# MONEY LAUNDERING AND TERRORISM FINANCING (ML/TF)

# RISK ASSESSMENT ON VIRTUAL ASSETS AND VIRTUAL ASSETS SERVICE PROVIDERS (VAs/VASPs)


# MONEY LAUNDERING AND TERRORISM FINANCING (ML/TF)

# RISK ASSESSMENT ON VIRTUAL ASSETS AND VIRTUAL ASSETS SERVICE PROVIDERS (VAs/VASPs)

# Contents

**TABLES AND FIGURES**

## ABBREVIATIONS

| | | |
|---|---|---|
| AG | - | Office of the Attorney General |
| AI | - | Artificial Intelligence |
| AML | - | Anti-Money Laundering |
| APG | - | Asia Pacific Group |
| API | - | Application Programming Interfaces |
| BoG | - | Bank of Ghana |
| CBDC | - | Central Bank Digital Currency |
| CDD | - | Customer Due Diligence |
| CFT | - | Countering the Financing of Terrorism |
| CSA | - | Cyber Security Authority |
| dAPI | - | decentralised Application Programming Interfaces |
| DeFi | - | Decentralised Finance |
| DNFBP | - | Designated Non-Financial Businesses & Professions |
| E-levy | - | Electronic Levy |
| EOCO | - | Economic and Organised Crime Office |
| FATF | - | Financial Action Task Force |
| FCU-GPS | - | Financial Crime Unit of the Ghana Police Service |
| FI | - | Financial Institutions |
| FIC | - | Financial Intelligence Centre |
| FINTECH | - | Financial Technology |
| G+D | - | Giesecke+Devrient |
| GCCH | - | Global Coin Community Help |
| GoG | - | Government of Ghana |
| GRA | - | Ghana Revenue Authority |
| HNWI | - | High-Net-Worth Individuals |
| ICO | - | Initial Coin Offering |
| ITO | - | Initial Token Offering |
| KYC | - | Know YourCustomer |
| LEA | - | Law Enforcement Agencies |
| ML | - | Money Laundering |
| NACOC | - | Narcotic Control Commission |
| NBFI | - | Non-Bank Financial Institution |

| | | |
|---|---|---|
| NIB | - | National Intelligence Bureau |
| NIC | - | National Insurance Commission |
| ASSESSMENT | - | National Risk Assessment |
| ORC | - | Office of the Registrar of Companies |
| OSP | - | Office of the Special Prosecutor |
| P2B | - | Peer-to-Business |
| P2P | - | Peer-to-Peer |
| PMMC | - | Precious Minerals Marketing Company |
| R | - | FATF Recommendations |
| SDI | - | Specialised Deposit-Taking Institutions |
| SEC | - | Securities and Exchange Commission |
| SIP | - | Strategic Implementation Programming |
| STO | - | Security Token Offering |
| STR | - | Suspicious Transaction Reports |
| TF | - | Terrorist Financing |
| TOE | - | Traditional Obliged Entities |
| USBTC | - | United States Bitcoin Corporation |
| USDC | - | United States Dollar Coin |
| USDT | - | United States Dollar Tether |
| VA | - | Virtual Assets |
| VASP | - | Virtual Asset Service Provider |
| VPN | - | Virtual Protocol Network |

# FOREWORD

In today's rapidly evolving financial landscape, the rise of Virtual Assets (VAs) and their associated service providers presents both transformative possibilities and notable risks. For Ghana to fully harness the potential of these innovations while maintaining the highest standards of financial integrity and security, proactive risk identification and mitigation are essential.

This sectoral risk assessment of VAs and VASPs is a timely and necessary intervention. It provides policymakers, regulators, and industry players with a clear, evidence-based understanding of the threats and vulnerabilities present in the virtual asset sector.

As Chairman of the Inter-Ministerial Committee on AML/CFT, I applaud the Financial Intelligence Centre and all partner institutions for leading this initiative with diligence and foresight. The collaborative spirit that shaped this assessment is exactly what is needed as we chart a balanced path between innovation and regulation.

Let this report serve not only as a risk assessment, but also as a call to action. Our next steps must be guided by the findings herein to strengthen our defences and ensure that Ghana remains a trusted partner in the global financial system.

**DR. CASSIEL ATO FORSON, MP**
**Minister of Finance**
***Chairman, Inter-Ministerial Committee (IMC)***

# MESSAGE FROM THE CHIEF EXECUTIVE OFFICER, FIC

The emergence and rapid evolution of Virtual Assets (VAs) and Virtual Asset Service Providers (VASPs) have presented both opportunities and complex challenges in the fight against money laundering, terrorist financing, and proliferation financing. As Ghana continues its journey toward a resilient and inclusive financial system, it is imperative that we understand and respond to the inherent risks within this dynamic space.

This sectoral risk assessment of VAs and VASPs represents a significant milestone in our collective effort to safeguard the integrity of Ghana's financial ecosystem. The findings offer valuable insights that will inform our regulatory approaches, supervisory strategies, and inter-agency cooperation moving forward.

I commend all the stakeholders both public and private who contributed to this critical exercise. Your expertise, commitment, and collaboration have been instrumental in producing a robust and actionable assessment. As we publish this report, the FIC reaffirms its unwavering commitment to enhancing national AML/CFTCPF frameworks and fostering innovation without compromising security and stability.

We look forward to working with all stakeholders to implement the recommendations and mitigate the identified risks effectively.

Albert Kwadwo Twum Boafo
Chief Executive Officer
Financial Intelligence Centre, Ghana.

# EXECUTIVE SUMMARY

The risk assessment on Virtual Assets (VAs) and Virtual Asset Service Providers (VASPs) in Ghana evaluates the risks associated with money laundering (ML) and terrorist financing (TF) within the emerging virtual asset landscape. This assessment aims to identify and assess the ML/TF risks related to VAs and VASPs, as well as evaluate the effectiveness of existing regulatory frameworks and control measures. The assessment leverages a combination of qualitative and quantitative methods to evaluate the risks. Data was collected from various stakeholders including regulatory bodies, law enforcement agencies (LEAs), financial institutions (FIs), VASPs, DNFBPs, students and the general public.

The assessment revealed that VA wallet providers, especially those managing hot wallets, are highly vulnerable to cyber-attacks and risk financial loss due to hacking, phishing and malware. Converting VAs to fiat and vice versa poses high risks due to the potential for ML and fraud. Similarly, stablecoins pose high risks due to regulatory uncertainties, potential for fraud, and market volatility. Virtual-to-virtual transactions are considered medium risk and remain susceptible to fraud, market manipulation and cyber threats.

To address the identified risks, key recommendations were proposed including strengthening Anti-Money Laundering and Countering the Financing of Terrorism (AML/CTF) regulations specific to VAs and VASPs, instituting robust cybersecurity practices for VASPs, encouraging collaboration among regulatory bodies, FIs and LEAs, conducting outreach programmes to educate the public and stakeholders and instituting periodic risk assessments to stay abreast of evolving threats.

# 1.0 BACKGROUND

## 1.1 Introduction

The use of VAs and VASPs has both benefits and challenges for global financial systems. VAs are digital representations of value that can be traded, transferred or used for payment or investment purposes online. They operate independently of traditional banking systems and use blockchain technology for security and transparency. The Financial Action Task Force (FATF) has identified VAs and VASPs as areas needing strict regulation and in 2019 updated Recommendations 15 and 16 to address these risks. Accordingly, Ghana has taken steps to conduct its maiden assessment on VAs/VASPs to ascertain the ML/TF risk associated with them and their impact on the economy.

## 1.2 Ghana's Financial Landscape and the VAs/VASPs Ecosystems

Ghana is witnessing rapid economic development, underpinned by a resilient financial system comprising banks, non-bank institutions, and an expanding fintech industry. Digital financial services, like mobile money, are becoming more accessible with the Bank of Ghana (BoG) reporting a significant GH¢1.07 trillion in mobile money transactions in 2022. Ghana's economy, with high inflation and exchange rate volatilities provides a fertile ground for some Ghanaians to adopt cryptocurrencies like Ethereum, Bitcoin, USD Coin (USDC) and Tether USD (USDT) to protect their finances from the declining value of the Ghana Cedis and low returns from traditional bank savings. Additionally, VAs/VASPs provide convenience for easy movement of funds as well as low transaction cost associated as compared to the traditional banking system.

The September 2023 Chainalysis Global Crypto Adoption Index ranked Ghana 29th for cryptocurrency adoption and 4th for peer-to-peer (P2P) exchange trade volume worldwide. A recent report by CoinGecko placed Ghana as the 4th highest country in Africa for crypto interest following Nigeria, South Africa and Morocco. These reports indicate a growing interest in crypto in Ghana, establishing it as a leading country for crypto adoption in Africa. In recent years, some cryptocurrency platforms have gained significant popularity among Ghanaians, including Binance, Paxful, YellowCard, and LocalBitcoins (before its closure). The LocalBitcoins' global closure was attributed to the prolonged "crypto winter," a term used to describe a significant downturn in cryptocurrency markets. Binance is the top choice for peer-to-peer trading which is the primary method used by Ghanaians offering payment options like mobile money and bank transfers.

Before Binance's rise in the P2P market, Paxful was a key player in cryptocurrency trading and remains popular among peer-to-peer traders. Like Binance, Paxful offers diverse payment options, including PayPal and gift cards, catering for a different segment of the trading community. Yellowcard has also gained traction as a platform for buying and selling cryptocurrencies in Ghana. Mazzuma, a Ghanaian Web3 startup focusing on Artificial Intelligence (AI) and blockchain, recently secured Cloud funding and launched MazzumaGPT as the platform expedites smart contract creation such as Ethereum transaction contracts for developers.

The rapid expansion of digital financial services has given rise to new vulnerabilities. With the increasing use of virtual assets, there is a growing risk of these assets being exploited for unlawful activities. Consequently, the Government of Ghana (GoG), in collaboration with various regulatory bodies, is dedicated to comprehending and addressing the risks associated with Vas/VASPs.

The Bank of Ghana (BoG) just as its peers within the global space is undertaking research of the VAs/VASPs activities to help develop and implement cryptocurrency regulations in the country. BoG as part of its regulatory mandate issued a notice (*NOTICE NO. BG/GOV/SEC/2018/02*) to caution the public on the risk associated with digital currency activities which are not currently licensed under Section 21 to 38 of the Payment Systems and Services Act, 2019 (Act 987). While this regulatory process is ongoing, cryptocurrencies are classified as digital assets rather than currency.

## 1.3 Objectives of Risk Assessment on VAs/VASPs

The primary objectives of the risk assessment on VAs/VASPs include:

a. Identify and assess the ML/TF risks associated with VAs/VASPs.

b. Evaluate the adequacy of existing regulatory frameworks and identify gaps.

c. Recommend national action plan to mitigate identified risks.

# 2.0 METHODOLOGY

In line with the Recommendations 15 and the emerging ML/TF risks in the VASPs sector, Ghana has conducted its maiden risk assessment on VAs/VASPs.

Key stakeholders including Financial Intelligence Centre (FIC), BoG, Securities and Exchange Commission (SEC), Office of the Registrar of Companies (ORC), Law Enforcement Agencies (LEAs), Financial Technology (FINTECH) Institutions, Financial Institutions (FIs), VASPs, DNFBP, Student Bodies and Experts collaborated to conduct this assessment.

## 2.1 General Approach and Processes

The World Bank's Risk Assessment Tool was used to comprehensively assess the threats and vulnerabilities of ML/TF risks associated with VAs/VASPs. Both qualitative and quantitative data were collected from relevant stakeholders.

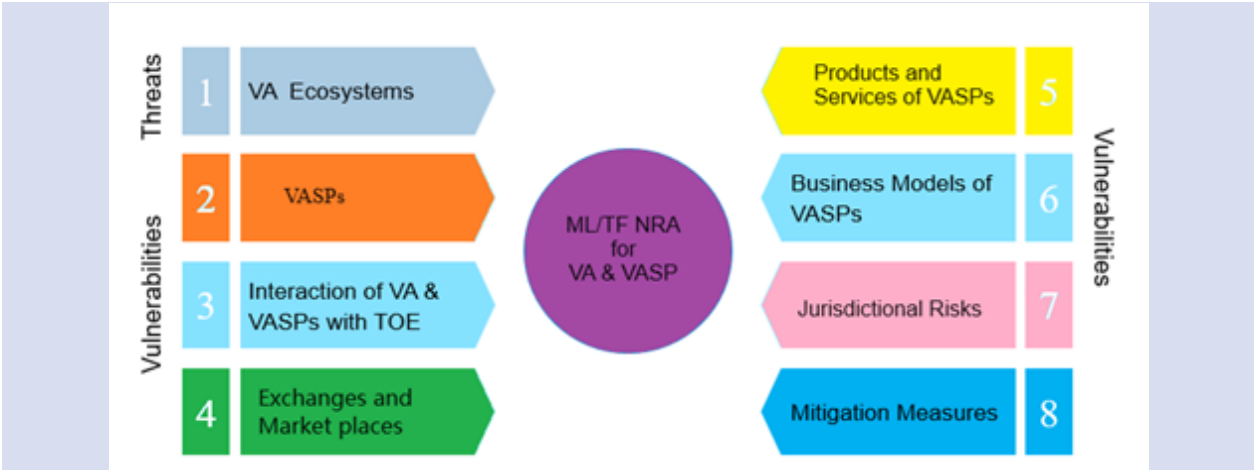


**Figure 2.1 Components of the Risk Assessment Model for VAs and VASPs**

The World Bank tool evaluated seven (7) categories, twelve (12) functions and twenty-seven (27) activities of VASPs that may interact with various sectors within and outside Ghana. The assessment questionnaires comprehensively covered the areas where these activities may intersect with Traditional Obliged Entities (TOE), considering the types, functions and activities involved.

**Table 2.1 Types of VASP and functions considered for the assessment**

| Categories | Functions | Activities |
|---|---|---|
| 1. Virtual Asset Wallet Providers | 1. Custodial Services | 1. Hot Wallet<br>2. Cold Wallet |
| | 2. Non-Custodial Services | |
| 2. Virtual Asset Exchanges | 3. Transfer Services | 3. P2P (Peer-to-Peer)<br>4. P2B (Peer-to-Business) |
| | 4. Conversion Services | 5. Virtual-to-Fiat<br>6. Fiat-to-Virtual<br>7. Virtual-to-Virtual |

| | | |
|---|---|---|
| 3. Virtual Assets Broking / Payment Processing | 5. Payment Gateway | 8. ATMs<br>9. Merchants<br>10. Cards |
| 4. Virtual Asset Management Providers | 6. Funds | 11. Funds Management<br>12. Funds Distribution<br>13. Compliance, Audit & Risk Management |
| 5. Initial Coin Offering (ICO) Providers | 7. Fund Raising | 14. Fiat-to-Virtual<br>15. Virtual-to-Virtual |
| | 8. Investments | 16. Development of Products & Services |
| | 9. Other Offerings | 17. Security Token Offering (STO)<br>18. Initial Token Offering (ITO) |
| 6. Virtual Assets Investment Providers | 10. Trading Platform | 19. Platform Operators<br>20. Custody of Assets |
| | 11. Emerging Products | 21. Investment in VA-related commercial activities<br>22. Non-Security Token, Hybrid Trading Activities<br>23. Stablecoins<br>24. Crypto Escrow<br>25. Custodian Services |
| 7. Validators, Miners & Administrators | 12. Proof of Work | 26. Fees<br>27. New Assets |

## 2.2 Threat and Vulnerability Assessment

This section of the risk assessment involves assessing risks associated with ML/TF and addressing common criminal techniques for illicit fund movement. It also seeks to understand predicate offences associated with VASPs, recognize their nature and measure their impact.

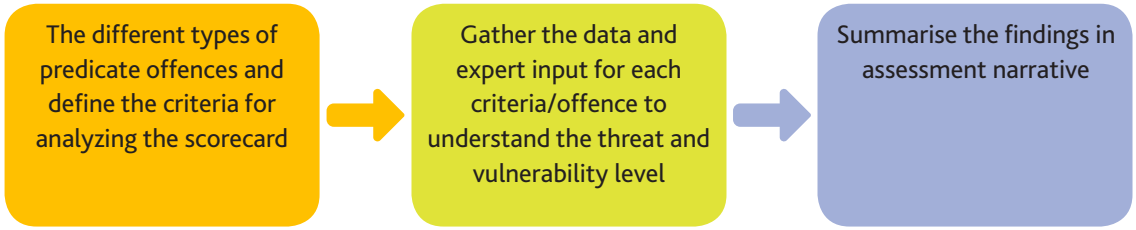


**Figure 2.2 Scorecard Approach for Threat and Vulnerability Assessment**

## 2.3 Mitigating Factors and Residual Risk

This part of the assessment aims to establish an accurate understanding of the current AML/CFT framework, the establishment of relevant institutions and to identify measures for improvement.

The evaluation of the impact of measures to reduce risk is structured around three key steps. First, criteria for assessing the impact of measures in place are defined, including prevention, supervision, detection and other relevant measures. Second, data and information are collected for each criterion to understand the effectiveness of the risk-reducing measures and a score is assigned to each criterion. Finally, the risk-

reducing measures that have been implemented are described in separate sections of the assessment report and the scores for these measures are combined for each sub-sector. The combined scores are then used to evaluate the remaining risk.

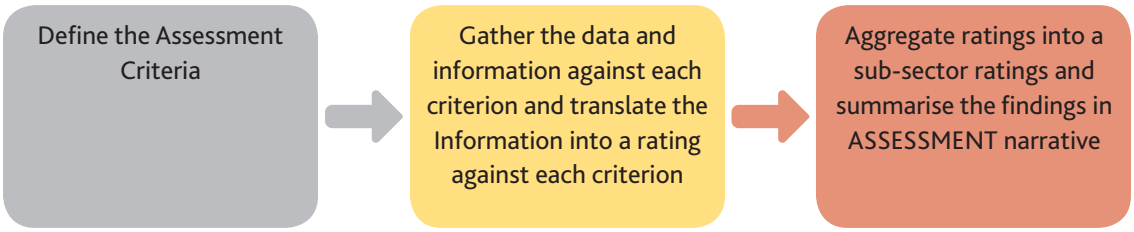


**Figure 2.3 Scorecard Approach to assess the impact of mitigating factors**

Ghana's residual risk prioritizes strengthening AML/CFT regime, focusing on prevention, detection, prosecution and collaboration between private and government sectors.


**Figure 2.4 Residual Risk**

# 3.0 SECTORAL ASSESSMENT – VAs and VASPs INTERACTIONS

## 3.1 Existing Traditional Obliged Entities (TOEs) sectors

The interactions among VAs/VASPs and TOEs (such as banks and other financial institutions) in Ghana have been shaped by regulatory guidelines, suspicious transaction reports (STRs) and the overall risk appetite of these entities. The Banks and Specialised Deposit-Taking Institutions Act, 2016 (Act 930), is a significant legislative framework in Ghana. Section 9(6) ensures that the operations of Banks and Specialised Deposit-Taking Institutions (SDIs) conduct on-going risk assessment of their business operations and identify emerging risks such as VAs/VASPs. Additionally, Act 1044 designates VASPs as accountable institutions requiring them to comply with AML/CFT obligations.

The risk appetite of TOE towards VAs and VASPs in Ghana varies significantly. Generally, banks and other FIs have adopted a cautious approach due to the inherent risks associated with VAs, such as volatility, lack of transparency and regulatory uncertainty. Subsequently, BoG has integrated blockchain solutions into its Regulatory and Innovation Sandbox, demonstrating its commitment to embracing emerging technologies such as VAs.

## 3.2 Financial Institutions (FIs)

FIs in Ghana are cautious about VAs/VASPs due to concerns about cryptocurrency potential for ML/TF and other illicit activities. The anonymity and volatility of cryptocurrencies make it difficult for FIs to monitor flow of funds and control, potentially leading to financial losses.

Customer risk in VAs/VASPs transactions is primarily due to the pseudonymous nature of user identity and background making it difficult for FIs to conduct effective customer due diligence (CDD). Transaction risk is a critical concern as the decentralised and borderless nature of cryptocurrencies means that transactions can occur across jurisdictions with varying regulatory frameworks leading to challenges such as tracing the origin and destination of funds, making it difficult to detect and prevent fraudulent activities. Counterparty risk is a significant concern in the cryptocurrency sector in Ghana, with FIs assessing VASPs credibility and reliability. The embryonic nature and lack of regulatory oversight exacerbate this risk. Thus, customer protection is crucial, as cryptocurrencies are volatile and speculative, causing substantial financial losses. Considering the various inherent risk associated with VAs/VASPs, FIs continuously conduct risk assessments, implement enhanced due diligence measures as well as ongoing transaction monitoring. Additionally, FIs provide adequate information and guidance to their customers about the risks associated with investing in and transacting with cryptocurrencies.

The digital asset marketplace in Ghana is still in its early stages with the local cryptocurrency exchanges playing a crucial role in the VA ecosystem. Over the past few years, the use of various digital assets by Ghanaians has recorded a significant increase on account of factors such as high mobile money penetration, a tech-savvy youth demography, high internet usage and the rise of online companies offering crypto and VASPs. Thus, regulatory oversight is essential to ensure transparency and security in marketplaces. This will

also ensure a conducive regulatory environment that promotes financial inclusion and enhances financial stability while fostering innovation and effectively managing risks associated with digital assets. BoG together with relevant stakeholders have taken steps to address the risk associated with the activities of VAs/VASPs in the financial ecosystem.

Subsequently, BoG per notice number *BG/GOV/SEC/2022/03* prohibits banks and payment service providers (PSPs) from facilitating crypto-asset transactions. In compliance with this directive, accountable institutions (AIs) are required to file suspicious transactions reports on all crypto-asset-related transactions. Table 3.1 shows some of the cases that have come to the attention of relevant agencies.

**Table 3.1 Cases from the FIs**

| S/N | CASES |
|---|---|
| *a.* | *Peter Johnson's accounts were funded by transfers from foreign and local sources, despite his claims of being a salaried worker and self-employed computer repairer. Due diligence revealed that some funds received were for family expenses, while others were for bitcoin trading. The bank suspended a pending balance of GH¢376,213.98 from a bitcoin transaction, and the case was referred to the National Intelligence Bureau and the Ghana Revenue Authority for further investigation.* |
| *c.* | *Kwaku Starky, who owned a smoke shop and sold shisha, opened an account with a bank in September 2020. On July 24, 2023, an anonymous debit transaction of GH¢2,360.00 bearing the code "BTC_GIP" was flagged as suspicious, leading to the account being marked for closure and the banking relationship being terminated. The bank was reminded of record-keeping provisions if the relationship was terminated.* |
| *d.* | *Emeka Ckukwu, a Nigerian Bitcoin and forex trader, opened an account with a Ghanaian bank in June 2022. A review of the account activities, revealed a pattern of anonymous inflows and structured withdrawals, which were deemed suspicious and unacceptable. The bank re-assessed his risk and terminated the business relationship.* |
| *e.* | *Senam Amegatse, a student, deposited GH¢790,650.00 into his account between December 11-13, 2023, which was not in line with his KYC profile. During due diligence, he claimed to trade in phones and cryptocurrency, asserting that the funds were business proceeds. Pursuant to the above-mentioned BoG Notice, subject's activities were deemed to be suspicious and the account was closed.* |

## 3.3 Securities Sector

In Ghana, the Securities and Exchange Commission (SEC) is the primary regulatory body overseeing the securities sector. The Securities Industry Act, 2016 (Act 929) governs the activities within this sector, aiming to ensure a fair, efficient and transparent market. The rise of VAs has prompted SEC to consider new regulations to address the unique challenges posed by digital assets. The regulatory framework for VAs/VASPs in Ghana is in its embryonic stage, but notices and guidelines have been issued to caution and protect investors. SEC is exploring defining permissible activities specific to VAs, such as operating VA exchanges, custody services and investment advisory services, to integrate VAs into the existing financial system without compromising regulatory standards.

The interaction between the securities sector and the VA/VASP sector in Ghana has been cautious but progressive. Traditional market operators such as investment firms and asset managers have started to explore VAs as part of their investment portfolios. However, the lack of a clear regulatory framework has limited widespread adoption. SEC's engagement with stakeholders in the VA/VASP ecosystem aims to

bridge this gap by developing regulations that foster innovation while safeguarding investor interests. The collaboration between traditional market operators and VASPs is crucial for creating a robust financial ecosystem that leverages the benefits of digital assets.

Digital assets and VAs are emerging as a new asset class in Ghana, offering both opportunities and challenges due to their high volatility, decentralization and technological underpinnings. Investment firms and asset managers are diversifying their portfolios, but this requires robust risk management strategies and regulatory oversight. SEC's role in classifying VAs, setting investment limits and ensuring disclosure is crucial for integrating VAs into mainstream investment practices. Regular audits and risk assessments are necessary to identify vulnerabilities and enhance the integrity and stability of the VA market.

VA investment providers, including VA exchanges, investment funds and advisory services, are crucial in Ghana's VA ecosystem. Platform operators, such as VA exchanges and trading platforms are central to the VA market. Regulatory clarity and investor education are essential to foster trust in VA investments. SEC and BoG are working to establish guidelines for operating standards, investor protection and market integrity.

## 3.4 Designated Non-Financial Business or Profession (DNFBP)

DNFBPs, including gaming, car dealers, real estate, dealers in precious metals and stones, significantly contribute to Ghana's economy and have minimal exposure to VAs/VASPs.

The gaming sector in Ghana has grown significantly due to digital platforms and internet penetration. The Gaming Commission regulates this sector, however the introduction of VAs/VASPs could change the gaming landscape. The anonymous nature of VAs can facilitate illicit activities, making it difficult for authorities to trace funds. The Gaming Commission and other regulatory bodies must therefore enhance their regulatory frameworks.

The real estate sector which is regulated by the Real Estate Agency Council (REAC) has in recent times experienced rapid growth driven by expanding middle class and increased foreign investment. The real estate subsector poses some level of ML risk due to the high value and relative liquidity of properties. The introduction of VAs exacerbates these risks as the sector is susceptible to the acceptance or use of VAs which, necessitates rigorous AML/CFT measures. Real estate professionals are required by the Real Estate Agency Act, 2020 (Act 1047) and the Anti-Money Laundering Act, 2020 (Act 1044) to adopt enhanced due diligence procedures and report suspicious transactions to FIC.

The trade in precious metals and stones, particularly gold, is a crucial part of Ghana's economy contributing a significant amount to its GDP annually. However, illegal small-scale mining (galamsey) remains a significant challenge, contributing to environmental degradation and regulatory non-compliance. The anonymous nature of VAs also makes it easier for illicit actors to launder proceeds from illegal mining activities. The sector is regulated by Minerals Commission and Ghana Gold Board (GoldBod), which oversee compliance with all relevant laws including Act 1044.

## 3.5 Informal Sector

The informal sector relates to VAs/VASPs in several important ways. Many individuals and businesses operating in the informal sector lack access to traditional banking services, making VAs an attractive alternative for saving, payments and cross-border transactions. VASPs, such as cryptocurrency exchanges and wallet providers, offer financial tools that can support financial inclusion for these underserved populations. It also offers remittances and investment opportunities with higher returns than traditional FIs.

Remittances form a crucial part of Ghana's economy, with many Ghanaians relying on money sent from relatives abroad. The traditional remittance process can be costly and slow, but VA/VASPs were noticed as a more efficient and cost-effective alternative offer for the general public. Cryptocurrencies facilitate faster and cheaper cross-border transactions, reducing the reliance on traditional remittance services. This has a direct positive impact on the livelihoods of many Ghanaians, allowing them to receive funds more swiftly and with lower transaction fees.

Additionally, VA/VASP activities have created new employment opportunities for university students and graduates in computer science, finance and related fields. The rise of cryptocurrencies and blockchain technology has led to internships and entry-level positions in start-ups and established firms. Universities are recognizing the demand for skills like blockchain development, cryptography and digital asset management.

However, this increased use also poses regulatory challenges. Because the informal sector often operates outside the purview of formal oversight, it can become a space where unlicensed or unregistered VASPs thrive, increasing the risk of ML/TF and other illicit activities.

With proper regulation and targeted engagement, VAs/VASPs can serve as a bridge to help integrate informal actors into the formal financial system, thereby enhancing transparency, security and economic inclusion.

# 4.0 VA/VASP THREATS AND VULNERABILITIES

VAs/VASPs present countless threats and vulnerabilities globally and these are no different for Ghana. The landscape is rapidly evolving and while virtual assets offer significant opportunities, they also pose substantial risks.

## 4.1 ML/TF Threat Assessment

VAs/VASPs have become integral components of the financial ecosystem, offering innovative solutions and services. However, they also pose threats, particularly in Ghana where regulatory frameworks and enforcement mechanisms are still evolving. These threats include ML, regulatory and compliance risks, cybersecurity threats, fraud, market volatility and cross-border transactions.

### 4.1.1 ML and TF

One of the threats posed by VAs and VASPs in Ghana is their potential use in ML/TF. Cryptocurrencies, due to their pseudonymous nature, can facilitate the concealment of illicit financial activities. Ghana, like many other countries, faces challenges in tracking and regulating these transactions effectively.

***Case Study 1: The 2019 Cryptocurrency Scam***

*In 2019, a significant cryptocurrency scam was uncovered in Ghana, where fraudsters used Bitcoin to launder money obtained through phishing attacks and other cybercrimes. The criminals exploited the lack of robust regulatory oversight and the anonymity provided by Bitcoin to move large sums of money across borders without detection.*

### 4.1.2 Regulatory and Compliance Risks

The rapid growth of the VA market in Ghana has outpaced the development of regulatory frameworks. This regulatory gap creates an environment where VASPs can operate with minimal oversight, increasing the risk of financial crimes and consumer exploitation.

***Case Study 2: Menzgold Ghana Limited***

*Menzgold Ghana Limited, a gold dealership and investment firm, offered exceptionally high returns on investments, claiming to leverage gold trading and cryptocurrency investments. However, in 2018, the company was shut down by the Securities and Exchange Commission (SEC) of Ghana for operating without a proper license. Investors lost millions of dollars.*

### 4.1.3 Cybersecurity Threats

VASPs are attractive targets for cyber criminals due to the significant value they hold in digital assets. Cyber attacks, including hacking and phishing, can lead to substantial financial losses and undermine confidence in the digital asset ecosystem.

***Case Study 3: Bitcash Currency Exchange***

*Bitcash Currency Exchange, a Ghanaian cryptocurrency exchange, suffered a major cyberattack in 2020, resulting in the theft of Bitcoin worth over $1 million. The hackers exploited vulnerabilities in the exchange's security systems, gaining unauthorised access to customer funds.*

***Case Study 4: Cyber Attack on a Telecommunication Company***

*Between February 2023 and August 2023, a cyber-attack was made on the Mobile Money Platform of a company where hackers used remote access control with a Virtual Private Network (VPN) to pilfer about GHS 48 million Ghana Cedis into cryptocurrency accounts. The attackers created Malware to duplicate mobile money transactions, which were first transferred to bank accounts and mobile money accounts of other telecommunication networks. The funds were all then channeled to three mobile money accounts for the purchase of Bitcoins (BTC). 14 BTC accounts were used to receive the funds, which were later channeled to two (2) BTC accounts and one crypto mixer account.*

### 4.1.4 Fraud and Ponzi Schemes

The rise of VAs has also led to an increase in fraudulent and Ponzi schemes. Bad actors take advantage of the public's limited understanding of cryptocurrencies and exploit them with promises of unrealistic returns on investments.

***Case Study 5: Global Coin Community Help (GCCH)***

*In 2017, Global Coin Community Help (GCCH) was exposed as a Ponzi scheme in Ghana. GCCH lured investors by promising high returns through cryptocurrency investments. Thousands of Ghanaians invested their savings, only to lose their money when the scheme collapsed.*

### 4.1.5 Market Volatility and Consumer Protection

The volatility of cryptocurrencies could pose significant risk to consumers in Ghana. Many investors are drawn to the potential high returns but are unaware of the substantial risks involved. The lack of consumer protection regulations exacerbates the risk of financial loss.

In 2024, BoG released draft guidelines to regulate digital assets, including cryptocurrencies like Bitcoin and Tether. These guidelines aim to ensure the integrity and stability of the financial sector, protect consumers and investors and guard against financial crimes such as ML/TF. The proposed measures include requiring VASPs to perform customer due diligence, report suspicious transactions and implement comprehensive risk assessments.

### 4.1.6 Cross-Border Transactions and Jurisdictional Challenges

Cryptocurrencies facilitate cross-border transactions, which can complicate regulatory oversight and enforcement. The decentralised nature of VAs allows for transactions that can bypass traditional financial systems and regulatory controls.

***Case Study 7: Two Central Americans visited Ghana to buy Gold***

*In August 2023, two Central Americans, specifically El Salvador and Guatemala citizens visited Ghana for a Gold business deal where they were defrauded of about 500,000 USBTC. The alleged fraudsters only accept cryptocurrency as a form of payment and transactions are made in artificial settings just for the fraudulent operation.*

### 4.1.7 Tax Evasion

VAs, such as Bitcoin and Ethereum, operate on decentralised networks that offer a degree of anonymity and privacy. These characteristics make them attractive tools for individuals and entities seeking to evade taxes. VASPs can be used to obscure the true nature of financial transactions, making it difficult for tax authorities to detect and trace taxable income and assets.

***Case Study 9: High-Net-Worth Individuals (HNWIs) Using Cryptocurrencies to Evade Taxes***

*In 2020, GRA discovered a case of HNWIs using cryptocurrencies to conceal their wealth and evade taxes. They converted significant income into digital wallets, avoiding tax declarations and allowing funds to move across borders. GRA's investigation revealed that these HNWIs had not reported millions of cedis in taxable income. The anonymity provided by cryptocurrencies allowed them to move funds across borders without detection, further complicating efforts to trace and recover evaded taxes.*

***Case Study 10: Cross-Border Crypto Transfers to Offshore Accounts***

*In 2021, GRA and international tax authorities discovered a network of businesses and individuals using cryptocurrencies to transfer funds to offshore tax havens, bypassing traditional banking systems and regulatory checks.*

### 4.1.8 Presence of the VASP Channels in Ghana

Ghana's growing ecosystem of VASPs is gradually integrating digital assets into its financial landscape, with a diverse array of channels operating within its borders as illustrated in Table 4.1, despite their novelty in many developing economies.

**Table 4.1 Presence of the VASP Channels in Ghana**

| VASP | Presence on the market (Yes / No) |
|---|---|
| Virtual Asset Wallet Providers | Yes |
| Virtual Asset Exchanges | Yes |
| Virtual Asset Broking / Payment Processing | Yes |
| Virtual Asset Management Providers | No |
| Initial Coin Offering (ICO) Providers | No |
| Virtual Asset Investment Providers | Yes |
| Validators / Miners/ Administrators | No |

Virtual Asset Wallet Providers and Virtual Asset Exchanges are key in the VAs/VASPs ecosystem, providing secure storage and management of digital currencies. They cater to the growing demand for secure personal digital currency management among Ghanaians.

Virtual Asset Exchanges serve as crucial platforms for the buying, selling, and trading of cryptocurrencies. Their operation within Ghana demonstrates the acceptance of digital currencies as it enables liquidity and provide a market for users to interact with various cryptocurrencies, promoting economic activities tied to digital assets. They also highlight the importance of having a regulated environment to protect investors and maintain market integrity.

Virtual Asset Broking/Payment Processing is another key area present in Ghana, underlining the practical application of digital assets in everyday financial transactions. These services bridge the gap between traditional financial systems and the emerging digital currency ecosystem, offering solutions for remittances, online payments and other financial services. Virtual Asset Broking/Payment Processing is beneficial in a country like Ghana, where remittances form a significant part of the economy. Digital payment processing enhances efficiency, reduces transaction costs and broadens access to financial services.

Virtual Asset Investment Providers operate within the country, catering to a growing number of individuals and institutions interested in leveraging digital assets for investment purposes. These providers offer various services, including advisory and management services for digital asset portfolios, indicating an increasing recognition of cryptocurrencies as viable investment vehicles. The emergence of such providers suggests a maturing market that is progressively understanding and capitalizing on the investment potential of digital assets.

The absence of Virtual Asset Management Providers and Initial Coin Offering (ICO) Providers points to areas where the market is still nascent. Virtual Asset Management Providers, which handle the strategic management of digital assets for clients, are critical for sophisticated investment and risk management strategies. Their absence could be due to regulatory uncertainties or a lack of mature demand for such specialised services. Similarly, the lack of ICO Providers, entities that facilitate fundraising through token sales, might reflect a cautious regulatory stance or limited local interest in such fundraising mechanisms, often viewed with scepticism due to historical instances of fraud.

The non-existence of Validators/Miners/Administrators in Ghana further emphasises the infrastructural and regulatory challenges. Mining operations require substantial investment in hardware and energy resources, which might be less feasible in Ghana due to high energy costs and infrastructural limitations. Additionally, the regulatory environment might not be conducive to large-scale mining operations, deterring potential investors.

### 4.1.9 ML/TF Threat Ratings by Input Variables

Table 4.2 outlines the inherent risk levels of various input variables in custodial services, emphasising the complex landscape of ML/TF threats and requiring stringent measures for effective mitigation.

**Table 4.2 ML/TF Threat Ratings by Input Variables**

| Intermediary variables | Input variables | Threat Ratings |
|---|---|---|
| VA Nature and Profile | Anonymity/pseudonymity | Medium Risk |
| | P2P Cross-Border Transfer and Portability | Medium Risk |
| | Absence of face-to-face contact | Medium Risk |
| | Traceability | Medium Risk |
| | Speed of Transfer | Medium Risk |
| Accessibility to Criminal | Mining by criminal | Medium Risk |
| | Collection of funds | Medium Risk |
| | Transfer of funds | Medium Risk |
| | Dark Web Access | Medium Risk |
| | Expenditure of funds | Medium Risk |
| Source of funding VA | Bank or card as a source of funding VA | Medium Risk |
| | Cash transfers, valuable in-kind goods | Medium Risk |
| | Use of virtual currency | Medium Risk |
| Operational features of VA | Regulated | High Risk |
| | Unregulated | High Risk |
| | Centralised Environment | Medium Risk |
| | Decentralised Environments | High Risk |
| Ease of criminality | Tax evasion | High Risk |
| | Terrorist financing | Medium Risk |
| | Disguising criminal proceeds to VA not regulated | High Risk |
| | Trace and Seize Difficulty | Medium Risk |
| | Circumvent Exchange Control | High Risk |
| Economic Impact | Underground economy – Impact on the country's monetary policy | High Risk |
| | Allow full integration with the financial services market | Low Risk |
| | Prohibit any interaction between the financial institutions and the VA market. | Medium Risk |
| | High level of accountability product provider | High Risk |

The nature and profile of VAs are marked as medium risk due to their anonymity, ease of cross-border transactions, lack of physical interaction, traceability challenges and fast transaction speeds. Criminal accessibility and sources of funding VAs in custodial services were also medium risk, with traditional and virtual funding methods posing similar levels of risk.

Unregulated and decentralized environments pose high risks due to vulnerabilities and lack of oversight, while regulated and centralised environments are more controllable. High risks include tax evasion, disguising proceeds and circumventing exchange controls. Moderate concerns are rated for terrorist financing and trace and seize difficulties, mainly due to Ghana's LEA efforts. The economic impact of VAs was assessed to be high, given that VAs encourage an underground economy.

The assessment revealed that the non-applicability of various variables for non-custodial services led to a threat risk rating of "Does not exist".

### 4.1.10 ML/TF Threat Ratings by VASPs Channels

The table analyses VASPs functions and activities, categorizing them by ML/TF threat levels. High-risk areas like P2P transfers, conversion services and asset custody require strict regulatory oversight and robust AML/CFT measures, while medium-risk activities require vigilant monitoring to mitigate potential misuse.

**Table 4.3 ML/TF Threat Ratings by VASP Channels**

| Categories | Functions | Activities | Threat Ratings |
|---|---|---|---|
| **Virtual Asset Wallet Providers** | Custodial Services | Hot Wallet | Medium Risk |
| **Virtual Asset Exchanges** | Transfer Services | P2P (Peer-to-Peer) | High Risk |
| | | P2B (Peer-to-Business) | Medium Risk |
| | Conversion Services | Virtual-to-Fiat | Medium Risk |
| | | Fiat-to-Virtual | Medium Risk |
| | | Virtual-to-Virtual | Medium Risk |
| **Virtual Assets Broking / Payment Processing** | Payment Gateway | Merchants | Medium Risk |
| **Virtual Assets Investment Providers** | Trading Platform | Platform Operators | Medium Risk |
| | | Custody of Assets | High Risk |
| | Emerging Products | Stablecoins | High Risk |

Hot Wallet, Peer-to-Peer (P2P) and Peer-to-Business (P2B) are digital wallets with varying risk ratings. Hot Wallets are medium risk due to their online presence, while P2P transactions are high risk due to their decentralised nature and potential anonymity. P2B transactions, while less anonymous, still pose significant risks, especially if businesses are not fully compliant with AML/CFT regulations.

Virtual-to-Fiat and Fiat-to-Virtual conversions were rated as medium risk due to the likeliness for ML and the anonymity of exchanging digital assets for traditional currencies. Virtual-to-virtual was rated as a medium risk due to the traceability of digital transactions within blockchain networks.

Merchants and Platform Operators were rated as medium risk, due to their potential for market manipulation, fraud and illegal transactions if not adequately monitored and robust security measures and compliance are not enforced. These services integrate digital assets into the mainstream economy. The custody of assets, which involves managing VAs on clients' behalf, was rated as high risk due to the potential for cyber-attacks and misuse. Emerging products like stablecoins pegged to traditional currencies, were also rated as high risk due to regulatory challenges and potential abuse in illicit financial activities.

## 4.2 ML/TF Inherent Vulnerability Assessment

The inherent vulnerability assessment of ML/TF was classified using specific criteria.

a. Country risks
b. Customer types
c. Dealing with unregistered VASPs from overseas
d. Institution dealing with VASPs
e. Licensed in the country or abroad
f. Methods of delivery of products/services
g. Nature, size and complexity of the business
h. Products and services
i. Rapid transaction settlement
j. VA anonymity and pseudonymity

**Table 4.4 ML/TF Inherent Vulnerability Assessment**

| Categories | Functions | Activities | Inherent Vulnerability Ratings |
|---|---|---|---|
| Virtual Asset Wallet Providers | Custodial Services | Hot Wallet | High Risk |
| Virtual Asset Exchanges | Transfer Services | P2P (Peer-to-Peer) | High Risk |
| | | P2B (Peer-to-Business) | Medium Risk |
| | Conversion Services | Virtual-to-Fiat | High Risk |
| | | Fiat-to-Virtual | High Risk |
| | | Virtual-to-Virtual | Medium Risk |
| Virtual Assets Broking / Payment Processing | Payment Gateway | Merchants | Medium Risk |
| Virtual Assets Investment Providers | Trading Platform | Platform Operators | Medium Risk |
| | | Custody of Assets | High Risk |
| | Emerging Products | Stablecoins | High Risk |

The high-risk rating of Virtual Asset Wallet Providers, especially custodial services, face inherent vulnerabilities in managing hot wallets, which are internet-connected and susceptible to cyber threats

like hacking, phishing and malware, potentially leading to financial losses. Virtual asset exchanges for P2P transfer services are high risk due to their decentralised nature, lack of oversight and potential for illicit activities like ML and fraud. The anonymity and speed of transactions exacerbate these risks making it challenging for exchanges to implement effective KYC measures.

P2B transfer services are rated as medium risk due to their business involvement, which introduces accountability and regulatory compliance. However, potential cyber threats and evolving regulatory landscapes still pose risks. Exchanges offering P2B services should update security frameworks and collaborate with regulatory bodies to mitigate vulnerabilities.

Converting VA to fiat currency and vice versa is a high-risk activity, attracting ML and fraud due to its unregulated nature. It is also a gateway for bad actors to obscure illicit fund origins. The anonymity and speed of transactions make it difficult to track suspicious activities. Virtual-to-virtual conversion services are medium risk due to concentrated risk within private groups, but still face inherent risks of fraud, market manipulation and cyber threats.

Virtual asset broking and payment processing services for merchants have a medium risk rating due to vulnerabilities like fraud and regulatory compliance. Investment providers offering trading platforms for virtual assets are at medium risk due to market manipulation and cyber security threats. The custody of large volumes of assets poses high operational risks. Stablecoins are at high risk due to fraud, regulatory uncertainties and market volatility.

# 5.0 OVERALL ML/TF RISK

The assessment of ML/TF risk involves considering both inherent risk and the effectiveness of controls. Most categories have high inherent risks, indicating that existing controls may not fully mitigate these risks. This suggests the need for enhanced compliance measures, improved monitoring and more robust risk management strategies to reduce residual risk.

**Table 5.1 Overall ML/TF Risk**

| Categories | Functions | Activities | Threat Ratings | Inherent Vulnerability | Total Risk Rating | Residual Risk Rating |
|---|---|---|---|---|---|---|
| **Virtual Asset Wallet Providers** | Custodial Services | Hot Wallet | Medium Risk | High Risk | High Risk | High Risk |
| **Virtual Asset Exchanges** | Transfer Services | P2P (Peer-to-Peer) | High Risk | High Risk | High Risk | High Risk |
| | | P2B (Peer-to-Business) | Medium Risk | Medium Risk | Medium Risk | Medium Risk |
| | Conversion Services | Virtual-to-Fiat | Medium Risk | High Risk | High Risk | High Risk |
| | | Fiat-to-Virtual | Medium Risk | High Risk | High Risk | High Risk |
| | | Virtual-to-Virtual | Medium Risk | Medium Risk | Medium Risk | Medium Risk |
| **Virtual Assets Broking / Payment Processing** | Payment Gateway | Merchants | Medium Risk | Medium Risk | Medium Risk | Medium Risk |
| **Virtual Assets Investment Providers** | Trading Platform | Platform Operators | Medium Risk | Medium Risk | Medium Risk | Medium Risk |
| | | Custody of Assets | High Risk | High Risk | High Risk | High Risk |
| | Emerging Products | Stablecoins | High Risk | High Risk | High Risk | High Risk |

## 5.1 High-Risk Areas

Hot Wallets, P2P transfers, conversion services, custody of assets, and stablecoins are all vulnerable to cyber attacks due to their online presence. P2P transfers were high-risk due to their private nature. Custody of Assets is perceived as having a high inherent vulnerability due to the responsibility of service providers safeguarding significant amounts of assets, making them targets for cyber-attacks and theft. Stablecoins, pegged to fiat currencies, pose high risks due to speculative activities and regulatory uncertainties.

## 5.2 Medium-Risk Areas

P2B transfers have a lower threat level due to business-level accountability and compliance but still carry some risk. Conversion services (Virtual-to-Fiat, Fiat-to-Virtual, and Virtual-to-virtual) were rated as a medium risk but present vulnerabilities. Payment Gateways for merchants have medium risk due to pooled oversight and blockchain technology, providing transparency and secure transaction processes.

## 5.3 Overall Risk Areas

Table 5.1 reveals that custodial services involving hot wallets are highly vulnerable due to their online nature, exposing them to hacking risks. P2P transfer services and conversion services are high risk, while P2B transfer services and conversions are medium risk. Payment gateways used by merchants are medium risk, requiring an effective AML/CFT compliance programme.

Trading platforms and custody services for virtual assets carry different risk levels. While trading platforms have medium risk ratings, custody of assets, due to their storage and safeguarding nature, are highly risky. Emerging products like stablecoins also present high risk across all dimensions.

## 5.4 Analytical Findings

Figure 5.1 compares the total risk level and VA risk exposure for stablecoins in Ghana's VA ecosystem.

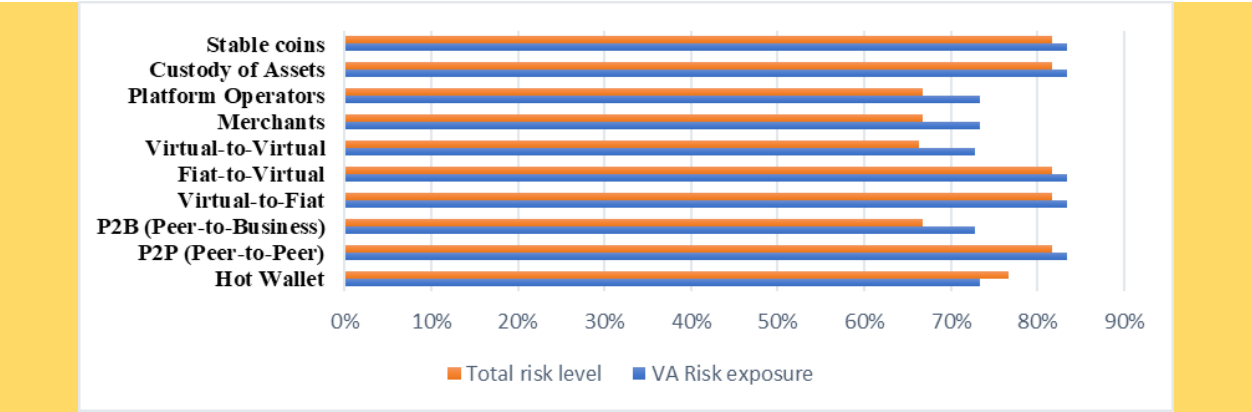


**Figure 5.1 Overall VA Risk Exposure**

Platform operators exhibit a total risk level of 67%, while the VA risk exposure is higher at 73%. This disparity highlights the specific challenges platform operators face, such as operational security, compliance with AML/CFT regulations and ensuring transparent operations. The higher VA risk exposure suggests additional vulnerabilities in the VA space that these operators must manage. Similar to platform operators, merchants show a total risk level of 67% and a VA risk exposure of 73%. This reflects the risks merchants face in accepting virtual assets as payment, including price volatility, fraud and regulatory compliance. The VA-specific risks might include additional transaction monitoring requirements and the need for robust security measures to handle VA transactions.

Virtual-to-virtual transactions, which involve the exchange of one virtual asset for another, have a total risk level of 66% and a VA risk exposure of 73%. The lower total risk level compared to other categories suggests that these transactions might be perceived as less risky in general. However, the higher VA risk

exposure indicates specific concerns in the virtual asset context, such as the potential for using these transactions to obscure illicit activities.

The process of converting fiat currency to virtual assets (fiat-to-virtual) carries a very high inherent risk exposure of 83%. This high level of risk is due to the potential for ML, fraud and other financial crimes. The risk is particularly pronounced in the conversion process, where fiat currencies, often subject to stringent regulatory scrutiny, are exchanged for virtual assets that may have less regulatory oversight. The total risk level for fiat-to-virtual transactions decreases only marginally to 82%, indicating that existing mitigating controls are not significantly reducing the inherent risks. This minimal reduction suggests that the current ML/TF risk management and regulatory frameworks in Ghana may not be fully effective in addressing the risks associated with fiat-to-virtual conversions. Enhanced regulatory measures, such as more rigorous KYC/AML protocols and better oversight of exchanges and service providers, are needed to effectively mitigate these risks.

Virtual-to-fiat transactions also have a high total risk level of 82% and a VA risk exposure of 83%, mirroring the trend seen in fiat-to-virtual transactions. This underscores the challenges and vulnerabilities associated with converting virtual assets back into traditional currency, including potential avenues for ML and the difficulty of tracing illicit funds once they are reintroduced into the traditional financial system.

P2B transactions involve individuals transacting directly with businesses using virtual assets. The inherent risk exposure for P2B activities is at 73%, indicating high vulnerabilities. These risks may include fraudulent transactions, inadequate KYC measures by businesses and potential non-compliance with AML/CFT regulations. The total risk level for P2B transactions drops to 67% after considering mitigating controls. This reduction suggests that businesses engaging in P2B transactions in Ghana may be employing effective risk management practices and compliance measures. Controls such as stringent KYC procedures, transaction monitoring and adherence to AML/CFT regulations help mitigate the risks associated with P2B transactions. However, the residual risk level of 67% remains notable, indicating that further improvements in risk management practices could be beneficial.

P2P transactions, where individuals directly exchange virtual assets with one another, have the same risk levels as peer-to-business transactions, with a total risk level of 82% and a VA risk exposure of 83%. P2P transactions are decentralised and often harder to regulate, making them attractive for illicit activities. The consistent risk levels highlight the importance of robust monitoring and regulatory frameworks to address these challenges.

Hot wallets, used for storing and accessing virtual assets online, show a total risk level of 77% and a VA risk exposure of 73%. Although slightly lower than some other categories, the risks associated with hot wallets could be attributed to their vulnerability to hacking and cyber-attacks. The lower VA risk exposure might reflect improvements in security technologies and practices within the VA ecosystem.

# 6.0 THE ML/TF MITIGATION MEASURES AND RESIDUAL RISK FOR VAs AND VASPs

## 6.1 Mitigating Measures

The assessment revealed gaps in Ghana's AML/CFT framework for VAs/VASPs, including regulatory oversight, entry controls and resource allocation compared to traditional FIs and DNFBPs.

**Table 6.1 Mitigating Measures on Input Variables**

| Intermediary variables | Input variables | Mitigating Ratings |
|---|---|---|
| Government measures | Comprehensiveness of AML/ CFT Legal Framework | Medium Mitigation |
| | Availability and Effectiveness of Entry Controls | Does not exist |
| | Adequate Supervision & Monitoring Mechanism | Does not exist |
| | Regulation for Customer Due Diligence (CDD) and source of funds & Availability of Reliable Identification Infrastructure | Medium Mitigation |
| | Financial and human resource capacity of law enforcement authorities to investigate, trace, seize and secure virtual assets | Medium Mitigation |
| | Effectiveness of international cooperation | Medium Mitigation |
| | Effectiveness of domestic cooperation | Medium Mitigation |
| | Quality of guidance issued to VASPs and engagement with VASPs | Does not exist |
| VASP measures | Transparency of shareholder Structure of VASP | Low Mitigation |
| | Quality of Governance structure and Level of accountability of VASP | Low Mitigation |
| | Effectiveness of compliance function and internal control mechanism | Low Mitigation |
| | AML/ CFT knowledge of VASPs staff | Low Mitigation |
| Financial Institution (FI) Measures and Designated Non-Financial Businesses and Professions (DNFPs) | Risk assessment and Risk Mitigation measures by Financial Institutions (FIs) and DNFBPs. Referred in this guidance as Traditional Obliged Entities (TOE) | High Mitigation |
| | Effectiveness of compliance function and internal control mechanism | Very High Mitigation |

Act 1044 designates VASPs as AIs and requires them to comply with their AML/CFT obligations. However, the non-existence of regulation and entry controls with regards to VASPs creates a gap in the regulatory environment. Entry controls are essential to ensure that only legitimate entities can operate as VASPs. Without these controls, the sector is vulnerable to exploitation by illicit actors. Also, the lack of supervision and monitoring mechanisms further exacerbates the risk, as there are no systems in place to oversee VASPs' activities, ensure compliance with AML/CFT regulations or detect suspicious activities.

Regarding the capacity of LEAs, Ghana has constituted a National Cryptocurrency Task Force comprising representatives from EOCO, NIB, GPS, Narcotic Control Commission (NACOC), Office of the Special

Prosecutor (OSP), FIC, BoG, SEC, GRA, Office of the Attorney General (AG) and Cyber Security Authority (CSA). The taskforce's mandate is to investigate, trace, seize and confiscate virtual assets linked to criminal activities. This notwithstanding, LEAs require funding, investment in new technologies, skilled experts and trained personnel for effective ML/TF mitigation.

Additionally, absence of guidance and engagement with VASPs is a critical shortfall. VASPs need clear regulatory guidelines and regular engagement with regulators to understand their obligations and ensure compliance with AML/CFT measures.

## 6.2 Residual Risk

Ghana has made progress in managing risks related to VAs/VASPs, however further scrutiny is needed due to varying risk levels and the need for targeted regulatory approaches and technological advancements.

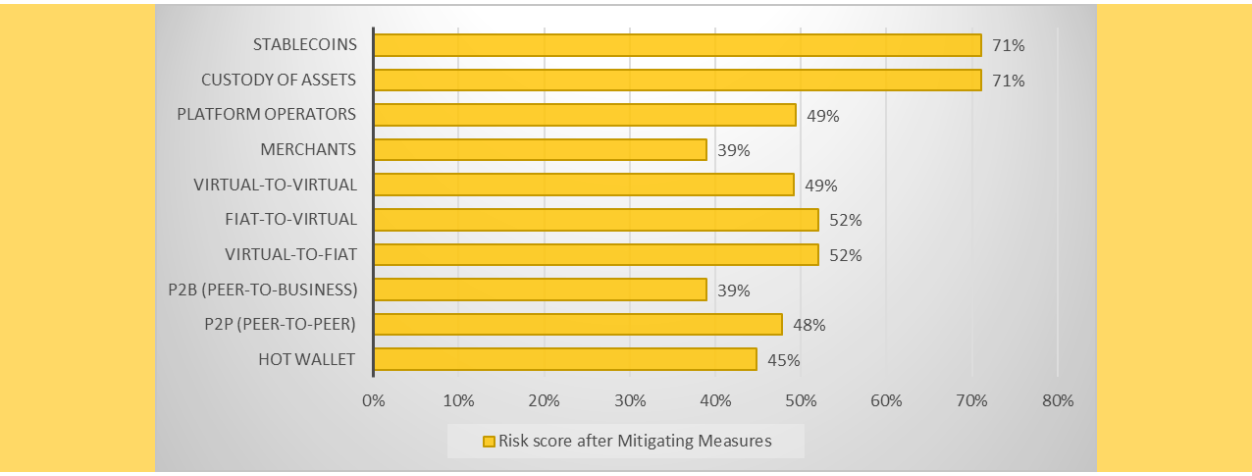


**Figure 6.1 Residual Risk Measures on Input Variables**

From Figure 6.1, the residual risk after mitigating measures for Hot Wallet is 45%. This indicates a significant risk reduction, suggesting that the mitigating measures are effective in securing assets stored in hot wallets. Also, under P2P and P2B, these activities have residual risks of 48% and 39%, respectively. The lower residual risk in P2B indicates that the mitigating measures are more effective in this context, possibly due to the structured nature of business transactions compared to peer-to-peer interactions.

Both Virtual-to-Fiat and Fiat-to-Virtual have a residual risk of 52%, indicating that the risks remain high despite the mitigating measures. This might suggest that the regulatory framework or technological solutions available are not sufficient to fully mitigate the inherent risks associated with these transactions. Further, virtual-to-virtual with a residual risk of 49%, is to some extent mitigated, possibly due to effective controls in place for transactions between different virtual assets. Merchants and Platform Operators have residual risks of 39% and 49%, respectively, indicating effective risk management practices in these areas, possibly due to the adoption of industry best practices and compliance measures.

Additionally, both Custody of Assets and Stablecoins have high residual risks of 71%, indicating that current mitigating measures are less effective in managing the risks associated with these activities. This is a critical area, as the custody of assets involves significant risks related to asset security and fraud.

# 7.0 KEY FINDINGS AND RECOMMENDATIONS

## 7.1 Key findings

The assessment on VAs/VASPs in Ghana is crucial for understanding ML/TF risk within the digital financial landscape and recommends appropriate mitigating measures. Below are some of the key findings from the assessment.

1. The assessment highlights the dual nature of VAs/VASPs as both innovative financial instruments and potential conduits for illicit activities such as ML/TF, emphasising the need for robust regulatory frameworks.
2. The challenges of regulatory oversight in the decentralized and anonymous nature of virtual assets can be exploited for tax evasion, fraud and illicit activities.
3. Despite the presence of various VASPs in Ghana, the lack of certain critical services such as virtual asset management and ICO providers points to areas where the market is still nascent and regulatory frameworks need further development.
4. The assessment underscored the need for a balanced approach to regulate VAs/VASPs in Ghana, combining strict regulations with public awareness initiatives. This approach is crucial for the safe and sustainable growth of the digital asset ecosystem and ensures market integrity and consumer protection.
5. The need for stricter KYC and AML protocols, especially for fiat-to-virtual and virtual-to-fiat transactions is evident.
6. Adopting industry best practices and advanced cyber security measures, such as global compliance standards, regular training, audits and multi-factor authentication are crucial for VASPs.

## 7.2 Limitations

The NRA exercise was confronted with some limitations which are discussed below:

1. Inadequate data on VAs/VASPs activities in the Ghanaian financial ecosystem.
2. Delay in receiving feedback from respondents on qualitative data.
3. Limited knowledge among stakeholders on VAs/VASPs activities.

## 7.3 Recommendations

To effectively mitigate the risks identified in the assessment, several key strategies and measures have been proposed.

1. Relevant stakeholders should develop robust regulatory frameworks, setting clear guidelines, mandatory registration, licencing and stringent compliance requirements.
2. Enhance cooperation among various regulatory, LEAs and international bodies to facilitate the tracking and combating of illicit activities involving virtual assets as such cooperation is crucial for addressing the cross-border nature of many of these transactions.

3. Increasing public awareness about the risks and responsibilities associated with virtual assets is essential. Educational campaigns aimed at both consumers and businesses can help reduce the incidence of fraud and promote responsible usage of digital assets.
4. Regulatory bodies/ relevant stakeholders should institute capacity building programmes on AML/ CFT obligations for VASPs.
5. Adequate resource allocation for regulatory bodies, FIC, LEAs and judiciary to facilitate investigation, asset tracing, seizure, confiscation and recovery.
6. Promote innovation in the digital asset space for economic growth and financial inclusion.

# GLOSSARY

| TERM | EXPLANATION |
|---|---|
| Bitcoin (BTC) | Bitcoin is the first and most well-known cryptocurrency, enabling peer-to-peer transactions without a central authority. |
| Blockchain | A blockchain is a decentralised digital ledger that records transactions across many computers securely and immutably. |
| Central Bank Digital Currency | A Central Bank Digital Currency (CBDC) is a digital form of a country's fiat currency issued and regulated by the central bank. |
| CentralisedExchange | A centralised exchange is a platform where cryptocurrencies are traded through a third-party service provider. |
| Cloud Mining | Cloud mining allows individuals to mine cryptocurrencies using shared processing power hosted in remote data centres. |
| Coin Mixer | A coin mixer is a service that anonymises cryptocurrency transactions by mixing coins of different users. |
| Contract | In traditional finance, contracts are legally binding agreements between parties. In cryptocurrencies, smart contracts are self-executing, written into code, which automatically enforce and execute agreed terms when specific conditions are met, all within the secure blockchain environment. |
| Crowdfunding | Crowdfunding is a method of raising capital for a project or venture by soliciting contributions from a large number of people, typically via the Internet. |
| Crypto Escrow | Crypto escrow services hold and release cryptocurrency funds upon fulfilment of specific conditions in a transaction. |
| Cryptocurrency | A cryptocurrency is a digital or virtual currency that uses cryptography for security and operates independently of a central bank. |
| Cryptography | Cryptography involves the techniques of secure communication, ensuring data integrity, confidentiality, and authentication. The information can only be decrypted and read with the necessary key. |
| Custodial Services | Custodial services involve a third party holding and managing assets on behalf of a customer. |
| Data Privacy | Data privacy refers to the handling of personal data to protect individuals' information from unauthorised access. |

| | |
|---|---|
| Decentralised API (dAPI) | Application Programming Interface (API) services are intrinsically interoperable with blockchain technology. This is aninvention of the API3 protocol. A decentralised API is an interface that allows applications to interact with decentralised services and data. |
| Dark Web | The dark web consists of parts of the internet not indexed by traditional search engines, often requiring special software to access. |
| Decentralised finance (DeFi) | Decentralised Finance, is a blockchain-based form of finance that doesn't rely on central financial intermediaries and makes transactions faster and cheaper. |
| Electronic Levy | An electronic levy is a tax imposed on electronic transactions. |
| Initial Coin Offering | An Initial Coin Offering (ICO) is a fundraising method where new cryptocurrencies or tokens are sold to early investors. |
| Initial Token Offering | An Initial Token Offering (ITO) is similar to an ICO but focuses more on offering tokens that may have utility within a specific ecosystem. |
| Money Laundering | Money laundering is the process of making illegally gained proceeds appear legal by transferring them through legitimate financial systems. |
| Non-Custodial Services | Non-custodial services allow users to retain control of their private keys and digital assets without relying on a third-party custodian. |
| Security Token Offering | A Security Token Offering (STO) is a public offering of tokenised digital securities, subject to regulatory oversight. |
| Stablecoins | Stablecoins are cryptocurrencies designed to minimise price volatility by pegging their value to a reserve asset like fiat currency. |
| Terrorist Financing | Terrorist financing involves the provision of funds for terrorist activities, often scrutinised by financial regulators. |
| Traditional Obliged Entities | These are institutions like banks and financial services that must comply with AML and CTF regulations. |
| United States Bitcoin Corporation | A hypothetical or specific entity focused on the development or management of Bitcoin-related activities in the United States. |
| United States Dollar Coin | United States Dollar Coin (USDC) is a stablecoin pegged to the U.S. dollar, backed by equivalent fiat currency reserves. |
| United States Dollar Tether | United States Dollar Tether (USDT) is another stablecoin pegged to the United States dollar, used for trading and transferring within cryptocurrency markets. |

| | |
|---|---|
| Validators, Miners & Administrators | Validators and miners are participants in a blockchain network responsible for verifying transactions and maintaining the blockchain. Administrators manage and oversee blockchain operations. |
| Virtual Asset | A virtual asset is a digital representation of value that can be digitally traded or transferred and used for payment or investment purposes. |
| Virtual Asset Exchanges | Platforms facilitate the trading of virtual assets, allowing users to buy, sell, and exchange different cryptocurrencies. |
| Virtual Asset Management Providers | These providers manage portfolios of virtual assets on behalf of clients. |
| Virtual Asset Service Provider | A Virtual Asset Service Provider (VASP) is an entity that provides services related to the exchange, transfer, custody, and management of virtual assets. |
| Virtual Assets Broking / Payment Processing | Services facilitating the buying, selling, and transferring of virtual assets, including processing payments for goods and services. |
| Virtual Assets Investment Providers | These are entities offering services related to the investment and management of virtual assets. |

# REFERENCES

1. Asia Pacific Group on Money Laundering (APG). (2021). *Virtual assets and their AML/CFT implications.* Sydney: APG.
2. Bank of Ghana. (2021). *Central Bank Digital Currency Feasibility Study*. Accra: BoG.
3. Blockchain Association of Ghana. (2022). *Blockchain Technology and Regulatory Challenges.* Accra: BAG.
4. Chainalysis. (2022). *The 2022 Geography of Cryptocurrency Report*. Retrieved from Economic Intelligence Unit. (2021). *The Impact of Cryptocurrencies on Emerging Markets.* London: EIU.
5. Elliptic. (2021). *Financial Crime Typologies in Cryptocurrency.* Retrieved from
6. European Union. (2021). *Regulation of Markets in Crypto-assets (MiCA).* Brussels: EU.
7. Europol. (2021). *Internet Organised Crime Threat Assessment (IOCTA) 2021*. Retrieved from https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2021
8. FATF. (2019). *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*. Paris: FATF.
9. Financial Stability Board. (2020). *Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets.* Basel: FSB.
10. Financial Technology Association of Ghana. (2023). *Fintech and Virtual Assets: Opportunities and Risks*. Accra: FinTech Ghana.
11. Financial Stability Review. (2023, 2024). *Digital Assets*. Accra.
12. Ghana Revenue Authority. (2020). *Cryptocurrency Tax Evasion Case Study*. Accra: GRA.
13. Ghana Revenue Authority. (2022). *Annual Tax Report 2021*. Retrieved from
14. Giesecke+Devrient. (2022). *Central Bank Digital Currency: Considerations for Ghana*. Retrieved from
15. Fraud and Ponzi Schemes. (2020). *Extradition of Ghanaian National for Multimillion-Dollar Fraud*. Retrieved from https://www.justice.gov.
16. GRA & International Tax Authorities. (2021). *Cross-border crypto transfers to offshore accounts*. Accra: Ghana Revenue Authority.
17. International Monetary Fund (IMF). (2023). *Economic outlook for Ghana*. Washington, DC: IMF.
18. International Monetary Fund. (2020). *Digital Currencies and the Future of the Monetary System.* IMF Policy Paper. Retrieved from
19. National Insurance Commission, (NIC). 2024. Sandbox Directive.
20. Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. Retrieved from

21. OECD. (2021). *Taxing virtual currencies: An overview of tax treatments and emerging tax policy issues*. Paris: OECD.

22. Securities and Exchange Commission Ghana. (2022). *Regulation of virtual asset service providers in Ghana*. Accra: SEC Ghana.

23. United Nations Office on Drugs and Crime. (2021). *Cryptocurrencies and Money Laundering*. Vienna: UNODC.

24. United States Bitcoin Corporation. (2021). *Global Bitcoin usage report.* New York: USBTC.

25. World Bank. (2021). Strategic implementation programming: An introduction. Washington, DC: World Bank.

FINANCIAL INTELLIGENCE CENTRE, GHANA

DESIGN & PRINT: PLACARD COMMUNICATIONS – 024 472 1821 | 026 464 3339