

Crypto-Assets

The financial sector is continuously evolving through the rapid development and adoption of new technologies. The term 'FinTech' generally refers to financial innovation that seek to provide enhanced financial service offerings through the utilisation of enabling technologies. These generally include Distributed Ledger Technology & Smart Contracts; Artificial Intelligence, Machine Learning & Big Data, Cloud Computing, Web 3.0, Application Programme Interfaces and Micro-Services; Robotic Process Automation and the Internet of Things.

As part of the MFSA's initiatives to generate awareness, drive culture and deliver a cross-sectoral knowledge platform which can support the MFSA's functions in preparing for the financial services of tomorrow, these insights will delve into enabling technologies, enabling innovations and their sectoral applications.

1 What are Crypto-Assets?

1.1 Definition

The recent evolution of Crypto-Assets ('CA'), that are also know as 'virtual assets' may be traced to the white paper titled '[Bitcoin: A Peer-to-Peer Electronic Cash System](#)' on 31 October 2008 by Satoshi Nakamoto which proposed a solution to the double-spending problem on a peer-to-peer disintermediated network. Since then countless CAs, initially coined as cryptocurrencies, have been issued, each having their individual characteristics, such as stablecoins, investment/security tokens, utility tokens, and non-fungible tokens ('NFTs').

Although CAs have been defined in a number of ways, to date, there is no generally accepted definition of the term 'crypto-asset'. One of the most comprehensive regulatory definitions is provided in the [Markets in Crypto-Assets \('MiCA'\) Regulation](#) proposed by European Commission, which refers to CAs as '*a digital representation of a value or a right which may be transferred and stored electronically, using [Distributed Ledger Technology](#) ('DLT') or similar technology*'.

Underpinned by DLT, cryptography, and the innovation brought about by Satoshi Nakamoto through the bitcoin blockchain, and the later the Ethereum Blockchain and Smart contracts, these assets may be used to issue, store, transfer, trade, lend and/or borrow assets/rights for various purposes in a decentralised manner without the need for a trusted centralised party. This enabling innovation has led to creation of an ecosystem with novel products and services both within the traditional centralised finance, through the creation of centralised CAs service providers and [Decentralised Finance](#) applications powered by [Smart Contracts](#).

1.2 Types of Crypto-Assets

CAs are sub-set of digital assets. This generally refers to any digital asset that may be assigned economic function and legal rights and may range from manuscripts, metadata, digital art and conventional financial instruments. Meanwhile, while there is no one accepted taxonomy, CAs have been attributed various labels depending on their characteristics, such as:

i. *Investment/Security Tokens*

These generally provide their holders with rights that are substantially similar in nature to those of traditional financial instruments, such as transferable securities.

ii. **Utility Tokens¹**

These tokens grant access rights to digital services and products and are generally limited to a single closed network controlled by the issuer of tokens. Some examples of such tokens include gaming tokens, tokenised shopping cards or even certain governance tokens that provide the holder with special rights on a decentralised platform.

iii. **Cryptocurrencies²**

These CAs whilst being used as a means of exchange, store of value or even for investment purposes, do not generally have any rights associated with them. Some examples of cryptocurrencies include [Bitcoin](#) ('BTC'), [Ethereum](#) ('ETH'), [Litecoin](#) ('LTC') and [Cardano](#) ('ADA').

iv. **Stablecoins³**

These CAs are designed to hedge against inflation and depreciation of cryptocurrencies by being value stable. Some prominent examples of such tokens include [USD Coin](#) ('USDC'), [Tether](#) ('USDT') and [Binance USD](#) ('BUSD').

v. **Central Bank Digital Currencies ('CBDC')⁴**

CBDCs represent digital money that may be issued by Central Banks ('CB') and are generally categorised as 'wholesale' and 'retail' CBDCs. The former pertains to the wholesale transactions in CB reserves and interbank settlements whilst the latter refers to the national digital currency having the function of money thereby serving as the unit of account, medium of exchange and store of value.

vi. **Non-Fungible Tokens**

A Non-Fungible Token ('NFT') is a special type of digital asset that can be proved to be unique and not interchangeable with another digital asset token (i.e. non-fungible). NFTs are created in accordance with certain frameworks or standards and deployed on DLT. NFTs generally represent digital files such as digital artworks, photos, videos, and audio, with their main feature being their uniqueness and non-fungibility (based on their programming, the limited copies of a digital artwork created etc).

2 Crypto-Assets Ecosystem

2.1 Tokenomics

Tokenomics, which is a combination of "token" and "economics," is an emerging field that deals with the study and development of economic systems that utilise CAs. The main objective of tokenomics is to design and implement a set of rules, incentives, and governance mechanisms that facilitate the efficient use and distribution of CAs within a specific ecosystem. This includes aspects such as CAs issuance, distribution, pricing, and the creation of mechanisms to incentivize CA holders to participate in the ecosystem. Effective tokenomics is crucial for the success and sustainability of CA systems, and it plays a vital role in shaping the broader CA landscape. By

¹In terms of the Virtual Financial Assets ('VFA') [Act](#) utility tokens are referred to as, Virtual Tokens and are defined as 'a form of digital medium recordation whose utility, value or application is restricted solely to the acquisition of goods or services, either solely within the DLT platform on or in relation to which it was issued or within a limited network of DLT platforms'

² For further details on Cryptocurrencies please refer to the [DLT Finsight](#)

³ For further details on Stablecoins please refer to the [DeFi Finsight](#)

⁴ CBDCs are also defined as a digital liability of a central bank that is widely available to the general public ([Federal Reserve](#), 03 Dec 2022).

leveraging tokenomics principles, developers can create robust and secure systems that foster adoption and growth within this sector.

2.2 Mining

Units of CAs are generated via a process of 'mining' or 'minting' that depends on the consensus mechanism of the underlying DLT, which varies based on the algorithmic design of the said DLT and its predefined cryptographic validation mechanisms. The two primary consensus mechanisms are Proof of Work ('PoW') and Proof of Stake ('PoS'). However, other methodologies have also been researched and utilised, including Proof of Elapsed Time ('PoET'), Proof of Authority ('PoA'), Proof of Burn ('PoB'), and Proof of History ('PoH').

These methods differ in their approach to validating transactions, with some relying on computational work while others rely on ownership stakes in the network. By utilizing various consensus mechanisms, developers can create more diverse and efficient systems, each with its unique advantages and limitations.

2.3 Custody

Custody of CAs is a critical aspect of this ecosystem. CAs can be stored in a digital wallet, also known as a crypto wallet, that stores the cryptographic keys to user's CAs. There are two forms of custody: hosted and un-hosted. In hosted custody, also known as custodial wallets, a third-party service provider controls the user's CAs and can intermediate buying, selling, or transferring virtual assets. In un-hosted custody, also known as non-custodial wallets, the user has full control and responsibility for the security of their private key and control of CAs.

Digital wallets require an internet connection to function, and those connected to the internet, even if not in use, are referred to as hot wallets. Hot wallets are user-friendly and provide quick access to CAs, but they are more susceptible to cybersecurity attacks and theft, making them riskier for users. Alternatively, cold wallets are hardware devices maintained offline and are considered more secure. Third-party operators generally use both hot and cold wallets, with only a small fraction of CAs held in hot storage.

Overall, custody is a critical element of the digital asset ecosystem, as it determines the level of control and responsibility that users have over their CAs. The choice between hosted and un-hosted custody depends on the user's preferences for control and security, while the use of hot and cold wallets is determined by the need for accessibility and security.

2.4 Crypto-Asset Markets and Service Providers

Operators within the CA space offer a diverse range of financial services and products, including issuing, exchanging, and custody of various types of CAs, as well as advisory services. These providers may be centralised ('CeFi'), decentralised ('[DeFi](#)'), or a combination of both, each presenting unique opportunities, benefits, and risks to consumers and businesses.

The CA market operates on a 24/7 basis and generate vast amounts of data on transactions, trading volumes, prices, and other financial metrics. When CA activity occurs on-chain, such as through DeFi protocols, all information about transactions is recorded on a public ledger, which makes it entirely transparent, open, and verifiable by anyone. On the other hand, data recorded off-chain is limited and subject to voluntary disclosure by the operator, making it less transparent and verifiable. As a result, it is essential for consumers and businesses to

carefully consider their preferred operator's transparency, security measures, and reputation when selecting a provider in the CA space.

3 Regulatory Approach to Crypto Assets

CAs are a fast-growing market that transcends national borders and operates globally. However, the regulatory landscape for CAs is highly fragmented, with many jurisdictions lacking clear guidance or taking a blanket approach by banning CAs altogether. This regulatory uncertainty has left many operators in the space largely unregulated, which poses risks to investors and consumers.

Some National Competent Authorities ('NCAs') have taken a more welcoming approach to CAs, viewing them as a means of fostering financial innovation. These authorities have applied existing legislation or introduced new regulatory frameworks that aim to promote responsible innovation while ensuring compliance with relevant laws and regulations. For example, in 2018, Malta became one of the first jurisdictions to enact a comprehensive legislative and regulatory framework for virtual assets called the [Virtual Financial Assets \('VFA'\) Framework](#). This framework sets out prudential, conduct and anti-money laundering ('AML')/combating the financing of terrorism ('CFT') requirements for operators within the CA ecosystem, providing for legal certainty for operators in this space.

At the European level, the European Union ('EU') has proposed a harmonized regulatory framework for CAs called the [MiCA Framework](#). The proposed regulation aims to provide a comprehensive framework for regulating the issuance and marketing of CAs, as well as the activities of third-party service providers such as custody, exchange, and trading. The MiCA Regulation will introduce clear rules and requirements for operators, enhancing investor protection, reducing fraud and market abuse, and promoting market integrity.

Moreover in 2022 the EU published the [European DLT Market Infrastructures \('DMI'\) Pilot Regime](#), which was a proposal presented as a part of the EU's 2020 Digital Finance Strategy. The pilot regime aims to create a regulatory sandbox framework for market infrastructures using DLT, such as blockchain-based platforms, to issue and settle securities. The DMI Pilot Regime will operate for a period of four years and provide a safe environment for regulated entities to experiment with DLT-based market infrastructures while complying with existing regulations. The pilot regime is expected to provide the EU with valuable insights and data on the use of DLT in securities markets and contribute to the development of a comprehensive regulatory framework for DLT-based market infrastructures in the future.

4 Benefits and Risks

Leveraging on the benefits and risks of DLT, Smart Contracts, CAs present their own specificities. Below is a non-exhaustive list of benefits and risk presented by such assets.

- BENEFITS**
- Decentralisation** – One of the most significant benefits of CAs is decentralisation. Unlike traditional financial systems, which rely on centralised intermediaries, CAs rely on decentralised networks of users and validators to operate. This means that no single entity has control over the system, making it more resilient and less prone to manipulation.
 - Security** – CAs utilise advanced cryptographic techniques to secure transactions and protect user data. The use of public and private keys ensures that only the owner of a CA can access and transfer it, and the

underlying blockchain technology provides an immutable record of all transactions, making it extremely difficult to alter or manipulate.

Speed and Efficiency – CAs can be transferred almost instantly and with minimal transaction fees, making them an attractive alternative to traditional payment methods. They also operate on a 24/7 basis, providing users with greater flexibility and accessibility

Programmability – Smart contracts, a feature of certain CAs, enable the creation of self-executing contracts that can automate various business processes, reduce transaction costs, and increase transparency.

Global Reach – CAs can be sent and received by anyone, anywhere in the world, making them a truly global payment solution. They also offer a potential solution to the issue of financial exclusion, providing unbanked individuals with access to financial services.

Privacy, Transparency and Auditability – due to the nature of DLT, CAs may offer varying degree of privacy to the user. Although public blockchain are generally pseudonymous, all transactions on the ledger are openly available to anyone for reconciliation.

Liquidity – Certain CAs are highly liquid, meaning they can be bought and sold easily and quickly on a range of exchanges. This provides investors with greater flexibility and the ability to take advantage of market opportunities.

Innovation – CAs represent a new and innovative asset class that has the potential to revolutionise the financial industry. As the technology develops, new use cases and applications are likely to emerge, providing users with a range of new opportunities and benefits.

RISKS **Regulatory risks** – The lack of clear regulatory framework and inconsistent approach towards CAs across jurisdictions creates uncertainty for businesses and consumers. Regulatory actions, such as banning or restricting the use of CAs, could result in a significant decrease in the value of CAs.

Market and Volatility risk – The prices of CAs are highly volatile and can fluctuate rapidly, resulting in significant losses for investors. This risk is amplified by the lack of transparency in the market, low liquidity, and the absence of established valuation models. Certain CAs may be deemed as highly speculative assets because they do not generally have any tangible/real underlying value associated with them, making valuation of CAs difficult. As a result, their price is driven exclusively by free market forces giving rise to high volatility risk.

Cybersecurity risks – The decentralised nature of CAs and the use of DLT make them vulnerable to hacking, cyber-attacks, and fraud. Malicious actors can exploit vulnerabilities in the system to steal private keys, manipulate transactions, or compromise the integrity of the DLT.

Operational risks - CA exchanges and wallets are subject to operational risks, such as system failures, downtime, and technical glitches. These risks can result in significant financial losses for investors and erode trust in the ecosystem.

Financial Crime risks – The use of CAs for illegal activities such as money laundering and terrorism financing has led to increased scrutiny from law enforcement agencies and regulators. Investors may face legal risks if they are found to be involved in such activities.

Supplementary Reads...

Satoshi Nakamoto (2008), Bitcoin: A Peer-to-Peer Electronic Cash System. [Available online](#)

European Commission (2022), Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets and amending Directive (EU) 2019/1937 (MiCA). [Available online](#)

U.S. Department of the Treasury (2022), Crypto-Assets: Implications for Consumers, Investors, and Businesses. [Available online](#)

IMF Fintech Notes (2022), Regulating the Crypto Ecosystem: The Case of Unbacked Crypto Assets. [Available online](#)

Check our other **FinSights** and should you have any queries or wish to discuss your ideas, even within the context of our **MFSA Fintech Regulatory Sandbox**, contact us at fintech@mfsa.mt.