MANAGEMENT OF MONEY LAUNDERING ("ML"), TERRORISM FINANCING ("TF") AND SANCTIONS RISKS FROM CUSTOMER RELATIONSHIPS WITH A NEXUS TO DIGITAL ASSETS

INDUSTRY PERSPECTIVES ON BEST PRACTICES

July 2023

CONTENTS

CONTENTS

Introduction and Objectives

In August 2022, a Digital Assets Risk Management Group was established under the AML/CFT Industry Partnership (“ACIP”) including representatives from the banks (OCBC, SCB, HSBC, JP Morgan, DBS, UOB, Citibank, Maybank), the Monetary Authority of Singapore (“MAS”), the Commercial Affairs Department (“CAD”) and Ernst & Young ("EY").

The objective of the Digital Assets Risk Management Group was to define and share best practices on the management of Money Laundering (“ML”), Terrorism Financing (“TF”), and Sanctions risks arising from customer relationships with a nexus to digital assets.

This paper provides Financial Institutions (“FIs”) with a foundational framework to advance understanding and management of ML/TF, and Sanctions risks arising from customer relationships with nexus to digital assets in the Singapore context by

(a) presenting a high-level overview on the classes of digital assets and proposing risk factors for assessing relevance of digital assets from the AML/CFT perspective;

(b) identifying the possible types of customer nexus to digital assets such as cryptocurrencies and analysing the underlying risk profiles; and

(c) clarifying risk management objectives and assessing incremental risk management capabilities required to manage these associated risks.

Background

History of Digital Assets

Digital assets originated with the emergence of the blockchain technology, a decentralised ledger that provided the foundations for the launch of the cryptocurrency "Bitcoin" in 2009 by a person or group of people using the pseudonym 'Satoshi Nakamoto'.

Since then, the digital assets landscape has evolved to encompass not just digital payment tokens, but also other non-payment digital assets such as non-fungible tokens.

Digital assets are becoming more widely accepted and the digital assets ecosystem has given rise to new types of customers and customer transactions. Some of these could suffer from light Know-Your-Customer ("KYC") controls, ineffective triggers for enhanced due diligence and/or lack of ongoing customer due diligence, making it easier for criminals to facilitate ML/TF or Sanctions evasion.

It is critical for FIs to strengthen their risk management frameworks to address any incremental ML/TF and Sanctions risks associated with these digital assets.

Definition of Digital Assets	**For the purpose of this paper, the term 'digital asset' refers to an asset whose ownership is represented in a digital or computerised form. It does not include the digital representation of fiat currencies[1].**

Types of Digital Assets

Based on the Working Group's research, the following are identified as the current major types of digital assets:

Digital payment tokens[2]

- **Cryptocurrencies:** Digital currency in which transactions are verified and records are maintained by a decentralised system using cryptography, rather than by a centralised authority

- **Stablecoins:** A subset of crypto-assets that aim to maintain a stable value relative to a specified asset (typically a unit of fiat currency or commodity) or a pool/basket of assets. They can be transferred either on a peer-to-peer ("P2P") basis using private crypto wallets or through third-party service providers[3]

(continues on next page)

[1]*Please refer to Annex B for the definition used for the purposes of this paper*
[2]*Per Payment Services Act ("PSA") definition. Please refer to Annex B for the full definition*
[3]*Per definition by Financial Stability Board ("FSB")*

Background

Types of Digital Assets (Cont'd)

Other digital assets

- **Transferrable gaming/streaming credits:** Digital assets which are sold in exchange for money, and can be transferred or spent on goods and services
- **Limited Purpose Digital Payment Tokens[4]:** Any digital representation of value that are non-refundable, non-transferrable, or non-exchangeable for money and used only for certain limited purposes (e.g., closed loop virtual gaming tokens)
- **Central Bank Digital Currencies ("CBDCs"):** Digital payment instrument, denominated in the national unit of account, that is the direct liability of the central bank[5]
- **Digital Capital Markets Products ("DCMPs") tokens:** On-chain representations of traditional capital markets products[6] that exist off-chain
- **Non-Fungible Tokens ("NFTs"):** Digital assets with distinct and unique features that are verified and secured by blockchain technology, used to represent either digitally native items (e.g., Metaverse land) or physical items that exist in the real world[7] (e.g., art)

[4]Per PSA definition. Please refer to Annex B for the full definition
[5]Per definition used in MAS Project Orchid Whitepaper
[6]Per Securities and Futures Act ("SFA") definition. Please refer to Annex B for the full definition
[7]Definition reference from 'Reply to Parliamentary Question on Regulation of NFT Activities'

ML/TF Risk Considerations

Relevance of ML/TF and Sanctions Risks

To assess whether a digital asset needs to be targeted for additional AML/CFT controls, FIs would need to consider whether 1) the digital asset is relevant from an ML/TF and Sanctions risk angle and if deemed relevant, 2) consider the extent of the digital assets' ML/TF and Sanctions risk.

1. Criteria FIs should consider when determining the digital asset relevance:

Criteria	Consideration
Can the digital asset be traded?	A digital asset that fulfills any 1 of the 4 criteria would be considered **relevant**, given it can be used to store or facilitate the movement of tainted proceeds
Can the digital asset be transferred?	
Can the digital asset be used for payment?	
Can the digital asset be used for investment purposes?	

2. Factors FIs should consider when determining the extent of the digital asset ML/TF and Sanctions risk:

Risk Factors	Higher Risk Scenarios
Governance model	• A digital asset not backed by Government or a consortium of regulated entities, hence not subjected to any regulations • A digital asset with governance model that is partially or fully decentralised and allows for anonymity
Ease of conversion into or from fiat currency	• A digital asset that can be easily converted to or from fiat currency, allowing for quick conversion into useable funds
Extent of public adoption	• Wide public adoption facilitating easier buying or selling of the digital asset and conversion between cryptocurrency and fiat currency, allowing for quick movement of funds

Focus of this Paper

The Working Group has assessed that cryptocurrencies currently pose the highest ML/TF and Sanctions risk. In view of this, **this paper focuses on discussing the management of cryptocurrency-related ML/TF and Sanctions risks.**

Digital Assets Type	Current Analysis of Risk Relevance
Cryptocurrencies (e.g., Bitcoin, Ether, USDT)	• Widely used, recognised, and wide-reach (wide public adoption) • High market capitalisation • Easily converted to fiat currencies

Risk Relevance of Other Types of Digital Assets

Digital Assets Type	Current Analysis of Risk Relevance
Transferrable gaming/streaming credits	• Less widely adopted • Lower ease of conversion or transfer of value relative to cryptocurrencies
Limited Purpose Digital Payment Tokens	• Less widely adopted; they are only used for payment in a closed-loop system[8] • Narrow group of captive users • Do not usually have any tangible value outside of that environment

Continues on next page

[8]*Closed loop as the digital asset can only be used for payment of goods and services provided by its issuer or any merchant specified by its issuer, or exchanged/transferred within the specific gaming/streaming platforms (i.e., do not leave these platforms)*

ML/TF Risk Considerations

Risk Relevance of Other Types of Digital Assets (Cont'd)

Digital Assets Type	Current Analysis of Risk Relevance
Central Bank Digital Currencies ("CBDCs")	• Issued by Central Banks - highly regulated source, and intermediated by government
Digital Capital Markets Products ("DCMPs") Tokens	• Typically issued by regulated FIs
Non-Fungible Tokens ("NFTs")	• Lower ease of conversion as NFTs typically need to be sold for cryptocurrency before being converted to fiat currency but note its potential use as store of value or means to transfer value. • Given that NFTs are typically sold for cryptocurrency first, and the cryptocurrency is then exchanged into fiat currency, the ML/TF and Sanctions risks of NFTs would be similar to the ML/TF risks identified for "cryptocurrencies" in page 6.

ML/TF Risk Considerations

Financial Crime Risks of Cryptocurrencies

These characteristics of cryptocurrencies makes them more vulnerable to abuse for criminal activity:

Anonymity: As cryptocurrencies can be traded anonymously, it is difficult for due diligence to be conducted on the identities of buyers/sellers and the sources of funds of the cryptocurrencies.

Cross-border: Cryptocurrencies can be traded across jurisdictions easily and rapidly, including jurisdictions with elevated risk for financial crime and Sanctions risks.

Lack of Identifiers: Due to the decentralised nature of cryptocurrencies, it is difficult to implement effective oversight on transactions as they may not always have verifiable on-chain information of wallet holders.

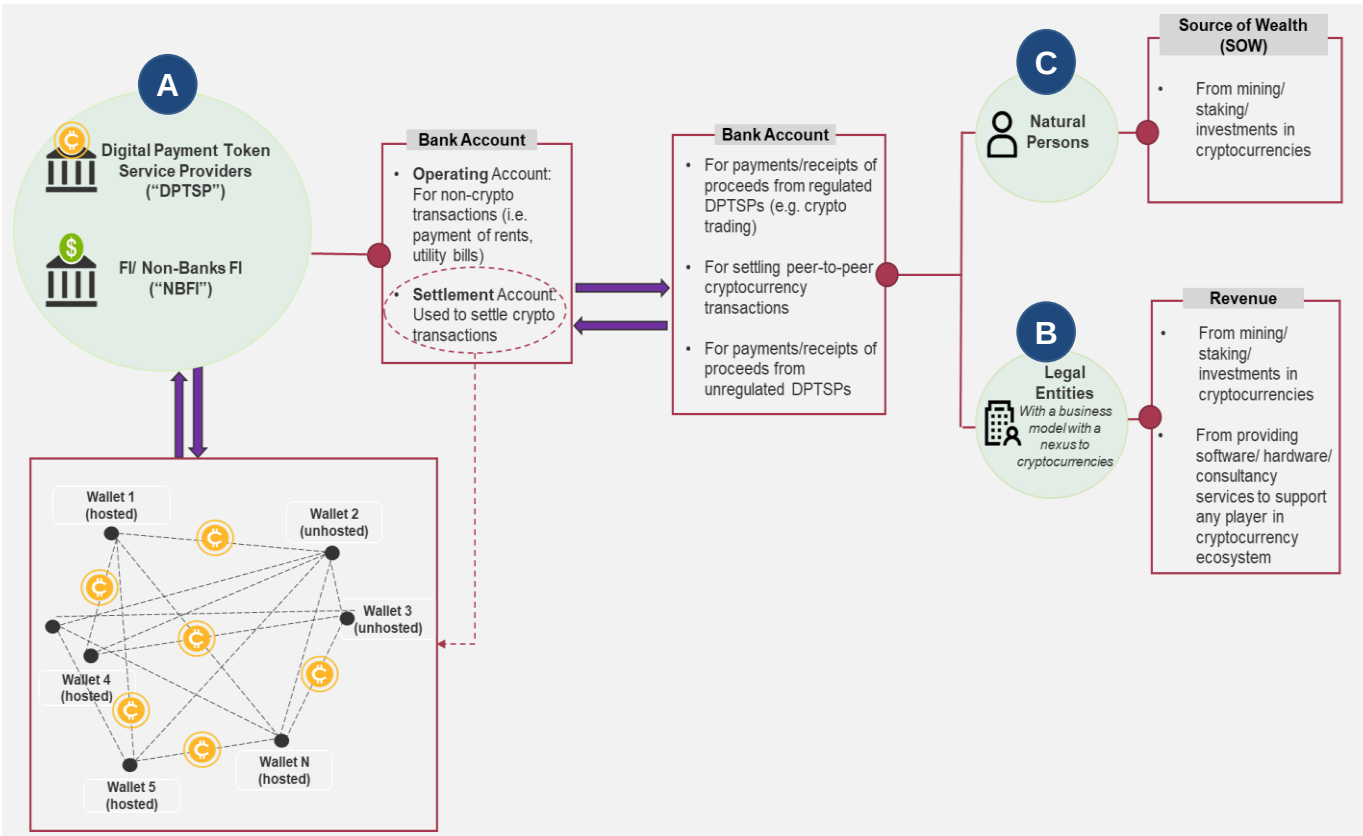
Wallet/Platform Security: If a wallet or platform is compromised and the cryptocurrency is stolen, it is difficult to retrieve the stolen cryptocurrency and prevent it from being laundered.

Types of Customer Nexus to Cryptocurrencies

While there may be other customers with nexus to cryptocurrencies, this best practice paper will cover three main types of customer nexus to cryptocurrencies.

A	**Digital Payment Token Service Providers ("DPTSPs") and FIs (including Non-Bank FIs ("NBFIs"))**
B	**Legal Entities with a business model that has nexus to cryptocurrencies**
C	**Natural Persons with source of wealth and/or funds related to cryptocurrencies**

The following diagram captures the point of, and flow of transactions where a bank account may be used to facilitate or receive cryptocurrency related proceeds.



Customer Nexus – Inherent Risks

Recommended Practices

FIs are encouraged to consider the additional risk factors, in conjunction with existing KYC risk factors.

Risk Category	Common Questions to Ask	Examples of Higher Risk Indicators
Customer Risk	• What is the regulatory status of the DPTSP? • How sophisticated is the DPTSP's AML/CFT program? • Does the DPTSP use anonymising techniques/privacy enhancing tools to obfuscate transaction or customer details? • What are the potential ML/TF and Sanctions risks associated with a DPTSP's connections and links to jurisdictions? • What is the extent and nature of the DPTSP's implementation of the travel rule? • Is Customer's source of wealth ("SOW") or revenue generated from mining/staking/ investments in cryptocurrencies?	• DPTSP's business operations and activities are not in-scope for licensing in the jurisdiction of operations • DPTSP is in a jurisdiction with weak or non-existent AML/CFT controls • Where cryptocurrency-to-fiat currency transactions occurs P2P and not through any regulated financial network[9] • Insufficient evidence to corroborate for SOW/revenue derived from cryptocurrency investments
Products and Services Risk	• Is Customer's bank account used to facilitate cryptocurrency transactions? • Are there any transactions with unregulated DPTSPs? • Are there any transactions with wallet addresses that are sanctioned or linked to illegal activity? • Is there exposure to DPTSPs that offers and/or accept privacy coins[10] with anonymity feature enabled? • Is there exposure to mixer/tumbler[11] services? • Are there transactions with/ associated with unhosted wallets? • Are there any P2P transactions?	• Insufficient evidence to corroborate for purported sale(s) and/or purchase(s) of the cryptocurrencies • Where applicable (e.g., through available tools during on-chain screening), Customer has exposure to transactions associated with DPTs / DPT wallet addresses on which anonymity-enhancing technologies (e.g., privacy wallets/coins, mixers and tumblers etc.) are applied
Geographical Risk	• Are there cross-border transactions with jurisdictions which may be subject to less robust AML/CFT obligations and oversight; or ban cryptocurrencies and its related activities? • Is the AML/CFT legislation in the jurisdiction under which the DPTSP is incorporated/licensed less robust? • Are there transactions with jurisdictions that have low regulatory enforcement or where there is no relation to where customer conducts business or lives? • Is the DPTSP incorporated in or operating out of a country that is subject to economic sanctions? • Is the DPTSP incorporated in a country that is known to setup offshore companies?	• Substantial cross-border transactions to jurisdictions with weak AML/CFT regimes[12] • Economic purpose of cryptocurrency related transactions could not be established

[9]Readers should also be wary of risks associated with centralised financial network
[10]Please refer to Annex B for the definition.
[11]Please refer to Annex B for the definition.
[12]FIs may consider jurisdictions with weak AML/CFT regime to comprise of countries for which FATF has called for countermeasure and jurisdictions determined by the FI to have inadequate AML/CFT measures.

Customer Nexus – Inherent Risks

Risk Appetite

FIs should identify, assess, and understand the ML/TF and Sanctions risks emerging from this space and should ensure that measures to prevent or mitigate ML/TF and Sanctions risks are commensurate with the risks identified.

It is recommended for FIs to set clearly defined client acceptance criteria for customers with nexus to cryptocurrencies to determine i) whether customer can be onboarded or whether to continue the banking relationship and ii) the appropriate level of due diligence to be applied on the customer.

FIs are encouraged to actively identify customers with nexus to cryptocurrencies for enhanced risk management measures where necessary.

The table below is an example of categorisation of client acceptance:

Risk Appetite Category	Client Acceptance
Within Risk Appetite[13]	*Relationship allowed subject to appropriate approvals. Customer due diligence ("CDD") controls*[14] *apply*
Limited Risk Appetite	*Relationship allowed but possibly subject to greater scrutiny and conditions, where necessary, approvals. Enhanced customer due diligence ("EDD") controls apply*
Prohibited	*No such relationship allowed*

[13] *Examples of lower ML/TF risk nexus are:*

- *A low-risk nature and scope of the account, product, or service (e.g. low value savings, accounts with limited value storage);*
- *A low-risk nature and scope of the payment channel or system (e.g. closed-loop systems, systems intended to facilitate micro-payments, government-to-person/person-to-government payments);*
- *The customer requests an exchange, and:*

i. the source of or destination for the money is the customer's own account with a bank in a jurisdiction assessed by the firm as low risk;
ii. the source of or destination for the crypto-asset is the customer's own wallet that has been whitelisted or otherwise determined as low-risk;
iii. the source of or destination for the crypto-asset relates to low-value payments for goods and services; and

- *The blockchain analysis results indicate a lower risk.*

[14] *CDD controls should address ML/TF and Sanctions risks.*

Onboarding and Ongoing Due Diligence

A. Digital Payment Token Service Providers

This section focuses on recommended due diligence measures for Digital Payment Token Service Providers ("DPTSPs"), FIs, and Non-Bank FIs ("NBFIs").

DPTSPs[15] are payment service providers[16] that provide any of the following services:
- a digital payment token service (i.e., deal in or facilitate exchange of DPT)
- a digital payment token transfer service (i.e., facilitate transmission of DPT)[17]
- a custodian wallet service[17]
- brokering of DPT[17]

FIs/NBFIs offer a range of **cryptocurrency activities, e.g.**:
1) Offering payment services to DPTSPs
2) Issuing financial products with cryptocurrency underlying (e.g., ETFs referencing basket of cryptocurrencies)

The level of incremental ML/TF and Sanctions risk could vary depending on the nature of the FI/NBFI's cryptocurrency-related activities. Where the FI/NBFI's activities are akin or closely linked to **the facilitation** of a DPTSP's cryptocurrency transactions, enhanced due diligence on the FI/NBFI may be necessary. In contrast, where FI/NBFI's exposure to cryptocurrency is due to structuring of investment products, incremental ML/TF and Sanctions risks may be limited.

Due Diligence Considerations

FIs are encouraged to consider the following factors when conducting due diligence for DPTSPs:

- Type of digital payment tokens being offered by DPTSP, including the listing criteria (e.g., ability for on-chain screening).
- Product or service anonymity and transferability
- Quality and status of regulation (i.e., robustness of the regulatory regime the DPTSP is subject to)
- Status of compliance to the Travel Rule[18]
- Strength of the DPTSP's financial crime risk governance, risk management framework, and controls
- Type of exchanges the DPTSP works with
- Type of custodial solution offered by DPTSP

FIs should consider the materiality of incremental risks arising from cryptocurrency nexus in assessing the appropriate level of due diligence. The table below outlines examples of due diligence measures the FI may perform (note: some may not be applicable to certain types of nexus), and where ML/TF and Sanctions risks are assessed to be higher, enhanced due diligence measures should be applied.

Onboarding	Periodic/Trigger Event Review
Obtain information on the DPTSP's profile regarding: • Types of products, including number and which cryptocurrencies are offered/supported. The listing criteria of cryptocurrencies offered including assessing if cryptocurrencies can be subject to on-chain screening. • Assessment of custodial solutions offered. Where the DPTSP transacts with unhosted wallets, understand the extent of transactions with unhosted wallets (e.g., expected monthly volumes and values)	Refresh information on the DPTSP's profile obtained during onboarding, with a view on: • Obtaining confirmation of updated regulatory status and licence to operate • Obtaining confirmation that the DPTSP's clients are from jurisdictions where the DPTSPs are licensed to operate • Review list of cryptocurrencies that the DPTSP supports to ensure that these cryptocurrencies remain within the FI's risk appetite (e.g., cryptocurrencies offered should be able to subject to on-chain screening)

[15] *Per definition in PSA.*
[16] *This includes banks offering DPT services.*
[17] *These DPT services are reflected in the Payment Services (Amendment) Act 2021.*
[18] *FATF Recommendation 16 requires DPTSPs to obtain, hold, and transmit required originator and beneficiary information, immediately and securely, when conducting digital asset transfers.*

Continues on next page

Onboarding and Ongoing Due Diligence

A. Digital Payment Token Service Providers

Onboarding	Periodic/Trigger event review

(Cont'd)
• Product or service anonymity and transferability e.g., lesser-known cryptocurrencies or privacy coins, associations with Darknets, mixers or tumblers, cryptocurrencies with higher velocity and volume, are perceived to be of higher risk
 	
• Quality and Status of Regulation[19]
  • Geographic risks (registered and operating locations) and whether regulated in those locations
  • Level of robustness of the operating location's legal and regulatory framework against financial crime
 	
• Compliance with Travel Rule:
  • Transparency: quality and completeness of information on the parties in transaction messages
  • Transactional Flow: process of fund transmission between the client and the FI, including any other parties involved (e.g., type of travel rule solution or bilateral arrangement with counterparty DPTSPs)
  • If DPTSP is unable to fully comply, assess the interim measures taken to mitigate the risks and action plan to fully comply with Travel Rule.
 	
• DPTSP's Exposure to High-Risk Entities:
  • Check for DPTSP's exposure to sanctions and other higher risk entities such as services relating to mixers/ tumblers etc., and privacy coins
 	
FIs should inform DPTSP clients that the concerned FI will not commence, continue the client relationship, or facilitate activity that is subject to the prohibitions set by the FI.
	(Cont'd)
	Review client's transactions to ensure they are in line with client's profile

Enhanced Due Diligence
For DPTSPs or where FI/NBFI's activities are akin or closely linked to **the facilitation of** cryptocurrency transactions, enhanced due diligence may be necessary: • Enhanced due diligence, including on-chain activities (e.g., DPTSPs had been dealing with adverse/sanctioned wallets, etc.) where necessary, should be undertaken by FIs which can also be leveraged on reputable third-party vendors • Site visits or walkthroughs of client's AML/CFT processes and controls (as applicable)[20] • DPTSP's senior management ML/TF and Sanctions risk awareness and endorsement on the importance of anti-financial crime culture and implementation of AML/CFT systems and controls to mitigate financial crime risks (e.g., client risk evaluation checklist) • Obtain senior management approval to ensure adequate management oversight of such clients with cryptocurrency exposure

[19]FIs should be mindful that having one licensed subsidiary does not necessarily mean that a DPTSP is of lower ML/TF and Sanctions risks if they have global operations (e.g., the DPTSP may take advantage of regulatory arbitrages, evident in the recent failures of DPTSPs).

[20]1. For Sanctions/risk management purposes, to review for example IP address monitoring and blocking capabilities, screening of geographic indicators, screening against sanctions list, etc.); 2. Understanding the measures DPTSPs take to mitigate the risks of dealing with unhosted wallets or with unregulated DPTSTPs/regulated DPTSPs that are not yet required to comply with travel rule

Onboarding and Ongoing Due Diligence

B. Legal Entities

This section focuses on recommended due diligence measures for legal entities with nexus to cryptocurrencies.

Legal entities may have a nexus to cryptocurrencies in the following scenarios[21]:

1. Usage of bank accounts for payments/receipts of proceeds from regulated and unregulated DPTSPs
2. Usage of bank accounts for settling P2P cryptocurrency transactions (in fiat currency)
3. Revenue is derived from mining, staking, and investments in cryptocurrencies

Due Diligence Considerations

FIs are encouraged to consider the following factors when conducting due diligence for legal entities:

- Transactions in line with nature of business (for legal entities under scenarios 1 and 2 above)
- Regulatory status and jurisdiction of client's DPTSP counterparties (for legal entities under scenario 1 above)
- The type of custodial solution being used by the legal entity (e.g., hosted or unhosted wallet)
- Nature of business
- The types of DPT that the legal entity is exposed to

FIs should consider the materiality of incremental risks arising from cryptocurrency nexus in assessing the appropriate level of due diligence. The table below outlines examples of due diligence measures the FI may perform (note: some may not be applicable to certain types of nexus), and where ML/TF and Sanctions risks are assessed to be higher, enhanced due diligence measures should be applied:

Onboarding	Periodic/Trigger Event Review

• Assess the nature of client's nexus to cryptocurrencies through requesting and documenting information about nature of customer's cryptocurrency exposure and the intended usage of account. This should include the client's nature of business, the types of DPT the client will be exposed to, and the type of custodial solution involved
 	
• Establish the SOW/Source of Funds ("SOF") or revenue obtained from cryptocurrency related activity, including through ownership of DPTSP
 	
• For merchant customers, FI should assess the regulatory status of the merchant's DPTSP counterparties if those DPTSPs contribute to a significant volume of customer's transactions
	• Refresh information on the client's profile obtained during onboarding, with a view on:
	  • For legal entities under scenario 2 above, the domicile of the counterparties and location of the FIs of the counterparties' accounts
	  • For merchant customers transacting with significant DPTSPs counterparties, obtaining the latest regulatory status of the merchant's DPTSP counterparties
	
	• Review the client's transactions to ensure they are in line with client's profile. This may include requesting corroborating documents for the concerned transactions.

Enhanced Due Diligence

For the legal entities assessed to be of higher risk, FIs should conduct or obtain one or several of the following as applicable to the type of nexus (where appropriate):

- Enhanced due diligence, including on-chain activities where necessary, should be undertaken by FIs; where necessary FIs can leverage reputable third-party vendors
- Obtain senior management approval to ensure adequate management oversight of such clients with cryptocurrency exposure

[21] *Entities that only provide technology or infrastructure solutions need not be subject to incremental Due Diligence measures.*

Onboarding and Ongoing Due Diligence

C. Natural Persons

This section focuses on recommended due diligence measures for natural persons.

Individuals may have a nexus to cryptocurrencies in the following scenarios:

1. SOW derived from mining, staking and investments in cryptocurrencies
2. Usage of bank accounts for settling P2P cryptocurrency transactions (in fiat currency)
3. Usage of bank accounts for payments/receipts of proceeds from regulated and unregulated DPTSPs

Due Diligence Considerations

FIs are encouraged to consider the following factors when conducting due diligence for natural persons:

- Type and nature of the cryptocurrency-holding and investment(s)
- The percentage of client's source of wealth which is derived from cryptocurrency-related activity
- Value and volume of cryptocurrency-related transactions
- Ability to corroborate sales/purchase of cryptocurrency transactions, if they contribute to a significant volume of customer's transactions
- The type of custodial solution being used by the individual (e.g., hosted or unhosted wallet)

FIs should consider the materiality of incremental risks arising from cryptocurrency nexus in assessing the appropriate level of due diligence. The table below outlines examples of due diligence measures the FI may perform (note: some may not be applicable to certain types of nexus), and where ML/TF and Sanctions risks are assessed to be higher, enhanced due diligence measures should be applied:

Onboarding	Periodic/Trigger Event Review

• Assess the nature of client's nexus to cryptocurrencies through requesting and documenting information about nature of customer's cryptocurrency exposure and the intended usage of account
 	
• Establish the client's SOW obtained from cryptocurrency related activity, including but not limited to the type and nature of cryptocurrency holding and investment(s). This may include requesting corroborating documents for purported cryptocurrency assets purchased from the DPTSP
	• Refresh information on the client's profile obtained during onboarding, with a view on:
	  • For natural persons under scenario 2 above, the domicile of the counterparties and location of the FIs of the counterparties' accounts
	  • Obtaining the latest regulatory status of the DPTSP counterparties that the natural persons deal with
	• Review the client's transactions to ensure they are in line with client's profile. This may include requesting corroboration documents for purported cryptocurrency related transactions.
	• Review client's SOW incremental changes and obtain corroboration where necessary

Enhanced Due Diligence

For the natural persons assessed to be of higher risk, FIs should conduct or obtain one or several of the following as applicable to the type of nexus (where appropriate):

- Enhanced due diligence, including on-chain activities where necessary, should be undertaken by FIs; where necessary FIs can leverage reputable third-party vendors
- Obtain senior management approval to ensure adequate management oversight of such clients with cryptocurrency exposure
- Where SOW is derived from ownership of DPTSP or ownership of cryptocurrencies, consider corroborating ownership and performing due diligence on the related DPTSP and assess the related DPTSP's risk profile.

Ongoing Monitoring

Fiat Currency Accounts

Purpose of Accounts

Bank accounts may be used for the following purposes by customers with cryptocurrency nexus:

1. Operating Account
- Used for supporting business operation needs such as payment to vendors and suppliers
- Not involved in facilitating underlying cryptocurrency transactions with clients or counterparties

2. Settlement Account (for DPTSPs)
- Used for settling fiat currency payments or transfers with clients or counterparties
- Involved in facilitating underlying cryptocurrency transactions with clients or counterparties
- Business operation involves crypto as a form of payment

3. Manage wealth generated from cryptocurrency-related business or investments
4. Manage funds generated from P2P transactions
5. Consolidate payments/receipts of proceeds from DPTSPs (regulated/unregulated)
6. Manage wealth/revenue from providing software/ hardware/consultancy services to support any player in cryptocurrency ecosystem

Ongoing Monitoring

Existing transaction monitoring controls and rules should continue to apply for fiat currency accounts. To address the cryptocurrency related ML/TF and Sanctions risks (e.g., presence of transactions involving unregulated and/or higher-risk DPTSPs), the table below outlines examples of incremental measures the FI may perform:

Ongoing Monitoring
• Monitor account activity to identify non-alignment with nature of business, purpose of account (e.g., operating account being used to facilitate settlement of cryptocurrency transactions)
• Screen cryptocurrency-related counterparty names to identify sanction hits and any adverse news
• Monitor for any changes in geographical risk profile (e.g., changes in location of operations and customer base)
• Where applicable, as part of banks' ongoing monitoring, identify transactions with a digital asset nexus using list-based monitoring/searches (e.g., search for specific DPTSP names or account number if available, relevant key words in payment messages)

Ongoing Monitoring

Fiat Currency Accounts

Investigations

In the event of an alert/event trigger on transactions with a digital asset nexus, the table below outlines examples of the additional queries the FI may raise during their investigation:

Suggested Queries

• For outflow of funds (e.g., cryptocurrencies investment/purchase) -
  • The nature, volume and value of the cryptocurrencies purchase/investment
  • The purpose of the cryptocurrencies purchase/investment
  • The beneficiary of the cryptocurrencies purchase/investment
  • If the DPTSP is not licensed/registered to offer the activity and/or is located in a country different from the client's residence country, the reason for using the DPTSP
 	
• For inflow of funds (e.g., sale of cryptocurrencies) -
  • The nature and volume of cryptocurrencies sold
  • The origin of the cryptocurrencies (e.g., obtained through mining) sold
  • Based on local regulation requirements (if applicable), the evidence of tax declaration/tax payment for the fiat currency transaction
  • Date of initial purchase/investment/acquisition
 	
• For both inflow/outflow of funds -
  • Wallet address used for the underlying transaction to be subjected to further checks on the blockchain using lists and patterns

Ongoing Monitoring

Cryptocurrency Accounts

Purpose of Accounts

FIs may interact with cryptocurrencies through:
1. Transfer of cryptocurrencies
2. Exchange of cryptocurrency to fiat currency and vice versa
3. Offering clients a custodian account to hold cryptocurrency on behalf of their customers

Ongoing Monitoring

FIs are encouraged to consider the following factors when conducting cryptocurrency transaction monitoring

- Presence of transactions involving unregulated and/or higher-risk DPTSPs
- Presence of transactions involving unhosted wallets
- Presence of transactions involving privacy coins, other forms of anonymising techniques
- Presence of transactions involving on-chain hits, i.e., sanctions

Transaction monitoring for cryptocurrency accounts and transactions typically revolve around the use of on-chain screening[22] to facilitate reviews based on the source and flow of DPTs between wallets on the blockchain.

On-chain screening	By configuring the monitoring rules based on linkages (and/or exposure) to certain labelled clusters and monitoring based on number of hops (i.e., how far away the labelled cluster of interest is from the current wallet / transaction that is being screened), this allows for identification of potential linkages to wallets related to other high-risk clusters and/or associated with higher ML/TF and Sanctions risks

To address the cryptocurrency related ML/TF and Sanctions risks, the table below outlines examples of the incremental measures the FI may perform:

Transaction Monitoring
• On-chain screening for all transfers based on transaction hash and/or originating/destination wallet ID For **DPTSP customers:** • Review of the DPTSP's cryptocurrency transactions facilitated by the bank to identify material changes/anomalies in flow of transactions • Utilise blockchain screening tools to review on-chain activity of DPTSP • Screen new and existing wallet addresses owned or controlled by the DPTSP against sanctions list and wallets designated by authorities on a timely basis • Assess if the observed transactions are in line with known client profile • Verification of customer's ownership/control over the hosted and unhosted wallet For **customers that are legal entities and natural persons:** • Review of the cryptocurrency transactions facilitated by the bank to identify material changes/ anomalies in flow of transactions • Verification of customer's ownership/control over the hosted and unhosted wallet • Risk assessment of wallet addresses to identify nexus to high-risk clusters (including but not limited to sanctions nexus, nexus to mixers, tumblers, etc.) • Assess if the observed transactions are in line with known client profile

[22] *Refer to Annex A for more details on on-chain screening*

Case Studies: Enhanced Due Diligence for DPTSP

Case Study 1 – Onboarding

Background

A prominent DPTSP approached a bank requesting a settlement account to receive and hold customer funds (of the DPTSP). The bank had established a review and governance process for new DPTSP relationships, which included reviews by a client selection committee, a reputational risk review, and an enhanced due diligence ("EDD") process tailored for DPTSP relationships.

During the EDD review, the bank identified several jurisdictions in which the DPTSP appeared to be offering customer accounts without a licence. The bank utilised blockchain analytics to identify the DPTSP's top on-chain counterparties and identified an elevated rate of high-risk wallet addresses and exchanges. During the review, the bank also observed that the DPTSP was hesitant to provide certain details about its ownership and business operations, or to provide a legal opinion on whether it is allowed to offer customer accounts without a licence in certain jurisdictions.

Ultimately, the bank declined to onboard the DPTSP due to the red flags identified during the EDD.

Red Flags

- DPTSP offered customer accounts in jurisdictions prior to obtaining a licence, and the DPTSP refused to provide a legal opinion regarding its lack of licence in those jurisdictions
- On-chain analytics identified that some of the DPTSP's top counterparties were high-risk wallet addresses and exchanges
- DPTSP was not fully transparent regarding details about its ownership and business operations

Best Practices

1. Verify that the DPTSP is licensed in jurisdictions where it offers customer accounts:

a) Request DPTSP to provide proof of all current and pending licences

b) Review DPTSP's website and other public sources to identify if DPTSP restricts customer accounts in jurisdictions where it does not hold a licence

c) If DPTSP appears to offer customer accounts in jurisdictions where it does not hold a licence, request DPTSP to provide an external legal opinion on whether it is allowed to offer customer accounts in such jurisdictions

2. Utilise on-chain screening where necessary (e.g., suspicions are raised, DPTSP exhibits high-risk characteristics) to assess the on-chain counterparty risk of the DPTSP

a) Engage on-chain screening companies that provide a due diligence product that identifies high-risk counterparties for DPTSPs. For example, to identify if a DPTSP has a higher counterparty risk exposure than comparable DPTSPs

b) Higher counterparty risk exposure may indicate that the DPTSP has a weaker on-chain screening program, or a higher risk appetite

3. Utilise public sources, including investigative journalism and regulatory investigations, to identify red flags in a DPTSP's ownership or business practices.

Case Studies: SOW Corroboration for Natural Person

Case Study 2 – Onboarding

Background

The KYC team within a bank received an account opening request involving a Personal Investment Company, G Pte Ltd ("GPL"), whose ultimate beneficial owner i.e., Prospect C, is a non-resident customer and a semi-retired professional.

Whilst the external appointments and business ownerships of Prospect C were duly corroborated with an external due diligence report, a substantial part of the incumbent's wealth is derived from cryptocurrency holdings.

Although the traded prices witnessed upwards price-surge during Year 2021, Prospect C did not actively sell his cryptocurrencies and declared:

a) That he invested in different cryptocurrencies since 2013 and converted all holdings into Ethereum ("ETH") and kept them in a certain digital wallet in 2016.
b) That he maintained a trading account, in GPL's name, with a licensed virtual asset service provider i.e., ABC Exchange, domiciled in an Asian country

During on-boarding, it was also noted Prospect C's home country is in the process of finalising the applicable tax-treatment of digital assets.

Red Flags

- Substantial percentage of UBO's SOW is derived from cryptocurrency holdings
- Tax evasion risk

Best Practices

1. Documents should be obtained to evidence the cryptocurrency SOW and the trading account[23]:

a) A screenshot of the digital wallet to evidence the total token size, if available
b) Statement of account from ABC Exchange, if available

2. Given the substantial SOW from cryptocurrencies, FI should consider requesting the prospect to physically log-on his wallet in a video-conference session for the FI to corroborate the prospect's cryptocurrency holdings

3. FI should independently corroborate SOW from Prospect's cryptocurrency holdings against the ETH price-per-day chart[23]

4. After onboarding, the FI should request the prospect to submit:

a) The latest Notice of Tax Assessment with the relevant disclosure(s) once the tax rules become effective
b) Where source of funds are from the sale of cryptocurrencies through ABC Exchange, evidence of sales transaction to be provided on as-and-when basis

5. FIs should further assess the behaviour of the client which could be indicative of a tax offence warranting an STR filing

[23]*For early cryptocurrency adopters, it might be based on circumstantial documentations for plausibility assessment (i.e., bought cryptocurrency in 2011 and onboarded by the FI in 2021, the customer might not be able to surface much documentation)*

Case Studies: SOW Corroboration for Natural Person

Case Study 3 – Event Trigger Review

Background

Customer Y, a wealth management client, was engaged in technology-related businesses. Post on-boarding, certain large transactions were triggered by the bank's surveillance system. Transactions involving two local companies, K Pte Ltd ("KPL") and R Pte Ltd ("RPL") caught the Bank's attention. The bank requested additional information and supporting document from the customer and ascertained that:

KPL-related transactions:
KPL's principal activity involved the wholesale trade of a variety of goods without a dominant product; information technology consultancy (except cybersecurity) was identified as a secondary activity. Customer Y engaged KPL to perform tests of certain trading bots and the execution of trading algorithms on major digital currency exchange platforms with an invested amount of USD 5 million. KPL was responsible for monitoring and ongoing sales; the observed inflows from KPL were the customer's purported trading gains.

RPL-related transactions:
RPL's registered activities were providing professional business and management consultancy services. Customer Y engaged RPL to purchase circa 28 billion BitTorrent ("BTT") Tokens at an agreed price of USD 5 million, which was to be paid into the Ethereum ("ETH") wallet of RPL. The observed inflows from RPL were represented as the customer's trading gains arising from the sale of BTT tokens as well.

Customer provided contracts with KPL and RPL and the below were noted during the review:

Contract with KPL:
a) It was unclear as to what algorithms and/or trading bot(s) was/were applied by KPL; and
b) The purported trading gains could not be corroborated

Contract with RPL:
a) It was unclear as to whether RPL had acted as an intermediary for the sale or if it was the actual seller of the BTT tokens
b) The BTT tokens were not delivered by RPL on "delivery versus payment" basis, but over a period of 9 months. Additionally, the sale of the BTT tokens was at the discretion of RPL and the proceeds of the liquidation would be held in RPL's custody. The arrangement appeared to be in RPL's favor and counter-intuitive without any known safeguards to prevent misappropriation
c) The purported trading gains could not be corroborated

It was further noted that KPL and RPL were newly-incorporated i.e., less than a year at that point of time.

Red Flags

- Unable to ascertain reason as to why Customer Y would risk investing USD 5 million each into a newly established company without credentials and/or known market reputation. Furthermore, there were no known safeguards as to how the interests of Customer Y would be adequately protected
- Documentation was insufficient to corroborate trading gains

Best Practices

1. Obtain supporting document(s) to corroborate the transactions

2. The FI should analyse the contracts to determine whether the transactional purpose (including the assessment of plausibility), is in line with customer's explanation

Case Studies: SOW Corroboration for Natural Person

Case Study 4 – Event Trigger Review

Background

Customer Y, a customer of the affluent segment, is employed as a consultant in a company dealing in the development of software and applications (except games and cybersecurity). The account was generally inactive except for a few large ticket transactions, which triggered the Bank's transaction surveillance system. Notwithstanding that the remitter was a regulated cryptocurrency trading firm, the Bank requested Customer Y to submit relevant supporting artefact(s) to evidence his purported crypto-asset holding(s), as this asset-class had not been profiled in the customer's assets, SOW and SOF during the on-boarding. The Bank was prepared to exit customer-relationship if the (a) transaction could not be duly validated and the (b) SOW could not be satisfactorily re-established.

The customer has been cooperative and provided relevant documents during the Bank's request for information.

Red Flags

- Transactions not in line with customer's profile
- Customer's cryptocurrency investment holdings not corroborated based on existing SOW established

Best Practices

1. Obtain documentary proof to evidence purported crypto-asset holding(s)

Examples of Documentary Proof

The following illustrative artefacts (non-exhaustive), may be applied to support the crypto-investment (if available) -

- Screenshots of purchase and withdrawal confirmations displaying the (a) Account ID / Name and (b) Transaction Details (Note: where available, the FI validates the screenshot(s) against publicly available source(s). This may facilitate the assessment if the screenshot(s) is/are bona fide, prima facie);
- Confirmation emails/receipts, which provide proof of purchases or withdrawals;
- Screenshot of the exchange account details, which should include the Name, Name of the Platform; and
- Statements of transactional history.

2. FI should update the customer's SOW journey in view of the change in customer's profile.

3. FI should establish a clear red line beyond which the customer relationship should be exited.

Case Studies: Travel Rule Compliance with Hosted & Unhosted Wallets

Case Study 5 – Ongoing Monitoring

Background

Customer Z, a retail customer, declared during on-boarding that he actively traded in cryptocurrencies through a Singapore-domiciled DPTSP where he maintained a hosted wallet with the DPTSP. Separately, he also maintained an unhosted wallet. Below is a snapshot of the KYC controls the DPTSP had in place.

	During Onboarding	During Transfers
Hosted Wallet	• KYC information obtained and KYC checks in place • Travel rule implemented through integration with a travel rule solution provider	• Travel rule implemented
Unhosted Wallet	• KYC information obtained and KYC checks in place • Proof of control/ownership required (Satoshi Test[24] implemented / evidence of customer login to wallet by officials of FI)	• Proof of control/ownership required (Satoshi Test implemented)

Examples of Due Diligence Measures to be Put in Place

While travel rule is only applicable for hosted wallets for regulated entities, incremental due diligence may be required for unhosted wallets.

Examples of controls that FIs can adopt include:

1. Identifying transfers where DPTSP counterparty is not able to share relevant details and subject to exceptional processes, cryptocurrency credit should only be provided to customer after the details are obtained.
2. Considering filing of Suspicious Transaction Reports or closure of relationship if required
3. Ensuring that details received or to be sent as part of travel rule is screened before the cryptocurrency credit is provided to the account or cryptocurrency transfer out is initiated
4. Evaluating appropriate due diligence when selecting travel rule solution provider by considering cyber and information security standards, as well as data privacy.

Due to differences in jurisdictions' thresholds and maturity of implementation of travel rule solution, FIs should work with Customer and DPTSP counterparty where required to ensure that information exchange is done in a safe and secure manner.

For transfers from unhosted wallets, FIs may evaluate controls which may include:

a) Identifying originator and beneficiary for transfers and subject them to screening.
b) ID/IV of originator/beneficiary in case of third-party transfers (change in beneficial ownership)
c) Proof of customer's ownership/control of the wallet

The following scenarios necessitate closer attention or additional due diligence as it may lead to non-compliance of travel rule related regulations:

a) No process for exchange of information for transfers from DPTSP (irrespective of regulatory status)
b) Challenges around interoperability of travel rule solutions if FI and DPTSP counterparty use different service providers
c) Details obtained are not subject to screening
d) Absence of checks (Satoshi / evidence of customer login etc.) for transfers from unhosted wallets

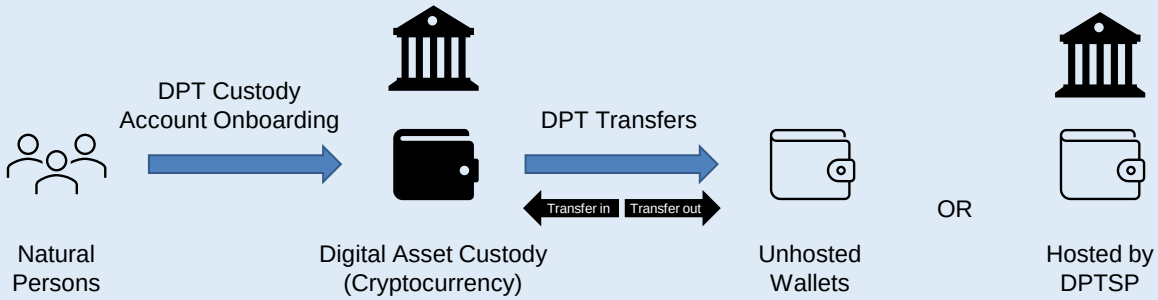
[24]Satoshi Test is a method to verify ownership / control of unhosted wallets by requiring the owner to send a small amount of cryptocurrency to the DPTSP within a specific time period. Some DPTSPs are assessing adoption of wallet signature checks as an alternate for Satoshi test – FIs to evaluate solutions best fit based on business needs and risk appetite.

Case Studies:

Case Study 6 – Holistic Due Diligence

Background

The FI intends to onboard a natural person for the provision of Cryptocurrency Custodial Services. The customer would be transferring his holdings from both his hosted and unhosted wallets to the FI.



Below are some of the due diligence measures the FI has in place.

	Customer FI custody account	Unhosted wallets	Hosted wallets by DPTSP
During On-boarding	• Customer selection i.e., accredited investors, existing customers, customers with account-based relationship etc • Incremental due diligence (for the cryptocurrency risks) • SOW corroboration for significant cryptocurrency investments.	• Unhosted or private wallet due diligence. This may include utilising on-chain screening through on-chain activity checks and proof of control or ownership	• Additional checks if DPTSP is unregulated/higher risk. Evaluate leveraging on-chain screening tools to review on chain activity of the DPTSP • Pre-approved list of DPTSP after conducting due diligence, including review of on-chain activity
Ongoing Monitoring	• Monitor activity in custody account of client (for alignment of transactions with client profile etc.) • All relevant checks to be completed before credit to customer • On-chain screening at time of transaction	• Identification and screening of originator or beneficiary • Pre-screening of wallets prior to transaction (on-chain as well as originator or beneficiary checks) and safelist such wallets	• Exchange originator or beneficiary details (Travel Rule), and such details to be screened

Case Studies:

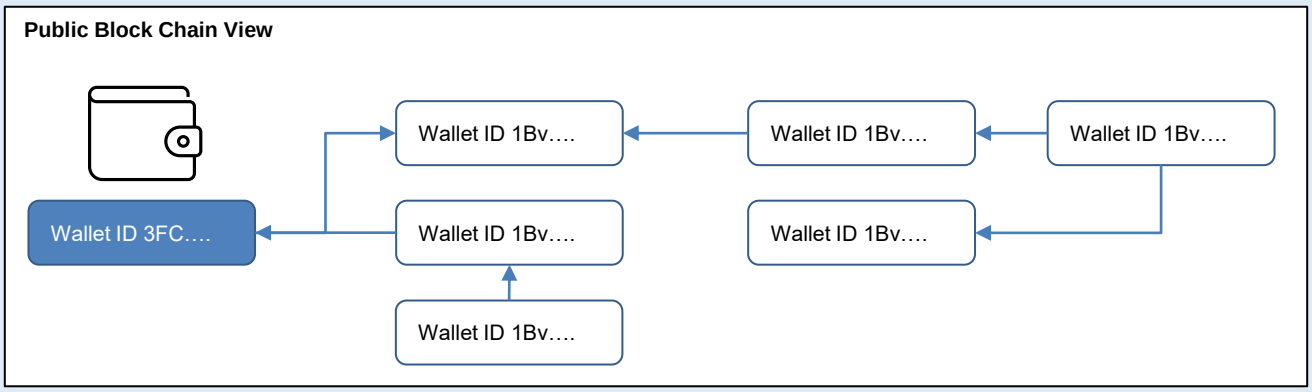
Case Study 7 – On-Chain Screening Assessment

Background

Use of a Blockchain Analytics Tool to facilitate on-chain screening

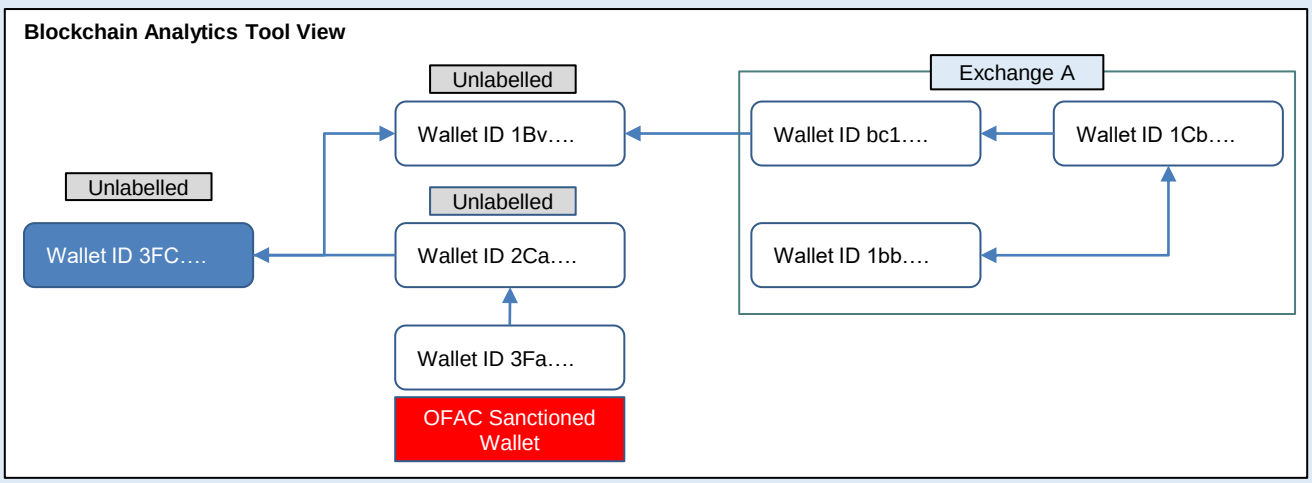
This case study illustrates how available Blockchain Analytics tools can visualise the flows to a customer wallet.

Customer A intends to transfer 10 Bitcoin (“BTC”) from his wallet (unhosted Wallet ID in Blue Box) to the FI. Based on the public blockchain, the below flows were identified between different wallets.



To manage the risk from this inflow, the FI screened the wallet using a Blockchain analytics Tool (“Tool”) with a rule setup to identify any nexus to Sanctioned entities/clusters – both direct and indirect.

A direct sanction nexus would mean direct flows from the cluster (one hop); an indirect sanction would indicate that there may be indirect flows (multiple hops).



The Tool based on proprietary ML/AI models was able to link some of these wallets to real world entities. It was able to identify that 3 wallets including the Wallet of customer are unlabelled (this could be because they may be unhosted and/or there is not enough evidence available for the Tool to label them). There are 3 wallets to the right above, which as per the Tool, are controlled by an Exchange (Exchange A); hence the Tool labels these wallets as Exchange A and clustered them together with the category as Exchange. There was another wallet (bottom-left of the above diagram) which belonged to the list of wallets sanctioned by OFAC; which was labelled as OFAC Sanctioned Wallet and would be added to a cluster which may contain such sanctioned wallets.

Continues on next page

Case Studies:

Case Study 7 – On-Chain Screening Assessment

A blockchain analytics tool is able to screen customers' wallet and:

1. Generate hits for rules that the FI configured e.g., the wallet had indirect interactions with sanctioned entities, as it is 2 hops away from the customer's wallet
2. Identify the flows from other clusters e.g., the wallet also had flows from Exchange A

Based on the above, the appropriate level of due diligence may be conducted.

Note: This is a very simple representation of the interactions/flows between wallets for ease of understanding. Depending on the business model, client base, cryptocurrency supported, and counterparties, there could be more complex flows. Hence, such tools could be leveraged by FIs after considering their efficiency and effectiveness.

Best Practices

Blockchain analytics tool should be considered as one of the many controls to strengthen the overall holistic due diligence and surveillance capabilities and not as a standalone control.

- FIs may leverage on the capabilities of blockchain analytics tools to monitor the on-chain activity as indicated above
- A risk-based approach that considers a bank's business model and focuses on effectiveness is key for successful implementation of this control
- It is important to integrate results/inputs from such on-chain screening to the existing monitoring methodologies to aid holistic surveillance
- While currently in most tools the effectiveness is dependent on their strength to label/cluster wallets; there are tools which are enhancing capabilities to identify certain out-of-pattern activities based on activities in the wallets (also known as behavioural indicators, behavioural rules, behavioural signatures etc.), cross-chain and multi-asset screening etc. FIs may consider such capabilities after evaluating their effectiveness
- FIs should assess the appropriateness of the thresholds and cluster identification methods used by the third-party providers

Annex A – On-Chain Screening

Capabilities of On-Chain Screening Technologies

The nature of blockchain provides opportunity to monitor the flow of DPTs between the wallets on the blockchain. Blockchain analytics tools based on their proprietary methodologies (which includes data analytics, application of ML/AI models) can link wallets on blockchains to real-world entities. A prerequisite for this is that the chains should allow access - should not be private blockchains or chains that promote privacy. Such blockchain analytics tools provide insights into the on-chain activity, thereby providing an opportunity for FIs to integrate the same into their overall risk management framework.

FIs may consider using insights from such tools to facilitate holistic risk management across off-chain and on-chain activity pertaining to their clients.

Some of the capabilities that could be leveraged are listed below for reference (Please note: The below is based on capabilities observed in various tools and some tools may have more advanced capabilities than others; FIs may evaluate specific capabilities provided by the tools as part of their evaluation).

	Feature	Capabilities
	**Cryptocurrency Wallet-Screening**	• Identify source and destination of DPT flows through the wallet • Identify linkage to any specific clusters of interest (e.g., sanctions nexus) • Identify ownership of wallet • Identify details related to on-chain activity in the wallet, such as wallet balance and transfer details • Provide risk scores at wallet level
	**Transaction Screening (DPT Transfers)**	• Identify source or destination of the transaction depending on whether it is a deposit or withdrawal request • Identify linkage to any specific clusters of interest to the transaction which is subject to screening (e.g., sanctions) • Enable configuration of risk rules at transaction level and any hits to the rules would be highlighted for appropriate review
	**Entity Due Diligence**	• Offer detailed insights into activities of entities (especially DPTSPs), through reports or features within the tool • Provide details of on-chain activity and off-chain information (may include regulatory status, location, details of group entities, adverse news) • Provide risk scores for entities
	**Other Capabilities**	• Provide modules to facilitate detailed investigations which would provide graphical representation of flows and further details • Provide capability to identify behavioral patterns based on the on-chain activity related to the wallet being screened • Develop capabilities to provide cross-chain and multi-asset tracing

Limitations:

- Dependency on strength of clustering/ labelling methodology used by the tools
- In most cases, tracing stops at labelled entities
- Given the nature of blockchain, it is quite easy to create multiple hops within a short period of time, hence this has to be considered while assessing monitoring approach
- Lack of specific identifiers (while the tool can provide indication of the cluster name especially for entities, specific identifiers like name, mobile number, email ID, national ID etc are not available)

Annex B – Definitions

Below are the definitions for the terms used across this paper:

Term	Definition
Digital payment tokens ("DPTs")	Per PSA, any digital representation of value (other than an excluded digital representation of value) that — a) is expressed as a unit; b) is not denominated in any currency, and is not pegged by its issuer to any currency; c) is, or is intended to be, a medium of exchange accepted by the public, or a section of the public, as payment for goods or services or for the discharge of a debt; d) can be transferred, stored or traded electronically; and e) satisfies such other characteristics as the Authority may prescribe.
Limited purpose digital payment token	Per PSA, any non-monetary customer loyalty or reward point, any in game asset, or any similar digital representation of value that — a) cannot be returned to its issuer, transferred or sold in exchange for money; and b) may only be used — i. in the case of a non-monetary customer loyalty or reward point — for the payment or part payment of, or in exchange for, goods or services, or both, provided by its issuer or any merchant specified by its issuer; or ii. in the case of an in-game asset — for the payment of, or in exchange for, virtual objects or virtual services within an online game, or any similar thing within, that is part of, or in relation to, an online game.
Fiat currency	A type of currency that is declared legal tender by a government but has no intrinsic or fixed value and is not backed by any tangible asset, such as gold or silver.
Capital markets products	Per SFA, any securities, units in a collective investment scheme, derivatives contracts, spot foreign exchange contracts for the purposes of leveraged foreign exchange trading, and such other products as the Authority may prescribe as capital markets products.
Mixer / tumbler	A service that mixes different streams of potentially identifiable cryptocurrency. This lends to the anonymity of transactions, as it makes it harder to trace.
Privacy coin	A type of cryptocurrency that uses technologies to make it difficult to link an individual to a transaction by providing anonymity to parties involved and confidentiality of details of the transaction like the amount.
Peer-to-Peer ("P2P") transactions	DPT transfers conducted without the use or involvement of a DPTSP or other obliged entity (e.g., DPT transfers between two unhosted wallets whose users are acting on their own behalf).

Annex C - Working Group Members and Other Contributors

Bank	Representative
OCBC	Loretta Yuen (Co-chair)
OCBC	Fairlen Ooi
OCBC	Tay Jun Yuan
SCB	Grace Ho (Co-chair)
SCB	Faith Tan
HSBC	Kwan Lai Heng
HSBC	Ben Chua
JP Morgan	Santanu Biswas
DBS	Nicolas Soh
DBS	Ramesh Krishnamoorthy
UOB	Yu Beng Soon
UOB	Lim Dewei
UOB	Chua Chek Ping
UOB	Nikhil Chogle
Citibank	Dylan Lee
Citibank	Dane Shelly
Maybank	Chen Jee Meng

ACIP Secretariat Representatives
Commercial Affairs Department
Monetary Authority of Singapore

Professional Services	Representative
Ernst & Young	Radish Singh
Ernst & Young	Lim Siew Lee
Ernst & Young	Patrick Hoehn
Ernst & Young	Charmaine Chong

Industry Associations
Association of Banks in Singapore (“ABS”)
Association of Cryptocurrency and Blockchain Enterprises and Start-Ups Singapore (“ACCESS”)