وحدة المعلومات المالية
Financial Intelligence Unit

Strategic Analysis on Virtual Assets

UAE-FIU 2021

UAE Financial Intelligence Unit – P.O.Box 854, Al Karamah Street – International Tower, Abu Dhabi.

Phone No: +97126919955

Email address: uaefiu@uaefiu.gov.ae

List of Acronyms

Terms & Definitions	Description
AML/CFT	Anti-Money Laundering / Countering the Financing of Terrorism
CBUAE	Central Bank of the UAE
ECDD	Enhanced Customer Due Diligence
FATF	Financial Action Task Force
FI	Financial Institution
GoAML	The Financial Intelligence Unit online reporting application
KYC	Know Your Customer
LEA	Law Enforcement Authority
RFI	Request for Information
SAR	Suspicious Activity Report
SD	Spontaneous Dissemination
STR	Suspicious Transaction Report
VA	Virtual Asset
VC	Virtual Currency
VASPs	Virtual Asset Service Providers
UAEFIU	Financial Intelligence Unit of the UAE

Content and Objectives

This report is part of the Strategic Analysis Plan (SAP) adopted by the UAE FIU also considering the requirements of the *National Assessment of Inherent Money Laundering and Terrorist Financing Risks in the United Arab Emirates* (NRA) and the following *UAE National Action Plan to Implement the Combating Anti-Money Laundering and Terrorism Financing National Strategy 2020-2023* (NAP).

The strategic analysis is based on the review and results of the strategic analysis relating **Virtual Currencies** and the risks/vulnerabilities associated with such assets and its possible abuse in the context of Money Laundering (ML) and/or Financing of Terrorism (FT).

The purpose of this analysis is to:

- Understand the Virtual Currencies and the risks/vulnerabilities associated with such assets;
- Develop list of possible red flag indicators aimed at assisting the identification and assessment of possible ML/FT schemes pertaining to Virtual Currencies.

Methodology, Sources and Timeline

This report is based on the strategic analysis of data and information held by the UAEFIU mainly, as well as data and information obtained from different domestic and international reports, other UAE Authorities, and the Suspicious Transaction Reports (STRs) received from Reporting Entities "REs", particularly in the period January 2020 to June 2021.[1]

[1] The data and information analyzed include but are not limited to: STRs and SARs databases; Cash declarations; information received from UAE Authorities; information received from REs.

I. Introduction

In about a decade ago, a revolutionary digital transformation in the world's financial sector has taken place. This innovative occurrence has initially fascinated the masses due to its presumed benefits of anonymity, efficiency, cheap and fast medium to transfer value around the world surpassing the value offered by the conventional financial sector. These digital instruments are also known as "virtual assets".

Virtual assets depend on a distributed ledger technology (DLT), such as 'blockchain'. DLT is a database that is stored, shared, and synchronized on a computer network. Data is updated by following rules for achieving consensus among the network participants[2].

The 'virtual asset' is a new sector that is fast moving and technology-dependent. Accordingly, the need for the regulators to adopt and assist to manage the risks associated with it is necessary. In some countries around the world, dealings related to virtual assets are strictly prohibited, while in other jurisdictions, regulators have started taking steps to assess virtual assets' mechanisms and put it under a particular regulatory framework. In the UAE, **Securities and Commodities Authority (SCA)** and **Central Bank of the United Arab Emirates (CBUAE)** share responsibility in regulating specific virtual assets.

Pursuant to the **Decretal Federal Law No. 26 of 2021** amending some provisions of the **Decretal Federal Law No. 20 of 2018** regarding Anti Money Laundering and Combating Financing of Terrorism and Illicit Organizations, "Virtual Assets" are digital representation of value that can be digitally traded or transferred, and so on, in accordance with what is specified in the Executive Regulations of the Decretal Federal Law No. 26 of 2021 (unofficial translation)[3].

On 03/11/2020, the **CBUAE** has issued the "**Stored Value Facilities Regulation"** or the **"SVF Regulation"**. Subsequent to this, the CBUAE has issued the "**Retail Payment Services**" and Card Schemes Regulation as a preparation for a new era of digital payments. As per the regulation, "The Regulation introduces a licensing regime for payment service providers operating – or wishing to provide – one or more of nine payment services or payment card schemes in the UAE. These include: payment account issuance, payment instrument issuance, merchant acquiring, payment aggregation,

[2] See IMF's Paper on Virtual Assets and Anti-Money Laundering and Combating the Financing of Terrorism at https://www.imf.org/en/Publications/fintech-notes/Issues/2021/10/14/Virtual-Assets-and-Anti-Money-Laundering-and-Combating-the-Financing-of-Terrorism-1-463654

[3] See UAE Federal Decree No. 26 of 2021 at https://www.uaeiec.gov.ae/en-us/laws-regulations-listing/federal-decree-no-26-of-2021

domestic and cross-border fund transfers, payment tokens, payment initiation, and payment account information services." [4]

In accordance with **Securities and Commodities Authority (SCA)**'s The Chairman of the Authority's Board of Directors' Decision No. (23/ Chairman) of 2020 Concerning **Crypto Assets Activities Regulation**, "crypto asset" is a record within an electronic network or distribution database functioning as a medium for exchange, storage of value, unit of account, representation of ownership, economic rights, or right of access or utility of any kind, when capable of being transferred electronically from one holder to another through the operation of computer software or an algorithm governing its use[5].

As specified by **Financial Services and Regulatory Authority (FSRA)**'s Financial Services and Markets (Amendment No.2) Regulations 2020, "virtual asset" is defined as a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status in any jurisdiction. A Virtual Asset is: (a) neither issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the Virtual Asset; and (b) distinguished from Fiat Currency and E-money[6].

As per **Dubai Financial Services Authority (DFSA)**'s Consultation Paper No. 38: Regulation of Security Token, 'crypto asset or token' is a digital representation of value, rights and obligations that are created, stored and transferred electronically, using distributed ledger technology (DLT) or similar technology[7]. DFSA has launched its Regulatory Framework for Investment Tokens on 25/10/2021[8].

The national law and the relevant stakeholders in the UAE may define Virtual assets differently, but the essence circles around the same concept of FATF's own definition of virtual assets, as "the digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes. Virtual assets do not

[4] See Retail Payment Services and Card Schemes Regulations at https://www.centralbank.ae/en/node/2648

[5] See SCA's The Chairman of the Authority's Board of Directors' Decision No. (23/ Chairman) of 2020 Concerning Crypto Assets Activities Regulation at https://www.sca.gov.ae/Content/Userfiles/Assets/Documents/8004151b.pdf

[6] See Financial Services and Markets (Amendment No.2) Regulations 2020 at https://en.adgm.thomsonreuters.com/sites/default/files/net_file_store/Financial_Services_and_Markets_(Amendment%20No%202)_Regulations_24_February_2020.pdf

[7] See DFSA's Consultation Paper No. 38: Regulation of Security Token at https://dfsaen.thomsonreuters.com/sites/default/files/net_file_store/CP138_Regulation_of_Security_Tokens.pdf

[8] See The DFSA Rulebook: General Module – Investment Tokens at https://dfsaen.thomsonreuters.com/sites/default/files/net_file_store/DFSA1547_1843_VER550.pdf

include digital representations of fiat currencies, securities, and other financial assets that are already covered elsewhere in the FATF Recommendations[9]"

Due to the complexity of the subject, limited comprehensive studies and lack of definitive regulations on virtual assets, the focus of this report will be on the most relevant type of virtual asset to the UAE, namely, 'cryptocurrency', also known as **'virtual currency'**. According to FATF Report in 2014, 'Virtual currency is a digital representation of value that can be digitally traded and functions as a (1) medium of exchange; and/or (2) a unit of account; and/or (3)) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction. It is not issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the virtual currency'[10].

Although in this study, no cases/scenarios have been identified by the UAEFIU involving Terrorist Financing via Virtual Currencies/Assets or even other associated concepts, the risks that cryptocurrencies and virtual asset service providers are misused for terrorism financing purposes cannot be certainly eliminated and is indeed seems to be on the rise globally. However, other emerging techniques demonstrating the misuse of Virtual Currencies are described later in the report.

II. Background

When a virtual currency is introduced to the public, fixed parameters are pre-set, for instance, its maximum supply available, rules in mining, buying and selling, and other important features. The concept was novel in the beginning but started to garner popularity leading to a dramatic rise in value in 2010. Up to date, Bitcoin (BTC) is the most well-known and most valued among thousands of virtual currencies around the world.

Virtual currency can be categorized into two types: convertible and non-convertible. Convertible (or open) virtual currency is a currency that has a corresponding value in fiat (or real) currency and can be traded for real currency[10]. For example, Bitcoin, Ethereum, Litecoin, etc. In contrast, non-convertible (or closed) virtual currency is a currency intended for use only within a particular virtual domain or community, and cannot be traded for real currency[10]. For instance, One Amazon Coin, G-Coin, etc.

[9] See FATF's Updated Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers at https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html

[10] See FATF Report on Virtual Currencies: Key Definitions and Potential AML/CFT Risks published on June 2014 at https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

Further, non-convertible virtual currency is considered to be centralized, due to the presence of a central authority that issues and establishes rules for its use. On the contrary, convertible virtual currency can be centralized or decentralized depending on the presence of a central authority and other factors. In general, centralized virtual currencies have a single administrating authority (administrator) that issues the currency, establishes the rules, maintains a central payment ledger and has authority to withdraw the currency from circulation. Alternatively, decentralized virtual currencies have no single administrating authority, no central monitoring or oversight, distributed, open-source, and math-based peer-to-peer virtual currencies[10].

Another important player in the world of virtual currency are the cryptocurrency exchangers. As per FATF paper, an exchanger (also sometimes called a virtual currency exchange) is a person or entity engaged as a business in the exchange of virtual currency for real currency, funds, or other forms of virtual currency and also precious metals, and vice versa, for a fee (commission). Exchangers generally accept a wide range of payments, including cash, wires, credit cards, and other virtual currencies, and can be administrator-affiliated, non-affiliated, or a third-party provider. Exchangers can act as a bourse or as an exchange desk. Individuals typically use exchangers to deposit and withdraw money from virtual currency accounts[10].

III. AML/CFT Risks of Virtual Currency

The emergence of virtual currency is a technological innovation specific to the financial industry. While it has a potential to benefit in many ways, it can also create opportunities for criminals as an avenue to launder ill-gotten funds or finance terrorist activities. Virtual currencies are attractive to criminals due to number of reasons enumerated below.

1. Greater anonymity – Although transactions can be viewed online and wallets (of sender and receiver) can be identified, the challenge lies on how financial investigators can link a wallet to the actual conductor or beneficiary. This is especially due to the availability of virtual currency features that allow obscurity of the flow of funds and transactions being kept in a distributed network, which is not readily accessible for the investigators.

2. Fast and irreversible transactions – A transfer of virtual currency is fast and feasible within minutes from the time of its initiation. This is unlike the traditional banking, which undergoes conventional transfer processing before a transfer can be successful. On top of that, once a miner has confirmed a transfer of virtual currency, the transaction cannot be recalled, i.e., it is irreversible.

3. Global reach – Accessible anywhere to any device that has internet connection, virtual currency can be used to conduct international transfers. Moreover, especially for decentralized virtual currencies, execution of fund transfers and payments through it heavily depends on infrastructures that are complex in nature involving several entities across several countries. In return, this can create difficulty for financial investigators, law enforcement and regulators to access these systems. Some virtual currency systems intentionally collaborate in ML schemes and target jurisdictions with weak or inadequate AML/CFT controls.

4. No physical presence requirement – Since virtual currency transactions are conducted online, a face-to-face interaction is not required. Lack of physical interaction can encourage criminals to use anonymous funding. Anonymous funding is a form of cash funding or use of third-party funding through virtual exchangers that do not properly identify the funding source[10].

5. Limited regulatory framework available – Some jurisdictions have acknowledged virtual currencies as financial instruments, while some are still hesitant to deal with it possibly due to lack of expertise or conventional financial institutions are still preferred. There is no established global standards yet clearly defining virtual assets including virtual currencies and its accompanying features and risks. Due to this, criminals try to exploit jurisdictions with no or weak supervision.

6. Lack of sufficient AML/CFT procedures – Virtual Asset Service Providers (VASPs) must implement the same preventive measures including CDD, transaction monitoring and reporting of STRs/SARs. Conducting proper AML/CFT procedures is vital in the identification and verification of the source of virtual currency funding.

IV. Emerging trends / Typologies

A review on a sample of **Suspicious Transaction Reports (STRs) and Suspicious Activity Reports (SARs)** received from the relevant Reporting Entities was conducted in this report. The review of the mentioned data is vital in order to assess the vulnerabilities of the UAE's financial system in relation to the emerging techniques that might possibly facilitate ML/TF activities through Virtual Currencies.

Based on an in-depth analysis and comprehensive review of all the available information, it was observed that the most common techniques used by criminals to launder funds or perpetrate illicit activities through Virtual Currencies are as follows:

1. **Online Scam Activities through Virtual Currencies**

Due to virtual currency being an internet-based asset and its growing demand around the world, it is becoming more susceptible to internet fraud, for instance, online scam activities.

In the review of the sample reports, it was observed that a common modus operandi used by fraudsters to approach the victims is through social media, such as Facebook and Instagram. The victims are lured to fake promise of obtaining high investment returns after virtual assets/currencies are transferred to the fraudster's wallet address. Subsequently, the fraudster either stops communicating with the victim or continues to extort more virtual assets by asking the victim to send more as a "fee" in order for the principal amount to be returned along with the supposedly promised "return".

2. **Sending or Receiving Virtual Currency Transfers to known Darknet Market or Fraud Shop Wallets**

Darknet Markets and Fraud Shops are examples of underground websites used by criminals to facilitate trade of illegal goods and/or services, or purchase data and information to be utilized for illicit activities (e.g. fraudulent activities). Transactions between two parties are commonly settled through virtual asset transfers.

The analysis of the sample reports suggests that almost 70% are instances involving Darknet Markets or fraud shops. Mainly, the risk lies on the user's exposure to these underground wallets – either receiving or sending virtual assets.

3. **Use of Fake Identities to Open Wallet Accounts**

Identity theft is rapidly growing across the financial systems in many jurisdictions, hence cited as the most growing and fastest crime of digital age. Using fake identities are a twofold benefit for criminals: one is hiding the criminals identities by using stolen identities; two is gaining credentials to access victims accounts/information/funds for self-gain (Account Take-over).

4. **Peer-to-peer networks**

Users purchasing Tether USDT (a stable-coin at the rate of one tether for one U.S. dollar) on a virtual asset platform for Peer to Peer (P2P) trading on other VASP platforms, repeated behaviors exhibited in the reviewed STRs such as the below:

- Fiat deposits are made on the VA platform using debit/credit cards (often through multiple cards, including third party cards).
- The fiat balance is used for purchasing Tether (USDT) on the VA platform.

- The Tether (USDT) balance is immediately withdrawn to wallets belonging to another platform.

V. Case Example

The UAEFIU has received an STR from a VASP, filed against an individual 'KAK' and his associates. KAK was on boarded on the platform of VASP recently. Since then, he was flagged during fiat transaction monitoring for excessively consuming his weekly deposit limits for (3) consecutive weeks. Multiple fiat deposits were made using a credit card; the fiat funds were used to purchase USDT and the virtual assets were withdrawn to an address on another VASP exchange. The user's (KAK) justifications provided were insufficient and do not sustain the source of funds and the purpose of such behavior.

The user's credit card was also flagged for being used by four (4) other users on the same exchange platform. During the analysis, it was observed that those four (4) individuals were also linked to another twenty five (25) users, who might be family members or associates of KAK. The connection between the users detected after manually reviewing the credit card transaction reports obtained from the reporting entity's card payment gateway. Further, the Credit Card found linked to multiple e-mail addresses.

A total of approximately AED 1,630,519 (amounts in this case converted to AED) in fiat deposits were made using KAK's Credit Card, out of which around AED 1,390,582 were fiat deposits made on KAK's account. The combined value of fiat deposits made by KAK's family members and close associates is AED 4,049,472; In which six (6) credit cards were used belonging to different individuals who were also found as associates of KAK. All users associated with KAK exhibited the same patterns of transactions: high frequency of fiat deposits via credit card, followed by USDT purchase orders on a virtual asset platform and withdrawal of USDT to another platform.