FINANSTILSYNET

Principles for the assessment of decentralisation in the markets for crypto-assets

FINANSTILSYNET

Table of contents

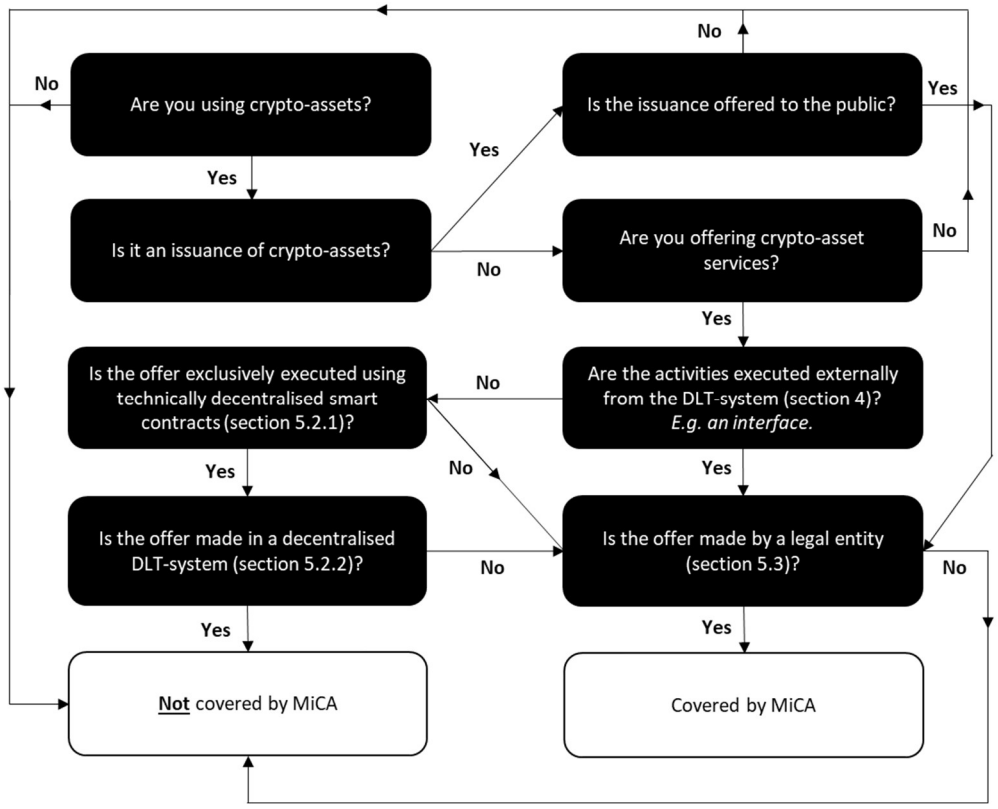
1. Introduction

The purpose of this briefing is to instruct actors on the crypto-asset markets about the Danish FSA's principles for the evaluation of decentralisation.

The reason for this briefing is that Regulation (EU) 2023/1114 of the European Parliament and of the Council on markets in crypto-assets (MiCA) does not apply to activities otherwise covered by the regulation if they are in practice provided in a fully decentralised manner. The Danish FSA therefore sees a need to identify the fundamental principles that all crypto market participants should consider before characterising their activities as decentralised - and thus not covered by MiCA. This may have significant implications for companies when considering how to structure themselves, including whether to seek permission to conduct activities under MICA. If a company conducts activities without permission on the grounds that the activity is entirely decentralized, it is essential that the company has carefully considered this matter and referred to the Financial Supervisory Authority's guidance, as an incorrect classification of an offering could be regarded as a misclassification of offered services could be considered provision of unlawful services.

Figure 1 outlines the questions actors should ask themselves to determine whether an offer of regulated activities is sufficiently decentralised or covered by MiCA.

Figure 1 - Is your offer decentralised or covered by MiCA?



Note: The figure is read from the top left corner. This is followed by the answers that reflect the assessment of the activity in the questions.

Source: The Danish Financial Supervisory Authority

Decentralisation within financial services is driven by the distributed ledger technology (DLT). A more commonly known variation of this technology is 'blockchain'. Blockchain has enabled market actors to develop and make self-executing and autonomous software (smart contracts) available which users can use to receive services with crypto assets and establish decentralised governance layers. This phenomenon is called 'decentralised finance' (DeFi).

Participants in the crypto-asset markets should by default consider whether the activities they intend to offer are regulated. A prerequisite for this is that the offering involves crypto-assets that cannot be classified as other classes of regulated assets – for example, financial instruments. If this is the case, it is important that the participants consider whether the offering can be characterised as decentralised from a technical and governance perspective. These two levels of decentralisation are discussed in detail in sections 5.2 and 5.3. It should be noted that there are certain aspects that are relevant to both assessments, but the assessments differ by first examining how the activity is technically offered (technical decentralisation) and then by looking more closely at how the managerial decisions related to the offering are made (decentralisation in terms of governance).

Even if a provider uses smart contracts issued on a conventional blockchain[1] such as Ethereum, the provision of an activity covered by MiCA cannot necessarily be characterised as decentralised. The offering of a regulated activity is only considered decentralised when there is no counterparty that constitutes a legal entity with which users of the activity can enter into a valid contract for the provision of the service (further elaborated upon in Section 5.1). In this context, it is important to distinguish between the types of activities that a legal entity actually governs and those it does not. For example, interface providers may be subject to MiCA even if the service they offer is in practice an integration to a fully decentralised service. This will often be the case for providers of interfaces for decentralised trading facilities. There may also be instances where the provider of the DLT system can constitute a legal entity for an otherwise technically decentralized offering of regulated activities available in the system, regardless of who has developed them in practice.

In relation to issuances, e-money tokens (EMT) and asset-referenced tokens (ART) should also be distinguished from issuances of other crypto-assets. The issuance of EMTs and ARTs involves compliance with a number of operational and organizational requirements. However, all issuances of crypto-assets are only covered by MiCA if they are offered to the public and if the issuer is identifiable. That is, there must be a legal entity behind the issuance to which the associated rights can be directed.

Reading guide

The next section elaborates upon the background for this briefing and guidance. Section 3 is a brief introduction to how the architecture of DeFI generally works. Section 4 reviews the Danish FSA's approach to the assessment of decentralisation, including the need to be able to identify a legal entity behind the offering and to be able to identify the specific activity that a legal entity has disposal over. Section 5 reviews the Danish FSA's principles for the assessment of decentralisation under MiCA.

[1] The concept of "conventional blockchains" which is used in this briefing is defined in more detail in Section 3 and Annex 1.

2. Background

MiCA, which enters into force on 30 December 2024, aims to regulate certain crypto asset issuers and crypto asset service providers. The regulation covers the legal entity providing the regulated activity. However, the regulation does not cover the provision of otherwise regulated activities if they are provided in a completely decentralised manner.

It is specified in recital 22 of MiCA that:

> *"This Regulation should apply to natural and legal persons and certain other undertakings and to the crypto-asset services and activities performed, provided or controlled, directly or indirectly, by them, including when part of such activities or services is performed in a decentralised manner. Where crypto-asset services are provided in a fully decentralised manner without any intermediary, they should not fall within the scope of this Regulation. This Regulation covers the rights and obligations of issuers of crypto-assets, offerors, persons seeking admission to trading of crypto-assets and crypto-asset service providers. Where crypto-assets have no identifiable issuer, they should not fall within the scope of Title II, III or IV of this Regulation. Crypto-asset service providers providing services in respect of such crypto-assets should, however, be covered by this Regulation."*

As can be read, MiCA does not address when a service can be regarded as being offered in a fully decentralised manner. MiCA or other legal acts also do not contain a clear definition of the concept of 'decentralised'. It is thus a new concept.

In 2022, the Danish FSA established a working group for decentralised finance. The purpose was to specify a number of principles that the Danish FSA can use as a basis for assessing when issuances and services otherwise regulated by MiCA fall outside the scope of the regulation because they are offered in a decentralised manner.

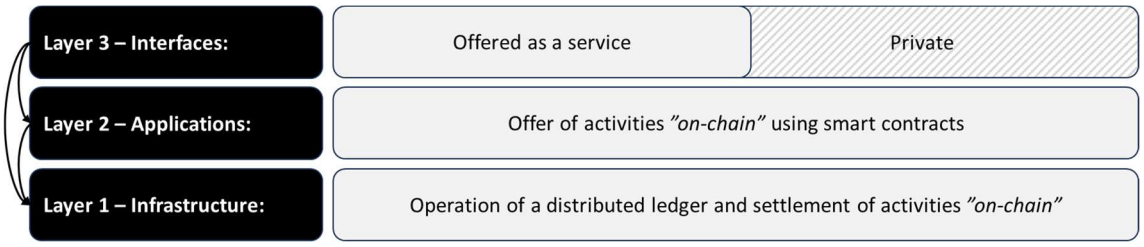
3. The architecture behind decentralised finance (DeFi)

The term DLT encompasses different variations of the technology, which can both resemble or be structured differently from blockchains. This includes, for example, more centralised variations or variations that use different methods for recording data in the distributed ledger. The Danish FSA's principles for assessing decentralisation in the provision of regulated activities are based on the conventional blockchain, but these principles can generally also be applied to other variations of DLT

In this briefing, the term 'conventional blockchains' is used as a collective term for blockchains that are structured with an application layer that allows the use of smart contracts, just like Ethereum does.

Figure 2 divides the conventional blockchain into three layers and each layer is then explained individually.

Figure 2 - The three layers of the conventional blockchain



Note: Private interfaces are generally not covered by MiCA.
Source: The Danish Financial Supervisory Authority

The infrastructure layer is the underlying registry where a set of network nodes settle and register transactions using a consensus mechanism, cf. Annex 1.1. The application layer enables the issuance of smart contracts. Smart contracts are software programs available on the blockchain that perform the crypto-asset transactions that the developer has programmed them to perform, cf. Annex 1.2. Smart contracts also enable users to issue their own crypto assets on the blockchain in question. These crypto assets are usually called tokens.

For a user to access services on a blockchain, it requires that the user has access to interact with the application or infrastructure layer. In practice, this is done through interfaces, cf. Annex 1.3. The term 'interfaces' includes both interfaces that are accessible to users and private interfaces. Private interfaces include both integrations developed by private users themselves and software developed by third parties that users can use to interact with the blockchain. The latter, however, is only considered private if the user has control over the software. Offering an interface as a service therefore implies that a third party controls the software that users can use to interact with the blockchain. This is typically the case for interfaces accessible through a web platform or an application, such as on the user's smartphone.

4. The Danish FSA's approach to decentralisation

MiCA regulates both crypto-asset issuances and crypto-asset services (regulated activities), cf. Annex 2. Pursuant to MiCA, the issuances can be divided into two types: issuances of so-called 'stablecoins' and issuances of other crypto assets.

The Danish FSA's principles for assessing decentralisation apply to the business models covered by MiCA. Other financial regulation does not contain an explicit exemption option for decentralised activities in the same manner. Directive on markets in financial instruments[2] (MiFID II) does for example not include a recital stating that a decentralised offering of a marketplace for trading of traditional financial instruments issued on blockchain is exempt. The Danish FSA does not further address this issue in this briefing.

4.1 Not all DeFI is offered in a decentralised manner

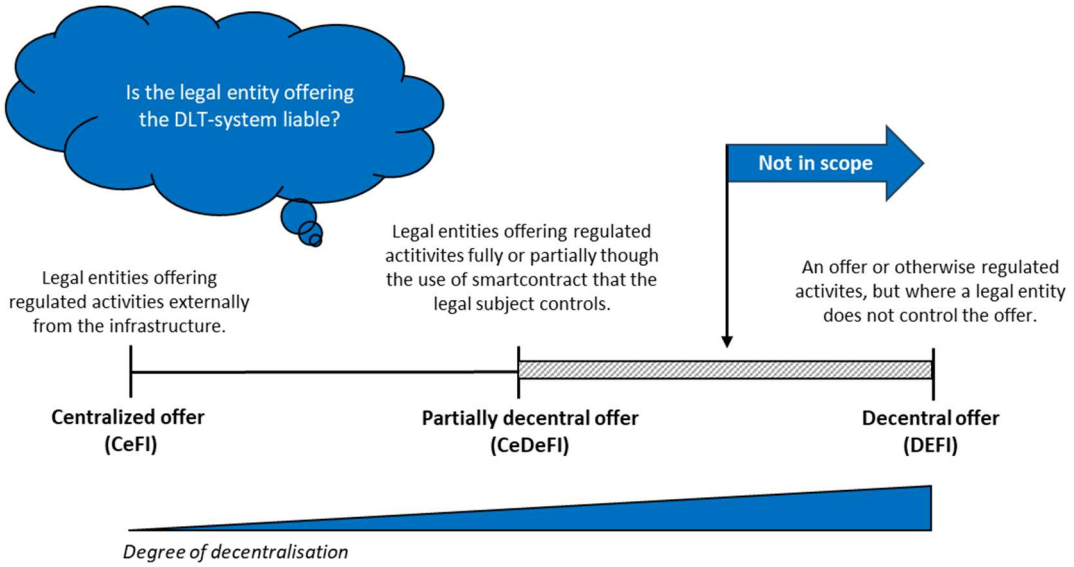
Figure 3 shows the Danish FSA's basic categorisation of different types of offerings of regulated activities in the crypto-asset market. When regulated activities are centrally offered

[2] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014.

(CeFI), a legal entity will have full control over the activity. In these cases, the regulated activities are offered exclusively through the companies' own systems and cannot be accessed directly on a conventional blockchain. In a partially decentralised provision of regulated activities (CeDeFI), a legal entity also controls the activities. However, they are offered in part or in full using smart contracts which are made available through the application layer. The provision of regulated activities can only be classified as decentralised (DeFI) if a legal entity cannot control the activity. In these cases, the regulated activity or the right of disposal over the activity will be structured through the use of smart contracts made available in the application layer.

It cannot be ruled out that a legal entity can develop and independently dispose of a DLT system in which regulated activities can be offered using smart contracts. This is generally not the practice today, and the assessment of whether the legal entity behind the DLT system controls the supply of regulated activities is complex. However, it cannot be ruled out that a legal entity behind the offering of a DLT system could in some cases be subject to the obligations under MiCA.

Figure 3 - Different types of offers



Source: The Danish Financial Supervisory Authority

The question of which regulated activities a legal entity actually has at its disposal is also a key factor in the Danish FSA's approach to the area of application of MiCA. Offering access to a decentralized service, for example, does not necessarily mean that the provider controls and thereby can be held responsible for the provision of that service The following example aims to clarify this. The example also forms the basis for a more detailed specification of the Danish FSA's principles for the assessment of decentralisation in Section 5.

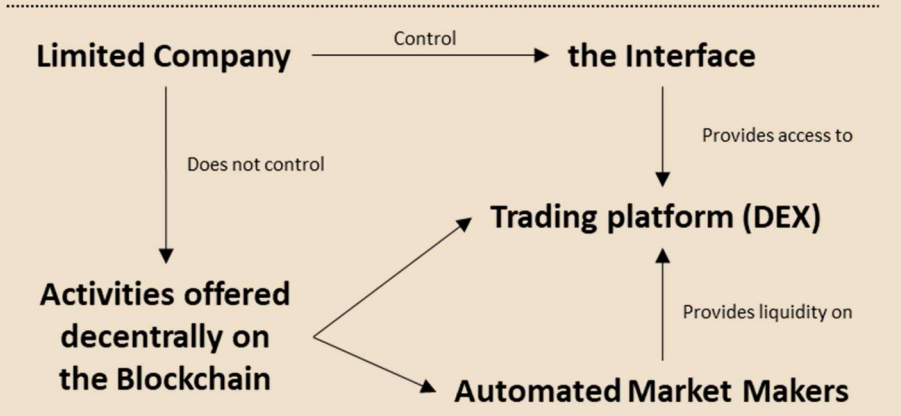
4.2 An example of making available a regulated decentralised service

Users typically access the crypto-asset markets via a mobile app that can be downloaded from an app store or website. Such interfaces are the usual way to access decentralised services. Therefore, it is generally also possible to identify a person behind the offering of an

interface as either the publisher of the app in the app store or the owner of the domain where the interface can be accessed.

Box 1 - Assumptions for the example[3, 4]

A traditional limited liability company provides an interface to a decentralised exchange (DEX). Liquidity on the DEX is provided by so-called Automated Market Makers (AMMs), which are also offered as decentralised services. The limited company therefore only controls the interface.



Source: The Danish Financial Supervisory Authority

The regulated activities relevant to the example reflect to some extent the activities regulated under MiFID II. This is also stated in Article 60(3) of MiCA. The regulatory classification under MiFID II therefore also forms the basis for the classification of similar activities under MiCA:

- MiFID II: Receiving and transmitting customer orders with one or more financial instruments
  - MiCA: Receiving and transmitting orders for crypto assets
- MiFID II: Execution of orders for the client's account with financial instruments
  - MiCA: Execution of orders for crypto assets on behalf of the client
- MiFID II: Operation of a multilateral trading facility for financial instruments
  - MiCA: Operating a trading platform for crypto assets
- MiFID II: Dealing financial instruments on own account
  - MiCA: Exchange between crypto assets and funds or other crypto assets.

[3] A trading platform is defined in Article 3(1)(18) of MiCA as: *"operation of a trading platform for crypto-assets' means the management of one or more multilateral systems, which bring together or facilitate the bringing together of multiple third-party purchasing and selling interests in crypto-assets, in the system and in accordance with its rules, in a way that results in a contract, either by exchanging crypto-assets for funds or by the exchange of crypto-assets for other crypto-assets."*

[4] An AAM (automated market maker) provides liquidity through so-called liquidity pools. In these pools, liquidity providers can deposit their assets in exchange for the right to a total share of the pool's assets and the right to receive a trading fee. A liquidity pool is also managed through the use of smart contracts, which specify a logic for pricing the assets included in the pool.

For both scenarios in the example, the limited liability company must have authorisation solely for the activities it controls. Identifying the actual activity performed therefore requires a technical understanding of the setup of the decentralised offer that the interface in question integrates with.

Financial companies execute client orders when they place orders on a multilateral trading facility on behalf of their clients. An example of this is a customer requesting to buy a share through their online banking solution, after which the credit institution buys the share for the customer on a trading platform such as Nasdaq Nordic. A credit institution executes a customer order in the same manner if the credit institution executes the trade by selling from its own holdings of the share to the customer. The latter form of order execution is an internalisation of the trade and requires authorised to deal on own account, cf. MiFID II.

Similarly, the Danish FSA considers the provider of the interface to be an order executor if the provider makes available to the user the software that converts the user's trading interests into an order entry on the DEX. Because the limited liability company has control of this software, the company also enters into an agreement with the user that the user can use the company's service to place orders on a DEX. Conversely, the limited liability company cannot be considered a provider of a trading platform for crypto assets because it does not control the smart contracts that make up the DEX.

Exchange services in MiCA are considered to be the same as dealing on own account under MiFID II. If a credit institution fulfils a customer's request to buy a share by selling the share from its own trading portfolio. The credit institution will also be an order executor, but because the permission to deal on own account also includes permission to execute the orders, the credit institution does not need a separate permission to execute orders on behalf of the customer unless the credit institution also trades on the DEX on behalf of the customer. If a legal entity transmits the order to the credit institution on behalf of the customer, the credit institution must be authorised to receive and transmit customer orders. The same would generally also apply to the interface in the example if the software allows users to communicate with a completely decentralised exchange service. It could potentially be in cases where the trade is done directly with an AMM, or in cases where a set of AMMs are predetermined as the only counterparties (liquidity providers) to trades that are matched in that or those smart contracts that constitute the DEX.

5. Principles for assessing decentralisation

This section reviews the principles that form the basis for the Danish FSA's assessment of whether a regulated activity is offered in a decentralised manner. In all cases, it will be necessary to concretely assess how the specific business model and the underlying DLT system is structured. In addition, the level of decentralisation can change over time. The establishment of a decentralised organisation will as a general rule start centrally but with a goal of moving towards decentralisation over time.

The Danish FSA's assessment of decentralisation will always be based on the point in time at which a regulated activity becomes available to the public. The offering of a regulated activity cannot be exempted from MiCA simply because the provider aims to make the tender

decentralised. The moment a regulated offer becomes decentralised, there will no longer be a legal entity to impose the licensing obligation on. This could, for example, be because the company that holds the license is either dissolved or for some other reason no longer controls the offer at the time the offer becomes decentralised.

5.1 MiCA requires a contractual relationship between two legal entities

For the provision of a service to be regulated, two or more parties must enter into a valid agreement to provide and receive the service. This applies in MiCA as well as in other financial regulation. Only legal entities can enter into contracts and therefore MiCA only applies in cases where the issuer or provider is a legal entity.

Legal entities and valid contractual relationships

A legal entity is a legal or natural person on whom rights and obligations can be imposed. This presupposes that the legal or natural person can dispose of these rights or obligations. This means, for example, that the legal entity has the power to fulfil, acquire or give up these rights. In order for a specific actor to have rights and obligations in connection with a regulated activity and thus to constitute a legal entity, it requires that the specific actor can control the activity. Please note that not all types of partnerships are independent legal entities[5].

What is essential for the Danish FSA's assessment of decentralisation is whether a party can be subject to the obligations specified in MiCA. This involves assessing whether a legal entity enters into a valid contract with a recipient of a service to provide a regulated activity. A contract is only valid if it is concluded between legal entities who make binding declarations of intent.

A declaration of intent is any statement by a party that they are willing to commit to another party, for example, by providing a crypto-asset service. There are no formal requirements for how a declaration of intent should be made. For example, making a service freely available to the public can constitute a statement of intent. Binding means, among other things, that the party making the declaration of intent also has the necessary legal capacity to enter into a binding agreement. Danish law does not contain an exhaustive list of invalid declarations of intent. Section 3 of the Danish Contracts Act regulates situations where a declaration of intent is not in accordance with the declaring party's will, but the Danish Contracts Act does not address cases where a declaring party lacks legal capacity. An example of this could be that the declaring party is under guardianship pursuant to Chapter 7 of the Danish Guardianship Act.

Software cannot independently enter into valid agreements

Under normal circumstances, the above does not present challenges in the provision of financial services or issuance of financial assets. This is because such activities can usually be attributed to a natural or legal person. However, the assessment can be challenged when an offer is executed using smart contracts on a conventional blockchain. Smart contracts are types of software that inherently have no will of their own but only performs the actions for

[5] The assessment should fundamentally relate to whether the partnership has such a character and is sufficiently binding for the community to be considered a legal entity in its own right. A partnership where several actors interact together - without a form of organisational community that goes beyond the internal relationship between the actors - will probably not be sufficient. The assessment will therefore require an identification of the conditions that determine that a legal entity can be said to be established.

which they are programmed. They can therefore neither constitute a legal entity nor enter into a binding declaration of intent - and thus neither incur legal liability nor enter into contracts in the traditional sense. On the other hand, software programs implement the will of others, such as the will of the natural or legal person who controls the software. However, a natural or legal person does not always control the offering of the regulated activities when the offering is carried out using smart contracts. The flexibility of the application layer on a conventional blockchain also enables a more decentralised arrangement of types of partnerships than traditional ones, such as limited liability companies. Therefore, in cases where such a partnership has a supply of regulated activities using smart contracts, it is necessary to assess whether the partnership is a legal entity.

Significance for the Danish FSA's assessment of decentralisation
The decisive factor for the Danish FSA's assessment of decentralisation is whether a legal entity is behind the issuance of a crypto asset or the provision of a crypto-asset service. For example, a legal entity could be a company that issues a crypto asset or has the power to dispose of the smart contracts used in the provision of crypto-asset services. If the right of disposal is structured in a more decentralised type of partnership, the Danish FSA will first look at whether the partnership can be equated with a traditional legal entity and then look at whether it is possible to identify conditions that can qualify the partnership or participants in the partnership as a legal entity.

The Danish FSA's assessment of decentralisation is thus two-fold:

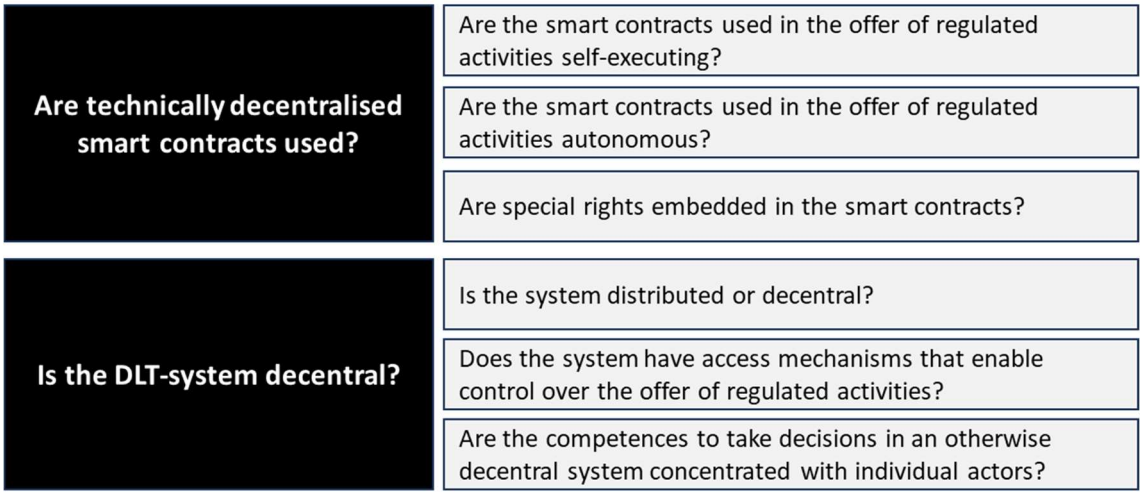
1. **Technical decentralisation:** The Danish FSA assesses whether the regulated activity is offered exclusively by the use of smart contracts that a legal entity cannot be said to control.
2. **Decentralised governance:** If the technical provision of a regulated activity is not assessed as decentralised, the Danish FSA will assess whether the managerial control over the offer can be attributed to a legal entity.

5.2 Technical decentralisation in the provision of regulated activities

Figure 4 is a summary of the questions that form the basis for the Danish FSA's assessment of technical decentralisation. Participation in the provision of the DLT system does not in itself constitute a regulated activity, but in some cases, it may entail liability for the regulated activities that can be accessed in the system. Therefore, the Danish FSA also reviews whether providers of DLT systems can be said to have control over regulated activities available in the systems.

Not all regulated activities can be offered technically decentralised. Smart contracts can only perform tasks according to a certain pre-programmed logic. Therefore, smart contracts cannot be used to provide services that require interaction with a customer or that require human judgment. Examples of such services could be investment advice and discretionary portfolio management plans.

Figure 4 - Questions to be clarified in the technical decentralisation assessment



Source: The Danish Financial Supervisory Authority

5.2.1 Offering regulated activities with smart contracts

Smart contracts on conventional blockchains can perform actions with crypto assets made available on the blockchain. They can therefore be used both to issue crypto assets and to provide multiple crypto-asset services covered by MiCA.

5.2.1.1 Self-executing programmable actions

Smart contracts issued on Ethereum are by definition self-executing. This means that they will perform the actions they are programmed to perform when requested by the user if the request meets the requirements for execution. In the example in Section 4.2, this means that the DEX will automatically start executing the order as soon as the interface has communicated the order to the smart contracts. If the user requests to trade a crypto asset that does not meet the rules for trading on the DEX, the order will be rejected.

> *Self-executing software is a prerequisite for technical decentralisation. The Danish FSA will therefore assess whether the software used in the provision of a regulated activity can independently carry out regulated activities in the same way as natural and legal persons.*

The action a user takes when interacting with smart contracts can be compared to the way a customer uses a financial company when receiving a service. However, a self-executing smart contract cannot independently constitute a legal subject of a contract because it cannot make binding declarations of intent.

DLT systems can also be set up with other forms of smart contract-like functionality. For example, the Danish FSA was introduced to the concept of Smart Financial Instruments (SFI) during testing in the Danish FSA's regulatory sandbox, FT Lab. An SFI is a digital representation of an asset that is also programmed with functionality that specifies how a number of actions associated with the asset's rights should be executed. For example, this could be conditions for transfers of the asset's financial rights. However, unlike Ethereum smart

contracts, an SFI cannot independently execute the actions. They can only be executed through other imbedded functionalities in the DLT system in which the SFI is issued. For example, a natural person can actively authorise and initiate transfers of the inherent financial rights and then complete the transfer in the system.

The Danish FSA was also introduced to Algorand's Stateless Smart Contract Technology (SSCT) in an FT Lab course. Among other things, this variation of the smart contract concept allows people to delegate access to perform activities with assets associated with their accounts on the blockchain by issuing so-called 'delegated keys'. Essentially, a person signs a delegated key which, for example, contains one or more transactions they want to perform with their private key. Control of the delegated key can then be transferred to another actor who stores the key locally - and not on the blockchain. This gives this actor the right to subsequently initiate the signed transactions on Algorand's blockchain.

For both examples, these types of smart contract-like functionalities cannot be said to execute activities independently. In its assessment of whether a regulated activity is technically decentralised, the Danish FSA distinguishes between activities that:

- are offered through self-executing smart contracts
- use software with similar functionality but is not self-executing.

The fact that the software is self-executing is a prerequisite for a regulated activity to be classified as technically decentralised.

5.2.1.2 Autonomy of smart contracts

The Danish FSA does not by definition consider the provision of regulated activities using self-executing smart contracts to be technically decentralised. Although the issuer cannot modify or delete the smart contract or its programming after it has been made available on a conventional blockchain, the smart contract can be programmed with editing access to the inputs that the contract uses in the execution of the programmed actions.

> *The Danish FSA assesses the autonomy of smart contracts used in the provision of a regulated activity. The degree of decentralisation will, all else being equal, decrease as the degree of control over the smart contract increases.*

If the smart contracts that make up the DEX in the example in Section 4.2 are programmed with specific editing accesses, it should be considered whether the editing accesses have a significant impact on the offering of the trading platform. For example, this could be in cases where a party, has the ability to control which public addresses can provide liquidity on the DEX or which users can buy crypto assets on the DEX. It could also be in cases where the editing access makes it possible to customise the structure of the integration between the set of smart contracts that make up the DEX, for example, in a situation where a new smart contract needs to replace an old and outdated smart contract. It could also be in cases where an external data source (a so-called 'oracle'[6])used in asset pricing needs to be updated.

[6] An oracle is an off-chain data source that provides input to a smart contract.

In its assessment of whether a smart contract can be considered technically decentralised, the Danish FSA therefore further distinguishes between so-called 'autonomous smart contracts' and smart contracts with built-in editing access:

- Autonomous smart contracts are self-executing and perform the programmed actions without the possibility of adjusting the inputs specified in the code of the smart contract.
- Smart contracts with built-in editing accesses are also self-executing, but they have embedded permissions in the programming that enable adjustments of the inputs that the smart contract uses to execute its programmed actions.

If an editing access gives control over matters that are central to the provision of the regulated activity, it indicates a degree of centralisation in the offer. It is therefore crucial for the assessment whether the elements of the activity to which the access relates are regulated.

5.2.1.3 Special inherent rights

In addition to having embedded editing access, smart contracts can also be structured with immutable inherent rights.

> *The Danish FSA will assess whether one or more legal entities have immutable rights embedded in a smart contract used in the provision of regulated activities and whether these rights are of such a nature that the legal entity can be said to control the provision of the activity.*

For example, a smart contract can be structured with specific remuneration flows. In the DEX example in Section 4.2, it could be envisaged that specific public addresses on the blockchain receive a payment for each completed trade. Such public addresses can, for example, be controlled by people who have been involved in developing the DEX. It is therefore possible that inherent links could be demonstrated between smart contracts and persons that would suggest that these persons are the legal entities in control of the provision of the regulated activity. The Danish FSA will therefore also consider whether third parties have special rights in connection with the provision of a regulated activity with smart contracts[7].

5.2.2 Potential implications of a centralised DLT system

Conventional blockchains form the basis for the principles of the Danish FSA's assessment of decentralisation. However, regulated activities can also be offered in other types of DLT systems which, for example, are more centralised. There may therefore be cases where the assessment of whether a regulated activity is offered in a decentralised manner must also include an assessment of whether the legal entities that control the DLT system also control the provision of the activity.

5.2.2.1 Distribution versus decentralisation

The definition of a DLT system in MiCA does not imply that the system is offered and operated by different independent third parties - although this is the general starting point for the

[7] This also raises the issue that decentralised financial services issued in immutable systems can neither be deleted or decommissioned.

conventional blockchain. A single legal entity can operate a distributed ledger across multiple network nodes located in different locations but still control them all. This highlights why it is crucial to distinguish between distribution and decentralisation.

> *The Danish FSA will assess whether the operation of the network nodes in a DLT system is in practice decentralised. If the DLT system is not decentralised, it is assessed whether the provider is obligated under MiCA in relation to the regulated activities that can be accessed in the system.*

Distribution covers distribution across network nodes. Decentralisation can only occur with distribution across independent third parties (independent legal entities) where each third party only has control over its own network nodes - and not the DLT system as a whole. Furthermore, distribution between several independent legal entities does not mean that the supply is decentralised. The decisive factor here is whether the partnership can in practice be said to be the legal entity controlling the offer, cf. Section 5.3.

The design of the consensus mechanism indicates whether the conditions for decentralisation are present. Widely used consensus mechanisms for the conventional blockchain such as Proof-of-Work (PoW) and Proof-of-Stake (PoS), for example, assume that new blocks can only be added to the ledger if there is agreement on the validity of the block across the participating network nodes. The same type of consensus mechanism is not needed in DLT systems, where one or more legal entities take responsibility for the offer. Therefore, centralised DLT systems can as a general rule use consensus mechanisms that do not require agreement across all network nodes.

The distinction between distributed (centralised) and decentralised DLT systems is not in itself a decisive factor when assessing whether the legal entity behind a centralised system can be said to independently control the regulated activities in the system. Therefore, the responsibilities and duties related to offering and carrying out regulated activities should also be clarified. Relevant circumstances could, for example, be cases where the provider can reverse entries in the general ledger through chargebacks or has control over users' access to make available smart contracts used to offer regulated activities in the system.

5.2.2.2 Control over access mechanisms

The Bank for International Settlement (BIS) characterises DLT systems as either centralised or decentralised in the article 'On the Future of Securities Settlement'[8]. The BIS distinguishes between permissioned and permissionless as well as private and public DLT systems. Permissionless and public systems, such as conventional blockchains, only require the participant's pseudonym - the public part of the participant's key pair - for identification[9]. On the other hand, a permissioned system has established an actual access mechanism for participation in operations. This is also how private DLT systems set access mechanisms for users of the system.

[8] https://www.bis.org/publ/qtrpdf/r_qt2003i.htm

[9] The barrier to participate in the operation of a permissionless DLT system is therefore lower, which can speak in favour of decentralisation. In practice, however, it is possible that the same person participates in operations with several different pseudonyms and thus possesses more significant decision-making powers.

The Danish FSA will assess whether a legal entity has the power to either make available or access technical decentralised regulated activities in the DLT system. The greater the degree of control the legal entity has, the more it can be argued that the legal entity controls the supply of the regulated activities - and is therefore obligated under MiCA.

Access mechanisms can be structured in different ways. Some require personal identification information only while others have more extensive requirements, such as common interest requirements. Among other things, this makes it possible to restrict participants in operations to only operate individual fragments of the overall ledger[10] and to limit users of the system to people who have gone through relevant onboarding processes. Similarly, access mechanisms can set conditions for when participation in the DLT system can be terminated. Control over the access mechanisms in a DLT system is thus also an indication of centralisation in the offer.

The design of access mechanisms for private DLT systems is relevant for the assessment of whether responsibility for technically decentralised regulated activities can be attributed to a legal entity[11]. Control over the framework for user participation in the system can include control over which smart contracts can be made available in the system but it can also involve control over which smart contracts users of the system can access. Control over the access mechanism for participation in operations can also matter. For example, this could be in cases where people operating network nodes are granted special rights to record and reverse records in the distributed ledger. Conditions like these are not typical in conventional blockchains. For example, Ethereum only has format requirements to ensure that the smart contracts developed are compatible with the system.

5.2.2.3 Concentration of decision-making power

Even though the foundation for decentralisation is present, it does not mean that one or more legal entities cannot have control over aspects of the system that in practice indicate centralisation.

The Danish FSA will assess whether one or more legal entities have decision-making powers to an extent that it in practice means that they control the supply of regulated activities in an otherwise decentralised DLT system. A more concentrated distribution of decision-making powers increases the degree of

The decision-making powers regarding, for example, operations and access mechanisms can be concentrated in individual persons (so-called 'whales') or in a group of persons with a common goal (so-called 'governance bodies'), cf. Section 5.3.1.3. If the decision-making

[10] For example, the operational contribution of participating nodes can be limited to a subset of the overall ledger (a fragment). Fragmentation of the ledger can have different purposes. It can be a fragmentation of the full data set for the sole purpose of decreasing the latency of the system, but fragmentation can also be more focused on functionality. For example, an FT Lab test of a DLT-based securities trading system showed that clusters of network nodes can be limited to processing the fragments of data needed to perform a given function for the system as a whole.

[11] Note that this means there is a distinction between access criteria built into the programming of the smart contracts and thus the assessment of the autonomy of the smart contracts used, cf. Section 5.1.1.

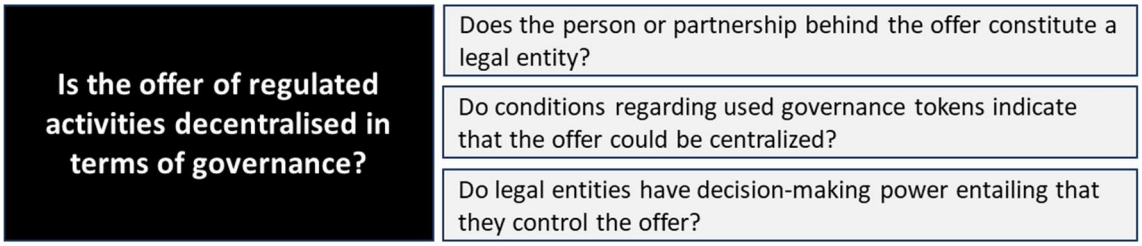
powers are concentrated in one legal entity, this is an indication of centralisation in the offer. This may argue in favor of the legal entity being subject to the obligations of MiCA in relation to the provision of regulated activities.

To the extent that it is possible and relevant, the Danish FSA will therefore include the degree of concentration of decision-making powers in the assessment of whether individual persons or groups of persons may constitute legal entities for the provision of otherwise technically decentralised regulated activities in DLT systems.

5.3 Decentralised governance of regulated activities

Figure 5 summarises the factors that form the basis for the Danish FSA's approach to assessing decentralisation in the governance layer. The provision of a regulated activity can be decentralised even if it is not technically decentralised. This is the case if there is no legal entity that has governance control over the offer.

Figure 5 - Questions for clarification in the assessment of decentralised governance



Source: The Danish Financial Supervisory Authority

A partnership can only be considered decentralised from a governance perspective if the governance structure does not mean that the partnership as a collective constitutes a legal person - and thus a legal entity. If the partnership as a whole does not constitute a legal entity, the Danish FSA will also assess whether individual actors (natural or legal persons) independently constitute a legal entity responsible for the regulated activity.

5.3.1 The DAO concept as a starting point for the assessment

A decentralised autonomous organisation (DAO) is not a legally defined concept in Denmark. The concept is based on the idea of using conventional blockchains and smart contracts to create decentralised partnerships. In the following, the term DAO is used for a cooperative providing financial services that meet both of the following conditions:

- they are not founded in a formal legal partnership
- they use so-called 'governance tokens' in combination with smart contracts to make decisions in the organisation (discussed in more detail in Section 5.3.2.2).

5.3.1.1 The partnership as an independent legal entity

In Denmark, companies are generally freedom of contract in corporate law. This means that the members of a company can set up a partnership in one of the existing company types or create a new type of company if this is deemed to be appropriate. Danish law makes a fundamental distinction between partnerships which consist of limited liability companies whose management structure is regulated by a number of mandatory rules and general partnerships

which are based to a greater extent on the contractual relationship between the parties to the partnership. Whether a collaboration is a general partnership depends on a specific assessment which, among other things, involves looking at how the collaboration appears from the outside and how the contractual relationship between the parties of the collaboration is structured. However, it is a prerequisite that the partnership is based on an agreement between two or more persons to conduct joint business activities.

The Danish FSA will assess whether a partnership behind a non-technical decentralised offering of a regulated activity can constitute a legal entity in the form of a legal person, e.g. a general partnership or a limited liability company.

A DAO is a different form of partnership than the traditional types of companies, although they may have some similarities. For example, there is no requirement for a general partnership to have a governing body. In comparison, many DAOs are trying to eliminate traditional management bodies such as the board of directors and executive board. They do this by using so-called 'governance tokens', which basically represent the decision-making powers of the owners in a partnership. This is explained in more detail in the next section. In stock companies, the shareholders' powers to make decisions also require participation in the general assembly. Holders of governance tokens can usually only exercise their decision-making powers if they cast their votes in proposals in the partnership or DAO. In these cases, the governance structures can be compared to those of a general assembly in a stock company. Therefore, it is not always clear that all proclaimed variations of the DAO concept in practice differ from traditional company forms

It is therefore not always the case that all proclaimed variations of the DAO concept differ in practice from traditional types of companies.

The Ookie Dao ruling from the United States is an example of a decision where a DAO was treated as a traditional type of company. Ookie Dao ran a service that, among other things, offered trading in futures contracts. The court determined that under Califorinia law, the DAO constituted a partnership and that the holders of the DAO's governance tokens were partners in the partnership[12]. In a Danish context, a partnership is most similar to an 'interessentskab', where all participants are jointly and individually liable for the company's obligations. The court emphasized in its decision that the governance tokens issued by Ookie DAO conferred rights to the holders similar to those of partners in a general partnership. Moreover, it was found that the holders' primary intent in acquiring these governance tokens was to obtain these rights.

In its assessment, the Danish FSA will initially consider whether the parties to the partnership can collectively be classified as a legal person providing a regulated activity. If this is the case, the Danish FSA will consider the collective as the legal entity for the requirements for providers in MiCA.

5.3.1.2 Rights and concentrations of governance tokens

Like the concept of DAO, the term governance tokens is not legally defined - neither in Danish or European law. However, the possession of governance tokens is generally a requirement

[12] Christian Sarcuni, et al v. bZx DAO, et al (Case No.: 22-cv-618-LAB-DEB)

for people being able to participate in a DAO. A deeper understanding of the distribution of governance tokens and the associated rights is therefore also relevant in the assessment of decentralisation in relation to governance. This applies both in relation to whether a DAO can be equated with a legal person and in relation to whether the possession of governance tokens can independently entail obligations under MiCA.

> *The Danish FSA will assess whether the rights, the concentration of holdings and the method of distribution of governance tokens give rise to the partnership or individual members of the partnership being considered a legal entity for the provision of regulated activities.*

Governance tokens, like other tokens, can be structured with the rights that the issuer wants them to have. They often contain voting rights and their possession can also be a condition for proposing resolutions in a DAO. In addition, if the service offered is profit-driven, they usually also entitle you to a share of the profit. In some cases, the rights can be exercised in a dividend-like manner where a DAO pays out a share of the accumulated profit to holders of governance tokens based on a vote. Other times, the financial rights are specified in the smart contract code so that profits are distributed and paid out as they are generated. These circumstances show that the rights represented by governance tokens can, to some extent, resemble the rights of owners of traditional types of companies. The governance rights that come with different governance tokens can differ significantly. Some governance tokens give holders the right to participate in decisions about the core services offered. Others only allow the holders to participate in decisions of a secondary nature to the core service, such as decisions about the service logo, name, etc.

In assessing decentralization, it is pivotal to examine the rights associated with the tokens in relation with the organisation of the holders. If these rights enable decisions on fundamental matters related to the provision of regulated activities, such as access to a service, this suggests centralization. This assessment is further supported if ownership of governance tokens is concentrated among a few actors.

Governance tokens, unlike traditional shares in companies, can be obtained both voluntarily and involuntarily:

- A voluntary obtaining is done as an investment in so-called ICOs.
- An involuntary obtaining happens in one of the following two ways:
    - through the use of the underlying service
    - as part of the marketing of the service.

For both involuntary scenarios, governance tokens are distributed regardless of whether the recipient wants them. In the example in Section 4.2, this could be in cases where a DEX is operated by a DAO and users of the DEX receive governance tokens for the DAO every time they trade on the DEX. This could also be done through so-called ‘airdrops’, where the DAO distributes governance tokens to holders of other tokens as part of its marketing.

It is therefore central to the Danish FSA's assessment of decentralised governance to consider which rights are associated with governance tokens and how they are acquired. This is especially true when it comes to assessing whether the partnership constitutes a traditional type of company. However, this also applies if the partnership does not collectively constitute a legal entity. This could be, for example, where decision-making powers are concentrated in the hands of a few individuals allowing them to control the regulated activity, such as where a single person holds over 50% of the governance tokens issued and therefore controls the supply of the regulated activity.

5.3.1.3 Independent decision-making legal entities

Even if a DAO as a whole is not classified as a independent legal entity, such as a traditional type of company, it is still relevant to assess whether individuals or governing bodies consisting of natural or legal persons can constitute legal entities in relation to the provision of the regulated activities. More specifically, this applies in cases where actors that may constitute legal entities have a role that allows them to independently control or manage the offer. Such actors are typically part of the DAO, but this is not a prerequisite for delegating decision-making powers for the DAO. The actors can also be hired by the DAO in return for some form of payment, for example, in DAO governance tokens or other crypto assets.

> *The Danish FSA will assess whether legal entities in the form of individuals or smaller partnerships (bodies) possess decision-making powers to such an extent that they control the provision of regulated activities, regardless of whether they hold a share in the collective partnership.*

There may be several reasons why decisions and responsibilities are outsourced from DAO members to these types of actors. For example, it may be for operational efficiency reasons in cases where certain operational decisions cannot await a decision-making process in the DAO. In practice, a DAO can delegate all kinds of tasks to actors that do not hold governance tokens, such as managerial tasks, compliance and risk management tasks or administrative tasks. The delegated competencies of the actors may resemble competencies that usually lie with executive boards or boards of directors in traditional types of companies. In this way, the actors can also gain decision-making powers that allow them to control the regulated elements of the DAO's activities without the influence of other participants in the DAO.

There may therefore be cases where such bodies, depending on their specific managerial powers, control the regulated activity - and must therefore be subject to the applicable obligations of MiCA. In the example in Section 4.2, this could be in cases where the body has full discretion over which AMMs can provide liquidity on the DEX.

The Danish FSA's assessment of whether a DAO is governed in a decentralised manner therefore also involves looking at the powers held by any potential governance bodies. It is particularly important whether it is possible to identify persons with managerial authority to dispose of the regulated activity, regardless of whether these persons are holders of the governance tokens. The assessment will also differentiate between cases where the decision-making power relates to the provision of the regulated activity and cases where the decision-making power is limited to matters secondary to the regulated activity.

6. Application and further development of the priciples

The Danish FSA's purpose with this guidance is to inform relevant market participants about the principles used by The Danish FSA for assessing decentralisation in the crypto-assets market. These principles and the outlined considerations are not exhaustive and can only be used as a baseline for the assessment. The Danish FSA's final decision will always be based on the concrete circumstances of the specific activity.

Actors for whom it is relevant to determine whether an offering of regulated activities under MiCA can be considered decentralised ultimately bear the responsibility for assessing whether the offering falls within the scope of MiCA. The Danish FSA emphasizes that an incorrect classification of an offering as fully decentralised and thereby exempt from MiCA may constitute provision of unlawful services. In this context, it should be highlighted that the Danish FSA is open to dialogue with relevant actors regarding the evaluation and interpretation of the principles for the specific offering. Relevant actors should be aware that complete decentralisation requires meeting numerous criteria and that interfaces for decentralized services may fall under MiCA, regardless.

The principles have been developed based on the work of the Danih FSA's working group on decentralised finance and ongoing supervisory activities. However, as new innovative solutions and business models in the crypto-assets markets and within decentralized finance are continually developed, the FSA remains attentive to circumstances that may necessitate adjustments or updates to these principles. The FSA will address these developments in its ongoing supervisory activities. The Danish FSA will strive to continuously develop the principles to align with efforts towards harmonizing the approach to assessing decentralization in The European Union.

The Danish FSA welcomes feedback from private actors interested in shaping the FSA's evaluation methods for decentralisation.

Annexes

Annex 1 - The three layers of the conventional blockchain

Conventional blockchains, we refer to DLT systems that are structured similarly to the Ethereum blockchain. This means that the system includes an application layer that enables the use of smart contracts. In addition, there must be free access to participate as a network node in the operation of the full distributed ledger and any user must be able to access and make use of the blockchain's functionality. As shown in Figure B1, a conventional blockchain can therefore also be characterised as permissionless, public and non-hierarchical.

Figure B1 - Elements of a distributed general ledger

Updating the ledger	Permissionless	Anyone can validate transactions on the ledger.
	Permissioned	Only trusted parties can validate transactions on the ledger.
Access to use the ledger	Public	Anyone can read and initiate transactions on the ledger.
	Private	Only trusted parties can read and initiate transactions on the ledger.
Access to view the ledger	Non-hierarchical	Everyone can hold a full copy of the ledger and can read all the information on the ledger.
	Hierarchical	Only some parties can hold a full copy of the ledger or read all information on the ledger.

Source: Bank for International Settlements (BIS)

B1.1 The infrastructure layer

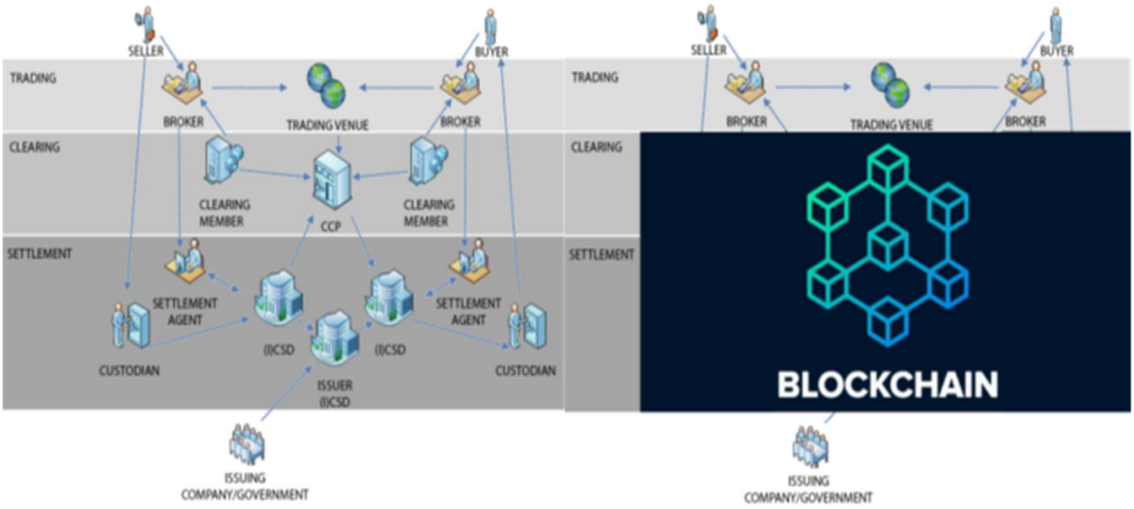
MiCA defines a DLT in Article 3(1)(1) as: *"... a type of technology that support the distributed recording of encrypted data."* This broad definition allows for some variation in the type of systems that can be covered by the regulation. Article 3(1)(2-4) specify the detailed criteria for the definition of a distributed ledger:

- **Distributed ledger:** An information registry that records transactions and is shared and synchronised between a set of DLT nodes using a consensus mechanism.
- **Consensus mechanism:** Rules and procedures by which DLT nodes agree that a transaction has been validated.
- **DLT network node:** A networked device or process that contains a complete or partial copy of records of all transactions in a distributed ledger.

DLT systems can essentially be viewed as the systems that can be used in the provision of regulated activities under MiCA. Today, these will often be conventional blockchains. However, DLT systems can have broader applications Figure B1.1 illustrates how blockchain, for example, can replace the step-by-step settlement process in the current arrangement of capital market infrastructure - an area of application that the Danish FSA has also investigated for a more centralised variation of DLT[13]. The Danish FSA has also examined how blockchain can be used as an alternative to the existing payment infrastructure[14].

[13]The Danish FSA's briefing: "DLT creates new opportunities for capital markets infrastructure, and the new DLT Pilot Regulation can help the technology to take off."
[14] The Danish FSA's briefing: "Blockchain technology can provide an efficient infrastructure for payment services".

Figure B1.1 - Use of blockchains in capital market infrastructure



Source: From a presentation by a participant in the Danish FSA's working group for decentralised finance.

The definition of DLT assumes that the ledger is distributed. In other words, that the ledger is replicated and synchronised across a peer-to-peer (P2P) network of nodes. A distributed ledger differs from a centralised ledger which is stored and operated at a central network node and thus also constitutes a so-called 'single point of failure'. Synchronising and replicating the ledger mitigates the risk of it becoming inaccessible if, for example, a network node is hacked or breaks down.

In most decentralised DLT systems, each node typically stores and maintains the full ledger and contributes to validating and including new data on an ongoing basis. This is done in accordance with the consensus mechanism which coordinates the operational contributions of individual nodes and ensures that registrations only occur if consensus is reached among the nodes on the validity of the registration.

There are many different consensus mechanisms, each using their own methods to distribute decision-making power. For example, on Bitcoin's blockchain, decision-making powers are obtained through the computing power provided (Proof-of-Work, PoW), while on Ethereum's blockchain they are granted based on the amount of resources provided as collateral by each node (Proof-of-Stake, PoS). The establishment of consensus mechanisms helps to secure a DLT system. The rules for consensus therefore also depend on whether the DLT system is operated in a centralised or decentralised manner. In decentralised systems, registrations are validated through the consensus mechanism rather than by a central infrastructure provider. It also brings with it a certain vulnerability to malicious actors, such as so-called '51 percent attacks'[15]. These consensus mechanisms are therefore designed with incentive structures to ensure a credible operation of the ledger.

DLT systems are also characterised by the fact that the ledger is transaction-based and cryptographic techniques are used to link the ledger in a chain structure to ensure that

[15] In essence, 51% attacks are cases where one or more malicious actors in a group control more than 50% of the decision-making power, thereby controlling what new entries are made in the ledger.

recorded data cannot be deleted or changed after it has been added without being identifiable (so-called 'immutability'). The design focus on immutability is a key difference from more traditional databases which do not require the use of cryptography to record data in the same way. Although immutability is a key security property, especially for the decentralised variations of DLT, immutability is not a condition in MiCA's definition of a DLT.

B1.2 The application layer

The application layer basically enables the development and availability of so-called 'smart contracts' in a DLT system. In practice, the application layer can therefore be used to make regulated activities accessible. This is basically done with a set of integrated smart contracts that together make the activity available to the user.

The term 'smart contract' is not clearly defined, neither in MiCA nor in the field in general. The wording indicates that a smart contract is more than just a digital representation of a contract or agreement. The more common perception of smart contracts is that they are standalone applications available in a DLT system for users to access. This is evident from the description of smart contract functionality on the Ethereum blockchain:

> *"A "smart contract" is simply a program that runs on the Ethereum blockchain. It's a collection of code (its functions) and data (its state) that resides at a specific address on the Ethereum blockchain. Smart contracts are a type of Ethereum account. This means they have a balance and can be the target of transactions. However, they're not controlled by a user, instead they are deployed to the network and run as programmed. User accounts can then interact with a smart contract by submitting transactions that execute a function defined on the smart contract. Smart contracts can define rules, like a regular contract, and automatically enforce them via the code. Smart contracts cannot be deleted by default, and interactions with them are irreversible."* [16]

This type of smart contract is characterised by the fact that they cannot be removed or changed once they are available on Ethereum. However, they may have built-in code that gives selected participants access to modify the inputs that the given smart contract uses when executing its programming. This can include inputs in the form of external data sources or other smart contracts that the smart contract needs to call. It is characteristic of this type of smart contract that they are represented on the blockchain in the same way as regular users. They also have an unique public key (account) and to some extent also a private key (the right to use the account), although in practice it is the programming of the smart contract that constitutes the action that leads to the use of the private key[17]. In other words, smart contracts are completely limited to acting according to their programming - unlike users who must actively sign actions with the private key.

B1.3 Interfaces for DLT systems

Interfaces play a central role, as they form the link between users and the DLT system. For example, it is practically possible for any actor to interact directly with a conventional

[16] https://ethereum.org/en/developers/docs/smart-contracts/

[17] The public key is comparable to a customer's bank account number and is thus the address on the blockchain where the rights to the crypto assets transferred to the given user are registered. The private key is the user's access to make transactions with the crypto assets registered to the user's public key.

blockchain and its associated DeFi services, but this requires significant programming skills and technical expertise. The broader user base will therefore typically access DeFi services through interfaces that either consist of web interfaces that can be accessed via an internet browser or various apps that can be downloaded from most app stores or software on so-called hardware wallets. Interfaces are both the graphical and technical interface that allows ordinary users without deeper technical knowledge to access DeFi services.

Web-based interfaces are the most common and can be accessed via browsers such as Chrome, Firefox or Safari.

Some DeFi platforms have also developed mobile apps that allow users to interact with DeFi protocols from their smartphones or tablets. This provides users with a more convenient and user-friendly experience where they can trade and manage their crypto assets anytime, anywhere. It is also possible to use desktop applications which the user can download and install on their computer. These applications offer advanced features and a more customised user experience, but they often require a higher level of technical knowledge.

A hardware wallet consists of a physical device, usually in the form of a hard drive or USB key, designed specifically for the secure storage of crypto assets. A hardware wallet differs from other types of crypto wallets, such as software wallets, by being a dedicated, isolated device that usually is not connected to the internet. Some hardware wallets contain software that allows users to communicate directly with a range of DeFi services if they are connected to the internet.

Annex 2 - Crypto-assets and the regulated activities

MiCA defines a crypto-asset in Article 3(1)(5) as: *"... a digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technology"*.

On a very basic level, the definition of a crypto asset is thus broad but tied to the use of DLT. On conventional blockchains, crypto assets can be divided into two basic categories: protocol coins (coins) and application tokens (tokens).

Coins consist of the crypto assets that make up the DLT system's inherent means of payment. Transaction costs and other financial incentives are therefore also calculated and paid with the blockchain coin. Ether, for example, is the coin for Ethereum. It follows from recital 26 of MiCA that the issuance and offering of coins are not covered by the regulation if they are generated automatically as part of the operation of the DLT system.

The conventional blockchain also supports the issuance of tokens, which are issued in the application layer of a blockchain. Token issuers can independently define which rights are to be embedded in the token. It is this type of token that can be used to issue everything from stock and bond-like instruments and so-called stablecoins to tokens with a more utility-like purpose, such as concert tickets.

MiCA regulates, with exemption of fully decentralized services in recital 26 and the exceptions described in Article 2 of the regulation, all issuances and offerings of all crypto-assets.

B2.1 Issuers of so-called 'stablecoins'

MiCA does not use the term stablecoins. However, the regulation regulates two types of crypto asset issuances which are often referred to as stablecoins. These two forms are classified as asset-referenced tokens (ART) and electronic money tokens (EMT) respectively. The term stablecoins is thus a collective term for these two types of crypto assets.

Asset-based tokens are defined in Article 3(1)(6) as "*a type of crypto-asset that is not an electronic money token and that purports to maintain a stable value by referencing another value or right or a combination thereof, including one or more official currencies*."

ARTs are crypto assets that are issued with the aim of maintaining the same value as a predefined underlying asset (reference asset) that is not an official currency. The value is maintained by a so-called 'stabilisation mechanism'. For example, an ART can be issued to maintain a stable value in relation to the market price of Ether, where the value is stabilised by investing in a pool of other crypto assets that together can replicate the value of Ether.

An electronic money token, or e-money token, is defined in Article 3(1)(7) as "*a type of crypto-asset that purports to maintain a stable value by referencing the value of one official currency."*

EMTs differ from ARTs in that the value against which they claim to maintain stability is the value of an official currency. Therefore, if the purpose of the issue is to maintain a fixed value against, for example, the euro, the issue is classified as an EMT. EMT issuers are subject to the same regulation as traditional e-money issuers.

Under MiCA, ARTs and EMTs may only be offered if the issuer has been authorised to do so. The license entails meeting a number of requirements in the same way as applies to providers of crypto-asset services, cf. Annex 2.3.

B2.2 Issuers of other crypto assets

MiCA also regulates the offering and request for admission to trading of tokens that cannot be classified as ART or EMT. Unlike stablecoins, the offering of other crypto-assets will not be subject to authorisation requirements in MiCA. However, they must meet the requirements of Title II of MiCA if the issuer is identifiable. Otherwise, the obligations rest with the crypto-asset services that offer their customers services with the issued crypto-assets.

B2.3 Crypto-asset service providers

Title V of MiCA sets out the regulatory requirements for crypto-asset service providers. The structure of the obligations can largely be compared to the regulatory requirements that financial companies such as payment institutions and investment firms are subject to today. These include capital requirements, conduct of business requirements and consumer and investor protection requirements.

Crypto-asset service providers are defined in Article 3(1)(15) as: *"a legal person or other undertaking whose occupation or business is the provision of one or more crypto-asset*

services to clients on a professional basis, and that is allowed to provide crypto-asset services in accordance with Article 59."

Article 3(16) of the Regulation further limits the scope to the following activities:

1. providing custody and management of crypto assets on behalf of clients
2. operation of a trading platform for crypto-assets
3. exchange of crypto-assets for funds
4. exchange of crypto-assets for other crypto-assets
5. execution of orders for crypto-assets on behalf of clients
6. placing of crypto-assets
7. reception and transmission of orders for crypto-assets on behalf of clients
8. providing advice on crypto-assets
9. providing portfolio management on crypto-assets
10. providing transfer services for crypto-assets on behalf of clients