BCAS

Decentralisation under MiCA: the definitive handbook for DeFi

BCAS.IO

BCAS

Office 11, Capital Workspace, Onsite Buildings,
Level One, Valley Road Birkirkara, Malta BKR9021
info@bcas.io | www.bcas.io

Table of Contents

Office 11, Capital Workspace, Onsite Buildings,
Level One, Valley Road Birkirkara, Malta BKR9021
info@bcas.io | www.bcas.io

Foreword

I have officially begun my 11th year in the crypto space, with BCAS itself venturing into its 7th year of successful operations, with its clients being some of the most renowned names in the industry. To say that I am proud to see the prominence to which the industry has risen, when I vividly remember the discussions of a handful of people on the 'Altcoin' section of *bitcointalk.org* not even remotely imagining the heights which we would reach... well, 'proud' is an understatement. Crypto, as an industry, has now gotten the attention of major institutions, politicians, and governments alike, for better or for worse. While the future is unknown, it is undeniable that as an industry, it has left its mark.

As a certain famous fictitious uncle once said: "with great power comes great responsibility". It can likewise be said, cheekily, that with great prominence comes great regulatory attention. It was no surprise, therefore, when the European Commission announced its Digital Finance Package, the crown jewel of which was the Markets in Crypto-assets Regulation (MiCA). Now verging onto being a 1000-page legislative instrument (considering its secondary and tertiary-level texts too), it is truly a behemoth, and it is safe to predict that the two years following its application will have everyone scratching their heads on the true extent of its applicability, its interpretation, and its effects on the industry.

The biggest question mark tends to be raised concerning its applicability or otherwise to DeFi. To state, categorically, that DeFi is outside of MiCA's scope is dangerous, not least because of the fact that there is no universal definition of DeFi. Similarly, to state that DeFi and online interfaces are within scope of MiCA can be baseless and untrue for most of the protocols and projects that perhaps have become synonymous with the meaning of DeFi itself.

To provide much-needed clarity and guidance on this ever-raging debate, we have leveraged the knowledge and experience gathered over the years, and prepared what we hope to be the go-to document for anyone in DeFi who is concerned about MiCA what mean for them. At a time where the risk of regulatory capture, rightly or wrongly, is increasing, we felt that the time is now right to release a handbook or tool-kit for all the stakeholders in DeFi to be informed about what to do, or not to do, in view of MiCA's imminent applicability.

In this handbook, we cover multiple key topics, including wrangling with the definition of decentralisation itself, exploring the multiple faces of decentralisation, understanding when it

matters under MiCA, and ultimately providing guidance on how to structure a protocol or project in a manner so as to fall outside the scope of MiCA.

Without any further ado, I invite you to step onto this journey with us, which should also serve as an open window into all the work that we've been doing over the years.

Jonathan Galea, Founder and Partner at BCAS.

Introduction

Much has been said about the concept of decentralisation in crypto over the years, with a widely accepted definition remaining elusive to this very date. While we are not setting out to define the global benchmark of decentralisation, there is sufficient ground to devise a workable standard in relation to the Markets in Crypto-Assets ('MiCA') Regulation. The primary objective of this handbook is to determine which regulatory considerations under MiCA may apply to projects and protocols that are branded as 'DeFi', cross-chain bridges, or Layer-2 ('L2') solutions, along with the relevant criteria that might lead to a platform or protocol to be considered within the scope of the Regulation, and what measures can be implemented to be outside of the scope of MiCA itself.

1. Decentralisation from Technical and Organisational Points of View

While presenting a single and undisputed definition of 'decentralised' represents a significant and elusive feat, it is necessary to ascertain, or at the very least narrow, the scope of this term to determine whether a project can be deemed to be 'fully decentralised'[1] and remain outside the scope of MiCA. In carrying out multiple Decentralisation & Legal Risk Audits on DeFi and L2 protocols over the years, we formed the opinion that a project's level of 'decentralisation ' can be approached from **five** distinct perspectives.

Firstly, 'decentralisation' can refer to the absence of a central server, organisation or authority exercising any control. Within the context of blockchain networks, decentralisation can be construed as the absence of centralised control over the processing of users' transactions and consensus achievement

[1] Recital 22 of MiCA makes reference to the fact that crypto-asset services are excluded from MiCA's scope when such are offered in a fully decentralised manner without intermediaries.

Office 11, Capital Workspace, Onsite Buildings,
Level One, Valley Road Birkirkara, Malta BKR9021
info@bcas.io | www.bcas.io

over the network's state. Compared to traditional finance, where a central authority has a material or full degree of control over the accounts, 'decentralised' blockchains are based on a network of nodes interconnected through a peer-to-peer communication protocol which maintains user account balances (i.e. the ledger) without a central authority. Such consensus at the **settlement layer** is usually achieved by implementing a Proof of Work ('PoW') or Proof of Stake ('PoS') consensus mechanism, in a Byzantine Fault Tolerant manner to account for the decentralised nature of the network.

Secondly, 'decentralisation' can refer to a project's **architecture**, which typically consists of a set of trustless smart contracts integrated with the off-chain components required for the application to function. Unlike traditional finance, where a central authority oversees security guarantees in exchange for compensation, smart contracts do not rely on intermediaries to function. Decentralised applications ('dApps') powered by smart contracts are able to prove their trustworthiness through transparency, executing automatically without the need for clearance from central authorities. This feature is facilitated by the fact that all possible outcomes when interacting with an open-source smart contract can be predicted, encoded and only triggered if the required conditions are met. In this context, decentralised financial applications ('DeFi') enable an environment of interconnected platforms where financial activities, such as lending and borrowing, are offered without intermediary interventions and permissions.

An architectural analysis typically extends to the off-chain components that a project may leverage to function, which may raise centralisation concerns. For instance, blockchain bridges tend to trust off-chain transaction verifiers to provide cross-chain communications. Moreover, L2s handle transactions off-chain to scale their settlement layers while relying on centralised sequencers to bundle transactions before sending them to a Layer-1 ('L1') blockchain for finalisation. In a similar vein, Zero-Knowledge ('ZK') L2s tend to rely on centralised ZK-proof generators to guarantee that transactions sent to the settlement layer are valid. Lastly, oracles can be present as either on-chain or off-chain components, implying different considerations when analysing the overall decentralisation of a project. In this case, off-chain oracles, which are run locally by specific project participants to validate between them the information sourced to the on-chain components, can act as points of centralisation. Following these examples, it is evident that the off-chain components of a project's architecture deserve their own analysis, and should be properly designed so as to avoid becoming centralisation vectors.

As a third point of perspective, 'decentralisation' can refer to the management, organisation and control of a protocol. Decentralised autonomous organisations ('DAOs') theoretically integrate a mode of

Office 11, Capital Workspace, Onsite Buildings,
Level One, Valley Road Birkirkara, Malta BKR9021
info@bcas.io | www.bcas.io

decentralised governance & oversight over DeFi projects. In such structures, constituents of a DAO can partake in decision-making processes, usually in a tokenised format, being the so-called 'governance tokens'. These generally grant a holder thereof the possibility of steering the direction in which a DeFi protocol or project veers, typically by giving them the possibility to vote on proposals raised by themselves or their peers. Although dubbed as 'governance tokens', it is curious to note that what the industry generally thinks of governance tokens are not always, in actual fact, the instruments which grant 'governance powers' to their holders, such as the possibility to partake in the revenue distribution generated by the same protocol, or to even vote on proposals. Such tend to be accessible through user-initiated actions of staking, which results in a non-transferable, separate token being received, such as a veToken; this would be the token that, in actual fact, can be used for governance purposes.

Going back to the matter at hand: metrics such as the governance token distribution and the voting power that some participants are able to accumulate are of major importance when analysing the actual decentralisation level of a DAO. Likewise, it becomes paramount to analyse if the project relies on entities, referred to as 'DAO-adjacent entities', such as foundations, which may retain a material element decision-making power, undermining the governance token holders' participation in the project direction while impacting the overall level of decentralisation.

Fourthly, 'decentralisation' can be analysed by identifying who controls or manages the interface that allows users to interact with this project. The user interface may consist of a website, desktop application, or mobile device application that provides front-ends for users to access the underlying smart contract-enabled applications. If any relevant party can potentially restrict users from accessing the underlying smart contract(s) by graphical means through its interface, and such graphical user interface is the sole means through which the underlying smart contracts can be accessed in such a manner, then the project may be limited in its extent of decentralisation, with possible ramifications for the operators of the interface.

Moreover, projects can provide their users with default Remote Procedure Calls, commonly known as RPCs, which serve as the points of contact for users to interact with any sending or retrieval of information on a blockchain network when accessing blockchain-based applications. While RPC services are vital when interacting with a blockchain application, they can act vectors of centralisation, and ideally a wide enough network of RPCs is available for users to connect through, without pre-set RPCs as defaults. Lastly, from a user interface perspective, there are instances of blockchain-based applications aiming to remove users' friction by providing their own wallets to grant straightforward

Office 11, Capital Workspace, Onsite Buildings,
Level One, Valley Road Birkirkara, Malta BKR9021
info@bcas.io | www.bcas.io

access to their projects, while at the same time managing the users' crypto-assets. However, the efforts to ease the onboarding process of new users can undermine the project's decentralisation if appropriate principles of self-custody and private-public key pair management are not implemented.

Fifthly and lastly, a further relevant criterion for determining whether a project is 'decentralised' is the existence of payments or royalties for the protocol allocated directly to its creators, owners, or operators. In such a scenario, it is possible to identify an entity that may be providing software on a commercial basis and, therefore, may assume the legal responsibility for a service it may be providing. If the same entity controls the interface to attract potential users, it may well result in the project possibly being sufficiently centralised. Of specific importance is the manner in which contributors to the protocol are approached and how their selection, definition of tasks, and corresponding payments are established. It is commonly understood that to remain decentralised, operational matters involving treasury management so as to contract the contributors required to support the ongoing project functionality, should be processed in a decentralised manner involving the project stakeholders, ergo the governance token holders.

In summary, the five angles from which the term 'decentralisation' can be approached are summarised below and will be examined in more detail in the following sections:

- Settlement Layer Decentralisation
- Architecture Decentralisation
- Governance Decentralisation
- User Interface Decentralisation
- Operations Decentralisation

1.1 Settlement Layer Decentralisation

The degree of decentralisation of the settlement layer in which a project or protocol chooses to deploy its smart contracts is essential; if this layer cannot be considered sufficiently decentralised it would undermine the efforts undertaken to address decentralisation from the remaining four perspectives that will be discussed in this handbook. As stated in the introduction to the decentralisation analysis from a technical perspective, an L1 blockchain can be considered decentralised when it operates by leveraging a permissionless & sufficiently distributed network consisting of nodes that store, share and update the same copy of a distributed ledger. To this end, unrestricted access to anyone who wishes to participate

Office 11, Capital Workspace, Onsite Buildings,
Level One, Valley Road Birkirkara, Malta BKR9021
info@bcas.io | www.bcas.io

as a user or node, which in turn take the responsibility for the task and complying with the hardware and software requirements described in the consensus mechanism, is crucial.

From a user perspective, since nodes enable users to read and send information to blockchains, having a geographically distributed array of nodes makes access to blockchains more efficient and decentralised. Therefore, L1s that allow users to participate as nodes without high hardware requirements are deemed for a higher level of decentralisation as they encourage users to operate their own nodes, facilitating and decentralising blockchain access.

Another important decentralisation parameter in L1 blockchains is the number of 'votes' a block needs to be considered valid. Considered from the opposite angle, this means how many nodes or voting power are required to censor transactions. While reducing the amount of voting power required to do so may protect against fraudulent actors, when a blockchain's consensus power is centralised in a few entities, the consequences may be less decentralisation and a higher level of transaction censorship.

1.1.1 Consensus Mechanisms

The most commonly used consensus mechanisms include Proof of Work (PoW), Proof of Stake (PoS) and a widely adopted variant of PoS known as delegated PoS ('dPoS').

1.1.1.1 Proof of Work

PoW involves nodes competing with each other to solve a mathematical problem that allows the one who succeeds first to mine the next network block. To reach a consensus on the blockchain state, this block must be confirmed by a certain number of network nodes. In principle, as long as there is a sufficiently distributed number of nodes participating in the block mining process, a PoW blockchain can be considered decentralised.

However, this fact can be undermined if certain entities gather a considerable amount of hashpower. Hashpower measures the number of operations a miner can perform per second to solve a mathematical problem and mine the next block. In this sense, the higher the hashpower, the higher the possibilities/chances to mine the next block.

Office 11, Capital Workspace, Onsite Buildings,
Level One, Valley Road Birkirkara, Malta BKR9021
info@bcas.io | www.bcas.io

Hashpower can usually be centralised in two different ways. The first is when entities acquire a significant number of devices dedicated to solving the mathematical problem to mine the next block. Meanwhile, the second form of centralisation is when different users or entities contribute with their hashpower to a so-called 'mining pool' in which the computational power will be gathered, increasing the chances to mine the next block and dividing among the participants the block rewards obtained.

Hashpower centralisation becomes a severe problem when a single entity reaches a sufficiently high level of control over the network's hashpower, potentially allowing it to manipulate blockchain information or even perform censorship practices. Additionally, if some entities collectively have sufficient hashpower to collude and reach more than half of the total network hashpower together, it can be deemed as problematic too.

As decentralised and permissionless protocols govern them, blockchain consensuses do not, and should not, include rules prohibiting hashpower concentration. In these cases, the defence of PoW blockchains relies on game theory. If hashpower 'concentrators' decide to attack the network, they will be acting against their own interest as their investment in computational devices and hashpower will potentially become useless or, at the very least, less profitable.

1.1.1.2 Proof of Stake

Blockchains that achieve consensus through a PoS mechanism involve nodes, usually known as validators, that must deposit ('stake') a certain amount of the blockchain's native crypto-asset. Validators are rewarded for validating transactions according to consensus rules. However, when these rules are not respected, validators will see their staking reduced ('slashed') by a predetermined amount.

PoS blockchains should unrestrictively allow users to become network validators to be considered sufficiently decentralised. Other considerations, such as how the validator's stake is distributed, can be an essential measure of the decentralisation of a settlement layer, as most PoS networks tend to determine the next block proponent based on the amount of its validators' stake.

In this sense, Ethereum's solution can be seen as somewhat aiming to lend itself towards a greater distribution of validators through the 32 ETH stake limit, although this can also be seen as somewhat of a barrier to entry for users wishing to participate as validators, as 32 ETH at current market rates are a

Office 11, Capital Workspace, Onsite Buildings,
Level One, Valley Road Birkirkara, Malta BKR9021
info@bcas.io | www.bcas.io

not-inconsiderable amount. Liquid staking solutions do serve to mitigate this issue, but in turn a large enough market share by a liquid staking solution provider can still cause concerns of centralisation.

On a similar note, Ethereum's consensus mechanism does not establish specific rules to prevent node operators from creating validator clusters. Validator clusters, which can form due to geographical immediacy, shared hardware infrastructure, or coordinated behaviour, can represent a potential point of failure. The security of PoS blockchains can be compromised if a validator within a cluster fails or acts maliciously, and its cluster represents a substantial percentage of the network's validator power. To address these risks, the Ethereum community proposed correlated attestation penalties.[2] These penalties aim to mitigate centralisation risks by penalising missed attestations (validators' votes on other validators' block validity) with greater emphasis when coordinated validators' behaviour is detected.

1.1.1.2.1 Distributed Validator Technology

Distributed Validator Technology (DVT) represents a significant step from the blockchain community to enhance PoS decentralisation at a validator level. In this context, DVT consists of a protocol that allows the splitting and sharing of a validator key into multiple KeyShares, thus effectively spreading the validator responsibilities across multiple parties, reducing single points of failure. By splitting the private key across multiple nodes in a cluster, DVT makes it difficult for attackers to access the full key and thus offers better security for node operators, allowing some nodes to go offline without affecting the validator's operation increasing the overall network resiliency.

Moreover, DVT implementations such as SSV.Network allows validators' keys to be split into multiple nodes, each of which can use different combinations of consensus and execution clients. This feature gives further resilience since, if a bug is found in one client, the overall validator can still function depending on the fault tolerance level set. The fault tolerance level depends on how the distributed validator is configured within a cluster of nodes. For instance, a cluster consisting of four nodes will give a fault tolerance of one when setting DVT leveraging SSV.Network.

1.1.1.3 Delegated Proof of Stake

[2] https://ethresear.ch/t/analysis-on-correlated-attestation-penalties/19244

Office 11, Capital Workspace, Onsite Buildings,
Level One, Valley Road Birkirkara, Malta BKR9021
info@bcas.io | www.bcas.io

Lastly, blockchains that reach their consensus through the most widely adopted variation of PoS, dPoS, allow native token holders to stake their tokens with validators to partake in the blockchain consensus mechanism without the requirement to run a validator themselves. The potential centralisation issues of this type of blockchain arise from the accumulation of staked tokens by validators. Generally, the total amount of staked tokens a validator holds, composed of the self-staked tokens, as a 'good behaviour guarantee', plus the token holders' delegations, settles the probabilities of being selected as the next block proposers and their percentage of voting power over the blockchain development and financial decisions.

There are certain measures in DPoS blockchains which serve to mitigate the potential adverse effects of staking centralisation by incentivising token holders to delegate to smaller validators in terms of staking, such as the possibility of receiving more bountiful airdrops in comparison to when staking with larger/more saturated validators, and a greater degree of influence by delegators over their validators' votes. Despite their efforts, it is common to find dPoS blockchains where the largest ten validators hold a significant percentage of the network voting power.[3] [4]

1.1.2 Maximum Extractable Value

Recently, the concept Maximum Extractable Value ('MEV') concept has been extensively discussed from different perspectives. MEV can be briefly defined as the additional value block proposers can obtain, on top of block rewards and transaction fees, by reordering, adding, or excluding transactions. MEV-related activities have entirely reshaped the landscape of block-proposing processes in blockchain networks. Initially, solutions to address the MEV issue aimed to democratise access to MEV profits while ensuring block proposers remain focused on their primary tasks of proposing new blocks and validating other proposers' blocks.

To this end, new functionaries were introduced with the goal of task separation, which typically leads to the following process:

1) Searchers identify transactions with the highest MEV profits.
2) Builders arrange searchers' transactions in the most profitable order.

[3] https://www.mintscan.io/cosmos/validators/ - Top ten validators holding 42% of the network's voting power.
[4] https://www.mintscan.io/osmosis/validators/ - Top ten validators holding 37.20% of the network's voting power.

Office 11, Capital Workspace, Onsite Buildings,
Level One, Valley Road Birkirkara, Malta BKR9021
info@bcas.io | www.bcas.io

3) Relayers deliver these block proposals to the actual block proposers, whether validators or miners.
4) Block proposers use those transactions to propose a block and share MEV profits with builders and/or searchers.

While the access to MEV profits for block proposers has been extended to those who do not have the hardware resources to do so on their own, this structure has inadvertently led to centralisation in block building. For instance, 90% of Ethereum blocks are built by just three builders[5], centralising the block-building process by leveraging superior software and hardware solutions. Consequently, the new block-building scenario acted as a double-edged sword, providing, from one side, democratised access to MEV for validators, but also introducing a degree of centralisation in the block-building process.

1.1.3 Client Diversity

Blockchain nodes are heavily impacted by the client that they run; consequently, client diversity represents a crucial aspect of maintaining a resilient and decentralised network. For instance, an Ethereum node requires a consensus client (such as Prysm, Lighthouse, Teku and Nimbus) and an execution client (such as Geth, Nethermind, Besu and Erigon). If two-thirds of Ethereum clients use a single client, there is a substantial risk of network disruption and potential financial loss for node operators, should the client used experience a material failing; a shutdown, even temporary, of 66% of Ethereum's validators would severely impact the validation process & network finality of Ethereum.

Therefore, if a client exceeding a market share of two-thirds encounters a bug leading to a forked version of the Ethereum network, its ongoing and unhindered availability may well become vital for the ongoing finalisation of blocks.[6] Once this fork is finalised, validators cannot revert to the original chain without incurring penalties. According to Ethereum's consensus rules, if two-thirds of the chain is simultaneously penalised, the slashing penalty represents the entire 32 staked ETH of each and every validator so penalised.[7]

Consequently, to prevent these security hazards and decentralisation threats, the objective is to maintain each client's market share below this one-third of the market share threshold. The risks highlighted are not exclusive to consensus clients but also apply to execution clients. In this sense,

[5] https://explorer.rated.network/builders?network=mainnet&timeWindow=30d&page=1
[6] https://supermajority.info/
[7] https://clientdiversity.org/

ensuring diversity across both types of clients is equally important for network security and overall decentralisation.

1.2 Architecture Decentralisation

Throughout this section, we will address decentralisation from an architectural perspective of the project, protocol, or application under analysis. As highlighted in the introduction to the technical analysis of decentralisation, while blockchain applications primarily depend on their smart contracts for core functionality, it is essential to consider the impact of its off-chain components on the overall degree of decentralisation.

In this sense, we will first analyse the commonly utilised on-chain components of blockchain projects and applications. Following this, we will conclude this section by reviewing the off-chain components typically involved in these projects, focusing on their centralisation concerns while presenting strategies to successfully maintain a high level of decentralisation.

1.2.1 On-Chain Components

The following subsection will cover the on-chain components that blockchain-based applications typically leverage. Our analysis aims to underscore the key on-chain elements of applications such as L2 solutions, cross-chain bridges, and DeFi platforms. After providing a definition of these components, we will tackle their potential impact from a decentralisation perspective while presenting strategies to address centralisation concerns they might inadvertently generate. To this end, we will be tackling the following on-chain components:

- Smart Contracts
- Oracles
- Proof Verifiers
- Multisigs
- Software Licenses

Office 11, Capital Workspace, Onsite Buildings,
Level One, Valley Road Birkirkara, Malta BKR9021
info@bcas.io | www.bcas.io

1.2.1.1 Smart Contracts

Smart contracts are computer programs stored on a blockchain that automatically execute when predetermined conditions and terms are met. Following this definition, a project leveraging smart contracts can allow, in a trustless manner, users to deposit their crypto-assets while retaining control over them. These crypto-assets are stored in a smart contract address for a specific duration without any involvement from centralised parties. The user interacts with the project autonomously, without the need for external intervention.
However, even though smart contracts inherit characteristics of the blockchain on which they are deployed, this does not necessarily mean that a project based on smart contracts will be decentralised because its contracts were deployed and run on a decentralised network of nodes.

Projects should ideally leverage a set of smart contracts that allow for unrestricted use. No single entity or individual should be able to control the smart contracts in question. In this context, control means restricting who can interact with the project's smart contracts, modifying their logic, or pausing them or their primary functions.

While, due to their nature, smart contracts cannot be modified once launched in most blockchains, developers have found a way to modify deployed smart contracts by developing proxy contracts. A proxy contract is a smart contract that allows the contract logic to be updated under specific conditions. Each proxy contract defines an implementation contract, a different smart contract on the same blockchain containing the current smart contract code logic. Proxy contracts allow for upgradability by changing the implementation contract referenced in the proxy contract.

In this context, defining who owns the smart contract or has the necessary role assignment to carry out this modification and pause the contract's functionality is of utmost importance. When a single person or group can modify the implementing contract reference or pause the contract, the project may risk being seen as taking on a significant element of permission, which tends to translate to centralisation.

However, smart contract upgradability, achieved through proxy contracts, is often necessary to adapt the protocol to evolving network or market conditions and to remain competitive in the DeFi ecosystem. Moreover, pausing powers can be a lifesaver when projects are under attack. As explained in the next

Office 11, Capital Workspace, Onsite Buildings,
Level One, Valley Road Birkirkara, Malta BKR9021
info@bcas.io | www.bcas.io

section, a suitable solution for a project to remain upgradable, but without centralising these functions in a few hands, is the establishment of DAOs that retain control over the exercise of certain key functions.

Control over smart contracts is inextricably related to privileged functions, another point from which concerns of centralisation can arise. Privileged functions entitle smart contract owners or their guardians to privileged powers by giving them exclusive authority to call specific functions for designated activities. The scope of privileged functions commonly extends to the following functions within a project:

- Administrative functions.
- Emergency functions.
- Whitelisting/blacklisting functions.
- Asset management functions.

Administrative functions include protocol upgrades, such as interest rates and fee management. While projects that rely on DAOs tend to delegate these decisions to their token holders, there are still plenty of cases where such decisions are still the prerogative of smart contract owners/controllers, guardians, or project founders.

Emergency functions are activated during 'crisis situations' and consist of pausing smart contract operations during anomalies or extreme events. On the one hand, to mitigate centralisation while protecting the protocol, one can argue that there is a need to decentralise the decision-making process involved in triggering the emergency functions. On the other hand, since emergencies require prompt actions, waiting for a decentralised vote to take place may well defeat the purpose of emergency-triggered functions. Therefore, a suitable compromise may involve the DAO designating a set of responsible delegates who must reach a consensus to call these functions, while ensuring that the DAO retains an element of material control in deciding, through voting proposals, which delegates to appoint or remove. This method decentralises, to a degree, the authority in 'emergency situations' rather than solely concentrating it within a few individuals.

Whitelisting/blacklisting functions may also negatively impact a project's level of decentralisation. Common in compliance-oriented projects like centralised stablecoins, these practices are facilitated by solutions such as Solana Token Extensions, as discussed in our article 'Solana Token Extensions and its Legal Implications'.

Lastly, asset management functions entitle protocol owners to rebalance, transfer, freeze or seize tokens without their holder's permission, with such typically being utilised in centralised stablecoins in order for their issuers to comply with regulatory requirements. Solana Token Extensions facilitate the straightforward implementation of these privileged functions, leading to smart contract control centralisation.

1.2.1.2 Oracles

Blockchains are closed digital circuits, in a sense, that cannot natively communicate or exchange information with the environment beyond their boundaries. However, to thrive in the competitive DeFi world and offer compelling services to users, decentralised applications need to consume data from outside of the blockchain boundaries within which they are deployed. Smart contracts rely on key infrastructure known as oracles to overcome this obstacle.

In this context, oracles connect blockchains to the outside world. They are responsible for retrieving external information, such as stock quotes, market rates, or real-world events, and delivering it to smart contracts. A thorough understanding of how and what oracles are used in a particular project and how these oracles are managed is relevant when analysing a project's degree of decentralisation. If a ‘decentralised protocol’ uses centralised oracles, its degree of decentralisation would be severely reduced.

For ease of understanding, oracles can be compared to the Bloomberg terminal. This software, provided by Bloomberg L.P., offers real-time financial data, related news and valuable information for those involved in the financial markets. As with oracles, anyone willing to pay the fee can access the information from Bloomberg. However, the big difference is how this information is sourced, verified and presented to final consumers. While Bloomberg operates as a centralised software under Bloomberg L.P.'s control, oracles should tend towards decentralisation in terms of information sourcing & their operations if they are to live up to the blockchain industry's decentralised narrative. Therefore, projects such as ChainLink, Band, or Pyth provide on-chain oracle networks capable of retrieving information from the outside world and delivering it directly to smart contracts without compromising its decentralisation.

This is achieved by having a network of oracles who obtain information from the outside world, using different sources to reduce the chances of being deceived or supplied with misinformation. Once the

Office 11, Capital Workspace, Onsite Buildings,
Level One, Valley Road Birkirkara, Malta BKR9021
info@bcas.io | www.bcas.io

oracles collect the information, they compare their results with each other, and once a consensus is reached on which piece of information is correct, they share it on-chain. Smart contracts can then access and use this information within their internal operations.

A suitable example is when DeFi applications offer crypto-assets linked to the price of gold. As gold prices are determined on the international market, which takes place outside of any blockchain, they will consume oracles' information to keep their crypto-asset price pegged to the gold price. A less obvious but appropriate example is the communication between Ethereum's consensus and application layers. Since these two layers cannot communicate directly, projects deployed on Ethereum's application layer needing to consume information from the consensus layer, such as rewards or penalties received by a validator, must rely on oracles. Through them, they obtain information from the consensus layer, where this action takes place, and bring it to the application layer, where the information will have an effect in a decentralised application.

Considering these precedents, it is essential to analyse from which source a smart contract consumes external information and how this source, in this case an oracle, works to determine the project's degree of decentralisation. Some projects rely on their network of oracles, which process information received off-chain to supply to the project. Naturally, this means there is still a risk of centralisation when dealing with external data.

A decentralised network of oracles should support permissionless participation, allowing users to engage as oracles and retrieve information from outside the blockchain. Then, once the oracles possess the information, it is necessary to establish a consensus mechanism to ensure that these oracles, in a decentralised way and without involving trusted third parties, decide the accurate information that can be delivered to the project that requires it. This process must be performed on-chain to guarantee the highest degree of transparency. When one of these characteristics is missing in an Oracle network or system, the project that consumes information from it can hardly be labelled as decentralised to the best extent possible. The degree of decentralisation of a project tends to have its limits tested when considering its most centralised elements.

1.2.1.3 ZK Proof Verifiers

In the context of L2 solutions that rely upon zero-knowledge (ZK) proofs, there is a key on-chain component that can have its own impact on the decentralisation of such an application. To verify the

cryptographic ZK-SNARK proofs generated by this type of solution and ensure the validity of their own processed transaction batches, a verifier contract is deployed on the corresponding L1. These contracts, key elements in any ZK-rollup architecture, should be analysed under the measures mentioned above, such as upgradability, ownership and privileged functions when evaluating the level of decentralisation of a project relying on ZK technology to scale.

1.2.1.4 Multisigs

As a specific type of blockchain wallet, multisigs enhance security by requiring transactions to be signed by multiple holders of its private keys. To establish a multisig, at least three public and private key pairs must be linked to the multisig, and to authorise transactions from a multisig, a pre-established number of signatures must be required.

Users leverage multisig wallets as an additional security measure, requiring transaction approval from more than one individual address. This means that if one of its addresses is compromised, the crypto-assets in the multisig are still safe. However, the use of multisigs has become contentious in applications such as bridges or L2 solutions.

Concerns about centralisation arise when projects establish a multisig to 'decentralise' ownership over critical smart contracts. While protocols can hold millions of dollars in their smart contracts, a multisig requiring five out of seven signatures indicates centralisation, undermining the protocol's broader decentralisation efforts. Moreover, the risk of collusion among 'multi-signers' cannot be dismissed. Therefore, using multisigs to distribute the ownership of crucial contracts is highly discouraged in order to safeguard decentralisation and security. As an alternative, protocols that completely renounce ownership of their smart contracts are generally considered more decentralised. However, crucial smart contracts of a protocol may require some form of control, especially when security issues arise. In this sense, establishing a DAO and granting *governance token* holders control over these smart contracts can be seen as the most secure and, at the same time, decentralised approach.

A different scenario arises when less critical smart contracts are assigned to a multisig. In this cases, there is a growing trend of DAOs that delegate specific functions to qualified token holders or chosen project contributors to manage non-critical smart contracts. In these cases, the ability of token holders to remove these 'multi signers' or reverse their decisions helps maintain the project's overall decentralisation.

Office 11, Capital Workspace, Onsite Buildings,
Level One, Valley Road Birkirkara, Malta BKR9021
info@bcas.io | www.bcas.io

1.2.1.5 Software License

While not an on-chain component in and of itself, the type of software licence applicable to the software in question can be of material importance, both for on-chain and off-chain components. In terms of software licenses applied to the smart contracts that power applications, two distinct avenues unfold, guiding blockchain projects down two different paths: open-source or closed-source. In terms of their impact on decentralisation, it is safe to say that closed-source licenses tend to centralise projects by impeding users from examining how the application/project, and tend to discourage collaboration. Since the open-source licensing model tends to contribute positively to the project's degree of decentralisation, it is worth analysing the most used licensing models used in this context and their contributions to a project's decentralisation.

The MIT Licence retains its position as the most widely adopted software licence to date. Under this licence, the code can be modified and distributed for commercial purposes as long as it includes the original copyright and licence notice. Alternatively, there exists the General Public Licence ('GPL') which is often witnessed in smart contracts. It is by virtue of a copyleft licence that ensures that derivative works or a licenced software remain free and open, requiring any derivative works to be distributed under the same licence, resulting in the extension of the spirit of decentralisation to possible forks and derivative SCs. Like the MIT licence, the Apache Licence 2.0 allows the grant of patent rights from contributors to users, which can incentivise broader adoption and contribution while also providing legal guarantees to users and contributors. Lastly, the BSD Licence is a permissive licence with minimal restrictions on the use and the distribution of the smart contract protected by it – arguably not lending as greatly towards the cause of decentralisation as the other licences.

1.2.2 Intro to the Off-Chain Section

A proper analysis of the level of decentralisation of blockchain applications typically merits a contemplation of any off-chain components. The off-chain components of a blockchain application may not be the ones that come to light at first glance; however, as the decentralised applications landscape continues to evolve, the current limitations of the most popular L1 blockchains at times give developers no other viable short-term solution than resorting to off-chain components. This growing trend can pose

Office 11, Capital Workspace, Onsite Buildings,
Level One, Valley Road Birkirkara, Malta BKR9021
info@bcas.io | www.bcas.io

several concerns regarding decentralisation. The use of on-chain, transparent components heavily jars with the use of off-chain components running on local instances that are often not transparent at all.

Despite the challenges, there is still some hope of maintaining a significant degree of decentralisation while recurring to off-chain components. The course towards a more decentralised future can be steered by applying specific implementations to manage such components. To present such implementations, we will first define the most commonly-used off-chain components leveraged by L2s, cross-chain bridges, and other decentralised applications. We will then propose ways to navigate the potential pitfalls of centralisation.

To this end, we will be addressing the following off-chain components:

- Oracles.
- Bridges Off-chain Agents.
- Sequencers.
- Aggregators.
- ZK Proof Generators.

1.2.2.1 Oracles

As mentioned in the introduction, oracles can be present an off-chain component in blockchain projects. While the most decentralised oracle services a project can rely upon are on-chain oracles, which reach their consensus and publish the outcome of their deliberations directly on-chain, it can be somewhat unavoidable for certain projects to rely on off-chain oracles.

For instance, a set of off-chain oracles may be suitable for the following situations:

1. To send information between different and uncommunicated layers of the same chain, such as the Ethereum consensus Layer and its execution Layer.
2. When using on-chain oracles would incur excessively high gas costs.
3. Where the complexity of the necessary smart contracts could result in infinite loops, leading to transaction failures and excessive gas consumption.

Generally, these off-chain services are provided by a type of software known as daemons. These daemons are programs that run in the background of computers without requiring active participation from those operating them.

Office 11, Capital Workspace, Onsite Buildings,
Level One, Valley Road Birkirkara, Malta BKR9021
info@bcas.io | www.bcas.io

When using on-chain oracles is not feasible due to the reasons mentioned above or other concerns, the best compromise possible is for DAOs to vote on which off-chain oracles are run by which persons, with the DAO retaining oversight over the behaviour and performance of such persons to determine their continued suitability as Oracle service providers.

1.2.2.2 Off-Chain Bridges Agents

Another concerning aspect is the reliance on off-chain agents for bridging communication between blockchains. Like the off-chain oracles discussed previously, these off-chain components that can be fundamental for cross-chain messaging can also, however, undermine a project's general decentralisation. While solutions, such as the latest version of LayerZero[8], have made significant strides in enabling decentralised oracle services to function as relayers, many bridge solutions still depend on off-chain services.

For example, optimistic bridges like the Nomad Bridge[9] rely on off-chain agents alongside their smart contracts to provide cross-chain communication. These off-chain agents are responsible for validating and signing messages from the source chain before transmitting them to the destination chain. Additionally, other off-chain agents monitor these messages' validity and contest them if necessary. Lastly, off-chain agents confirm to the source chain when the destination chain has received its message. Despite establishing economic incentives, staking guarantees, and penalties designed to discourage misbehaviour, the risk of centralisation remains significant in this setup.

Cosmos' Inter-Blockchain Communication (IBC) protocol utilises off-chain relayers for cross-chain messaging. However, the IBC approach appears somewhat less centralised compared to other off-chain solutions. In the IBC framework, relayers focus mainly on message transmission, while on-chain components exclusively manage critical tasks such as verification and message construction.

As we will explore in the off-chain software license section, making these off-chain components open source and encouraging broader participation can bolster the project's decentralisation, ensuring as

[8] https://docs.layerzero.network/v2/home/v2-overview
[9] https://docs.nomad.xyz/the-nomad-protocol/off-chain-agents

much as possible that all contributors have access to essential tools and resources to participate in the project.

1.2.3 Off-Chain Scaling

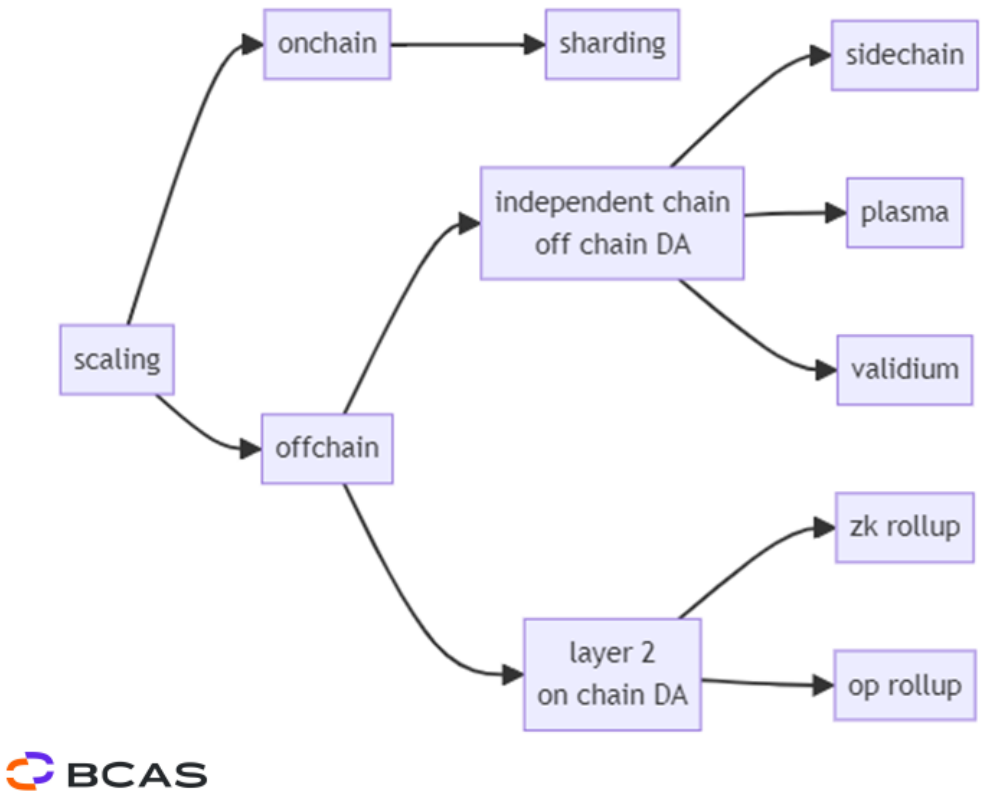

Figure 1: A visual overview of blockchain scaling solutions

Multiple solutions are being researched and implemented to try to solve the blockchain scaling trilemma (i.e. the challenge of achieving decentralisation, security, and scalability simultaneously in blockchain networks, where enhancing two aspects often compromises the third.) While on-chain scaling solutions refer to scaling the main settlement layer, off-chain scaling solutions use components that are separate from the L1 network and thus do not need changes to the settlement layer protocol. When analysing any scaling solutions, a closer look is needed at the off-chain components to determine their potential impact on the overall level of centralisation.

1.2.3.1 DA Layers

Office 11, Capital Workspace, Onsite Buildings,
Level One, Valley Road Birkirkara, Malta BKR9021
info@bcas.io | www.bcas.io

The first point of consideration for off-chain scaling is the data availability (DA) layer. In blockchain networks, data availability is defined as the capacity to retrieve and verify every transaction across a decentralised network. It ensures that all transactions contained within a block are accessible to each participant for independent verification.

From a scalability perspective, moving the DA layer out of the L1 network removes significant data load hence increasing speed, response time and throughput while decreasing transaction fees. However, when looking at a scaling solution that uses a separate DA layer rather than the L1 itself, we can note that they introduce additional trust assumptions on top of it. For instance, a Validium rollup which stores transaction data on a separate DA layer could be considered more centralised than a ZK rollup which posts each transaction data on a L1.

	Validity Proofs	Fraud Proofs
Data On-chain	ZK-Rollup	Optimistic Rollup
Data Off-chain	Validium	Plasma

1.2.3.2 Rollups

Rollups, as the name implies, combine multiple transactions that are executed off-chain into a batch which is then posted on the L1. There are two methods on how we can verify if the transactions are legitimate – either by using ZK proofs in ZK systems, or by using fraud proofs in Optimistic rollups. When looking at the architecture, it is important to define all the off-chain components such that their level of decentralisation can be assessed.

1.2.3.3 Sequencers

The act of sequencing in a blockchain refers to the process of ordering transactions. In L2s, since transactions are off-chain, they need to be ordered, formed in a batch and submitted to the L1 consensus contract. Most rollups use centralised and trusted sequencers. While a sequencer cannot 'steal' users' funds, user transactions can be censored and network liveness can be impacted if this trusted/centralised sequencer goes offline. There have been numerous occasions where a bug is

discovered[10] or a hack is ongoing on an L2 dApp[11], and the team behind the L2 pause the sequencer in order to protect user funds. While it is commendable to primarily consider the users' own interests, this is also resulting in a heavy element of centralised control exerted by the team in halting the network. There are several solutions being researched into decentralising the sequencer for example: based rollups (where the sequencing is the responsibility of an L1 node)[12] and shared sequencer networks.[13]

1.2.3.4 Aggregators & ZK Proof Generation

In ZK rollups, the main role of the aggregator is to take the L2 batches committed by the sequencer and generate ZK-proofs attesting to the batches' computational integrity. These ZK proofs are easy to verify however they are computationally intensive to generate. This can be seen from the high system requirements for running a prover. For instance, a Polygon ZK prover required 1TB RAM with a 128-core CPU. Naturally, such high requirements would tend to centralise this service and in fact, this seems to be the current trend in ZK Layer 2s. Work is ongoing in decentralising the proof generation by, for example, having an open marketplace to generate these proofs.

1.3 Governance Decentralisation

In the spirit of decentralisation, and in light of the fact that consensus can be achieved in trustless environments, DAOs have merged with the aim of following the same ethos. They essentially exist when a sufficiently large number of participants work collaboratively and take decisions on the general path forward and growth of projects. Typically, these autonomous organisations rely on a crypto-asset, being the *governance token* mentioned in the introduction, which serves as a quantifiably weighted measure of voting participation and other relevant actions.

DAOs can grant the *governance token* holders the ability to steer the organisation's direction by enabling them to both submit and vote on proposals and, in some cases, the opportunity to participate in the distribution of a protocol's generated revenues. Governance token holders typically stop short of enjoying rights that are otherwise attributable to equity; for instance, typically there are no proprietary

[10] https://cointelegraph.com/news/polygon-zkevm-mainnet-beta-sequencer-issues
[11] https://x.com/Scroll_ZKP/status/1814275555681771784
[12] https://taiko.xyz/
[13] https://www.espressosys.com/

Office 11, Capital Workspace, Onsite Buildings,
Level One, Valley Road Birkirkara, Malta BKR9021
info@bcas.io | www.bcas.io

rights whatsoever, and one may even argue whether governance token holders enjoy any 'rights' in the traditional sense of the word. However, DAOs per se do not guarantee the decentralisation level of a project. To understand the extent of decentralisation of a DeFi protocol that has implemented a DAO, it is necessary to discern what kind of control is granted to these token holders and how governance tokens are distributed among the token holders.

Some blockchain-based projects have implemented systems where all governance powers are handed over to the token holders to purportedly achieve a higher degree of decentralisation. This allows them to participate in the project's overall management by creating a mechanism where any token holder can propose, discuss and vote on any changes that need to be implemented. However, when the responsibility for implementing the code that emerges from a governance proposal remains in the hands of a few, the decentralisation of the whole project may be impacted as a result.

It has become commonplace to find projects that claim to be DAO-governed, with the token holders seemingly responsible to carry out an established (or non-established) roadmap. In reality, token holders would only be allowed to propose, discuss and vote on any improvements that are ultimately within the admin key holders' discretion to implement. In these governance designs, control rests mostly with the creators, owners or operators responsible for implementing any proposed changes. With such an obvious elephant in the room present, governance tokens in such instances may well represent nothing more than a non-binding sentiment indication, falling short from truly granting 'power to the people'.

Another concerning point regarding DAOs and their actual degree of decentralisation remains in the power that some 'DAO-adjacent entities' hold over the protocol (or more widely, the project) in question. Such centralisation of power often manifests itself in decisions these 'DAO-adjacent entities' take without involving the DAO or the governance token holders. For instance, projects claiming to be decentralised through tokenised governance may not live up to a sufficient level of decentralisation should such DAO-adjacent entities refrain from seeking the approval of their mandate from the DAO itself or, at the very least, keeping the DAO itself regularly updated with their day-to-day operations.

As mentioned before, the dynamic operation and management of blockchain-based projects, especially those which are still subject to regular and ongoing development, may not adequately be done if each decision concerning the protocol has to undergo a formal DAO voting process each time. Therefore, the establishment of 'DAO-adjacent entities' to conduct specific activities on their behalf can perhaps be said to be an almost-indispensable requirement given the current realities. However, in such cases, the

Office 11, Capital Workspace, Onsite Buildings,
Level One, Valley Road Birkirkara, Malta BKR9021
info@bcas.io | www.bcas.io

best approach is to establish, by a decision involving the governance token holders, what functions these 'DAO-adjacent entities' will perform (even through a mandate that is voted upon once, but with specific parameters), and how they will be held accountable to the DAO.

1.3.1 Decentralised Governance Frameworks

A proper decentralised system where governance token holders are the project's controllers is neither the most straightforward of implementations, nor is it one that can reasonably be achieved over a short time-frame. However. by implementing such solutions, project creators, owners, or operators can renounce the admin keys of the protocol that allow them to unilaterally shut down or turn off smart contract-enabled applications, handing them over to the project's governance to implement upgrades and act in cases of emergency.

Such can best be accomplished through on-chain governance. In on-chain governance systems, users have to perform an on-chain transaction to vote, and the outcome of each proposal and each user's decisions are recorded and stored on-chain. Although this approach may seem costly, as voting will incur transaction costs, transparency increases in this context. Furthermore, when implementing on-chain schemes, proposals can be submitted with a script, a brief program or a set of instructions containing the implementations the proposal intends to carry out in the project. Once a proposal is approved, the script can be implemented automatically, or allow any user to implement it by calling a function. However, while on-chain governance is an excellent tool to ensure the highest degree of control over a project by the relevant governance participants, still, off-chain tools are often necessary to complement the proper day-to-day functioning of a DAO. Combining the discussion of governance forums with a non-binding (sentiment) off-chain vote to ensure support, and critically-constructive discussions, for proposals seems to be a useful catalyst for a well-balanced implementation of on-chain governance.

1.3.2 Governance Token Distribution

Lastly, another critical parameter to consider when analysing the decentralisation level of governance is the distribution of governance tokens amongst their holders. Concentrated holdings of governance tokens tends to take a heavy toll on the actual degree of decentralisation; the use of tools to decentralise

Office 11, Capital Workspace, Onsite Buildings,
Level One, Valley Road Birkirkara, Malta BKR9021
info@bcas.io | www.bcas.io

a project may well all be in vain, if ultimately a significant portion of governance tokens are held by one, or a few individuals.

To determine whether an amount of governance token holdings can be deemed to be significant, one yardstick that can be used is to evaluate the implemented quorum required for proposals to pass, and also the average turnout of votes for proposals which meet the quorum. If a particular holder retains enough governance tokens to single-handedly meet a quorum and, moreover, is likely to be able to sway proposals in their favour by voting, then the holder in question may be deemed to be significant. This can also be extended to other notable holders especially if there are indications that they may be acting in collusion. While such criteria may not necessarily, on their own, result in a death knell in terms of decentralisation prospects, they may well negatively affect a project's level of decentralisation.

Such points, however, cannot be considered in a vacuum. It may be argued that even if only a few governance token holders vote on proposals and reach a consensus to approve them, the project can still be categorised as decentralised if such token holders still are not generally holding a high percentage of the overall circulating governance token supply. When a few users significantly influence the project's future based on the inaction of the rest of the token holders, the project/protocol may still be seen as *capable* of decentralisation, with an ideal solution being the incentivisation of dormant token holders (without, however, turning them into mercenary voters).

1.4 User Interface Decentralisation

One advantage of smart contracts deployed on permissionless blockchains is that any user can interact directly with them without permission. However, interacting directly with a smart contract requires certain technical skills that can hardly be said to be widely diffused. To foster wider adoption, projects build graphical user interfaces that make it easy for non-technical users to interact with them. Interfaces allow users to access the functions provided by smart contracts in a simplified manner.

1.4.1 Front Ends (Website)

However, interfaces may well present another potential element of centralisation. When the interface integrates a component, controlled by one entity or a small group of entities, that could restrict users

from accessing the underlying smart contract or certain features thereof, the decentralisation of a project may be undermined especially if it is the sole means of accessing, through a GUI, the underlying protocol.

One possibility to avoid potential unilateral restrictions is to establish appropriate tools that allow the DAO to have control over an interface's implementation to ensure that no user is restricted from accessing smart contract functions through the interface. While protocols can set up a special commission of relevant individuals chosen by the DAO, who are accountable to the DAO in managing the development of the interface, and owning the web domain or application in question, these can at best be described as half-way compromises, given that ultimately it is still one person (natural or legal) that owns the domain due to the nature in which domain name systems are registered and held.

A better solution to somewhat overcome this considerable obstacle is to dedicate efforts promoting the set-up of alternative interfaces. As long as the project code is available, any developer can create an interface to interact with the underlying smart contracts. While this may be easier when projects only have a web front end, some DAOs have chosen to compensate those who build an interface to access their services through websites, desktop or mobile apps. Offering incentives to create different interfaces tends to be a commendable option.

However, the user interface components comprise two other aspects that need to be assessed when assessing a project's level of decentralisation: a) RPCs, and b) wallets.

1.4.2 RPCs

When users interact with a blockchain, messages (whether reading data from an on-chain contract or broadcasting a transaction) need to be sent to a node. An RPC node is a piece of infrastructure that allows applications to communicate with the blockchain. The RPC node is a full node that also has an RPC Application Programming Interface ('API') endpoint available, with the most common being a JSON-RPC. Most users tend to keep the default RPC set in their wallets, and by using centralised RPC providers, their transactions can be monitored and censored. There have been cases in the past where large RPC providers blocked access to certain websites, like tornado.cash[14], as well as blocking users

[14] https://cointelegraph.com/news/alchemy-and-infura-block-access-to-tornado-cash-as-vitalik-buterin-weighs-in-on-debate

coming from certain regions such as Venezuela from accessing or managing their funds.[15] Alternatively viable RPCs are important in ensuring a greater degree of decentralisation.

1.4.3 Wallets

As the blockchain industry still struggles to significantly increase its overall user base, there is a growing trend among decentralised applications to offer their own developed wallet solutions to facilitate new user onboarding. Some precautions should be considered when offering such types of 'facilitated' user interfaces, since the manner in which the wallet is built can harm the overall decentralisation of the project providing it. Unfortunately, there tends to be a trade-off when balancing decentralisation and user experience. One of the most discussed points in this regard is the storage of private keys or seed phrases related to custodial wallets, that provide its holder with the exclusive disposition and management of the crypto-assets under that key pair and how it complicates the experience for new users.

It is undeniable that 'non-custodial' wallets, meaning where users do not have sole and exclusive custody of their crypto-assets, certainly run counter to the concept of decentralisation. In order to still maintain a healthy degree of decentralisation while enhancing the user experience and reducing some barriers to entry, projects can opt for the following types of wallets:

- **Account abstraction.** When applied to crypto-wallets, account abstractions allow the separation of wallet functionality from the underlying blockchain protocol rules. In this sense, by creating smart contracts to handle transaction logic and wallet creation, the user experience can be enhanced without losing transparency and crypto-assets custody while maintaining a decentralisation approach.
- **Multi-party computation.** This software concept, when applied to crypto wallets, implies dividing the private key into several parts and storing each part in a different location. In this context, while users avoid dealing with private keys and seed-phrases storing, there is no single entity entitled to the whole private key. However, the overall decentralisation of this type of wallet depends on the constitution of such entities.
- **Guardians' system.** A system pioneered by Argent Wallet [16] prevents users from handling private keys and seed-phrases storage. Instead, a user's private key is locally stored on the

[15] https://crypto.news/consensys-infura-metamask-venezuelan-users/
[16] https://www.argent.xyz/

Office 11, Capital Workspace, Onsite Buildings,
Level One, Valley Road Birkirkara, Malta BKR9021
info@bcas.io | www.bcas.io

user's device, while recovering the private key itself in case of a loss would require a set of Guardians. These guardians are other crypto-addresses designated by the user. If a recovery is required, the guardians must sign a transaction confirming the identity of the user, thereby allowing the private key recovery to take place.

1.5 Operations Decentralisation

Decentralised projects usually require input from external actors, such as service providers, in order to scale effectively, obtain relevant advice (such as legal), or otherwise generally ensure the proper running of the project in question. To address this demand, collaborators who may not necessarily be governance token holders may need to be involved. In some cases, external collaborators are also brought in to modify the project code and assist with its maintenance.

Roping in such external parties in the overall maintenance of a project should be properly structured in order to lessen the impact over the level of decentralisation. While certain service providers may be seen as offering non-key services, especially if in an advisory capacity, others that do offer key services should either be integrated within a DAO's overall structure, or as a minimum, governance token holders should have an appreciable degree of decision-making power in appointing such key external service providers. The setting-up of committees dedicating to such outsourcing measures could be a possible compromise, albeit one that may still somewhat lesson a DAO's overall level of decentralisation. These committees can also take the form of sub-DAOs, which tend to be larger and more structured in nature, perhaps even with their own governance processes and funding.

Should sub-DAOs or committees be considered, the project's governance token holders should still have a material say in their constitutive setups and tenure, retaining some form of accountability towards the main DAO itself. If properly implemented, DAO-governed projects can remain competitive, dynamic, and efficient, without necessarily sacrificing much in terms of the overall level of decentralisation.

A similar ethos would apply in terms of funding such sub-DAOs or committees, where a budget can be approved by the governance token holders and assigned to the sub-DAOs or committees in question. Principles-based parameters can be set by the DAO in terms of budget spending, with day-to-day spending left within the discretion of the sub-DAOs or committees themselves. Additional measures can include pre-defined limits set by the governance token holders and appropriate DAO mechanisms

Office 11, Capital Workspace, Onsite Buildings,
Level One, Valley Road Birkirkara, Malta BKR9021
info@bcas.io | www.bcas.io

for selecting, removing, and overseeing committee members' accountability, thereby ascertaining fluidity in day-to-day operations while maintaining a sufficient degree of decentralisation. It goes without saying that such options are mostly applicable to DAOs exceeding a certain size.

1.6 Technical and Organisational Conclusion

To summarise, from a technical point of view, one can conclude that the level of decentralisation of a project requires a comprehensive approach that addresses multiple facets of its design and operation. To avoid centralisation and, as a result, align with the core principles of decentralisation, the following five key perspectives should be considered:

- **Settlement Layer Decentralisation:** From a settlement layer decentralisation perspective, it is essential to guarantee that the blockchain on which a project is deployed, whether it relies on a PoW, PoS, or dPoS consensus mechanism, operates across a sufficiently large number and geographically distributed network of nodes. In this sense, unrestricted access for node participation is crucial as it allows a diverse range of participants to contribute to the network, enhancing its overall decentralisation. Specifically focusing on PoW networks, the distribution of hashing power among numerous miners is essential for reducing the risk of central control. In blockchains that reach their consensus through a PoS mechanism, the distribution of native tokens across many holders supports decentralisation by ensuring that no single participant can retain a significant influence in the consensus process. Lastly, for dPoS blockchains, the greater the number of validators and the more evenly the stake is distributed among them, the more decentralised the network will be, preventing any single entity from exercising an excessive influence over the network. All in all, a broad distribution of power and participation over the network consensus mechanism helps to mitigate the risks associated with centralisation from a settlement layer perspective.

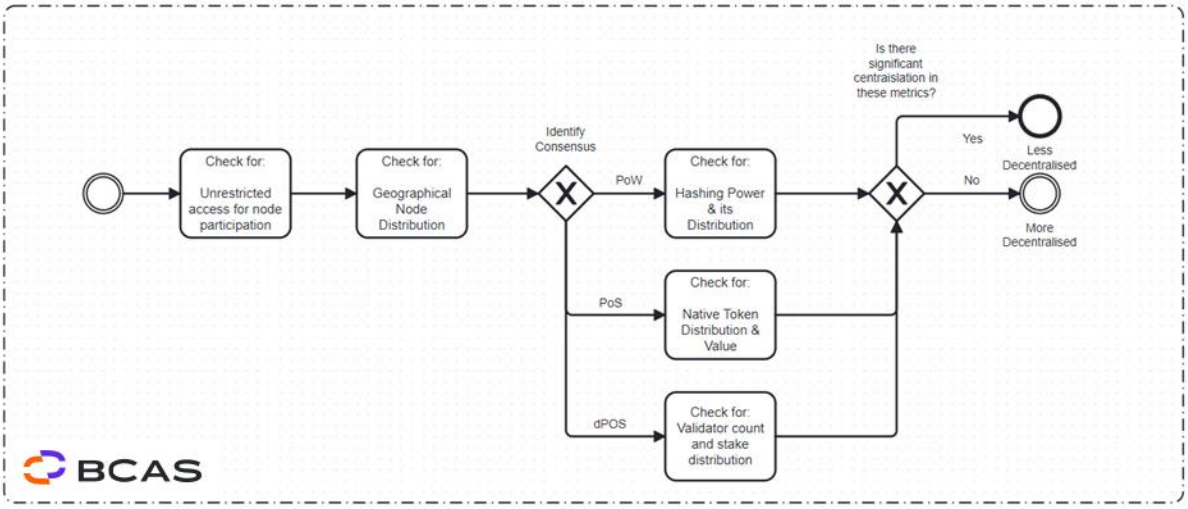

Figure 2: Settlement Layer

- **Architecture Decentralisation:** Under this element, both on-chain and off-chain components must be considered. Regarding on-chain components, while smart contracts themselves embody decentralisation by being executed without intermediaries, the possibility of upgrading them and how such is managed can pose concerns of centralisation. In the same vein, the existence of functions to be triggered under special conditions, such as those that pause smart contract under emergency situations, and who is authorised to call them, can likewise give rise to issues of centralisation. Ideally, when updates to smart contracts are needed or special functions must be called, such should either be performed or sanctioned by a DAO, rather than by a single individual related to the project, or a group of operators designated without involving *governance token holders*.

  Additionally, as oracles are essential for providing external data to blockchain projects, not relying on a private and centralised oracle network contributes towards a project's level of decentralisation. Although it can be challenging to rely on a fully decentralised oracle solution, as the number of oracles retrieving information from outside the blockchain and achieving consensus on that information increases, the overall decentralisation of a project can be enhanced too. Furthermore, allowing anyone willing to participate in the oracle network contributes to the same sense.

  Contrary to on-chain components, off-chain components may, due to their nature, introduce centralisation concerned. In this regard, it is important that these components, when unavoidable, are ideally open-sourced. By adopting this measure, transparency and

unrestricted access for users can be achieved, somewhat off-setting part of the centralisation risks associated with proprietary off-chain elements.

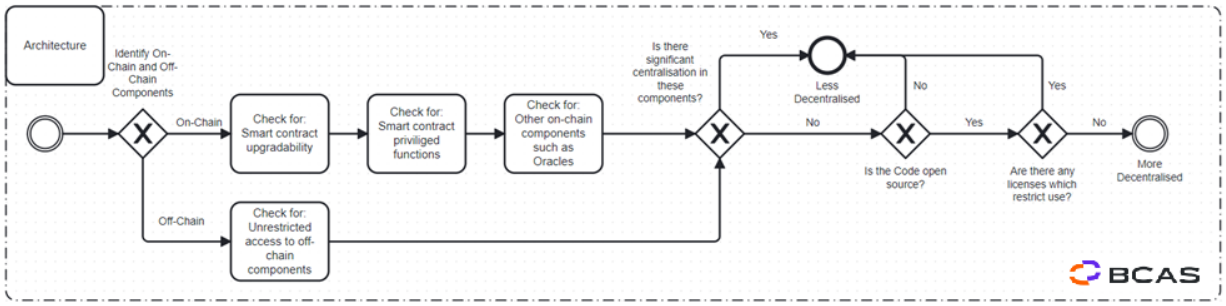

Figure 3: Architecture

- **Governance Decentralisation:** The establishment of the governance structure of a blockchain project and how its day-to-day decisions are made, are vital when it comes to analysing its decentralisation level. In this context, DAOs provide a framework to establish decentralised governance, enabling governance token holders to vote on proposals and steer the direction of the project. However, while establishing a mechanism to submit and vote on proposals is a valuable first step, it must be paired with a widespread distribution of governance tokens to avoid situations where proposals are being overly influenced by a reduced group of participants. Additionally, it is important to highlight that governance token holders must have influence over key project decisions, in contrast to a scenario in which governance token holders decide on matters that do not have a significant impact on the direction of the project.

  As mentioned in the Governance Decentralisation section, relying on 'DAO-adjacent entities', such as foundations, can be necessary to streamline the efficient development of a project. In order to not undermine the decision-making rights of governance token holders, they should be involved in the selection of these entities, as well as in the definition of their functions and related payments. Finally, decentralised governance systems should also have transparency and accountability mechanisms, such as on-chain voting and clear rules for the roles of external actors and committees, in order to maintain a balance between operational efficiency and decentralised control.

- **User interface Decentralisation:** Management and control over an interface typically should be viewed from a broader perspective. While mainstream domain registrations remain a point of centralisation that is difficult to circumvent, efforts should be undertaken to ensure that there

is a degree of separation between those managing the interface, and those developing the underlying protocol. However, more importantly than that, ensuring that the user interfaces that allow the same users to interact with the project's smart contracts are implemented through multiple independent providers contributes to a higher level of decentralisation.

As mentioned in the user interface decentralisation section, to read or send information to a blockchain, users interact with nodes through RPCs. Once these RPCs are centralised by a project, they can lead to surveillance or censorship activities. In this sense, to increase their level of decentralisation, it is recommended to rely on decentralised RPC providers. Finally, another point of concern, in relation to the decentralisation of the user interface, are the wallets provided by blockchain projects. Balancing decentralisation with user experience is crucial. Therefore, options that include account abstraction, multi-party computation and guardian systems are considered more decentralised compared to custodial wallets and, at the same time, simplify the user experience compared to traditional non-custodial wallets.

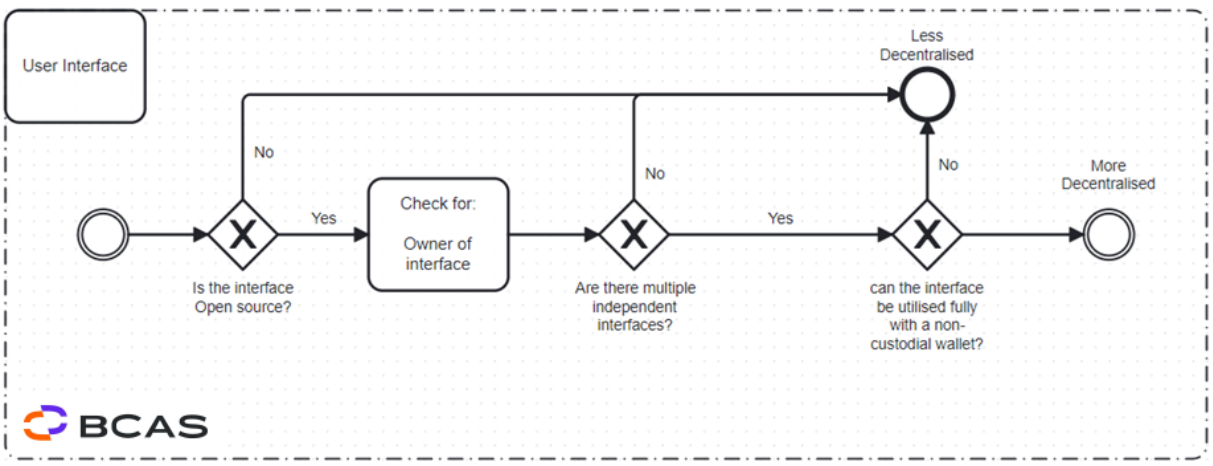

Figure 4: User Interface

- **Operations Decentralisation:** The final angle from which the level of decentralisation of a project can be approached relates to its operations. Examples of operational decisions, such as payments to contributors, must be properly managed in order for projects to remain sufficiently decentralised. To avoid being seen as a centralised project, these operational decisions should be made in as decentralised a manner as possible, such as through a DAO, rather than centralising these decisions to individuals related to the project. Where external service providers are engaged, it is recommended to integrate their accountability into the DAO structure and ensure that governance token holders can participate in their selection and removal. In this context, a decentralised approach warrants that governance token holders

maintain oversight of project operations without interfering in the day-to-day running of the project.

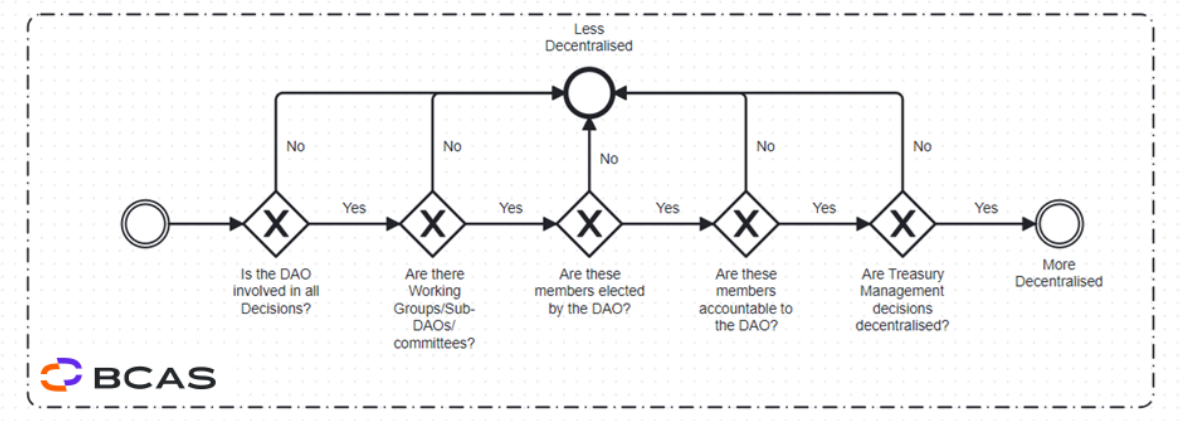

Figure 5: Operations

2. Decentralisation under MiCA

While the term 'decentralisation' can be, and in fact has been, approached from various angles, its meaning can be said to have a more nuanced angle under the Markets in Crypto-Assets Regulation (MiCA). Typically, decentralisation is linked to the provision of crypto-asset services as defined under MiCA, with a general understanding that if there is sufficient decentralisation, then there should be no person qualifying as a crypto-asset service provider (CASP), thereby falling outside of scope of MiCA. This second half of the handbook will delve into the regulatory considerations under MiCA with respect to the concept of decentralisation, dissecting the definition of a CASP along the way, and ultimately reaching a conclusion on how, and why, decentralisation matters.

2.1 A MiCA Refresher

MiCA can safely be said to be the most comprehensive effort, to date, in regulating the crypto-asset industry. While the first part relating to EMTs and ARTs already became applicable earlier on the 30th of June, the major date to watch out for is the 30th of December 2024, when the rest of its Titles become applicable in full. MiCA seeks to regulate the industry by bringing within its remit the following:

- Persons issuing and offering crypto-assets to the public in the EU/EEA;

- Persons seeking admission to trading of crypto-assets on trading platforms in the EU/EEA; and
- Persons offering crypto-asset services.

While it does not directly regulate crypto-assets in and of themselves, as it regulates *persons issuing, offering, seeking the admission to trading, and providing services* vis-a-vis crypto-assets, it does cater for an interesting crypto-asset taxonomy split into three distinct categories as follows:

1. E-Money Tokens (EMTs), being crypto-assets that purport to maintain a stable value by referencing one official currency.
2. Asset-referenced Tokens (ARTs), being crypto-assets that are not an EMT, and which purport to maintain a stable value by referencing any other value or right or combination thereof, including one or more official currencies.
3. Other crypto-assets (OCAs), being crypto-assets that are neither an EMT nor an ART, or any other crypto-asset excluded from MiCA under Article 2(4), such as financial instruments and structured deposits. 'Utility Tokens' are a sub-set of OCAs, and are defined as *crypto-assets that are only intended to provide access to a good or a service supplied by their issuer.*

While offers to the public of crypto-assets may pose some issues for front-end operators in the crypto space, the main headache for DeFi seemingly stems from the (in)famous Recital 22, which states 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.*

The good news is that there is a difference between Recitals and Articles; the latter are the actual law. Recitals therefore do not have the weight of the law; however, Recitals convey the intent of the legislator and the spirit within which the actual law was written. This often means that whatever is in the Recitals, is likely to be found within the letter of the law itself – sometimes buried quite deeply indeed. What follows next is a digging exercise to unearth what the legislator meant with the enigmatic wording of 'fully

Office 11, Capital Workspace, Onsite Buildings,
Level One, Valley Road Birkirkara, Malta BKR9021
info@bcas.io | www.bcas.io

decentralised', and the practical implications thereof for DeFi. To do so, we shall break down every single word constituting the definition of a CASP, and by setting the boundaries for a CASP, simultaneously discover the ether within which DeFi can exist – outside of scope of MiCA.

2.2 Crypto-Asset Service Providers

MiCA defines a CASP, under 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*".

This definition can be broken down into 6 distinct elements as follows:

1. A legal person or other undertaking
2. Acting by way of an occupation or business
3. The provision of one or more crypto-asset services
4. Targeting clients
5. On a professional basis
6. Authorisation to provide crypto-asset services

We shall now take each element in turn, and dissect it further to its bare molecules; in turn, linking each element to the other, and as a result determining what can be outside the scope of the definition of a CASP.

2.2.1 A Legal Person or other Undertaking

While the term 'legal person' is self-explanatory, the term 'undertaking' deserves a profound analysis, as it is a term that may well capture most of the structures that we think of as decentralised autonomous organisations (DAOs).

The term 'undertaking', although consistently present across multiple pieces of EU legislation, is not formally defined anywhere. Instead, it has been defined in piece-meal fashion across the years through case-law decided by the European Court of Justice (ECJ) across different areas of EU law. While the relevant cases were mostly decided in relation to the conduct of legal persons constituted as limited liability companies, the findings can be applied to other forms of legal persons, incorporated or unincorporated. References to parent and subsidiary companies can be extended to refer to natural

Office 11, Capital Workspace, Onsite Buildings,
Level One, Valley Road Birkirkara, Malta BKR9021
info@bcas.io | www.bcas.io

person shareholders, or persons exercising decisive influence and control. The key cases are summarised below.

i. Hofner and Elser v Macrotron (C-41/90), decided on April 23rd, 1991, is deemed to be the first case where the ECJ had defined an undertaking as "*any entity engaged in economic activities, regardless of its legal or financing form*". The ECJ had maintained this position in various, more recent cases, such as *Ministero dell'Economia e delle Finanze v Cassa di Risparmio di Firenze SpA and Others (C-222/04, decided on 10 January 2006)*.

ii. In the case of Pavlov and Others v Stitching Pensioenfonds Medische Specialisten (Cases C-180/98 to C-184/98, delivered on September 12, 2000), the ECJ clarified that "*entities offering services on a not-for-profit basis can still be considered undertakings if they compete with other operators that do seek to make a profit*". In this decision, the ECJ emphasises the functional aspect of activity over the form of organisation or profit motive.

iii. The ECJ detailed further this position in the case of Motosykletistiki Omospondia Ellados NPID (MOTOE) v Elliniko Dimosio (C-49/07, decided on 1 July 2008) where the Court stated that "*the fact that the offer of goods or services is made on a not-for-profit basis does not prevent the entity which carries out those operations on the market from being considered an undertaking, since that offer exists in competition with that of other operators which do seek to make a profit*".

iv. Perhaps one of the most important cases is the Akzo Nobel case (C-97/08, decided on 23rd April 2009), where the Court has ruled that "*the absence of autonomy of the subsidiary in terms of its market conduct is only one possible connecting factor on which to base an attribution of responsibility to the parent company. It is not the only connecting factor, for, according to the Court's caselaw, attribution of conduct to the parent company is possible 'in particular' where the subsidiary, although having separate legal personality, does not decide independently upon its own conduct*". With respect to the connecting factors, the Court went on to say: "*the decisive influence of the parent company does not necessarily have to result from specific instructions, guidelines or rights of co-determination in terms of pricing, production and sales activities or similar aspects essential to market conduct. Such instructions are merely a particularly clear indication of the existence of the parent company's decisive influence over its subsidiary's commercial policy. However, autonomy of the subsidiary cannot necessarily be inferred from their absence [...] A parent company may exercise decisive influence over its subsidiaries even*

Office 11, Capital Workspace, Onsite Buildings,
Level One, Valley Road Birkirkara, Malta BKR9021
info@bcas.io | www.bcas.io

when it does not make use of any actual rights of co-determination and refrains from giving any specific instructions or guidelines on individual elements of commercial policy. Thus, a single commercial policy within a group may also be inferred indirectly from the totality of the economic and legal links between the parent company and its subsidiaries".

The ECJ had further upheld the interpretation of the Commission's decision on the meaning of company responsibility in competition law. It has been established that the concept of undertaking for the purpose of competition law includes any entity engaged in economic activity, regardless of its legal status and the way in which it is financed. The ECJ confirms that such economic units may consist of several legal persons and that if any part of that entity infringes the competition rules the whole undertaking is liable to answer for that infringement.

v. In the case of SIA 'VM Remonts' and Others v Commission, (C-542/14) in line with the judgements in Akzo Nobel, it was stated that an undertaking must be understood as designating an economic unit even if in law that economic unit consists of several persons. Nevertheless, "*Where a service provider offers, in return for payment, services on a given market on an independent basis, that provider must be regarded, for the purpose of applying rules at penalising anti-competitive conduct, as a separate undertaking from those to which it provides services and the acts of such a provider cannot automatically be attributed to one of those undertakings*." This is a crucial case establishing situations where a service provider offering services on a completely independent basis would be considered as a separate undertaking.

vi. Although it's an older case, the ECJ in SA Musique Diffusion Française and others v Commission (Cases 100 to 103/80, decided on 7th June 1983) stated that "*it is not necessary for there to have been action by, or even knowledge on the part of, the partners or principal managers of the undertaking concerned; action by a person who is authorised to act on behalf of the undertaking suffices*".

vii. Lastly, on the concept of 'economic activities', the ECJ in Congregación de Escuelas Pías Provincia Betania v Ayuntamiento de Getafe (C-74/16, decided 27 June 2017), stated that "*Services normally provided for remuneration are services that may be classified as 'economic activities*".

Office 11, Capital Workspace, Onsite Buildings,
Level One, Valley Road Birkirkara, Malta BKR9021
info@bcas.io | www.bcas.io

In summary, the term 'undertaking' can be defined as follows**: a natural or legal person(s) engaged in economic activities, regardless of their legal or financing form. The economic activities per se can be offered or undertaken with or without the intention to make a profit; what matters is that those economic activities, ergo the offering of goods or services, would be in competition with the offerings of other operators which do seek to make a profit. The term itself includes several legally independent undertakings participating in an economic activity, or in an agreement, as one party; an assessment of decisive influence cannot be made only by reference to policies and contractual wordings, but all other elements relating to economical, organisation, legal, and structural links between the various parties involved must be taken into consideration.**

2.2.2 Applying the Definition of an Undertaking to DAOs

How does the term 'undertaking' potentially impact DAOs? First and foremost, the term 'DAOs' itself is not one on which there is clear consensus in terms of its definition. It is perhaps safe to say that DAOs, in the truest and purest sense of the word, are very rare. It is more realistic to take an assumption that DAOs tend to be a mix of governance token holders, corporate entities, and links of varying degrees between the two, including of a statutory (catered for in the constitutive charters of the corporate entities) and/or fiduciary nature.

If there are no corporate entities, otherwise referred to as 'DAO-adjacent entities', it does not automatically mean that the DAO is not capable of legal form. Such DAOs may still meet the conditions of other legal forms, such as an unincorporated association, and potentially qualify as such depending on the applicable legal regime. An unincorporated association could still be seen as an undertaking, with the token holders possibly regarded as the members of that same unincorporated association.

However, the term 'undertaking' can also cohesively capture various elements in a 'DAO-governed' set-up, including other corporate entities which are separate and distinct from governance mechanisms or bodies that are DAO-ruled. Let's take a typical setup as an example:

1. DAO governance token holders which decide on criteria such as protocol upgrades, treasury management, etc;
2. Cayman Islands foundation company which acts as the 'front-facing entity' of the DAO as it is capable of entering into contractual relationships;
3. A dev-co which is one of (if not the only) main contributors to developing the code vis-à-vis the protocol or system in question; and

4. Multi-sig arrangements for smart contract deployment, treasury management, etc.

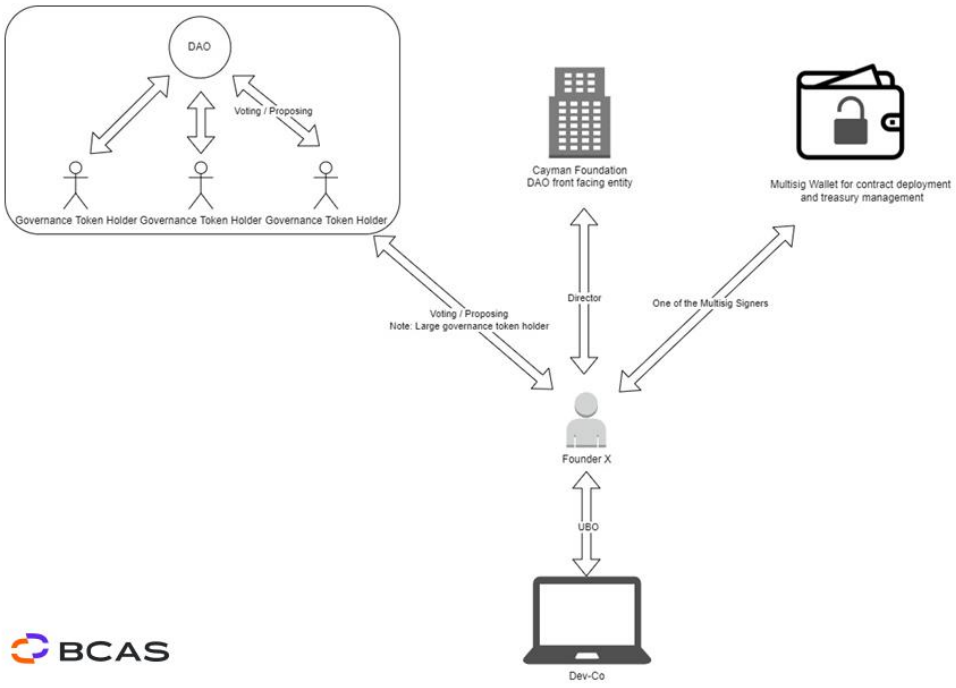

Figure 6: DeFi Protocol – Founder X

Let's say that the founder of a DeFi protocol, which we'll call Founder X, holds a notable amount of the protocol's governance token. Founder X is also a director of the foundation company and a UBO of the dev-co. To top things off, Founder X is also one of the signers in all of the multi-sigs (admin keys). Such a setup is likely to result in meeting the definition of an undertaking since it is highly likely that Founder X is exercising decisive influence, as well as control, over the management of the DeFi arrangement itself. This would be regardless of any wording in constitutive charters or 'soft' agreements that Founder X cannot vote on proposals put forward for the DAO's consideration and vote.

Naturally, the same can be said for any other person who is not necessarily a founder, but can be seen as exercising decisive influence and control – each and every constitutive piece of a 'DAO' in the general sense of the word must be truly autonomous and not subject to a 'hidden hand' controlling everything from the shadows, in order for such not to be considered as an undertaking.

2.2.3 Acting by way of an Occupation or Business

This second element may seem straightforward and self-explanatory, but it is interesting to note that the legislator opted for both 'business' and 'occupation'. It can well be interpreted that it does not matter whether a person is acting on their own behalf (as a business) or on behalf of others (by way of an

Office 11, Capital Workspace, Onsite Buildings,
Level One, Valley Road Birkirkara, Malta BKR9021
info@bcas.io | www.bcas.io

occupation, such as would be the case in employment). Moreover, the motif of economic activity as opposed to profit-seeking continues, since the use of both terms denotes a wide variance in the capacity under which persons may act. Last, but not least, this second element also points towards the likelihood that such acts should be the main activity being undertaken by the relevant person, and not on a one-off basis.

2.2.4 The provision of one or more crypto-asset services

Article 3(1)(16) provides us with the following list of crypto-asset services that are regulated under MiCA:

a. providing custody and administration of crypto-assets on behalf of clients;
b. operation of a trading platform for crypto-assets;
c. exchange of crypto-assets for funds;
d. exchange of crypto-assets for other crypto-assets;
e. execution of orders for crypto-assets on behalf of clients;
f. placing of crypto-assets;
g. reception and transmission of orders for crypto-assets on behalf of clients;
h. providing advice on crypto-assets;
i. providing portfolio management on crypto-assets; and
j. providing transfer services for crypto-assets on behalf of clients.

While each and every crypto-asset service may be relevant when making any assessments vis-à-vis DeFi, there are four in particular that tend to be the greatest causes for concern:

1. Providing custody and administration of crypto-assets on behalf of clients
2. Exchange of crypto-assets for other crypto-assets
3. Reception and transmission of orders for crypto-assets on behalf of clients
4. Providing transfer services for crypto-assets on behalf of clients

We shall now tackle each in turn, and clarify why they may pose issues for DeFi.

Providing custody and administration of crypto-assets on behalf of clients

This is defined under Article 3(1)(17) as:

The safekeeping or controlling, on behalf of clients, of crypto-assets or of the means of access to such crypto-assets, where applicable in the form of private cryptographic keys

First off the bat is the emphasis on there being either safekeeping or controlling. The two may be similar, yet not necessarily the same. "Safekeeping" denotes a duty to keep the crypto-assets safe, and diligently employ means to protect against external attacks; "controlling", on the other hand, is a much lower threshold, and simply refers to any means by which an element of control is exercised over the crypto-assets or the means of access to such. It would have been better had the legislator opted for the word "and" rather than "or", so that the two acts are cumulatively required in order for the crypto-asset service to subsist. Since either safekeeping *or* control can subsist, this means that a much wider net is cast.

The implications are somewhat limited through the use of the term "on behalf of clients", which requires a fiduciary obligation to be in place, and a client relationship to subsist (as we shall be covering later on). The safekeeping or controlling can be with respect to either the crypto-assets themselves, or the means of access to such crypto-assets through the possession of the relevant private cryptographic keys – although, on this last point, the legislator leaves open the possibility for other means of access to subsist and still fall within the scope of the definition.

The broad scope of this crypto-asset service leaves open to scrutiny many so-called DeFi arrangements out there, especially those which employ multi-sig wallets as their preferred means to both deploy and exercise control over their smart contracts, typically utilised in locker smart contracts which are a key element to most bridging architectures currently.

Exchange of crypto-assets for other crypto-assets

Article 3(1)(20) simply defines this as:

The conclusion of purchase or sale contracts concerning crypto-assets with clients for other crypto-assets by using proprietary capital

Contrary to perhaps popular belief, a purchase or sale contract does not need to be subject to standard terms, or even be in writing; contracts, after all, can be verbal too. What matters here is that there is the conclusion of a purchase or sale contract, with the service provider concluding such a transaction using its own proprietary capital.

This can well be the case if, for instance, a liquidity pool (LP) is set up by a person with the intention of trading a crypto-asset that forms part of their proprietary capital; while all the elements of a 'CASP' would still need to be satisfied, it is dangerous to presume that an LP on an AMM protocol is automatically outside of scope of MiCA just because it's deployed on a potentially decentralised protocol. The AMM protocol itself may be outside of scope (depending on how it is structured), but the

creation of an LP with the intention to operate it by way of a business or occupation is conversely likely to fall within the scope of MiCA.

The same service can also subsist in cases where DAO-owned crypto-assets are exchanged with another DAO's crypto-assets, commonly referred to as 'treasury swaps', or simply exchanged for other crypto-assets as part of a treasury management policy or process. If the 'DAO' is, for instance, 'wrapped' (i.e. represented within a legal entity), then such crypto-assets forming part of the treasury may well constitute proprietary capital of the 'DAO'.

Lastly, cross-chain bridges which allow for a swap of crypto-assets to occur (for example: sending ETH from Ethereum to receive OP on Optimism) could be seen as offering this service, depending on whether proprietary capital is being utilised for the swap to occur.

Reception and transmission of orders for crypto-assets on behalf of clients

This particular crypto-asset service can also pose issues for certain players in the DeFi space. It is defined under Article 3(1)(23):

Reception from a person of an order to purchase or sell one or more crypto-assets or to subscribe for one or more crypto-assets and the transmission of that order to a third party for execution

Immediately, DEX aggregators come to mind when reading the definition above. Most aggregators are centralised, and they are ultimately acting as recipients of purchase/sale orders by users, with the order then being transmitted for execution on a third-party platform – namely, AMMs. If the aggregator in question is not transmitting the order directly to the place of its execution but is simply acting as a router/relayer, then possibly the following service may subsist.

Providing transfer services for crypto-assets on behalf of clients

Article 3(1)(26) defines this crypto-asset service as:

Providing services of transfer, on behalf of a natural or legal person, of crypto-assets from one distributed ledger address or account to another

While miners, validators, and nodes seem to be given a pass as explained under Recital 93[17], other operators may fall within the scope of this service. Cross-chain bridges which facilitate transfers

[17] Such transfer service should not include the validators, nodes or miners that might be part of confirming a transaction and updating the state of the underlying distributed ledger.

between VM-incompatible networks risk being seen as providers of this service, as a transfer from one distributed ledger address or account to a completely different one is likely to occur.

Targeting clients

The above-mentioned crypto-asset services must be provided to clients for the service provider to meet the definition of a CASP.

Traditionally, the term 'client' refers to the person who receives the services provided. It is defined as such under the Markets in Financial Instrument Directive (MiFID II) to highlight the existence of a service provider-client relationship. MiCA aligns with MiFID II on this point, as its Article 3(1)(39) defines 'client' as "*any natural or legal person to whom a crypto-asset service provider provides crypto-asset services*".

Therefore, the definition of a CASP requires this service provider-client relationship by mentioning that crypto-asset services are provided to clients. The main question arising from this reference to a service provider-client relationship is whether it involves financial or economic compensation for the services provided. In this regard, remuneration should be treated as a major, albeit not sole, indicator of such a relationship. Indeed, other indicators must be taken into consideration, such as the contractual terms or, in the absence of such, the basis of the relationship between the presumed service provider and the presumed client.

It is important to note here that contractual terms can take various forms, including tacit. Therefore, they do not require a specific form, such as a written contract. For instance, the sole usage of a service might suffice to tie users to certain terms or rules. Therefore, those terms or rules must also be assessed when assessing the existence of a service provider-client relationship.

On a professional basis

While many EU directives and regulations use the term 'on a professional basis', EU regulators have not formally defined this notion. While assessing the scope of this term, the ECJ considered that it should be interpreted broadly to encompass all activities conducted as part of a business or professional activity, not limited to 'core' business functions but also including ancillary activity.

However, this interpretation does not fully uncover the meaning and implications behind the reference to 'on a professional basis'. At first glance, this condition, related to the way crypto-asset services are provided to clients, might be seen as an extension of the term 'business or occupation' previously mentioned and analysed. Indeed, it denotes and confirms the existence of economic activity, as it is highly unlikely that crypto-asset services are provided as a business or occupation without being provided on a professional basis.

Furthermore, considering the previous condition – ergo the existence of a service provider-client relationship – the question of whether the definition of a CASP requires some type of economic or financial compensation arises again. Indeed, it is safe to say that if an entity provides services to clients as a business and on a professional basis, such an entity expects to receive compensation or remuneration for the services provided. Therefore, the term 'on a professional basis' may also contribute to the need for one to receive a consideration so as to be considered as a CASP.

Authorisation to provide crypto-asset services

The last condition for an entity to meet the definition of a CASP is to be authorised to provide crypto-asset services in accordance with MiCA's Article 59.

It is clear that a person providing crypto-asset services without being allowed to provide such services in accordance with Article 59 does not fall within the definition of a CASP. However, such a person would not easily be let off the hook; instead, such a person would be put on a register of entities that provide crypto-asset services in violation of Article 59 or 61, as provided for in Article 110 of MiCA.

With the definition of a CASP being extensively covered, it is also worth dedicating some time to the definition of an "online interface" under MiCA, since this has also been the subject of debate.

2.3 Online Interface

When crypto-asset services are provided through the means of an online interface, the question arises whether the entity that owns and/or manages this interface can be seen as the entity providing services – and thus qualify as a CASP. MiCA stipulates the following as the definition of an online interface:

"'online interface' means any software, including a website, part of a website or an application, that is operated by or on behalf of an offeror or crypto-asset service provider, and which serves to give holders of crypto-assets access to their crypto-assets and to give clients access to crypto-asset services".

This definition can be broken down into 3 different elements as follows:

1. Any software, including a website, part of a website or an application
2. Operated by or on behalf of an offeror or CASP
3. Serves to give holders access to their crypto-assets and give clients access to crypto-asset services.

Office 11, Capital Workspace, Onsite Buildings,
Level One, Valley Road Birkirkara, Malta BKR9021
info@bcas.io | www.bcas.io

2.3.1 Any software, including a website, part of a website or an application

This first part of the definition is particularly broad. The term 'software' is used in different EU laws, where it is usually associated with the term 'computer program'. The European Commission issued a "Proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements" on September 15th, 2022, in which the term 'software' is defined as "the part of an electronic information system which consists of computer code."

This broad definition encompasses a wide range of electronic information systems, including websites and applications, which EU legislators specifically mentioned. Moreover, by stating 'part of a website', the legislators seem to consider that specific parts of a website, such as a dedicated landing page or app, can constitute software independently of the rest of the website.

One question arises from this definition: whether the different elements with which users may interact on a website, such as smart contracts, constitute software. In its report "Decentralised Finance: A Categorisation of Smart Contracts", published on October 11th, 2023, ESMA defined 'smart contracts' as "immutable computer programs that run deterministically on the blockchain and execute automatically, interacting with other accounts on the blockchain according to the code that defines their actions". Based on this definition, a smart contract may fall within the definition of 'software'.

2.3.2 Operated by or on Behalf of an Offeror or CASP

A software may meet the definition of an online interface if it is operated by or on behalf of an offeror or CASP. This condition is particularly important and denotes a certain intention of legislators to target interfaces provided by offerors and CASPs – on the basis of an inverse interpretation, interfaces provided by crypto-asset issuers that do not qualify as offerors do not meet the definition of an online interface. An offeror is a person who conducts an offer to the public, defined under MiCA as "*a communication to persons in any form, and by any means, presenting sufficient information on the terms of the offer and the crypto-assets to be offered so as to enable prospective holders to decide whether to purchase those crypto-assets*".

It is very important to differentiate an "online interface" from "a communication to persons in any form, and by any means". To conduct an offer to the public, you do not need to have an online interface, or conduct an offer through an online interface. An offer to the public can even consist of a speech at a conference that presents sufficient information on terms of the offer and the crypto-assets, as an example. This is a distinction worth making, as the definition of an offer to the public is much wider in

scope than the definition of an online interface. We shall be covering the concept of an offer to the public in detail under Section 3.

Another question subsists regarding the location of the entity operating the online interface. Indeed, CASPs are regulated under MiCA only when they provide crypto-asset services in the EU, while the offer to the public is within the scope of MiCA if it is likewise made in the EU. However, the online interface through which services are provided does not necessarily need to be hosted within the EU, specifically when an entity registered outside the Union operates the interface on behalf of the CASP. If the interface remains accessible to persons in the EU, then it can be taken as an indication, albeit a rebuttable one, that any potential crypto-asset services, or any potential offer to the public, is targeting persons located in the EU.

2.3.3 Gives Holders Access to their Crypto-Assets and gives Clients Access to Crypto-Asset Services.

Under MiCA, an 'online interface' is a software that allows holders to access their crypto-assets and/or allows clients to access crypto-asset services. These two aspects must be assessed separately.

At the risk of stating the obvious, 'access to crypto-assets' under MiCA does not refer to read-only access, such as block explorers. Access to crypto-assets should be interpreted as write-access, requiring signatures resulting in a change of state in the underlying blockchain.

With that being clarified, the first point to be considered is whether an online interface serves to grant holders access to their crypto-assets. Strictly and technically speaking, online interfaces in DeFi do not serve as gatekeepers for users attempting to access their crypto-assets. They tend to be nothing more than graphical user interfaces (GUIs) that allow a user to interact with a particular protocol or smart contract(s), something that can also be done directly without the need for such a GUI. Generally, therefore, online interfaces in DeFi do not grant users access to crypto-assets.

At the risk of going off on an academic tangent, but speaking of interactions with crypto-assets: the subject becomes a bit more complex when considering external signing software, aka wallets. While it is doubtlessly certain that wallets do not store crypto-assets, wallets are often used to generate private keys. Wallet software is also used to sign transactions using private keys. Do wallets, therefore, provide users with access to their crypto-assets? Not exactly – you access crypto-assets through private key signing. At the same time, without 'software', you cannot sign transactions – so wallet software, in a sense, does give one access to their crypto-assets. Again, this is mostly an academic point, because

wallet software providers tend *not* to be CASPs in the first place – unless they are, for instance, charging fees to their users or otherwise operating in a manner which makes them CASPs.

Let's get back on track. Do online interfaces, on the other hand, facilitate access to crypto-asset *services*? This is a trickier question to answer. However, it's a question which does not need answering, because an online interface has to both give users access to crypto-assets, as well as access to users to crypto-asset services. An online interface granting users access to crypto-asset services, in and of itself, would not be sufficient to satisfy the definition laid out in MiCA.

This last point dovetails neatly with the conclusion for this section, being that the definition of an "online interface" needs to be interpreted in its totality. It is clear, through such an interpretation, that the term itself is far narrower in scope than perhaps initially thought by the industry at large, and that widespread worries that anyone hosting a 'DeFi online interface' would be in the scope of MiCA are largely unsubstantiated. Naturally, it does not mean that it is a blanket-exclusion of sorts – what matters, again, is whether a person or persons satisfy the definition of a 'CASP', regardless of whether they are operating an 'online interface' as defined under MiCA.

2.4 Does all this mean that one can ignore the Term 'Fully Decentralised'?

While, once again, it is true that Recital 22 ultimately is just that - a recital - it does not do to ignore it and make nothing of it. At the very least, it shows the intent of the legislator, and the European Securities Markets Authority (ESMA), as the lead regulatory authority on MiCA, certainly has not ignored the use of the term either.

In point 108 of the Second Consultation Paper on Technical Standards under MiCA[18], ESMA acknowledges that "*(...) Where crypto-asset services are provided in a fully decentralised manner without any intermediary*", they should fall outside the scope of MiCA; however, ESMA also notes that the exact scope of this exemption remains uncertain. In the absence of an explanation of what "fully decentralised" is, national competent authorities (NCAs) such as the Danish Financial Supervisory Authority are providing their own interpretation[19] of what this term can be interpreted to mean.

[18] https://www.esma.europa.eu/sites/default/files/2023-10/ESMA75-453128700-438_MiCA_Consultation_Paper_2nd_package.pdf
[19] https://www.dfsa.dk/Media/638549094736906876/PrinciplesCryptoAssetsPDF_250624.pdf

Before providing our own interpretation of the term within the context of MiCA, and thereby near the conclusion of this extensive handbook, it is appropriate to first consider further literature published by ESMA on the matter.

2.4.1 Decentralisation of the Distributed Ledger Technology

As highlighted in the section titled *Settlement Layer Decentralisation*, the decentralised nature of the underlying technology is an essential requirement for a project to be deemed decentralised.

MiCA refers to the DLTs as "*a technology that enables the operation and use of decentralised ledgers*". It is worth noting that this definition, again, does not differentiate between permissionless DLTs (which can potentially also be decentralised) and permissioned DLTs (solely capable of being centralised). It is only in the abovementioned ESMA Second Consultation Paper on MiCA[20], that ESMA proposed a definition for a permissionless DLT as "*a technology that enables the operation and use of distributed ledgers in which no entity controls the distributed ledger or its use or provides core services for the use of such distributed ledger, and DLT network nodes can be set up by any persons complying with the technical requirements and the protocols.*"

ESMA's definition of a permissionless DLT covers both the control over the operation of the DLT itself, as well as control over its very use. Moreover, for a DLT to be permissionless, no entity should have control by providing core services that become fundamental and indispensable for such a distributed ledger. Other institutions, such as the Financial Action Task Force ('FATF')[21] and the International Organisation of Securities Commissions ('IOSCO')[22], have similar approaches and consider that no single entity should have control over the underlying ledger for a permissionless or decentralised ecosystem to exist. This certainly puts DLTs such as L2 networks under the spotlight, given the significant element of centralisation, and resulting control, present in such networks.

On the other hand, ESMA also clarified in its second Consultation Paper that MiCA is not intended to prevent or prohibit the use of permissionless DLT by CASPs. Under point 71 of its paper, the Authority

[20] https://www.esma.europa.eu/sites/default/files/2023-10/ESMA75-453128700-438_MiCA_Consultation_Paper_2nd_package.pdf
[21] https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf.coredownload.inline.pdf
[22] https://www.iosco.org/library/pubdocs/pdf/IOSCOPD754.pdf

Office 11, Capital Workspace, Onsite Buildings,
Level One, Valley Road Birkirkara, Malta BKR9021
info@bcas.io | www.bcas.io

mentioned that regulators should not favour one over the other when setting certain differences between the uses of permissioned and permissionless DLT infrastructures by CASPs. Unreasonably requiring CASPs to adhere inflexibly or indiscriminately to outsourcing requirements, as outlined under Article 73 of MiCA, when the usage of permissionless DLT infrastructures are involved would arguably unintentionally prohibit their use of permissionless DLTs by a failure to comply, would be "an outcome that would be contrary to the spirit of MiCA".

Furthermore, in point 63, the Authority stated, "*As it relates to contractual arrangements, Article 73 of MiCA (on outsourcing) elaborates how CASPs should address the risks associated with third-party providers*." However, there is no legal basis to consider a permissionless DLT used by a CASP as a third-party provider because no formal contractual relationship (such as a service level agreement) is required to interact with permissionless DLTs. If permissionless DLT infrastructure does not constitute a third-party provider relationship (in the traditional contractual sense), then it would not fall under the scope of the requirements of the MiCA outsourcing article. In this case, permissionless DLTs may be considered a "common good" resource. In contrast, a permissioned DLT operated by a commercial enterprise will likely have contracts for 'white-labelled' DLT products, which can be considered a "third-party provider".

Therefore, ESMA's reasoning is based on the demonstration of a contractual relationship in the operations of permissioned DLTs and the absence of the provision of contractual services for the operation of permissionless DLTs.

2.4.2 Decentralisation within a Specific DeFi Protocol

Following ESMA's approach and applying the same reasoning to DeFi protocols, it is safe to say that if a specific protocol meets the threshold of decentralisation established within the definition of a 'permissionless DLT', ergo with no single entity governing the technology used within the protocol or its application, and with no single entity providing services that are essential for its operation, then such a protocol can be deemed to be permissionless to the degree established in the definition and, therefore, decentralised. Indeed, because a "permissionless protocol" cannot be controlled by any single party, it means that such protocol can be said to be sufficiently decentralised.

However, to be deemed decentralised, DeFi protocols must also run on top of a DLT that likewise meets the definition of a 'permissionless DLT'. Provided that a DeFi protocol, generally comprising a set of smart

contracts run on a permissionless DLT, is not under the control of a single entity, and no single entity governs its usage or provides indispensable core services, then such a protocol should likewise meet the standard set in the definition of a 'permissionless DLT' meaning that such a protocol can be considered to be – using ESMA's own wording – a "common good" resource. However, even if a protocol itself qualifies as a "common good" resource that can be accessed by anyone, and is not within any person's control or influence, it does not necessarily mean that anything happening on or through such a decentralised and permissionless protocol is outside of scope of MiCA. The provision of crypto-asset services through such a protocol can *still* subsist – naturally, only if and where the person(s) providing such services do, ultimately, qualify as CASPs.

This is where decentralisation from governance[23] and operational[24] perspectives matters; specifically, to ensure that there is no person, or group of persons, be it whichever way they are constituted, that qualify as an undertaking as defined under Sections 2.2.1 and 2.2.2 of this handbook. If there are persons that are, on the surface, acting separately and independently, yet it transpires that there is actual collusion to the point that they are acting as one party, and additionally, there is the provision of one or more crypto-asset services as defined under MiCA (for a consideration), then regardless of the technology being utilised, the definition of a CASP is likely to be satisfied. The point being raised, however, is that the likelihood of such subsisting, tends to be exacerbated **if the protocol in question fails to qualify as a permissionless DLT protocol.**

2.4.3 The Problem of the Sum being Geater than its Parts – L2 Networks

It is perhaps time to call a spade a spade, and concede that L2 networks, for the major part, are likely not to satisfy the definition of a 'permissionless DLT' as proposed by ESMA. Reliance on admin multisigs, centralised sequencers, and general control over the network itself is something that is commonplace in most of the L2 networks currently operating.

This presents a crucial issue to be considered, which we shall try to explain as best as possible. Imagine an L2 network, with admin multisigs controlled by a group of persons, with the same group of persons also being in control of an entity (such as a foundation) which acts as the front-facing entity of a DAO, and the majority of governance tokens is likewise owned by the same group

[23] Section 1.3 of this handbook
[24] Section 1.6

Office 11, Capital Workspace, Onsite Buildings,
Level One, Valley Road Birkirkara, Malta BKR9021
info@bcas.io | www.bcas.io

of persons. Let's say that this same group of persons also run validator nodes for the network. The power to halt the network, make crucial changes to it, manage treasury funds, etc. are all in the hands of this group of persons. Clearly, the definition of an undertaking here is met in full.

The L2 network as a whole is generating fees, ranging for transaction fees that go to validators, to protocol fees for any protocols or dApps running on top of it. The group of persons has a business interest in some validator node setups, and some protocols/dApps running on top of the network. Apart from that, they have a vested interest in the form of token allocation, be it the native token of the network itself (which can double up as the governance token over the L2 network itself), and perhaps governance tokens in some of the projects built on top of the network. Clearly, a consideration, a hefty one even, is being paid and going into the pockets (directly or indirectly) of this group of persons.

Are crypto-asset services being provided? It is certainly a question that cannot be easily answered, and may leave one to ponder. One can claim that the users' crypto-assets remain custodied by themselves, and that can be a point well-granted – but can one say that the mentioned group of persons do not have *control to the access* of such crypto-assets? If they can ultimately decide, at any point, to halt transaction processing in the network, or utilise the admin key to transfer crypto-assets from a particular address (even freezing such), and there is a consideration being paid one way or another, can it really be said that, due to the overarching control being exercised by the group of persons, that such group does not qualify as a CASP?

The jury is still out on this, at least in our view. The problem does not lie with each and every constitutive piece of a network or protocol – more often than not, each moving part considered on its own (such as validators) tends to be completely in the clear in that it is not subject to MiCA. The same can be said for protocols like AMMs which, solely on their own merits and excluding considerations for LPs, tend to likewise not be captured by MiCA. The problem does, however, become more complex if ultimately the various moving parts are controlled by one person or group of persons. There, it can truly be an issue of the sum being greater than its parts, harking back to the long-standing criticism of some projects in crypto being DINO. This general critique is not solely aimed at L2 networks, but also any other protocol over which a clear element of centralised control is present, and such control can inhibit a user's access to their crypto-assets.

Office 11, Capital Workspace, Onsite Buildings,
Level One, Valley Road Birkirkara, Malta BKR9021
info@bcas.io | www.bcas.io

3. Issuances and Offers to the Public

Although the concept of decentralisation under MiCA does not, per se, extend to crypto-asset issuances or their offer to the public, it would be quite remiss of us to leave out the possible implications of such, when the minting of tokens tends to be an essential element of DeFi platforms such as bridges and lending protocols – and where, as a result, an issuance of crypto-assets may take place.

3.1 Issuers

Under MiCA, an issuer is defined as *"a natural or legal person, or other undertaking, who issues crypto-assets"*[25]. Quite a dry definition, if you ask us.

While the Articles of MiCA do not define what an 'issuance' of crypto-assets is, Recital 20 gives us some further depth, stating that *"Issuers of crypto-assets are entities that have control over the creation of crypto-assets"*. This *control over the creation of crypto-assets* might be the criterion to determine who is the issuer of these crypto-assets. If no entity or person can be identified as having control over the creation of the crypto-assets, the issuer may be deemed to be non-identifiable. In this scenario, MiCA's Recital 22 states that *"Where crypto-assets have no identifiable issuer, they should not fall within the scope of Title II, III or IV of this Regulation"*, depending on the token's qualification.

In turn, therefore, we have to ask on what constitutes control over the creation of crypto-assets. This is a bit of a thornier question to answer. On one hand, at a technical level, the control over the creation of crypto-assets can be argued to be in the hands of whichever person calls the minting function in the relevant smart contract, triggering the very issuance of the crypto-asset itself. On the other hand, one cannot ignore the fact that in the cases where the smart contract's logic is upgradeable, and the power to upgrade it is in the hands of a person or persons, then such ultimately qualifies as control over the creation of the crypto-assets; the power to halt the issuance of a crypto-asset certainly qualifies as control over the creation of the crypto-asset. Indeed, we tend to be of the opinion that the latter scenario presents a greater latitude of control than the former.

This may well mean that persons which can somehow restrict or change the manner in which a crypto-asset is issued, should be seen as the issuers of the crypto-asset. If no such person exists,

[25] MiCA Article 3(1)(10)

Office 11, Capital Workspace, Onsite Buildings,
Level One, Valley Road Birkirkara, Malta BKR9021
info@bcas.io | www.bcas.io

due to, say, the smart contract being immutable and ideally renounced, then the only persons who can control the issuance of a crypto-asset are the very users themselves .

However, even if a person, other than the user itself, has control over the issuance of crypto-assets (such as being able to determine the parameters of issuance and even halt it completely) and is therefore the issuer, it is also important to note that in most scenarios, the mere issuance of crypto-assets does not tend to present much in terms of regulatory implications under MiCA, However, depending on the crypto-asset's classification, issuers may be required to comply with MiCA's Titles II, III or IV, but mostly – save in some exceptional instances – if they are ***offering the crypto-asset to the public, or seeking its admission to trading.*** This can be seen, in instance, under Title III, where Article 16 stipulates the requirements to be adhered to by an issuer offering an ART to the public in the Union, or seeking its admission to trading on a trading platform in the Union. So, what is an offer to the public?

3.2 Offer to the Public

An 'offer to the public' is defined as "*a communication to persons in any form, and by any means, presenting sufficient information on the terms of the offer and the crypto-assets to be offered so as to enable prospective holders to decide whether to purchase those crypto-assets*".

First of all, it is important to note that an issuer and an offeror do not need to be the same person or entity. One can have an offer to the public being conducted by a person who has no connection to the issuer; issuances and offers to the public can be mutually exclusive acts.

Secondly, before delving into the definition itself – **airdrops can still constitute an offer to the public and fall within scope of MiCA**, if the purchasers of the crypto-asset are required to provide, or to undertake to provide, personal data to the offeror in exchange for that crypto-asset, or where the offeror of a crypto-asset receives from prospective holders of that crypto-asset any fees, commissions, or monetary or non-monetary benefits in exchange for that crypto-asset.

The definition of an offer to the public can be broken down into the following constitutive elements:

1) A communication to persons in any form
2) Sufficient information on:
    i) the terms of the offer, and

Office 11, Capital Workspace, Onsite Buildings,
Level One, Valley Road Birkirkara, Malta BKR9021
info@bcas.io | www.bcas.io

ii) the crypto-assets to be offered

3) The information has to be sufficient to the point that it enables prospective holders to decide whether to purchase those crypto-assets

The first element is self-explanatory and all-encompassing.

Sufficient information on the crypto-assets to be offered

The second element, however, merits a profound analysis. Starting with the second sub-element, being *sufficient information on the crypto-assets to be offered* – this is quite an interesting point, as it absolves most front-ends from being seeing as conducting offers to the public, if they would solely be offering an interface listing token tickers, or other denominations to identify the crypto-asset in question, without however including any other information about the crypto-assets themselves.

Conversely, information which not only identifies the crypto-assets, but includes information about its technical features, its intended and possible uses, the price at which it can be acquired, tokenomics, and other materially-relevant information can reasonably be seen as sufficient information on the crypto-assets being offered. Generally, a whitepaper, a populated Gitbook, or any other documentation displaying such information or more would contain sufficient information on the crypto-assets.

Sufficient information on the terms of the offer

However, *sufficient information on the crypto-assets to be offered* is only one part of the equation. The second, equally important element that must be cumulatively met is *sufficient information on the terms of the offer*. In order for a purchase to subsist, there must be a contract, which contract can be concluded on the basis of an agreement on the terms and conditions being offered. Without such terms of the offer, it can reasonably be concluded that a decision to purchase cannot be made.

'Terms of the offer' typically are the domain of civil, commercial, and consumer protection laws. EU laws do not seem to define this term anywhere; however, academia has provided a workable definition vis-à-vis European private law, defining it as follows:

(1) A proposal amounts to an offer if:

a) it is intended to result in a contract if the other party accepts it; and

b) it contains sufficiently definite terms to form a contract.

(2) An offer may be made to one or more specific persons or to the public. [26]

(3) A proposal to supply goods or services at stated prices made by a business in a public advertisement or a catalogue, or by a display of goods, is treated, unless the circumstances indicate otherwise, as an offer to sell or supply at that price until the stock of goods, or the business's capacity to supply the service, is exhausted.

Point 3 above needs to be applied *mutatis mutandis* to the offering of crypto-assets; the applicable interpretation refers to offers to the public being either time-limited or perpetual. MiCA refers to 'time-limited' offers as one form of public offers, meaning that perpetual public offers are also possible.

Point 1 is the focal point for the purpose of analysing the words "terms of the offer", as it contains material information on when a proposal amounts to an offer. Point 1(a) of the definition being proposed highlights the importance of the *intention* behind a proposal. If the intention is *not* for a contract to result, but the information/proposal being presented is simply of an educational nature without any intention to form a contract, then it can hardly be said that a proposal amounting to an offer is being made. It is very important to note as well that the offer is being made by the offeror, and the offer solely stands between the person making the offer (the offeror), and the person to which the offer is made. Elementary principles of contractual law dictate that a person cannot make an offer on behalf of a third party, unless that third party has given their authority for such to be made on their behalf.

Point 1(b) is complementary to point (a) – if there are sufficiently definite terms to form a contract, then it can safely be said that the intention for the proposal to result in a contract is confirmed. While the authors of the quoted paper stop short from defining 'sufficiently definite terms', criteria such as the consideration, terms & mode of payment, and the mode of delivery of the crypto-asset can all be deemed to be essential criteria for the terms to be sufficiently defined. Arguably, without the consideration (price) being stipulated, or without information on how such crypto-assets can be acquired, it is difficult to say that the terms can ever be seen as sufficiently defined.

[26] Principles, definitions and model rules of European Private Law – Draf Common Frame of Reference', *Study Group on a European Civil Code and Research Group on the Existing EC Private Law (Acquis Group)* < *https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/EUROPEAN_PRIVATE_LAW/EN_EPL_20100107_Principles__definitions_and_model_rules_of_European_private_law_-_Draft_Common_Frame_of_Reference__DCFR_.pdf*> accessed 25 June 2024

Enabling prospective holders to decide whether to purchase those crypto-assets

The third element ties the two constitutive sub-elements of the second element together (sufficient information on the crypto-assets and the terms of the offer); if either of those two are lacking, then it can be said that there isn't sufficient information to enable prospective holders to decide whether to purchase the crypto-assets. It also confirms that the terms of the offer must include information to enable a purchaser to be able to make a decision based on a balance of probabilities, ergo whether to purchase the crypto-assets or otherwise.

The term 'purchase' is material to the boundaries of the definition of 'an offer to the public'. A purchase denotes the acquisition of crypto-assets, which typically involves a transfer of title or right (applied, *mutatis mutandis*, to crypto-assets). However, purchases can be conditional, such as in the case of hire purchases; moreover, the use of alternative terms does not affect whether a purchase can subsist or otherwise as an act.

Lastly, the definition of an 'offer to the public' does not require that a purchase contract is ultimately concluded in order for an offer to the public by the offeror to subsist.

3.3 What are the Implications of an Offer to the Public?

Unlike issuances, offers to the public in the Union carry with them regulatory obligations under MiCA, depending on the classification of the token in question. The implications and obligations are summarised below:

1. **Crypto-assets falling under Title II of MiCA, being OCAs**. Offerors of OCAs must draft a whitepaper in compliance with Article 6, notify it to their national competent authority in line with Article 8, and publish it in compliance with Article 9. There are also general obligations to abide by within the same Title II, such as offering the right of withdrawal to purchasers.
2. **Crypto-assets falling under Title III of MiCA, being ARTs**. Offerors of ARTs must first be approved by their national competent authority, and as part of the approval process outlined under Article 19, draft a whitepaper in compliance with Article 19 and likewise have it approved by the competent authority. There are other obligations applicable to ART offerors under Title III.

Office 11, Capital Workspace, Onsite Buildings,
Level One, Valley Road Birkirkara, Malta BKR9021
info@bcas.io | www.bcas.io

3. **Crypto-assets falling under Title IV of MiCA, being EMTs**. Offerors of EMTs must firstly be licensed as an e-money institution or a credit institution. Second, they must draft a whitepaper in compliance with Article 51, and notify it to their national competent authority in line with the same Article. There are other obligations applicable to EMT offerors under Title III.

As an important side-note, the obligations above extend lock, stock, and barrel to persons seeking the admission to trading of such crypto-assets on a trading platform operating in the Union – in other words, any person seeking listing onto a trading platform operating in the Union must follow the procedures applicable in relation to the drafting, publication, and notification/approval of the whitepaper as the case may be.

3.4 Tying the above to DeFi

As mentioned in this same Section 3, typically the minting of tokens is synonymous with the issuance of crypto-assets. However, the mere issuance per se does not typically attract regulatory obligations under MiCA; unless that crypto-asset happens to be an electronic-money token (EMT) that is referencing the value of an official currency of the Union, such as the Euro, in which case its issuance is deemed to be an offer to the public within the Union. Any DeFi protocol in which tokens are minted, including wrapped tokens such as aTokens on Aave's protocol and wETH, should not, due to this function alone, have cause for concern.

The music can, however, change if there is a communication, including through an online interface, that is tantamount to an offer to the public of crypto-assets. This, from our experience, tends to be an element that is often ignored by the industry at large, which seems to be solely preoccupied with the idea of crypto-asset services. Online interfaces, whitepapers/Gitbooks, and terms that constitute terms of offer for a crypto-asset can collectively constitute an offer to the public, if ultimately the prospective holder has enough information to decide whether to purchase those crypto-assets from the offeror. An airdrop of crypto-assets is not exempt from the definition of an offer to the public, if in order to acquire the crypto-asset, a prospective purchaser must provide any data or perform any act that will benefit the offeror of that crypto-asset.

Therefore, it is important for any DeFi operator to ensure that they are ultimately not conducting an offer to the public of a crypto-asset, with ARTs and EMTs in particular resulting in comparably heavy regulatory obligations under MiCA.

Office 11, Capital Workspace, Onsite Buildings,
Level One, Valley Road Birkirkara, Malta BKR9021
info@bcas.io | www.bcas.io

4. Legal Conclusion

As we reach an end to what is arguably the most detailed thesis, to date, on the concept of decentralisation within DeFi and its link to MiCA, we will start by marrying the concepts of technical, organisation, and legal decentralisation, in relation to DeFi, in this concluding piece.

First of all, at the risk of sounding like a broken record, it can well be said that "full decentralisation" is a myth. Since it is a myth, it does not really matter. What matters is that decentralisation, to a greater or lesser degree, is possible – and that, in and of itself, is a victory that DeFi can claim under its belt, showing that finance can indeed operate within a realm that challenges the status quo. However, it can likewise be said that meeting the lofty thresholds of decentralisation established from each and every of the five angles explored in Section 1 is very difficult, to the point that it can safely be stated that no DeFi protocol has yet, in our books, scored perfectly across all five. This is not much of an issue, because decentralisation, after all, is a range – and the concept of 'sufficient decentralisation' is malleable depending on its application. That being said, if DeFi is to truly live up to its name, then satisfying decentralisation from the five angles identified in this report should remain the target.

The application of 'decentralisation' within MiCA is as singular as it is multi-faceted. Singular, in that in order for one to be exempt from the scope of the Regulation when the offering of crypto-asset services is involved, then one should simply stop short from qualifying as a CASP. Multi-faceted, because the definition of a CASP captures within it the element of decentralisation or lack thereof, where in the case of the latter, the risk of qualifying as a CASP increases – especially if there is the offering of crypto-asset services for a consideration.

Online interfaces remain the subject of much debate, and we, for one, believe that they should for the large part be simply seen as means of graphical access to the underlying world of smart contract protocols. However, the provision of information coupled with the actual use & function of the interface should not be taken lightly. While token issuances tend not to present any ramifications under MiCA, offers to the public of crypto-assets, on the other hand, do. DeFi online interfaces that simply serve to give access to an underlying protocol ordinarily do not amount to an offer to the public of crypto-assets, especially since no purchase contract per se tends to be even possible. However, in instances where a purchase contract can subsist, even through a seemingly innocuous airdrop, then care should

Office 11, Capital Workspace, Onsite Buildings,
Level One, Valley Road Birkirkara, Malta BKR9021
info@bcas.io | www.bcas.io

be taken, as the applicable obligations for an offer to the public can range from mild to significant, depending on the crypto-asset type in question.

This brings us to the end of the BCAS Decentralisation Handbook for DeFi. We hope that this serves as a point of reference for everyone in the DeFi space which is looking to directly or indirectly operate within the EU, and as always – stay frosty, stay decentralised.

Office 11, Capital Workspace, Onsite Buildings,
Level One, Valley Road Birkirkara, Malta BKR9021
info@bcas.io | www.bcas.io

Annex A: Glossary

Aggregators	In a zero-knowledge (zk) L2, an aggregator is in charge of checking the validity of the transaction batched from a sequencer and provides a validity proofs for the batch.
API	An Application Programming Interface (API) is a way to enable two software components to communicate with each other using a set of rules called a protocol.
Asset-Referenced Tokens (ARTs)	An 'Asset-Referenced token' means "a type of crypto-asset that purports to maintain a stable value by referencing another value or right or a combination thereof, including one or more official currencies".
Bridges	Bridges, are protocols or mechanisms that enable the transfer of data across different blockchain networks. Bridgers facilitate cross-chain interoperability, allowing users to move tokens, NFTs, or other digital assets between otherwise isolated blockchains.
Byzantine Fault Tolerance	Byzantine Fault Tolerance (BFT) refers to a property of a distributed system that allows it to continue operating even if some participants (nodes) fail or act maliciously. A BFT system can reach consensus on the correct state of the network even when some nodes behave unpredictably or dishonestly.
Client	A 'client' is "any natural or legal person to whom a crypto-asset service provider provides crypto-asset services".
Consensus Client	A consensus client is software responsible for ensuring that nodes in a blockchain network agree on the correct state of the ledger. In Ethereum's Proof of Stake system, the consensus client enables nodes to participate in block validation, proposing, and finalizing the state of the blockchain. Examples include Prysm, Teku, Nimbus, Lighthouse & Lodestar.
Consensus Mechanism	A consensus mechanism is a protocol that ensures all participants (nodes) in a decentralized network agree on the state of the blockchain. Common examples include Proof of Work (PoW), Proof of Stake (PoS), and Delegated Proof of Stake (dPoS). It plays a critical role in maintaining the security and integrity of blockchain networks by preventing double-spending and ensuring valid transaction confirmations.
Controlling	Means "any means by which an element of control is exercised over the crypto-assets or the means of access to such".
Crypto-Asset Service Provider (CASP)	A 'crypto-asset service provider' is "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"
DAO	A DAO, or Decentralised Autonomous Orginisation is an organisation governed by smart contracts and run by its members through token-based voting mechanisms.
dAPPs	Decentralized applications (dApps) are software programs that run on blockchain networks without the need for intermediaries. They rely on smart contracts for backend functions and are accessible by users directly through their crypto-wallets.
DeFi	Decentralised Finance (DeFi) is an ecosystem of interoperable dApps, that provide financial services powered by smart contracts without intermediaries.

DLTs	A 'DLT' is "a technology that enables the operation and use of distributed ledgers in which no entity controls the distributed ledger or its use or provides core services for the use of such distributed ledger, and DLT network nodes can be set up by any persons complying with the technical requirements and the protocols".
dPoS	Delegated Proof of Stake (dPoS) is a variation of Proof of Stake (PoS) where token holders can delegate their tokens to validators, which are in charge of securing the network.
DVT	Distributed Validator Technology (DVT) is a mechanism to enhance the resilience and decentralisation of blockchain validators. It splits a validator into multiple components across different machines or operators, reducing the risk of single points of failure and enhancing security.
Economic Activities	An 'economic activities' are "services normally provided for remuneration"
Electronic Money Tokens (EMTs)	An 'Electronic Money Token' means "a type of crypto-asset that purports to maintain a stable value by referencing the value of one official currency".
Exchange of crypto-assets for other crypto-assets	Means "the conclusion of purchase or sale contracts concerning crypto-assets with clients for funds by using proprietary capital".
Execution client	An execution client processes and executes transactions, manages the state of the blockchain, and interacts with smart contracts. In Ethereum, the execution client works with the consensus client to maintain the correctness of transactions and the network's overall functioning. Examples include Besu, Erigon, Go-Ethereum (Geth) & Nethermind.
Fork	A change in a blockchain protocol leading to the creation of an alternative version of the chain.
JSON	JavaScript Object Notation (JSON) is a lightweight format for storing and transporting data. JSON is often used when data is sent from a server to a web page. In blockchains, JSON-RPC nodes transfer data between the blockchain and user wallets
L1 / Layer 1	Layer 1 refers to the base layer of a blockchain, where the core transactions and smart contracts are processed. Ethereum, Bitcoin, and Solana are examples of Layer 1 networks.
L2/ Layer 2s	Layer 2 solutions are designed to scale Layer 1 blockchains by processing transactions off-chain while relying on the Layer 1 for transaction finalisation.
MEV	Maximal Extractable Value is the profit a validator or miner can extract by reordering, including, or censoring transactions within a block.
MPC – Multi Party Computation	Multi-Party Computation (MPC) is a cryptographic method that allows multiple parties to jointly compute a function over their inputs while keeping those inputs private. It ensures that sensitive data remains confidential, even as parties collaborate.
Node	A node is any device (computer) connected to a blockchain network that participates in maintaining the distributed ledger.
Off-Chain	Off-chain refers to processes, transactions, or data management that occur outside of the blockchain network. These activities do not immediately interact with or are not recorded on the blockchain. Example: an oracle fetching the price of Gold from and external sources.

Offer to the public	An 'offer to the public' is "a communication to persons in any form, and by any means, presenting sufficient information on the terms of the offer and the crypto-assets to be offered so as to enable prospective holders to decide whether to purchase those crypto-assets".
Offeror	An 'offeror' is "a natural or legal person, or other undertaking, or the issuer, who offers crypto-assets to the public".
On-Chain	On-chain refers to operations or transactions that are directly recorded, validated, and secured on a blockchain. Once added, these activities are immutable and can be verified by all network participants.
Online interface	An 'online interface' means "any software, including a website, part of a website or an application, that is operated by or on behalf of an offeror or crypto-asset service provider, and which serves to give holders of crypto-assets access to their crypto-assets and to give clients access to crypto-asset services".
Oracles	Oracles are services that provide off-chain data to smart contracts on a blockchain
Other Crypto-Assets (OCAs)	An 'Other Crypto-Asset' means "a type of crypto-assets that are neither an EMT nor an ART, or any other crypto-asset excluded from MiCA under Article 2(4), such as financial instruments and structured deposits".
PoS	Proof of Stake is a consensus mechanism where validators are chosen to propose and verify new blocks based on the number of tokens they hold and are willing to lock up (stake). Validators earn rewards for their participation, and malicious behavior results in slashing penalties.
PoW	Proof of Work is a consensus mechanism that requires participants (miners) to solve complex cryptographic puzzles to validate transactions and add new blocks to the blockchain. It is resource-intensive and it relies on computational power as a security mechanism.
Providing custody and administration of crypto-assets on behalf of clients	Means "the safekeeping or controlling, on behalf of clients, of crypto-assets or of the means of access to such crypto-assets, where applicable in the form of private cryptographic keys".
Providing transfer services for crypto-assets on behalf of clients	Means "providing services of transfer, on behalf of a natural or legal person, of crypto-assets from one distributed ledger address or account to another".
Reception and transmission of orders for crypto-assets on behalf of clients	Means "the reception from a person of an order to purchase or sell one or more crypto-assets or to subscribe for one or more crypto-assets and the transmission of that order to a third party for execution".
RPC	RPC refers to a protocol that enables one program to request services from another program on a different machine in a network. In a blockchain context, RPCs are used for communication between clients and nodes, allowing users to interact with the blockchain.
Safekeeping	Means "a duty to keep the crypto-assets safe, and diligently employ means to protect against external attacks".

Office 11, Capital Workspace, Onsite Buildings,
Level One, Valley Road Birkirkara, Malta BKR9021
info@bcas.io | www.bcas.io

Sequencers	In a L2,a sequencer proposes transaction batches to the L1 network upon executing them. It rolls up transactions into batches and adds them to the consensus contract held on the L1.
Settlement layer	The settlement layer is the foundational layer of a blockchain where transactions are finalised and confirmed. This layer ensures the finality of transactions, making them immutable and secure.
Slashing	Slashing is a penalty mechanism in Proof of Stake (PoS) and Delegated Proof of Stake (dPoS) networks that punishes validators for malicious behaviour or negligence, such as double-signing or failing to propose valid blocks. Validators lose part or all of their staked assets if they are slashed.
Smart Contract	A 'smart contract' is "an immutable computer programs that run deterministically on the blockchain and execute automatically, interacting with other accounts on the blockchain according to the code that defines their actions".
Smart Contracts	A smart contract is a self-executing program on a blockchain that automatically executes the terms of a previous agreement when predefined conditions are met.
Software	A 'software' is "the part of an electronic information system which consists of computer code".
Undertaking	An 'undertaking' is "a natural or legal person(s) engaged in economic activities, regardless of their legal or financing form. The economic activities per se can be offered or undertaken with or without the intention to make a profit; what matters is that those economic activities, ergo the offering of goods or services, would be in competition with the offerings of other operators which do seek to make a profit. The term itself includes severall legally independent undertakings participating in an economic activity, or in an agreement, as one party; an assessment of decisive influence cannot be made only by reference to policies and contractual wordings, but all other elements relating to economical, organisational, legal and structural links between the various parties involved must be taken into consideration".
Utility Tokens	An 'Utility Token' means "a type of crypto-assets that are only intended to provide access to a good or a service supplied by their issuer".
Validator	A validator is a participant in a PoS or dPoS blockchain that is responsible for proposing, validating, and attesting new blocks. Validators lock up (stake) native assets to participate in consensus and earn rewards for maintaining the network's integrity.
Wallet	A wallet in aa blockchain context, is a software or hardware tool that stores private and public keys, enabling users to interact with blockchain networks.
ZK	Zero-knowledge (ZK) refers to cryptographic protocols that enable one party (the prover) to prove to another party (the verifier) that a statement is true without revealing any additional information beyond the validity of the statement itself.

BCAS

Get in touch with our team:

info@bcas.io

bcas.io

x.com/BCAS_io

Read more MiCA content:

blog.bcas.io/tag/mica