have studied and understand this trend and are responding to the growing use of digital systems. PNG will be vulnerable if it does not enact

		laws to clarify virtual currency treatment under AML statutes including not implementing digital monitoring systems
#11	7/15/2020 9:39	Flexible and unenforced regulations, corruption being rife from Government to companies at all levels
#12	7/20/2020 1:57	Absence of Local List in the SWIFT may good example of pose risk money laundering/TF undetected.

Q8 In your opinion, what might PNG authorities do to detect money laundering or terrorist financing involving virtual assets in the future?

Answered: 47

Skipped: 6

No.	Date/Time	Comments for Question 8
#1	7/02/2020 12:10	On-Going Due Diligence on Adverse Media to keep abreast of what is happening globally.
#2	7/02/2020 15:22	PNG authorities would be well versed to look towards introducing specific regulations to address the known AML/CTF vulnerabilities of this sector-virtual assets are perceived to be vulnerable to criminal misuse by criminals to launder illicit funds and fund terrorism as they; -allow greater levels of anonymity -have global reach making it easier to transfer funds/value cross border outside of PNG regulatory reporting requirements -they can be traded freely and easily FATF guidance issues in 2018 would be a good starting point in terms of guidance. This includes assessing and understanding the risk associated with virtual assets in their jurisdictions, applying risk-based AML/CTF regulations to virtual assets service providers and identifying effective systems to conducts risk based monitoring or supervision of virtual assets service providers.

#3	7/03/2020 11:29	I have no Knowledge of any activity, I think training is good
#4	7/03/2020 11:29	Not well versed in virtual assets.
#5	7/03/2020 12:54	No opinion at this stage
#6	7/03/2020 13:57	I have no idea
#7	7/06/2020 9:47	Firstly, the PNG authority would look at introducing specific regulations to address the known AML/CTF vulnerabilities of this sector -Virtual assets are perceived to be vulnerable to criminal misuse by laundering illicit funds and to fund terrorism as they are: * Allow greater levels of anonymity * have a global reach making it easier to transfer funds and or values cross boarder outside of PNG regulatory reporting requirements. * they can trade freely and easily FATF guidance issued in 2008 would be a good starting point in terms of guidance, " this includes assessing and understanding the risks associated with virtual assets in their jurisdictions, applying risk-based AML/CTF regulation to virtual asset service providers and identifying effective systems to conduct risk-based monitoring or supervision of virtual asset service providers."
#8	7/06/2020 14:46	List down the websites/platforms that are used for trading of virtual assets so FIs can track and monitor internet transfers and TTs to those sites.
#9	7/07/2020 13:55	Simply don't allow customers who are engaging in virtual assets
#10	7/07/2020 14:05	The Central bank has to come up with a regulatory requirement that Commercial banks do not on-board clients whose nature of business fall under Virtual Asset Business.
#11	7/07/2020 15:29	Invest in database systems and digital solutions
#12	7/07/2020 15:45	Develop a regulatory framework to identify and manage AML/CTF risks associated to virtual assets.
#13	7/07/2020 16:05	The natural person or entity involving in virtual asset must be known, meaning any business that this person or entity enters into must be carefully scrutinize, performing KYC and Enhanced Customer

		Due Diligence on these type of Customers.
#14	7/07/2020 16:49	1. Enforce stringent KYC requirements in Financial Institutions and hold FI accountable if their KYC is not up to standard. 2. Create more awareness to the Public so that the people are aware of what VA is and what it means and if why PNG Law allows or do not allow Virtual Assets.
#15	7/08/2020 12:47	PNG Authorities should be able to have a sophisticated tracking system to be able to identify money laundering and terrorist finance involving virtual assets
#16	7/08/2020 15:33	More public awareness of AML & CTF in PNG and how it can affect the business and individuals.
#17	7/09/2020 11:15	1. PNG Authorities should look at amending both the AML/CTF Act such that Virtual Asset Service Providers and Virtual Assets are subjected to the same or similar obligations that apply to financial institutions and DNFBPs under the AML/CTF Act and the BFI Act; and 2. PNG Authorities should also consider taking a conservative view by imposing very strict controls on the exchange/conversion of Virtual Assets to fiat currency in PNG, by way of Regulations made under the AML/CTF Act. Under such Regulations, prior approval and authorisation from FASU in respect of any exchange/conversion of Virtual Assets to fiat currency in PNG would be required with FASU given the power to impose heavy fines on Virtual Asset Service Providers, financial institutions or DNFBPs it has reasonable grounds to believe have failed (knowingly or recklessly) to comply with any such requirements under those Regulations. To cater for the long term, such Regulations could also have in-built flexibility that allows for liberalisation of controls over time, when FASU and global regulatory authorities may be in a stronger position to regulate and control Virtual Asset Activities and Virtual Asset Service Providers (e.g. allow exemptions to be issued under the Regulations).

#18	7/10/2020 17:09	Targeted monitoring via AI capabilities which would track any reference to virtual asset linked beneficiary
#19	6/24/2020 9:07	Issue licenses for exchanges and regulate the on and off ramps from virtual assets into fiat. Regulate the choke points.
#20	6/25/2020 11:11	More technical capacity building programs is needed, public awareness and surveys to identify regulatory gaps. In terms of Capital Markets, strengthen the role of Securities Commission of PNG to fully implement the capital market laws of 2015.
#21	6/25/2020 3:10	Implement appropriate awareness activities for VA's and how the VA's are translated into PGK currency.
#22	6/25/2020 4:00	See suggestions to Q6 above.
#23	6/26/2020 4:52	If it can be regulated then ML/TF policies or regulations can be issued. The same obligations under regulated monetary system is effective so apply same methods. You can also start regulating online services for PNG.
#24	6/26/2020 9:01	1. Create an AML database 2. Enforce all form of transactions by banks/nbfc/fx to be uploaded to this database before actual transactions takes place; any suspicious accounts should have clearance before payments are made especially for FX or online payments 3. Get all ISP to impose strict rules for reporting any suspicious activities based on rules BPNG should set for identification
#25	6/26/2020 9:11	Monitoring of international transactions such as western union.
#26	6/26/2020 9:21	It is in PNG's interest to create a central database that is live for all FX remittances and also a central database for PEPs and High Risk clients or individuals and businesses. This will help FIs police AML/CTF activities in PNG.
#27	6/26/2020 9:45	Create an intelligence network from highly reliable sources that can work closely with the PNG authorities to detect and deter any money laundering activities or any terrorist financing.
#28	6/29/2020 11:14	Monitor closely those high risk individuals
#29	6/29/2020 11:21	Monitor all politician's and head of state enterprises/government departments for any transaction more than K10,000

#30	6/29/2020 11:24	Adopt and implement the relevant recommendations under the FATF Recommendation 15 through the AML/CTF Act 2015. Ensure regular monitoring of bank accounts belonging to Politically Exposed Persons (PEP's) and/or activities of other identified high-risk persons.
#31	6/29/2020 11:34	Monitor High rank government official's bank and politician's accounts. Monitor the transactions of foreign companies closely
#32	6/29/2020 11:53	PNG authorities should conduct random check/audit on high-risk clients.
#33	6/29/2020 12:10	Implement rigorous Anti-money Laundering and Terrorist Financing controls and mechanisms in place by our regulatory authorities such as the Bank of Papua New Guinea, Internal Revenue Commission and Customs.
#34	6/29/2020 9:02	Set up a dummy organization that would be involved in virtual assets and report to the authorities. In that way, the authorities can know and understand how these organization work.
#35	6/30/2020 12:54	Screen daily newspapers and social media to ascertain whether there is local persons or organisations trying to recruit citizens to trade in virtual digital assets.
#36	6/30/2020 3:16	That would be very difficult given that transactions do not appear on a PNG Register.
#37	7/14/2020 1:14	1. Amendment to the AML/CTF legislation to deal with the treatment of virtual currency and 2. implement digital monitoring systems
#38	7/15/2020 1:02	Establishing a PIX in PNG for probing internet traffic going in/out
#39	7/15/2020 1:38	Proper laws to be enacted Come up with proper policies and procedures around virtual assets concerning money laundering or terrorist financing.
#40	7/15/2020 2:41	Public awareness, provide information via newspaper, TV, social media. Run short 30 min sessions at various private/public offices.
#41	7/15/2020 5:57	Stay vigilant. Moreover, ask the same of us. We must work together to detect and avoid this.
#42	7/15/2020 9:39	Outsource this to an external offshore vendor to police

#43	7/16/2020 11:21	No PNG FX service should be allowed to convert... but it is tricky as these can be traded off shore through non-Kina currencies off shore and then brought on shore in legitimate currencies. Standard AML cross border controls should assist / protect this...
#44	7/17/2020 5:55	We should have a total ban at a country level on provision of Virtual Assets or Virtual Assets Providers Service in the absence of a proper and effective regulatory framework.
#45	7/20/2020 1:57	Collaboration is important. Key organisations are BPNG, Securities Commission, IRC, IPA, Finance Department, NEC (AML/CTF Secretariat). Work together to implement the existing laws in regard to AML/CTF Act, Proceeds of Crime Act, etc.
#46	7/14/2020 2:11	Strong inter governmental relationships ASIO / interpol etc
#47	6/25/2020 11:04	More technical training for PNG authorities and implementation and enforcement of laws by PNG.