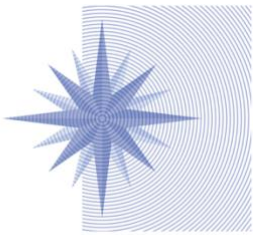


Banco Santander
Bank of America
Barclays
Citigroup
Deutsche Bank
Goldman Sachs
HSBC
JPMorgan Chase
MUFG Bank
Société Générale
Standard Chartered Bank
UBS

the Wolfsberg Group

The Wolfsberg Group Frequently Asked Questions (FAQs) on Defining Digital Assets

Introduction

Financial Institutions (FIs) are increasingly engaging directly and indirectly in the digital assets market.[1] In parallel, other electronic money technologies continue to evolve to support real-time or near real-time payments at a scale that could foreseeably compete with existing fiat currencies. Innovations in digital assets present new and emerging financial crime risks. While many countries are evolving their Money Laundering and Terrorist Financing (ML/TF) risk frameworks, and in spite of the Financial Action Task Force (FATF) drive for consistency of approach via the Recommendations, there remains a significant amount of inconsistency in terms of the implementation of the requirements. Many jurisdictions are still identifying basic foundational elements, such as assigning prudential regulators responsible for supervision and defining market participants to come under any appropriate supervisory regime.

In order to aid FIs with assessing the risks generated by the emergence of digital assets for ML/TF purposes, the Wolfsberg Group (the Group) is proposing definitions in these Frequently Asked Questions (FAQs) with the understanding that the continued evolution of these technologies will warrant periodic review of these terms.[2] The definitions can be used by FIs, policymakers, supervisors and regulators to understand the characteristics of the assets, the ML/TF and operational risks that they generate, including the impact on the financial system; serve as an input to FIs developing policies and appropriate controls; as well as act as a resource for supervisors and regulators. Certain terms and definitions in this paper have been created by the Group to aid understanding of this space and they may differ from those used in some jurisdictions. The Group intends to supplement these FAQs in future with guidance on the risks and associated controls for digital assets in line with the concepts developed here.

[1] *See* OECD, Institutionalisation of crypto-assets and DeFi-TradFi interconnectedness, p.14 (May 2022).
[2] All information is current at the time of publication.

Table of Contents

I. Defining Digital Assets

Q1. What is a Digital Asset?

A **digital asset** is a cryptographically secured digital representation of value or rights and/or cryptographically secured token, recorded in digital form, that often relies upon the use of a form of distributed ledger technology (DLT) or cryptography and which can be transferred, traded or exchanged, and can be used for payment or investment purposes.

Digital assets include a variety of products including for example virtual assets, virtual currencies, non-fungible tokens (NFTs) of value, payment tokens representing value, and digital securities.[3] Virtual assets and virtual currency are sub-categories of digital assets. Virtual currency is also referred to as cryptocurrency or convertible virtual currency.

Q2. What falls within the scope of a Digital Asset within these FAQs?

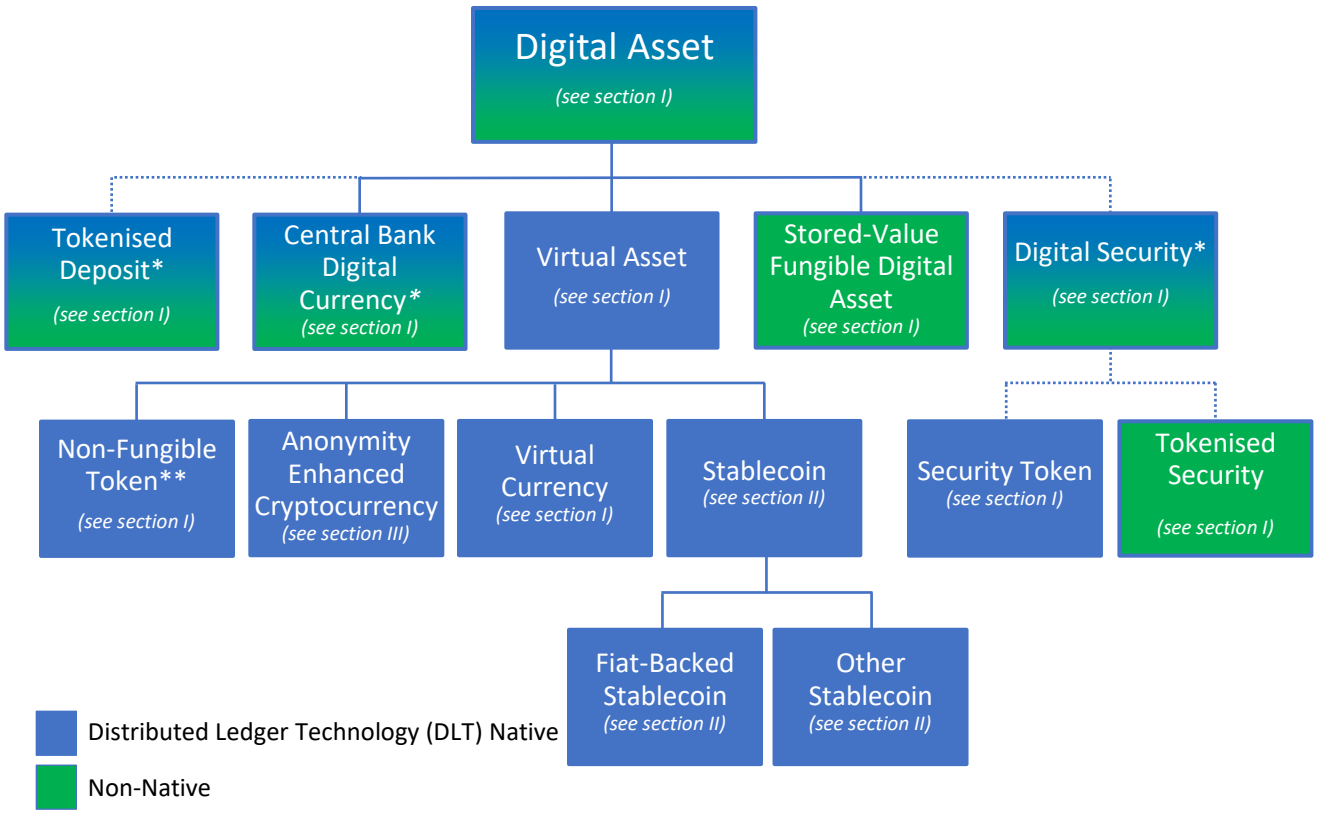
These FAQs are intended to define digital assets. Digital assets typically include virtual assets (such as stablecoins and certain non-fungible tokens of value), tokenised deposits, central bank digital currencies (CBDCs), stored-value fungible digital assets (which the Group defines later in this Section), and digital securities.

Excluded from above are other forms of electronic money (including prepaid cards, magnetically stored instruments of value and similar stored-value bearer instruments) and other tokenised instruments such as governance tokens, for as long as these exclusions are not interpreted as falling into any of the above aforementioned categories. At the time of this writing, tokenised deposits and digital securities are also excluded from these FAQs unless otherwise specified.

Figure 1 below depicts a high-level hierarchy of the relationship between virtual assets, CBDCs, and other underlying forms of digital assets.

[3] Digital securities are outside the scope of these FAQs unless otherwise noted.

Figure 1: Hierarchy of Digital Assets



*CBDC, tokenised deposit and digital security may include both native (i.e. primary record exists on DLT) and non-native (i.e. primary record exists off-chain) form. Tokenised deposits and digital securities are outside the scope of this document unless otherwise specified.

**Non-fungible tokens "of value" as detailed further in section I.

Q3. How do Digital Securities relate to Digital Assets?

For the purposes of these FAQs, a **digital security** is defined as a subcategory of digital asset and the Group recognises that digital securities in many jurisdictions are subject to existing securities regulation pertaining to the underlying asset. The two most common forms of digital securities are tokenised securities and security tokens.

Tokenised securities arise when issuing a digital representation of an underlying security instrument, such as tokenisation of an exchange traded fund (ETF) or bond. Tokenised securities reference the underlying security or asset through a token, sometimes with the intended purpose of increased transferability through blockchain, but local laws may or may not prescribe rights with respect to the underlying security asset and form of custody depending on the jurisdiction.[4]

[4] Based upon publicly available information, an example of a tokenised security is the UBS AG "3-year CHF senior unsecured" dual bond tradeable on the blockchain through SIX Digital Exchange and conventionally through SIX Swiss Exchange (SIX SIS).

A native **security token** is issued and custodied on a distributed ledger (e.g. blockchain) and meets the legal definition of security or financial instrument under local securities law.[5]

There are other forms of digital securities including where other DLT-based instruments may be interpreted as digital securities. Digital securities may present inherent ML/TF risks unique from other digital assets, including where local regulatory requirements for custody of digital securities vary. The scope of these FAQs excludes digital securities unless otherwise noted.

Q4. What is a Virtual Asset and how does this subcategory of Digital Asset relate to the Financial Action Task Force (FATF) definition of Virtual Assets?

A **virtual asset** is a type of digital asset that can include a variety of products, such as privately issued stablecoins and virtual currency.

The Group supports the FATF's definition of virtual asset in its Updated Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers. Published in October 2021, the guidance states that a virtual asset is "a digital representation of value that can be digitally traded or transferred and used for payment or investment purposes".[6] However, the Group recommends that the term "digital assets" be used to refer to both central bank and privately issued virtual assets, which is broader than the FATF's definition of virtual assets.

This proposed definition of digital asset also differs from the view taken by other organisations including the Basel Committee on Banking Supervision that digital assets exclude digital representations of fiat currencies.[7] The decision to include CBDCs is a deliberate choice by the Group to keep pace with the increasing adoption and inherent ML/TF risks of electronic funds, including those which may be issued by jurisdictions presenting heightened ML/TF risk. CBDCs present further ML/TF risks if designed to present cash-like anonymity. In the view of the Group, a CBDC is still a digital asset, regardless of who issues it.

Q5. What is a Central Bank Digital Currency?

A CBDC is a digital asset, or a digital form of money used for payment activity, issued by a central bank, denominated in the national unit of account for wholesale or retail purposes and representing a direct liability of the issuing central bank.

CBDCs are distinct from virtual currencies and stablecoins as they are legal tender and backed by a central bank or governmental authority. CBDCs may or may not be designed for offline payment usage with cash-like features.[8] Furthermore, CBDCs may or may not use DLT.

---

[5] Based upon publicly available information, an example of a security token is the World Bank Blockchain Bond "bond-i".

[6] FATF, Updated Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers, para. 44 at p.21-22 (Oct. 2021).

[7] Basel Committee on Banking Supervision, The Basel Framework, Scope and definitions: SCO60 Cryptoasset exposures, § 60.131 (Dec. 14, 2023, effective Jan. 1, 2025), (defining digital assets to "not include digital representations of fiat currencies").

[8] At the time of publication, no offline CBDC exists. However, the Group agrees with the BIS Innovation Hub that risk management for any offline CBDC should include a threat and risk assessment for ML/TF and fraud. *See* BIS Innovation Hub, Project Polaris, Part 4: A high-level design guide for offline payments with CBDC at p.37 (Oct. 2023); *see also* Bank of Canada, Staff Analytical Note 2023-2, A central bank digital currency for offline payments (Feb. 2023), (highlighting concerns that "[m]alicious actors may be incentivised to exploit an offline CBDC as a tool to conduct activities that contravene anti-money laundering, anti-terrorist financing and other applicable legislation").

Q6. Is a Non-Fungible Token[9] (NFT) of value considered a Digital Asset?

The FATF defines NFTs as "[d]igital assets that are unique, rather than interchangeable, and that are in practice used as collectibles rather than as payment or investment instruments…."[10] Notably, the FATF indicates that NFTs "are generally not considered to be V[irtual] A[sset]s under the FATF definition" unless "the nature of the NFT and its function in practice" proves otherwise regardless of marketing terms used.[11]

The Group takes a different view from the FATF with respect to NFTs of value. NFTs of value include NFTs that retain value over time due to collectability or tradability in secondary markets. NFTs of value need not necessarily include rights of substantial value to property or royalties. However, NFTs of value do not typically include NFTs designed for a particular use even when purchased for value, such as an NFT issued solely for purpose of admission to a general sporting event or concert on a fixed date, as a substitute of a coupon to redeem for a good of limited value by a fixed date, or redemption for a virtual item or costume in a video game.

The Group considers that, given the ML/TF risks of this emerging asset class, FIs should consider that NFTs of value are digital assets in the absence of information to the contrary. An assessment of NFTs of value may be undertaken to evaluate whether the value presents ML/TF risks similar to other digital assets. In the view of the Group, value can be derived from storage of value, prescription of value by the issuer of the NFT, or can be tangible and attributable to actual market value. For example, independent appraisal of value or transferable value are not the sole source of risk. ML/TF risks may arise even in circumstances where an issuer (or creator) of an NFT arbitrarily assigns a value and uses the instrument to facilitate money laundering.

Q7. Is an NFT not of value considered a Digital Asset?

The Group generally agrees with the FATF that NFTs not of value should be viewed from a functional perspective[12] and such NFTs are excluded from the scope of this document.

Q8. What are Stored-Value Fungible Digital Assets?

Stored-value fungible digital assets are digital assets which are neither DLT-based nor issued by a central bank or authorised FI that operate as a unit of value or means of payment. Although stored-value fungible digital assets may be cryptographically stored, they do not require DLT and are not electronic money. Examples include Hub Culture Limited's Ven currency launched in 2007, eCash, NetCash and e-gold in the 1990s and early 2000s and the M-PESA "e-Float" in the 2010s. Excluded from stored-value fungible digital assets are non-convertible virtual currencies specific to a particular centralised virtual domain which cannot be readily exchanged for fiat currency or digital assets, such as Fortnite V-Bucks, Roblox Robux, Perfect World Zen, World of Warcraft Gold, or similar closed-loop video game currencies.

---

[9] Fungibility typically refers to the interchangeability of an asset. NFTs, by their nature, are uniquely identifiable and therefore non-fungible.

[10] *See* FATF, Updated Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers, para. 53 at p.24 (Oct. 2021), (referring to NFTs alternatively as "crypto-collectibles").

[11] *See ibid.*

[12] *See* FATF, Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers, para. 49 at p.33 (Jun. 2023), (noting jurisdictions vary in classifying NFTs as either virtual assets, art, or collectibles and advocating a functional approach to determining NFT classification).

II. Defining Stablecoins and Tokenised Deposits

Q9. What is a Stablecoin?

A **stablecoin** is a digital asset, token or form of digital cash that is designed to maintain a stable value or peg its market value to some external reference relative to a specified asset or a pool or basket of assets including fiat currency. Stablecoins are neither issued by a central bank nor a financial market infrastructure (FMI). Stablecoins are intended to be used as a means of payment or store of value and may represent a claim on the issuing entity, if any, and/or the underlying assets. The FATF refers to these digital assets as "so-called stablecoins" due to potential risks associated with price stability of certain protocols.[13] Mindful of these risks, the Group proposes distinguishing certain fiat-backed digital assets from other stablecoins which may present unique or higher inherent ML/TF risks.

Stablecoins achieve their price stability using several collateralisation mechanisms, including:

- **Fiat-backed stablecoins**: collateralised/backed solely by hard reserves of the pegged fiat currency or backed by hard reserves in combination with cash-equivalents presenting minimum market and credit risk approved by prudential authorities such as demand deposits, treasury bills or high quality commercial paper;
- **"Other stablecoins"**: backed by reserves of one or a basket of commodities, digital assets, or other assets other than fiat currency or cash-equivalents of (ideally) equal or greater value, or alternatively of lesser value utilising algorithms.[14]

Stablecoins may leverage algorithms or incentivise a user's buy/sell behaviour to manage supply-and-demand to achieve target value through the buying and selling of the stablecoin's reference asset or its derivatives. But a fiat-backed stablecoin cannot be solely algorithmic as defined due to the requirement for collateralisation by hard reserves of pegged fiat currency. The Group recommends that FIs implement risk-based thresholds to determine whether collateralisation levels are appropriate for fiat-backed stablecoins that utilise partial algorithmic backing.

Fiat-backed stablecoins should be distinguished from "other stablecoins" and classified separately from a ML/TF risk perspective. The ease of issuance and global transferability of "other stablecoins" may present heightened risk of ML and fraud compared to fiat-backed stablecoins due to inconsistent reserve requirements and disclosure rules in many jurisdictions. Inconsistent licensing requirements and regulatory oversight of stablecoin issuers in some jurisdictions may contribute to these heightened risks.

Q10. What is a Tokenised Deposit?

A **tokenised deposit** is issued on a private or permissioned blockchain by an FI or other entity and cannot be transferred outside the private or permissioned blockchain; examples include tokenised commercial bank money. For purposes of these FAQs, a tokenised deposit is distinct from stablecoins and other digital assets. Although a tokenised deposit may or may not pay interest, the tokenised deposit also may not create value separate from the underlying deposit account and may create a liability from an account perspective. Tokenised deposits reflect a deposit ownership claim on DLT for a fixed amount of fiat money

[13] *See ibid.* at p.34 footnote 43; FATF, FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins, para. 18 at p.5 (June 2020).

[14] Examples of other stablecoins which are algorithmic include Ampleforth (AMPL), FRAX, USDD, Kava Labs' USDX, Synthetix USD (SUSD), Celo Dollar (CUSD) and TerraUSD (UST).

denominated in a single currency by the token-holder against the token issuing FI. These FAQs exclude tokenised deposits unless otherwise noted.

III. Defining Anonymity-Enhanced Cryptocurrency

Q11. What is an Anonymity-Enhanced Cryptocurrency?

An anonymity-enhanced cryptocurrency (AEC), commonly referred to as a privacy coin, is a digital asset which by design is neither traceable nor linkable to transaction history on the blockchain, which favours the anonymity of users, the opacity of financial flows (thereby inhibiting payment transparency requirements), and can be traded anonymously. AEC presents additional heightened ML/TF risks due to the inherent lack of payment transparency, even where the use of AEC privacy features is marketed as optional.

Some AECs originate as digital assets with built-in privacy features, while other AECs are created by adding privacy protocols to preexisting digital assets. For example, Monero (XRM) is inherently an AEC but Litecoin (LTC) is not. However, LTC becomes an AEC where it utilises a privacy enhancer such as MimbleWimble Extension Blocks (MWEB) which obfuscates transaction records from the distributed ledger.

To preserve anonymity and obfuscate traceability, AECs employ a variety of strategies, including for example:

- use of zero-knowledge technology to bypass recording on the distributed ledger,
- use of one-time wallet addresses (also known as stealth addresses),
- use of ring signatures shared by a group of users, which obfuscates the actual signatory,
- use of mixer technology which limits traceability, and
- other anonymisation features designed to mask the source typically through decentralised networks or chain hopping across multiple currencies sometimes referred to as atomic swaps.

AECs also include digital assets which provide the option for applying these anonymity enhancements in their design. Examples of AECs include, but are not limited to, Monero (XMR), Monero Classic (XMC), Zcash (ZEC), Ycash (YEC), FIRO, GRIN, BEAM, DASH, Oasis Network (ROSE), Vine Money vUSD, Secret Network (SCRT), and Pirate Chain (ARRR), all of which the Group views as presenting heightened ML/TF risks due to their design or purpose for peer-to-peer activity without full payment transparency.

Q12. What is a Privacy Enhancer?

A **privacy enhancer** is an AEC protocol or software extension designed to protect the anonymity of users and the opacity of financial flows, or to enable anonymous trading. Examples include, but are not limited to, Ring Confidential Transaction (RingCT), CoinJoin, Whirlpool, Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (Zk-SNARK) and similar software implementations at the protocol level.

Blockchain-based digital assets, including virtual currency and AEC, authenticate and relay transactions across network nodes which validate transactions referred to as **validator nodes**. Validator nodes operate based on rules agreed upon for the blockchain network which is known as **consensus**. There are four primary methods for implementing a privacy enhancer protocol or software on a blockchain:

1. **Native tokens**: A token is developed with the privacy enhancer protocol at the native level, creating an AEC. One example is the MimbleWimble blockchain protocol which is a privacy enhancer utilised by MimbleWimbleCoin. MimbleWimbleCoin is a native token issued on the MimbleWimble protocol. Therefore, MimbleWimbleCoin is the AEC.
2. **Hard forks**: A change that significantly alters consensus causing backward incompatibility with existing validator nodes, thereby resulting in a permanent chain split and creation of a unique AEC.[15] One example of a hard fork that significantly altered consensus rules is Zcash (formerly known as Zerocash) which hard forked from Bitcoin (BTC) in 2016. Therefore, Zcash (then referred to as Zerocash) could not be transferred through Bitcoin validator nodes creating a unique AEC. An AEC can also fork from another AEC, such as was the case with prior hard forks of Monero (XMR) which resulted in various AEC projects including, for example, Monero Classic (XMC).
3. **Soft forks**: A change to the blockchain that adds new consensus rules without significantly altering existing consensus rules. New blocks created using the combined existing and new consensus rules remain backward compatible with existing validator nodes. However, blocks created solely under the existing consensus rules are not backward compatible with validator nodes that adopt the new consensus rules.[16] A soft fork implementing a privacy enhancer protocol or software through a majority of validator nodes would typically be viewed as creating an AEC.
4. **Extension blocks**: Extension blocks, also known as pegged sidechains, utilise parallel blockchains and may be implemented through any of the above three means. When transactional activity migrates to the extension block, this is referred to as "pegging in." While pegged into an extension block utilising a privacy enhancer, transactions occurring on the extension block may limit transparency and traceability. Migrating back to the original block and exiting the extension block is referred to as "pegging out."[17] An extension block applying a privacy enhancer to digital assets typically qualifies as an AEC if the majority of validator nodes on the native blockchain support transfers of Digital Assets which include rules for accessing extension blocks. Further risk assessment may be needed for a digital asset capable of using an optional extension block where adoption is through means other than native token or hard fork implementation.

Privacy enhancer protocols can be utilised in connection with multiple forms of digital assets such as virtual currencies and NFTs held in wallets. Privacy enhancers applied to NFTs of value also present heightened ML/TF risks of anonymised NFT trades.

Privacy enhancers can be distinguished from mixers/tumblers which are services used to obfuscate the source and destination of digital asset transactions. However, some jurisdictions may classify certain privacy enhancers as a mixer or tumbler.

Q13. What is a Mixer?

A mixer, also known as a tumbler, is not an AEC. However, mixers create similar heightened ML/TF risks for digital assets which are not AECs. A mixer obfuscates activity on the ledger by, for example:

1. Pooling or aggregating digital assets from multiple persons, wallets, addresses, or accounts;

[15] *See* Dylan Yaga et al., Blockchain Technology Overview (2018), U.S. Department of Commerce: National Institute of Standards and Technology, Internal Report 8202 at p. 29-30 (defining hard forks as not backwards compatible).
[16] *See ibid* (defining soft forks as backwards compatible).
[17] *See* Elliptic, Explaining MimbleWimble: the privacy upgrade to Litecoin (Jun. 1, 2022), (explaining LTC blockchain ledger includes records of pegging-in and pegging-out of privacy enhancer MWEB).

2. Using programmatic or algorithmic code to coordinate, manage, or manipulate the structure of a transaction;
3. Splitting digital assets for transmittal through a series of independent transactions;
4. Creating and using single-use wallets, addresses, or accounts, and sending digital assets through such wallets, addresses, or accounts through a series of independent transactions;
5. Exchanging between various types of digital assets including chain hopping through cross-chain bridges; or
6. Facilitating user-initiated delays in transactional activity.[18]

The above list provides illustrative examples and the definition of mixer may vary between jurisdictions. Mixers may or may not include the provision of protocols to accomplish mixing, may be centralised, such as in the case of Blender.io, or decentralised, such as in the case of Tornado Cash and Sinbad. Additional examples of mixers include Cyclone Protocol, Buccaneer V3 (BV3), Unijoin, Mixero, Tumbler.io, YoMix, Coinomize, RAILGUN, Bitcoin-Laundry and wallet-level services such as Wasabi, Samourai, Chaincase and JoinMarket.

IV. Digital Asset Industry Stakeholders

Q14. How does the definition of Digital Asset apply to industry stakeholder classification?

Whether in the form of issuance, administration, transfer, or custody, understanding the role of digital asset industry participants is essential for appropriate ML/TF risk management. In recent years, the growth of providers in the digital assets industry has continued to grow, particularly with the emergence of new products, services and technologies. To address the changing risk landscape, the Group proposes two overarching categories for digital asset industry participants: **digital asset service providers (DASPs)** and **digital asset supply chain operators (DASCOs)**. While some authorities may refer more narrowly to virtual or cryptoassets (e.g. virtual asset service providers), the Group believes the principles suggested below for DASPs and DASCOs should be considered in the broader context of the definition for digital assets presented in Section I above.

Q15. What is a Digital Asset Service Provider (DASP)?

Digital assets can be transferred or transacted through a DASP. DASPs, such as virtual/fiat currency exchange platforms and custodians of digital assets, are the main entry points between the world of digital assets and the traditional regulated financial system. The Group proposes an expanded definition of the term DASP to include any individual, legal entity, or organisation which, as a business, conducts one or more of the following activities or operations, or supplies one or more of the following services, for or on behalf of another individual or legal entity:

- Exchanging or making arrangements with a view to exchanging digital assets for fiat currencies or vice versa;
- Exchanging or making arrangements with a view to exchange between forms of digital assets;

[18] These examples are based upon mixing services identified by the US Financial Crimes Enforcement Network (FinCEN) with respect to convertible virtual currency in the bureau's Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern, 88 Fed. Reg. 72701 at 72722 (Oct. 23, 2023).

- Transfer of digital assets, including conducting a transaction on behalf of another individual or legal entity that moves a digital asset from one digital asset address, account or wallet provider to another;
- Intermediary, brokerage, or agency services that allow for reception and transmission or transfer of digital assets on behalf of third parties;
- Operating an automated teller machine (ATM) which utilises automated processes to exchange digital assets for money/fiat currency or money/fiat currency for digital assets;
- Operating a trading platform to exchange digital assets;
- Operating or maintaining a hosted (custodial) wallet solution;
- Safekeeping, safeguarding, custody or administration of:
  - Digital assets on behalf of third parties; or
  - Instruments enabling control over digital assets, including private keys on behalf of third parties;
- Placing[19] of digital assets;
- Providing transfer services for digital assets on behalf of third parties;
- Providing portfolio management on digital assets, including the movement of digital assets;[20]
- Providing lending of digital assets, including staking; or
- Providing lending that involves direct movement of digital assets, including for example direct lending of digital assets.

In some jurisdictions, providing either investment allocation or transactional advice for digital assets or use of digital asset services also qualifies as an activity of a DASP.[21]

Q16. Do DASPs exclude ancillary service providers and other financial instrument exchanges?

DASPs do not include an ancillary service provider (e.g. software provider, hardware infrastructure, cloud service provider) that is not operating, maintaining or involved in the operations or administration of a digital asset hosted (custodial) wallet, exchange, or custody operation.[22] DASPs also do not include traditional business exchanges or central clearing counterparties engaged in facilitating trading in various derivatives and equities markets. See Q18 for further information on participants in the digital assets supply chain and Q23 for further information on "hosted" and "unhosted" wallets.

Q17. Is a DASP a form of Centralised Finance (CeFi) or Decentralised Finance (DeFi)?

DASPs typically fall within either centralised finance (CeFi) or decentralised finance (DeFi) classifications. **CeFi** refers to a financial ecosystem where a centralised governing body controls financial assets and the flow of money. The centralised governing body sets the rules and standards for how assets are managed

[19] Placing of digital assets is distinguishable from issuance of digital assets and may vary in definition from jurisdiction to jurisdiction. However, the Group anticipates that an issuer not placing digital assets will still frequently qualify as a DASP by nature of the other activities listed in the definition, such as staking.

[20] Portfolio management of digital assets may also be included in the absence of movement of digital assets depending on the level of exposure and jurisdiction where the portfolio management is occurring.

[21] *See* Regulation (EU) 2023/1114 on Markets in Crypto-Assets, art. 3, points 1(16)(h), 1(24) & art. 60, points 3(g), 5(b,) (defining "providing advice on crypto-assets" to include providing, offering, or agreeing to offer advice and indicating it is "deemed equivalent to investment advice").

[22] Some jurisdictions may impose additional conditions or requirements for certain ancillary service providers.

and transacted. **DeFi** refers to a financial system that uses blockchain or other DLT to remove the need for traditional financial intermediaries including for example banks and exchanges.

Within CeFi, **Centralised DASPs** are entities that meet the definition of a DASP and are managed/operated by a central governing body. The central governing body is an entity that demonstrates control over the service/product by being able to change the product attributes post-deployment of a product. For example, if a central governing body could change the block reward awarded to miners of a blockchain product directly, then that product would be considered centralised. However, a party controlling a wallet is not, in isolation, considered a defining factor to classify a DASP as centralised.

Within DeFi, **Decentralised DASPs** are organisations or protocols that meet the definition of a DASP and do not have a central governing body that can demonstrate control or governance over the product offering and lack clearly identified senior managing person(s) or control prong(s). Decentralised DASPs include services/products that run automatically without a central governing body to change the product offering. Smart contracts that utilise algorithms to change product attributes automatically are an example of a decentralised product.[23] However, some centralised DASPs may market themselves as "decentralised" to increase market appeal. Therefore, decentralised DASPs may require additional scrutiny by FIs to confirm the lack of centralised control or governance by parties. This confirmation is necessary to rule out heightened ML/TF risks associated with centralised DASPs portraying themselves as decentralised DASPs.

In circumstances where a DASP operates dual-hatted as a central governing body with respect to some operations but also offers other digital asset products through primarily decentralised means, the DASP is considered akin to a decentralised DASP unless an analysis of the dual-hatted DASP reveals the decentralised protocols are immaterial to the centralised governance structure of the DASP. For example, if a DASP operates utilising both centralised and decentralised protocols, the DASP presents the heightened risk of a decentralised DASP unless information corroborates that its centralised governance model operates free of hindrance from any decentralised protocols.

Q18. What is a Digital Asset Supply Chain Operator (DASCO) and how does it relate to a DASP?

A **DASCO** is an individual or legal entity which is not a DASP and which, as a business, engages in one or more of the following activities or operations:

- Mining of digital assets only;[24]
- Providing non-custodial software solutions only, including for example solely operating or maintaining unhosted (non-custodial) software wallets;
- Primarily developing applications for the activities, operations or services of DASPs;
- Primarily developing applications or protocols for the interoperability of the activities, operations or services[25] of one or more DASPs; or

[23] See Section VI (*Architecture of Digital Assets)* for the definition of smart contract.

[24] Mining pools are inherently DASCOs but may engage in activities, such as conducting a transaction on behalf of another individual or legal entity that moves a digital asset from one digital asset address, account or wallet provider to another that may qualify it as a DASP.

[25] An entity which solely provides data analytics used for AML or other compliance purposes is neither considered a DASCO nor a DASP.

- Primarily operating a marketplace for the purchase, sale or transfer of NFTs not of value.[26] The activities and operations of a DASCO listed above are provided as examples and other DASCOs may exist.

The Group believes that the inherent ML/TF risks associated with DASCOs differ from those associated with DASPs and that DASCOs, in certain circumstances, may present a decreased ML/TF risk compared to DASPs due to the limited nature of their activities.

Q19. When is a Customer Relationship established with DASPs, DASCOs and their investors?

In general, the definition of customer relationship should not typically differ between a DASP, DASCO or investor and/or other individual or entity customer types. The following is a non-exhaustive list of circumstances frequently associated with entering into a customer relationship with market participants.

An FI enters a **customer relationship** with a DASP or DASCO when, for example:

- Providing access to fiat-based products for DASPs or DASCOs;
- Providing access to fiat-based products for consumers accessing a DASP's or DASCO's digital asset exchange (including for example virtual currency exchanges, NFT marketplaces, and other local exchange trading systems);
- Providing correspondent services to DASPs and DASCOs creating a correspondent relationship;[27]
- Providing digital asset-based products directly to DASPs and DASCOs including for example to provide liquidity;
- Onboarding customers for traditional financial service products whose main business or source of revenue is related to digital assets, for instance through the customer's offering of blockchain services such as wallet hosting, Staking-as-a-Service, Crypto-as-a-Service or the trading of digital assets; or
- Providing services to DASPs such as cash management, equity and capital markets (ECM), debt and capital markets (DCM), or merger and acquisition (M&A) advisory services.

Q20. Who is an investor of a DASP or DASCO?

A **DASP investor** or **DASCO investor** is any individual or legal entity which is not a DASP or DASCO but has an ownership interest in or direct investment in a DASP or DASCO at a percentage level or threshold considered by the FI to be material. For decentralised DASPs (and DASCOs), the equivalent of ownership interest or direct investment may be represented in the form of governance token ownership. Governance tokens utilise smart contracts which confer control over the decentralised DASP protocols or project and may impact all aspects of functionality including, for example, the processing of change in voting rights, listing and delisting of tokens, halting or resuming transactions, cybersecurity issues, and adherence to financial crime controls such as adding or removing restrictions on a validator node[28] for ML/TF or sanctions compliance purposes.

[26] An assessment of NFTs of value may be undertaken to evaluate whether the nature and value of the NFT presents ML/TF risks; such risks may arise even in circumstances where an issuer (or creator) of an NFT arbitrarily assigns a value and uses the instrument to facilitate money laundering.

[27] *See* The Wolfsberg Group, Wolfsberg Financial Crime Principles for Correspondent Banking (Oct. 2022).

[28] Validator nodes authenticate and relay transactions for Blockchain-based digital assets. For further illustration of validator node usage, see for example Section III (*Defining Anonymity-Enhanced Cryptocurrency*).

V. Digital Assets as a Product or Service

Q21. What products and services are associated with Digital Assets?

Products and services that are used in relation to digital assets will vary based upon the nature of the FI, whether a traditional FI, DASP, DASCO or other non-bank financial institution, offering the product or service, as well as the jurisdiction in which the product of service is offered from and to. These products and services may often be extended to any customer type in addition to DASPs or DASCOs.

The following table sets out a non-exhaustive set of examples of products and services that may involve digital assets including traditional fiat-based financial services as well as those unique to digital assets and other asset classes.

	Examples		Examples (continued)
1	Advisory	16	NFT (of value) exchange/trading
2	Asset management	17	Payments using virtual assets or CBDCs
3	Brokerage	18	Pool investing
4	Clearing	19	Retirement
5	Digital asset exchange-traded product (ETP) execution	20	Stablecoin administration/issuance
6	Custodian of native or tokenised assets	21	Staking-as-a-Service (StaaS)
7	Digital asset derivative trading	22	Tokenisation of assets
8	Digital asset investment funds	23	Trading on behalf of clients[29]
9	Escrow	24	Unsecured digital asset-backed loans
10	Fiat custodian of stablecoin reserves	25	Digital asset derivative trading
11	Finance for mining equipment	26	Digital asset exchange/trading
12	Lending and cash management services	27	Virtual currency issuance/administration
13	Market making (without touching underlying digital assets)	28	Plug-and-Play/white labelling (including, for example, Banking-as-a-Service, Fintech-as-a-Service, Support-as-a-Service, Staking-as-a-Service, Mining-as-a-Service, Crypto-as-a-Service,[30] and Wallet-as-a-Service[31])
14	Mining-as-a-Service (MaaS)	29	Unhosted (non-custodial) wallets
15	NFT (of value) administration/issuance		

Q22. What delivery channels are associated with Digital Assets?

The delivery channels where an FI, DASP or DASCO may provide or offer products and services associated with digital assets are broad. Examples of delivery channels for products and services that may be

[29] Trading refers to both open-loop and closed-loop trading. For purposes of this FAQ, closed loop excludes video game currencies or similar non-convertible virtual currencies specific to a particular centralised virtual domain which cannot be readily exchanged for fiat currency or digital assets.

[30] Crypto-as-a-Service refers to circumstances where a DASP designs and offers a plug-and-play solution to third-parties seeking to offer digital asset services to their customers but the customers do not interact with the DASP designer. In these arrangements, the designer DASP typically maintains licensure to provide custodian or exchange services.

[31] Wallet-as-a-Service refers to custodian or semi-custodian solutions to integrate wallet services into existing platforms. Examples of wallet-as-a-service offerings include Web 2.5 wallets that combine Web 3 wallet infrastructure with Web 2 user interface that may offer additional services such as activity feeds and reward systems.

impacted by digital assets can include the extension of banking services, brokerage services, advisory services, electronic trading initiatives, transactional services, sales and distribution, insourcing, and other business associated with the financial industry such as trade products, investment products, credit and financing products, indices, platforms and operations.

Q23. How are Digital Assets exchanged peer-to-peer?

Digital assets may be exchanged peer-to-peer (P2P) including where the transfer of digital assets occurs without an intermediary between unhosted wallets.

An **unhosted wallet**, also known as a non-custodial wallet, is a wallet or solution that allows users to maintain self-custody or control of digital assets without the use of, or dependency on, any third-party service provider, including for example a third-party custody service provider. By contrast, a wallet custodied by a DASP is considered a **hosted wallet**, also known as a custodial wallet. Transactions originating from or directed to a hosted wallet are not considered P2P. In the case of so-called "**Web 2.5 wallets**" where the user maintains one portion of a key but utilises a third-party service to reconstruct the complete key to transact or sign a smart contract (including sharding[32]), the Group considers the wallet service as an unhosted wallet so long as the wallet service provider does not maintain any control over the third-party service provider used to reconstruct the complete key. P2P transactions and other transactions either originating from, or directed to, unhosted wallets may present heightened ML/TF risks due to an inconsistent application of controls including, for example, on customer due diligence.

Q24. Who qualifies as a Custodian of Digital Assets?

A **custodian** is an entity which provides services to safeguard, or to safeguard and administer, the following:

- Digital assets on behalf of its customers (or for an underlying beneficiary e.g. the customer's customer as a sub-custodian); or
- Private cryptographic keys (or equivalent means) on behalf of its customers in order to hold, store and transfer digital assets.

The Group notes that the obligations for a custodian of certain digital assets such as CBDCs or NFTs may vary from those of a custodian of others such as virtual currency or stablecoins.

VI. Architecture of Digital Assets

Q25. How are Digital Assets designed and distributed?

As detailed in Section I, digital assets include certain digital representations of value and/or tokens. There are several underlying technologies that support digital assets which are detailed further below. Layer technologies, including base Layer 1, give rise to native tokens and their progeny. In turn, tokens are typically issued through processes referred to as initial coin offerings (ICO) either by centralised or decentralised DASPs. Decentralised DASPs predominantly conduct automated transactions including ICOs for certain DLTs through smart contracts as defined later in this Section.

[32] Sharding refers to the splitting of private cryptographic keys into multiple pieces which then can require either all or a designated portion of the keys together in order to control a digital asset.

Q26. How is value represented in Digital Assets?

Value can arise as a function of supply and demand and be represented in digital assets via **DLT tokens.** Value can also be derived in certain instances without tokenisation such as in the form of non-tokenised CBDCs or stored-value fungible digital assets.

Q27. What are Distributed Ledger Technology Tokenisation and Tokenised Assets?

DLT tokenisation is the act of creating or holding a digital representation of an asset where such representation creates or derives value, including for example representations of assets (including physical or digital assets) on a blockchain or other DLT. Examples of tokenisation include the issuance of physical asset classes or commodities in tokenised form on a blockchain.

Tokenised assets are created through tokenisation when deriving value from the underlying value of an asset or commodity.

Q28. As part of tokenisation, what are the Layer Protocols of blockchain?

A blockchain consists of a series of layer protocols with Layer 1 (L1) and Layer 2 (L2) considered as primary layers. Third-party integrations building upon network infrastructure continuously develop on the blockchain, including for example protocols referred to as Layer 0 and Layer 3. These additional layers may support increased blockchain functionality by, for example, utilising bridges or similar protocol solutions to allow interoperability between multiple blockchain networks or to integrate third-party data from the real world.

Q29. What is a Layer 1 (L1) Protocol?

L1 is a base blockchain network and protocol. **Native tokens** are developed and exist on L1 of blockchains because they are the underlying foundation on which various L2 networks build.

Q30. What is a Native Token?

A **native token** is a digital asset of a blockchain, used to incentivise security, contribution of computing power and usage of L1 protocol. Native tokens are created directly on a blockchain, including circumstances where the record of value is primarily recorded on the blockchain ledger. For example, a digital means for storing value in the form of a fungible or non-fungible token is considered a native token. By contrast, an FI holding a fiat account which is tokenised (also known as a tokenised deposit), is not a native token, nor is an ERC-20 smart contract token for value built on the Ethereum (ETH) network, whereas ETH is the native token on the L1 blockchain main network (also known as a mainnet).

Q31. What is a Layer 2 (L2) Protocol?

L2 is a collective term to describe a specific set of mechanisms for scaling transactions utilising relay chains, bridges or other scaling protocol solutions. Rollups are the leading mechanism for processing activity independent of L1 including, for example, batching of transactional activity through relay chains and bridges. Relay chains and bridges are methods of interconnectivity across blockchain layers, whereas L2 is a separate blockchain from an underlying native token but inherits the security guarantees of the L1 base chain and utilises proofs to achieve validity. The main goal of scaling protocols is to increase transaction speed (faster finality) and transaction throughput (higher transactions per second) without

sacrificing decentralisation or security on L1 through platform-based activity and public mirroring on L2, also known as sidechain activity.

By removing this transaction load from L1, the base layer becomes less congested and the native token becomes more scalable allowing greater volumes of activity, although L2 activity may not be fully reflected in the L1 blockchain ledger. L2 can sometimes present distinct challenges for applying ML/TF transaction monitoring controls due to the additional degree of separation from the L1 blockchain main network and use of scaling protocols. This separation necessitates data analytics tools which monitor activity transacted through L2 in addition to an L1 mainnet.

Q32. What is an Initial Coin Offering (ICO)?

An ICO is an initial issuance and offer of certain digital assets, typically in the form of virtual currency or stablecoins, to the public or a fundraising transaction issuing tokens which cannot be qualified as financial instruments.[33] An ICO can be administered through a centralised exchange (known as an Initial Exchange Offering, or "IEO") or via a decentralised exchange (known as an Initial DEX Offering, or "IDO"). The ICO involves various stakeholders, including the issuer, offeror and contributors, but also, where applicable, one or more DASPs, such as virtual/fiat currencies exchange platforms, custodians of digital assets or placement agents.

The Group notes that this is an area of continued discussion, including the definition of digital security, which may be governed under securities and other applicable regulations.

Q33. What is a Smart Contract?

The FATF defines a **smart contract** as "a computer program or a protocol that is designed to execute specific actions automatically such as [digital asset] transfer between participants without the direct involvement of a third party when certain conditions are met."[34] This is an area of increasing development for institutional purposes and will be a focus of risk profiling in future discussions and case studies by the Group.

Regardless of the contractual behaviour of the smart contract or views of the parties, any binding legality of a smart contract would need to be determined in each jurisdiction.

Conclusion

While the proposed terms and definitions in this paper may differ in some jurisdictions, the Group believes alignment with the above definitional hierarchy and related terms are critical to assessing the ML/TF risks of digital assets. The Group intends to provide periodic updates through FAQs, guidance, case studies and/or deep dives to support the continued risk profiling and treatment as the use and application of digital assets continue to evolve.

[33] In some jurisdictions, an ICO issuance may meet the legal definition of issuing a security or financial instrument.

[34] *See* FATF, Updated Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers, para. 42 at p.19 (Oct. 2021), (defining smart contract in the context of virtual assets as FATF uses the term).