AUTORITÉ
DES MARCHÉS FINANCIERS

AMF

DECENTRALISED FINANCE (DEFI),

TRADING PROTOCOLS AND GOVERNANCE ISSUES:

OVERVIEW, OBSERVED TRENDS, AND REGULATORY DISCUSSION POINTS

AMF Discussion Paper

June 2023

AUTORITÉ DES MARCHÉS FINANCIERS

AMF

Contents

Introduction

Blockchain technology has provided an innovative and disruptive mechanism which has challenged the technological infrastructure upon which the digital economy is built. This has been underpinned by the use of distributed ledger technology, the development of new activities and market structures, and the emergence of new governance mechanisms.

Building on the use of blockchain, Decentralised Finance (or "DeFi") is no stranger to such disruption. It presents itself as providing an alternative to traditional financial services, aiming to replicate a number of its activities, such as lending and investing. DeFi however proposes an alternative way of doing this, and displays certain novel characteristics in this regard.

One such feature is its use of automated blockchain infrastructure, which is often portrayed as fully decentralised and disintermediated. In this new format, the functions traditionally performed by centralised institutions are replaced by the use of automated software, such as protocols and smart contracts (concepts further explored in this paper). Though such a novel approach to financial services may offer opportunities for technological innovation, it also leads to the emergence of new questions, challenges, and risks. In particular, a number of these risks have crystallised with the crash of the Terra / Luna protocol in May 2022, which has raised questions around the need to regulate DeFi.

This paper aims to provide a definition of what constitutes DeFi, providing a high-level overview of the sector, an in-depth and focused review on specific areas of interest, including of decentralised trading protocols and governance-related mechanisms, and will further raise broader issues and thoughts for consideration.

The views expressed in this paper are not an official position from the AMF on decentralised finance. They seek however to encourage discussions with ecosystem stakeholders, both public and private, with a view to foster the development of a balanced regulatory approach.

Given the discussion points raised in this paper, the AMF welcomes respondents to contribute their thoughts prior to 30 September 2023, by contacting innovation@amf-france.org.

I) What is Decentralised Finance?

1. Automated, decentralised and disintermediated blockchain protocols

DeFi is a recently emerged phenomenon, which purports to provide an alternative to traditional financial services (or "TradFi")[1] by replicating certain activities such as borrowing, lending and investing. Having developed since the launch of the *Ethereum* blockchain, DeFi claims to provide such activities in a fully decentralised, automated and disintermediated manner, both without the need for human intervention, and solely relying on the use of decentralised blockchain protocols[2], thereby defining new models of activity and governance, in which stakeholders can actively participate "on-chain".

In this sense, DeFi contrasts more broadly with "centralised finance" (or CeFi), which regroups service providers that use off-chain systems (including those that offer crypto-asset related services), which are operated by identifiable parties, entities or individuals. DeFi is thus an idiosyncratic term describing activities that have emerged in contrast to existing means of providing financial services (whether TradFi or CeFi, see figure 1). Though there is no single definition of DeFi, several elements can be attributed to it, based on some of the novel technical aspects (or "stack") that it displays (see figure 2).

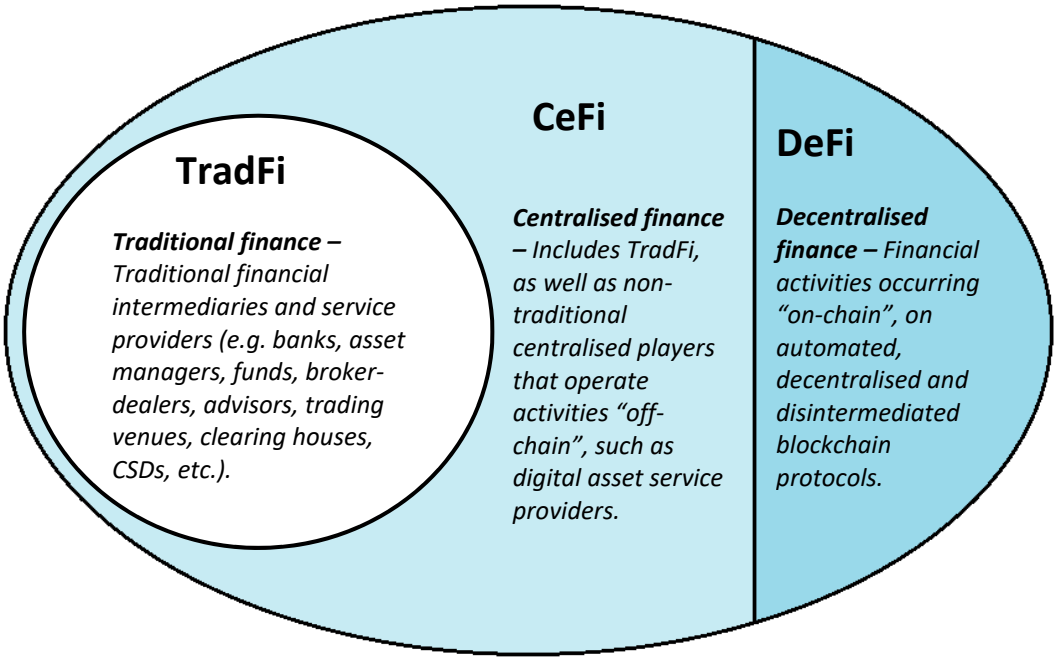


Figure I: Distinguishing between TradFi, CeFi and DeFi

[1] See: "ethereum.org/en/defi"
[2] See further details regarding *protocols* in box 1.

Box I – What is a protocol?

A protocol is a standardised set of rules that allows computers to format, process and transmit data. It is a common language that allows them to communicate in a standardised manner. These computers collectively then form the nodes of a network (with each node being able to operate, or "run" the protocol).

For instance, the hypertext transfer protocol (or "http") allows to generate information on webpages. Web browser applications can run the protocol, generating webpages and the information they contain.

Protocols can be more or less complex depending on the different types of tasks they perform (e.g. identifying communication channels, formatting data, routing and delivering messages, etc.). As a result, protocols can be superimposed into various "layers" that perform these different tasks, where each new layer depends on the successful operation of the layer below it, and so on.

The http protocol for instance runs on top of the TCP / IP protocol ("Transmission Control Protocol / Internet Protocol"), which serves to interconnect network devices, therefore forming the base layer of the internet.

A protocol will generally be named according to the function it performs. For instance, blockchain protocols allow for the registration of transactions in a sequence of blocks within a distributed ledger across a network of nodes. DeFi protocols are protocols that allow users to participate in decentralised finance activities, and DeFi trading protocols are protocols that allow specifically for the performance of DeFi exchange-type activities (see section III).

DeFi primarily builds upon the infrastructure provided by the *Ethereum* blockchain. Similarly to traditional protocols (see box 1 above), blockchain protocols can operate across different layers. For instance, the *Ethereum* protocol is a "layer 1" protocol, which provides a base layer that performs functions of settlement and recording of transactions into sequential blocks. Multiple "layer 2" protocols can be built atop this first layer. For instance, several protocols have been developed over *Ethereum*, performing a function known as "scaling" (i.e. aiming to make the function of the *Ethereum* protocol more efficient in the scale of transactions it can process)[3]. Finally, on top of these layers, several further protocols (or pieces of code such as smart contracts and DApps, see sections I. 2 and I. 3 below) can be custom built and integrated. Collectively, these layers form the ecosystem today known as DeFi.

While the automated nature of DeFi derives from the way in which software protocols operate, its decentralised aspect comes from the fact that a blockchain theoretically operates in a distributed manner across the nodes of a network, with no one single party deciding on the processing of transactions, or as to whom can participate. In practice however, different DeFi protocols can experience varying degrees of decentralisation, whether by design (see hereafter), or by virtue of how users participate in their governance (see section IV).

Concerning blockchain design, though *Ethereum* is the main protocol associated with the emergence of DeFi, others such as *Solana*, *Cardano*, *Polkadot*, or *Hyperledger* also offer similar functionalities, with certain notable differences however. In the debate as to whether the nature of a DeFi protocol is decentralised or not, a key difference resides in the distinction between the permissionless and permissioned nature of these blockchains. For instance, while access to *Ethereum* is open and not restricted by any central node or authority (making it a "permissionless" system), others (such as *Hyperledger*) only allow certain nodes to participate on its network (making them "permissioned" networks).

[3] See: "ethereum.org/en/layer-2"

Discussion point I – Permissionless versus Permissioned blockchain protocols

One aspect to consider when developing a regulatory framework for DeFi would be to assess the nature and degree of permissibility of blockchain protocols. Indeed, though certain aspects of a permissioned blockchain's activity require approval from certain entities or nodes on the network (and that such blockchains can be to a certain degree centralised), it can also be considered that the distributed nature of the nodes across a network give it a decentralised aspect.

Evaluating whether an activity falls within the remit of DeFi could thus include an assessment of whether a blockchain is permissionless or not, including an assessment as to the degree of permissibility of the blockchain. In this regard, a variable could be to evaluate how many entities, individuals, users or nodes can control the activity on the network (for instance in terms of onboarding of users, or for validating transactions).

Regardless of their permissioned or permissionless nature, a common trait of DeFi blockchain protocols is that they enable certain functionalities, chief among which is the notion of smart contract.

2. Smart contracts

Aside from decentralised protocols, smart contracts[4] are another key distinguishing feature of DeFi. A smart contract is a piece of code that aim to mirror the functionality of a "real-world" contract between parties, by automatically assessing whether a number of pre-determined conditions have been met for the purposes of carrying out a transaction. When these conditions are verified, the smart contract subsequently executes the transaction and transmits it to the underlying blockchain for it to be recorded. Examples of pre-determined conditions written into a smart contract's code can for instance include triggering price thresholds, which, once met or exceeded, lead to the transaction being executed. Smart contracts are automated and operate autonomously by nature, meaning that they are "self-executing" (i.e. operating continuously without the need for human intervention), locking in transactions and making them irreversible (or "immutable") once the execution criteria defined within the code have been met.

Smart contracts are executed by a quorum of blockchain nodes once transaction requests are initiated by a user. A transaction request can be initiated via any node, which broadcasts it to the rest of the network, where the other nodes will see the transaction and automatically verify that it is executed according to the pre-set rules provided by the code. If the transaction is executed successfully, the blockchain is then updated with a record of the event. A smart contract may also consider the input to be invalid and reject the transaction, in which case the state of the blockchain is not affected.

In the same way that real world contracts can be tailored to fit certain terms, smart contracts can also be developed to build in specific functionalities. Certain smart contracts for instance provide for the concept of a "hash timelock"[5], whereby their rules will require a buyer to confirm payment prior to a given deadline. Once the payment is confirmed, the transaction is executed, with the assets transferred simultaneously[6], making the entire process near instant. This leads in turn to the notion of "atomic settlement". Building in such optionality as a condition also allows for transactions to be cancelled where payment is not confirmed within a defined time period.

The function of smart contracts is to execute software logic that performs various tasks, processes or transactions that have been pre-programmed into them to respond to a set of conditions, and therefore smart contracts do not on their own constitute a legally binding agreement. To make them enforceable in the same way that a "real-world" contract would be, separate legal steps should thus be undertaken to link their execution to a legally binding agreement.

Despite their immutability, the code of smart contracts can be modified, though their autonomous nature requires that where changes are made, the underlying protocol be split, or "forked" from its previous iteration. This means that both versions of the smart contract will continue to operate in parallel, independently from one another. Previous

[4] Though the concept of smart contract was first formally coined in 1994, developers of the *Ethereum* blockchain implemented the functionality within the protocol.
[5] See: "Corporate Finance Institute.com - hashed timelock contract"
[6] See: "imf.org - DeFi's promise and-pitfalls"

versions of a smart contract can still be used as long as access is provided to them via an interface. This role is fulfilled by applications known as DApps (see section I. 3 below). The fundamental ability to evolve the code of a smart contract rests with the developers who can physically implement these changes, though users of the protocol can also be involved in the decision-making process (see further details regarding this under section IV below).

Discussion point 2 – Smart contracts

A first challenge is to determine a legal basis for the enforceability of a smart contract, as though their functionality may aim to mirror in some aspects that of "real-world" contractual agreements, their coding may not necessarily be fully translatable into the language of such agreements. A further aspect in this regard is to consider how to define the legal liability of parties that participate in the creation, development, or use of a smart contract, including assessing whether those who have written or developed its code, as well as those who use it, can be the subject of legal or regulatory requirements.

As smart contracts are able to execute transactions according to pre-determined rules, it could be possible for them to include rules that meet legal or regulatory requirements. However, the automated and autonomous nature of smart contracts can contrast with the interventionist aspect that is required by regulatory oversight (e.g. such as the need to halt or resume operations). In this regard, legislation for the regulation of DeFi protocols could require that smart contracts be designed to include rules that mirror such requirements, including a "stop / start" type mechanism, or a form of compliance certification of their code with applicable regulatory requirements.

It should also be considered which smart contracts can (and should) be the subject of legal or regulatory requirements, and how those smart contracts that are already developed and operating should be considered in this regard.

3. Decentralised applications (DApps)

Decentralised applications (DApps) are software applications that allow users to engage with the functionalities of smart contracts. In the same way that a new "layer" within a protocol can perform a different function (see box 1 above), DApps are built atop the smart contract layer, facilitating access by users to the functions of the smart contract they interface with. DApps also mirror the decentralised structure of the blockchain they are built upon, as they allow users to transact in a peer-to-peer manner within the bounds of the smart contract and network they provide access to.

DApps therefore act as interfaces that provide access to the on-chain functionalities of smart contracts, whereby a user submits a transaction request via their interface, after which it is transmitted to a designated node, before being forwarded to the smart contract. Once the criteria for the transaction have been met, the smart contract executes it and broadcasts it to the blockchain.

Though there is currently no simple standard definition of DeFi, there have been attempts by actors to define DApps[7]. One key aspect of a DApp so defined requires that its code be made available on an open-source basis[8]. This is a major difference with TradFi software applications, which are typically developed using closed-source software, and built on top of proprietary systems.

[7] See: "Github - The General Theory of Decentralized Applications, Dapps"
[8] Open source code is code which is made freely accessible, and can be re-used and modified as such.

Discussion point 3 – Use of open source software

Similarly to discussion point 1 above regarding permissioned versus permissionless protocols, another aspect to take into account when defining a regulatory scope for DeFi is to consider whether only open-source code or software should be included, as the use of open-source code raises a number of further questions from a legal perspective, since it can be distributed freely without licensing terms, as opposed to code which is closed-source in nature.

Due to the open-source nature of their code, DApps present several key attributes, where they differ from closed-source software[9]:

1. Transparency: DApps are designed and available for use in a transparent manner, allowing to identify the functions, user permissions and data that the underlying smart contract processes.

2. Auditability: Due to such transparency, the code is readily auditable, and provides the ability to openly measure metrics such as flow of funds (including volume and value traded), amount of collateral secured, etc.

3. Composability[10]: Due to the shareable nature of open-source code, DApps can be re-tailored and re-used within other applications. For instance, smart contracts can reference other open-source smart contracts, creating the property known as "composability"[11].

The below diagram presents the different layers that make up the technological stack of the DeFi ecosystem:

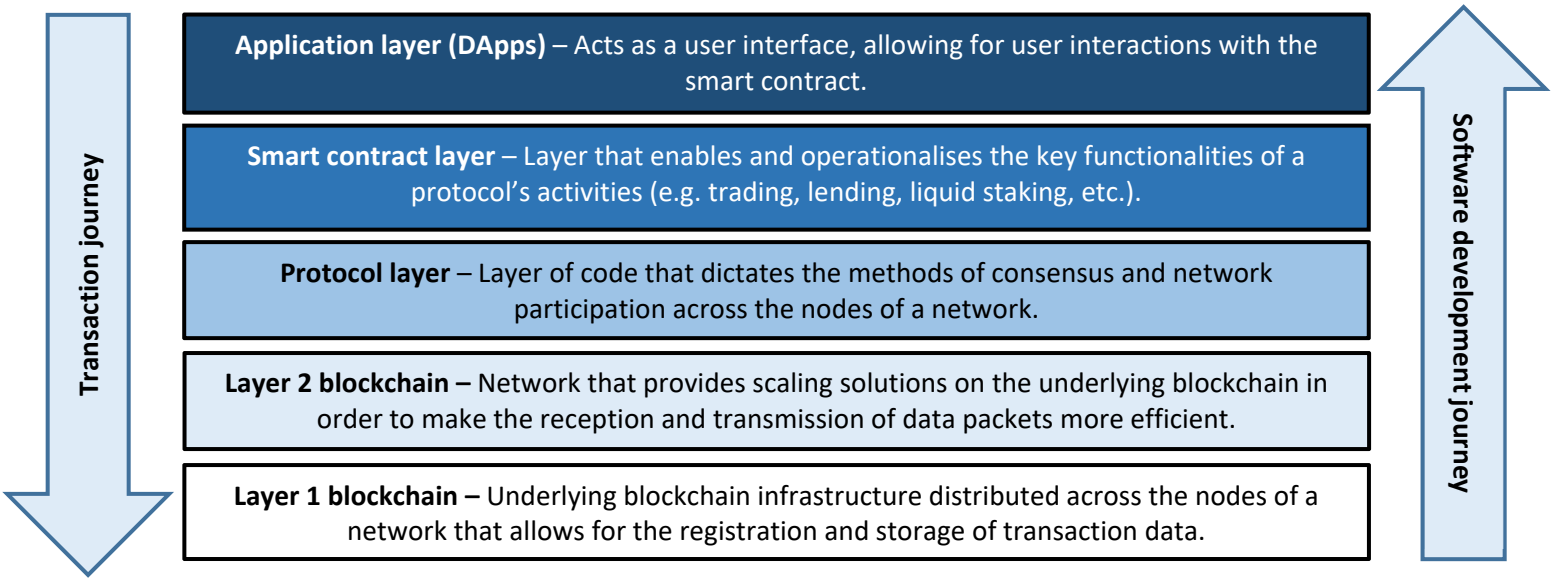


Figure 2 – The DeFi "stack"[12]

[9] See: "medium.com - DeFi Infrastructure 101 - Overview & Market Landscape"
[10] Composability is a principle of software development applying to the inter-relation between components of a system. A software system developed in this manner can allow for its components to be assembled so that they respond to specific user needs.
[11] See: "imf.org - DeFi's promise and-pitfalls"
[12] Source: AMF

II) The DeFi market: activities and products

1. Overview and observed trends

It is estimated that there were close to 2,000 DeFi protocols in existence at the start of 2023[13], which is more than twice the number registered in early 2022 (855). Of these, around 650 are reported to be Decentralised Exchanges (DEXes). Sources also estimate that several thousands of DApps give access to these protocols. An overall estimate of the exact number of DApps is difficult to establish due to a lack of consistency between sources. Certain sources indicate there are over 3,500 DApps overall[14], while the *Polygon* blockchain reported towards the end of October 2022 that over 53,000 DApps had been developed on its network alone[15].

Other indicators, such as Total Value Locked (TVL) are useful to measure the total value of assets "locked" into on-chain smart contracts at any given point in time.

As at end January 2023[16], TVL in DeFi protocols amounted approximately to 80bn USD, down from a high point of 258bn USD at the end of 2021, following a 60 % drop in crypto-asset prices in 2022 (see figure 4 below).

Among the various activities of DeFi protocols, Automated Market Makers (AMMs), Decentralised Exchanges (DEXes), and lending & staking protocols (see further details under section II. 2 below with regards to different activity types) account for approximately two thirds of DeFi TVL.

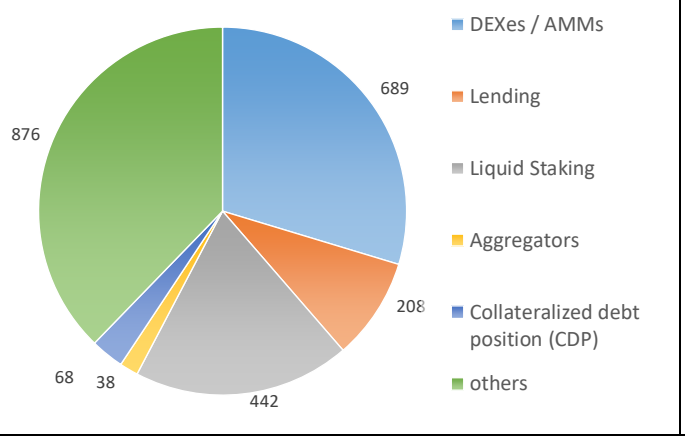
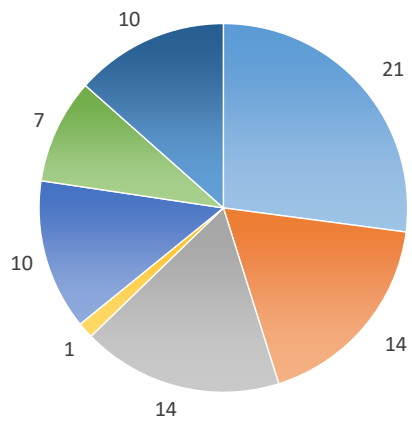
Number of DeFi protocols[17]	Total Value Locked (in USD bn)
	
Source: DeFiLlama	

Figure 3 – Overall number of DeFi protocols and Total Value Locked

Despite its emerging nature, DeFi has already experienced some major swings in its short lifespan. Following an initial period of growth where TVL reached heights of 260bn USD in late Q4 2021 (commonly referred to as the "DeFi summer"), it then fell abruptly from Q2 2022, with levels more recent approximating a third of the value measured since its high point (around 80bn USD as of late January 2023). This can notably be explained by the impact of the Terra / Luna crisis (see further explanations under box 2 below) and a general slump in crypto-asset prices. Despite this, the number of DApps and protocols in existence seems to have grown drastically over the same period (as seen above).

[13] See: "Defillama.com"
[14] See: "Tap Global - What are Dapps?"
[15] See: "Polygon Labs - Polygon Crosses 53,000 DApps Mark in a Major Adoption Milestone"
[16] Data retrieved 25 January. Sources used: DeFiLlama, Stelareum.
[17] A collateralised debt position (CDP) is a DeFi protocol locking collateral into a smart and that generates stablecoins in exchange.

Figure 4 – Historical DeFi TVL (in USD bn)[18]

Box 2 – The Terra / Luna crisis in focus

Summary

In May 2022, the Terra stablecoin (UST) and the closely linked Luna (LUNA) token crashed in a near-simultaneous manner, wiping out approximately 60bn USD in value over the course of a few days[19], and sending ripples through crypto-asset markets. As the first major crisis faced by the DeFi ecosystem, the Terra / Luna crash and its scale raised broader questions around the reliability and robustness of DeFi protocols, along with more specific questions on the use of algorithmic stablecoins[20].

Terra / Luna is a DeFi blockchain protocol[21] that, at the time of its crash, relied on an algorithmically-driven relationship between the UST stablecoin that purported to maintain a 1-to-1 peg in value against the US Dollar (USD), and Luna (LUNA), the protocol's native token. Unlike many other stablecoins, UST was not collateralised and thus not directly backed by any reserve. Instead, its overall supply was linked to that of LUNA, whilst it purported to maintain its 1-to-1 value measure against USD. LUNA meanwhile served as a stabilising mechanism that was designed to act in synchronicity with changes in the value of UST, whereby the supply of LUNA would be adjusted to absorb any volatility resulting from price changes in UST. This relationship was reliant on a demand and supply-type mechanism between the quantity of the two tokens, whereby destroying (or "burning") one led to the creation (or "minting") of the other.

To illustrate, whenever the value of UST dropped below 1 USD (for instance to 0.98 USD), users looking for arbitrage opportunities could buy 100 UST for 98 USD, subsequently converting the amount into the equivalent of 100 USD of LUNA, as the protocol's algorithm would maintain a stable value between 1 UST and 1 USD for the purposes of converting between both tokens. The resulting increased demand for UST by arbitrageurs thus increased the value of UST in the market, while in turn the Terra / Luna Protocol burned UST in exchange for the minting of LUNA, thus reducing the available supply and value of UST. This in turn caused the arbitrage opportunity to disappear when the value of UST reached 1 USD once again. The opposite would occur whenever the value of UST was above 1 USD.

[18] See: "Defillama.com"
[19] See: "Forbes - What really happened to Luna crypto"
[20] See: "banking.senate.gov - The Financial Stability Oversight Council Annual Report to Congress"
[21] Despite the events, the Terra / Luna protocol continues to operate to this day.

Timeline

After its initial 2019 launch, the Terra / Luna ecosystem gained gradual interest from investors, driving demand in both UST and LUNA tokens. Market capitalisation of LUNA grew until it reached a record amount of 139bn USD In April 2022[22]. However, shortly thereafter on 7 and 8 May 2022, the tides turned abruptly as users withdrew (or "de-staked") over 2bn USD in UST from the protocol, leading to a de-pegging of the stablecoin to 0.91 USD.

On 8 May 2022, the Luna Foundation Guard, a non-profit organisation set up in January 2022 by founders of the protocol to support the development of projects within the Terra / Luna ecosystem[23], began drawing down on its own reserves in response to the event, and sold more than 80,000 bitcoins (BTC) (valued at the time at over 3bn USD) in order to buy the equivalent amount in LUNA to help maintain the UST peg[24]. The sale generated a major drop in prices across crypto-asset markets, also affecting the value of the LUNA token. Separately, users continued to sell UST, which led to further LUNA minting, thereby compounding the effect of a drop in value. Prior to this, on 6 May 2022, LUNA had been priced at around 80 USD, dropping to below 1 USD just a week later, whilst UST dropped to 0.50 USD on 9 May, before plummeting to less than 0.15 USD on 16 May.

Risks observed and lessons learned

Use of algorithmic stablecoins – Though stablecoins play a key role in DeFi protocols via their on-chain representation of fiat value, the model used in the case of the Terra / Luna protocol shows how an automated mechanism can, under highly-stressed conditions, cause unintended or adverse effects on the operation of a protocol as a whole.

Complexity and lack of transparency – A lack of understanding and disclosure of the complex nature of the Terra / Luna protocol's stabilisation mechanism has also been blamed for the crash, whereby participants may not have had a sufficient understanding of the model, or lacked confidence in it, which may have also contributed to the continued sell-off.

Run risks – The Terra / Luna protocol crisis has shown that DeFi protocols are not immune to "run" risks, instances of which have been previously observed in the TradFi world. The run on Terra / Luna also had a cascading effect, whereby users continued to de-stake UST or sell-off LUNA after the initial de-pegging and fall in value.

Contagion and spillage – Though the crash of UST and LUNA was confined to the operation of a specific protocol, the event led to spillage into other DeFi protocols that had associations with UST[25], and further impacted crypto-asset markets more broadly due to the subsequent sell-off in BTC. Some have estimated the overall impact to be around 500bn USD[26].

Recovery and resolution – At this stage, there has been no clear recovery or resolution mechanism since the fall of the Terra / Luna protocol, including with regards to the compensation of users. As of October 2022, the Luna Foundation Guard indicated it was still not able to provide a timeline for the compensation of users who had been affected[27].

[22] See: "coinmarketcap.com - Terra Luna"
[23] See: "medium.com - Formation of the Luna Foundation Guard (LFG)"
[24] See: "twitter.com - LFG | Luna Foundation Guard"
[25] See: "cointelegraph.com - Terra contagion leads to 80%+ decline in DeFi protocols associated with UST"
[26] See: "washingtonpost.com - Crypto's meltdown refocuses regulator attention on the industry"
[27] See: "twitter.com - LFG | Luna Foundation Guard"

2. A variety of activities and products

As previously indicated, there are many different types of DeFi protocols and applications, which perform different functions. Though some mirror those activities found within TradFi, some display new features or have permitted the emergence of novel products, sometimes combining several types of activities. Detailed below are the principal activities and products observed within the DeFi ecosystem:

- **Automated Market Makers (AMMs)** and **Decentralised Exchanges (DEXes)** – These are types of protocols that bring together parties by allowing them to exchange crypto-assets. Though this can sound similar to what TradFi or CeFi trading platforms offer, the novelty lies in the fact that AMMs and DEXes do this on-chain, using smart contracts that manage trade flows in an automated manner without human intervention. In the case of AMMs in particular, trading is permitted by the existence of "liquidity pools" which provide liquidity in tradeable pairs that are offered on the AMM. This aspect is further explored in more detail in section III of this paper.

- **Lending –** Lending protocols bring together lenders and borrowers of crypto-assets, allowing depositors to stake their assets in exchange for a loan, usually in the form of stablecoins, whilst the assets deposited are a form of collateral provided against the loan. Most protocols require that loans be over-collateralised in order to minimise the risk of exposure in the case of default. Where a loan is not returned, the collateralised assets become the property of the lender.

  Due to the near-instantaneous nature of smart contract transactions, new product types have emerged such as "flash loans", whereby uncollateralised loans can be made with an immediate repayment term. This is often used in the context of arbitrage trades, whereby a purchaser can sell the proceeds of a loan at a higher value, before immediately repaying the borrowed principal at par. This could be likened to a repurchase-type agreement in the context of a short sale in TradFi, however the near-instantaneous and fully on-chain nature of the issuance, sale, and repayment (that can all occur within a single transaction, or "block") without the use of multiple intermediaries, grant it a novel aspect.

- **Staking and liquid staking –** Staking protocols allow users to deposit their assets in order to earn rewards (e.g. in the form of interest). For instance, certain protocols allow users to stake *Ethers*, which (as the native tokens of the *Ethereum* protocol) are used to validate transactions via the blockchain's proof of stake (PoS) mechanism[28]. The mechanism allows the creation of new *Ethers* as further blocks are generated on *Ethereum*, distributing these to validators as a reward, proportionally to their relative deposited stake[29].

  Liquid staking is a specific instance of staking, in which the reward for staking the assets is a "liquidity token" (representing said assets), which can then be used for trading on other protocols. The token however must be returned in order to access the staked assets.

- **Aggregator-type activities –** Such protocols are able to read activity across several protocols, aiming to offer better liquidity and / or pricing by aggregating data. Instances can include creating efficiencies across AMM or DEX type protocols by seeking to provide better asset or price allocation, while others may look to bridge gaps in rates across lending or staking protocols that can occur due to inefficiencies.

- **Prediction markets** – Prediction markets are a tool that allow users to participate in contracts that provide a payout based on the results of future events. Though this can be likened in some ways to certain TradFi products that provide such types of outcomes (e.g. the provision of a payout based on future asset prices being met), prediction markets provide a reward based on events, not underlying assets or their values. In this sense, prediction markets could be most likened to betting, as a type of economic activity.

- Some activities or products offered via DeFi protocols are referred to in a manner similar to certain TradFi activities, namely:

[28] Currently, the minimum amount of Ether to be staked so that a node may become a validator of transactions on the *Ethereum* blockchain is of 32 Ethers.
[29] See: "ethereum.org - How The Merge impacted ETH supply"

- **Asset management –**These are DeFi protocols that allow users to manage their assets, including in relation to purchasing, selling or transferring them. Certain protocols for instance enable various types of trading strategies (such as arbitraging, latency optimisation, etc.). Differently to more traditional forms of asset management services however, asset holders are also those that set and define a strategy in this case, whilst the smart contract carries out the execution.

- **Margin trading –** Protocols with margin trading allow for assets to be traded using borrowed funds from third parties, giving users access to more capital to trade with. This is similar to what can be observed in certain TradFi markets that allow for margin or leverage trading, such as Forex.

- **Derivatives and synthetic assets –** As in TradFi, some protocols allow to trade products whose value is determined by reference to the price of another "underlying" asset, thereby providing indirect exposure to that asset or to its market. In DeFi, certain new product types such as perpetual futures have become particularly popular[30].

- **Insurance –** Certain DeFi products can also insure users against losses. While some may seek to replicate or replace traditional insurance products, others can specifically provide payouts against losses that might occur due to events taking place in relation to DeFi protocols. This can include losses arising from attacks, price crashes, or protocol hacks.

Discussion point 4 – Assessment of risks posed by DeFi activities

Developing a regulatory framework for DeFi should take into account the characteristics of the various activities that can be observed within DeFi. To this effect:

Where activities within DeFi are seen to have similar characteristics to those within TradFi, legislators or regulators should first consider whether existing regulation can be applied to DeFi activities where these are considered to display similar features.

Where DeFi displays activities that offer novel characteristics, or combine several activities including TradFi and DeFi-type activities, it should be considered whether an "ad hoc" type regulation would offer better protection for users, due to the specificities of DeFi protocols. In some cases, certain aspects of the activities carried out could be subject to existing legal or regulatory requirements, however such requirements could also prove impractical or sometimes even impossible to implement, or enforce against, in certain cases.

III) Decentralised Exchanges (DEXes) and Automated Market Makers (AMMs)

This section seeks to provide a more in-depth focus on the activities of decentralised exchanges (DEXes) and automated market makers (AMMs), which can display similarities to centralised markets. It will include an overview of their model, the identification of similarities and differences with traditional trading platforms, and potential risks to consider.

1. Model overview

At first glance, DEXes and AMMs (collectively shortened to "DeFi trading protocols" where relevant within this section) can appear to provide activities similar to those of centralised trading platforms, as they bring together buying and selling interests, allowing users to trade their assets with one another at defined quantities and prices.

[30] See: "synthetix.io - Decentralized Perpetual Futures"

DeFi trading protocols however do not operate centralised off-chain order books in the same way that TradFi or CeFi platforms do, as they instead make use of on-chain smart contracts that dictate the terms of how participants can trade. In such a model, assets are priced according to an automated formula (written into the code of the smart contract), which may differ from the price-formation process observed within traditional off-chain order books.

The smart contracts that operate within DeFi trading protocols can also require (in the case of AMMs, as further explored below) that assets be locked within liquidity pools, which are in turn supplied by liquidity providers, who bring crypto-assets to the pool, as this allows the smart contract to determine the available tradeable supply. Meanwhile, liquidity providers are remunerated by transaction fees generated by the trading activity on the protocol, and are rewarded proportionately to the amount of liquidity they have provided within the pool. In exchange for the liquidity they provide, liquidity providers also receive tokens that represent a claim to withdraw their fraction of the pool.

The pricing formula considers both the current price of the assets within the pool (which necessitates an external point of reference prior to trading taking place), and the quantity of assets available. Based on the transaction orders submitted by users who wish to take liquidity from the pool, the pricing formula then recalculates prices according to the updated relative value of the assets available in the pool. This mimics a supply and demand mechanism, whereby an asset that becomes rarer (i.e. one that decreases in quantity) is priced accordingly as more expensive.

One limitation of DeFi trading protocols is that they can rely on the use of external information, such as for pricing, as evaluating the total assets in a liquidity pool implies to have a pre-existent knowledge of prices. This reliance comes in the form of external data sources (that can originate from other DeFi protocols, as well as from CeFi platforms) that link in to the protocol's smart contract, known as "oracles". The use of such sources of data raises a number of questions from a policy perspective, as further detailed in section III. 4 below.

In practice, DeFi trading protocols are characterised by high-levels of concentration. The top 1 % in terms of TVL (6 protocols) account for 15bn USD and 75 % of the total TVL (approximately 20bn USD) for trading protocols.

Overall DeFi trading protocol volumes have decreased since the end of 2021 (from approximately 260bn USD to 200bn USD at the start of 2022), dropping even further since May 2022 (to under 80bn USD today). The monthly trading volume is currently estimated to be around 50bn USD, while it was approximately three times the value in the first half of 2022.

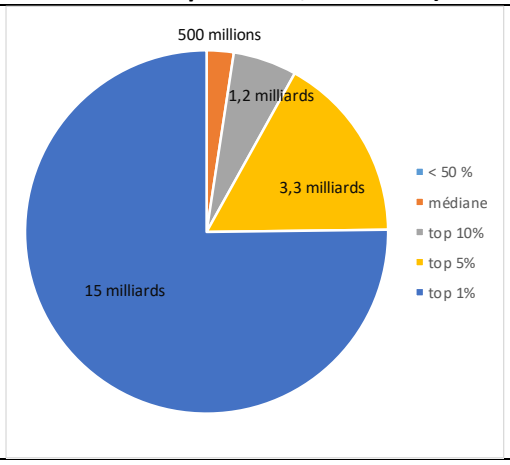
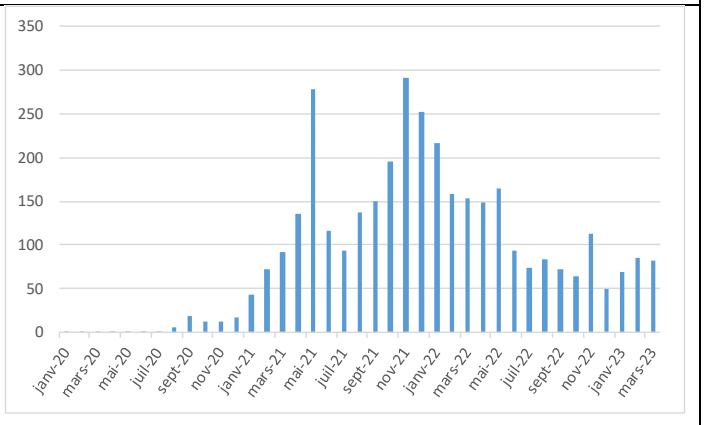
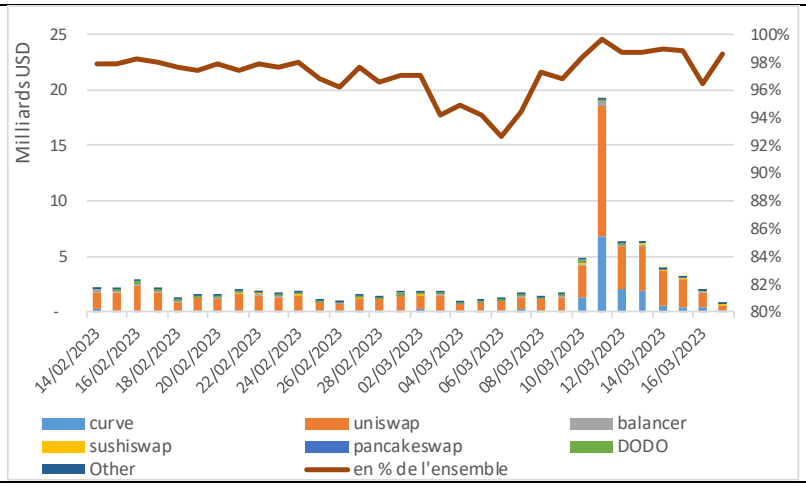
TVL in DEXes and AMMs (across 650 observed protocols, in USD bn)	***Average monthly DEX / AMM TVL (in USD bn)***
	
Source : DeFiLlama	

Figure 5 – Overall and average monthly TVL in DeFi trading protocols

The average daily volume registered by DeFi trading protocols recently stabilised around 2bn USD, whereas it fluctuated between 3 to 5bn USD towards the beginning of 2022. A more notable spike at 19bn USD was observed on 11 March 2023 surrounding the uncertainty that resulted from the de-pegging of the USDC stablecoin, as users sought to sell their assets. As a comparison, the daily trading volume on CeFi crypto-asset trading platforms was 52bn USD in May 2023[31], while the average daily trading volume in April 2023 on Euronext alone was of 8bn USD (across all asset classes)[32].



Sources: Dune, AMF calculations

Figure 6 – Daily average volumes of the top 6 DeFi trading protocols as a share of total daily volume (USD bn)

2. Differences and similarities between DeFi trading protocols and centralised trading platforms

DeFi trading protocols differ from centralised trading platforms, as the latter operate an order book and record transactions off-chain. In on-chain trading however, the operation of smart contracts allows for the automated initiation, trading, settlement and recording of transactions in a single cycle, which marks a key difference in the model of DeFi trading protocols versus that of centralised trading platforms.

A further differentiating factor is that DeFi trading protocols allow for a peer-to-peer model of transacting, providing a direct form of user access to on-chain smart contracts, whereas many traditional trading platforms typically operate using a membership model, whereby access is provided via intermediaries that are registered as members. As such, DeFi trading protocols are more comparable to some of the more recently established CeFi crypto-asset markets which, though they operate off-chain order books, also can provide a direct form access to their market without use of other intermediaries.

In the case of AMMs, another differentiating factor is that these allow any participant to bring assets to a pool, providing them with the ability to become a liquidity provider. In this way it could be argued that DeFi trading protocols make the provision of liquidity and the benefits derived more accessible to participants, whereas traditional trading platforms might use designated liquidity providers or market makers to manage this aspect.

Finally, due to their decentralised nature, DeFi trading protocols usually adopt the organisational structure of a DAO (see section IV below for further details), which allows the users of the protocol to participate in matters relating to its governance. In CeFi, though a member or a participant on a market can also be a shareholder of the platform which operates the market in which it participates, this is not always the case. DeFi trading protocols democratise such a model, by allowing users to participate in the governance structure of the protocol (for instance by allowing them to vote on decisions relating to evolving the code or functionality of the smart contract).

[31] See : "coingecko.com - Top Crypto Exchanges Ranked by Trust Score"
[32] See : "euronext.com - Statistics"

Further, in TradFi, many trading venues are regulated, whereby they are subject to certain requirements (such as under MiFID II in the EU[33]) including that of having a market rulebook, which is typically reviewed and approved by a regulator.

Discussion point 5 – DeFi trading protocol market rules

In the context of developing rules for DeFi trading protocols, it could be envisaged that requirements apply to the code of smart contracts, whereby it be made translatable into non-technical language, so that it can be read, reviewed and approved by regulators. This would ensure proper disclosure of a DeFi trading protocol's market rules, potentially enabling better compliance with them.

3. Differences between DEXes and AMMs

As indicated above, there are two main types of DeFi trading protocols, which are distinguishable on the basis of how their smart contract is designed:

Decentralised Exchanges[34] (DEXes) typically operate using an on-chain order-book type mechanism, allowing a maker to send an order to a smart contract, specifying the crypto-asset to be traded, the rate at which a crypto-asset can be sold against another, and an expiry date. The taker can decide whether or not to fill the order. Though the technology used aims to replicate the functionality of traditional order books, it presents certain limits due to the difficulties experienced by smart contracts in processing a potentially high number of transactions in an on-chain manner, as queries have to be sent to multiple nodes across a network, as opposed to a centralised database or server. This process gives rise to operational challenges, characterised by a lack of liquidity within DEXes. Poor liquidity in turn deteriorates bid-ask spreads, which, in addition to the cost of high fees derived from the operationally intensive implementation of order books on-chain, then causes further lower liquidity. Due to these issues, certain DEX protocols might offer an off-chain layer to ease interaction between the DApp and the smart contract.

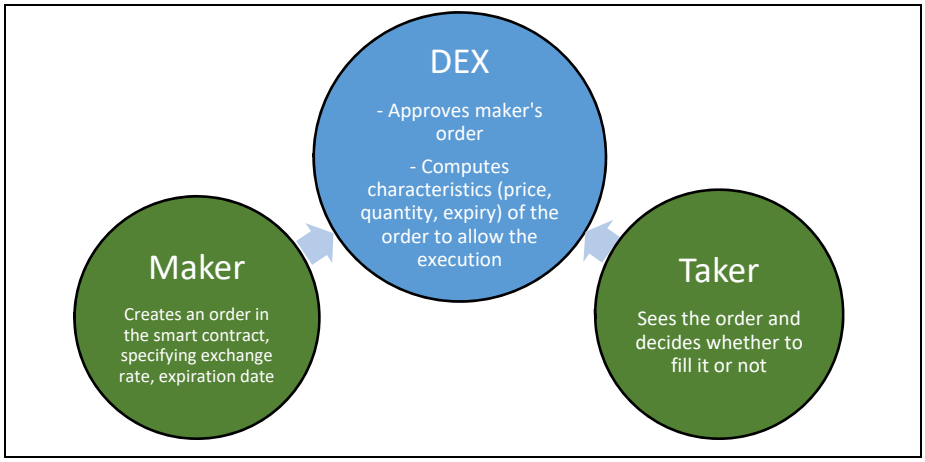


Figure 7 – Trade between a maker and a taker on a DEX

[33] See article 47 of MiFID II.
[34] Also defined as "Order book based DEXes".

Automated Market Makers (AMMs) enable users to trade (or "swap") crypto-assets at an exchange rate that is algorithmically determined on-chain, based on supply and demand factors. The trading on AMMs is permitted due to the existence of "liquidity pools", which provide liquidity in tradeable pairs that are offered on the AMM. The initial value of the assets in the pool is pre-determined, often by reference to "oracles", external sources of data that also ensure that the exchange rate remains coherent with that on other markets (see risks described under section III. 4 below)[35].

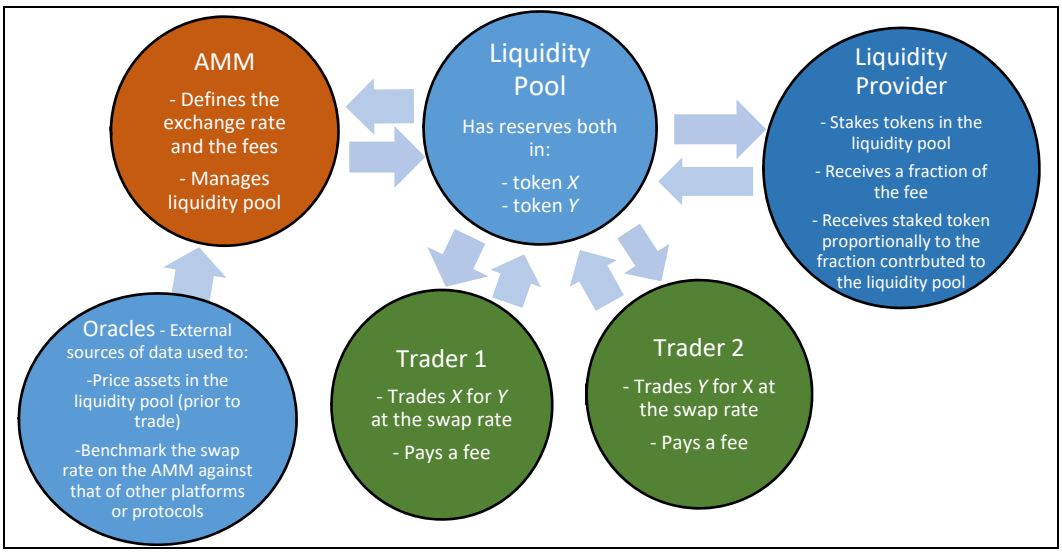


Figure 8 – Swapping tokens on an AMM

As described above, the development and implementation of order book-based DEXes can be rendered difficult due to the cost-intensive process of replicating an order book on-chain. Consequently, gas fees (the cost of processing transactions occurring on the blockchain) of DEX-based smart contracts can be significantly higher than gas fees on AMMs. Due to the limitations of DEXes, AMMs are thus the most prevalent form observed among DeFi trading protocols[36], and there is a tendency to use "DEX" or "AMM" interchangeably as an acronym to wrongly describe both trading protocol models.

This is in contrast with TradFi markets, where roles between different intermediaries and exchange operators are usually clearly defined.

International bodies such as the International Organisation of Securities Commissions (IOSCO) and the Financial Stability Board (FSB) have indicated that certain criteria could be used to distinguish between AMMs or DEXes[37, 38]. For instance, a protocol would be considered a DEX where it contains an off-chain order book element, whereas in contrast the operation of an AMM would be considered as entirely based on-chain.

[35] Bartoletti, M., Chiang, J. H. Y., & Lafuente, A. L. (2021). SoK: lending pools in decentralized finance. In *Financial Cryptography and Data Security. FC 2021 International Workshops: CoDecFin, DeFi, VOTING, and WTSC, Virtual Event, March 5, 2021, Revised Selected Papers 25* (pp. 553-578). Springer Berlin Heidelberg.

[36] Among the top 10 DeFi trading protocols with the largest volumes for the month of March 2023, trading volumes on AMMs represent 98% of the total (source: DeFiLlama, AMF calculations).

[37] See: "iosco.org - IOSCO Decentralised Finance Report (March 2022)"

[38] See: "fsb.org - The Financial Stability Risks of Decentralised Finance (16 February 2023)"

Discussion point 6 – Definitions of DEX and AMM

- There is a general question as to whether integrating an off-chain element is constitutive of a DeFi trading protocol model, since many centralised crypto-asset trading platforms make use of such a model. It should therefore be made clear what distinguishes a DeFi trading protocol from a CeFi trading platform in this regard. One differentiating factor could be to consider whether trading occurs entirely on-chain or not.
- When considering how DEX and AMM models may differ, one aspect to take into consideration could be to identify the nature of the pricing mechanism being used. For instance, one element could be to understand whether the DeFi trading protocol makes use of a pricing model that uses a demand-supply mechanism based on the value of assets contained within liquidity pools, or an order-book based price-formation process.

4. Risks of DeFi trading protocols

Like any type of financial activity, DeFi trading protocols present a number of risks for their stakeholders. Some of these are comparable to those created by traditional trading platforms, whilst others could be considered as emerging or novel due to the specific nature of DeFi trading protocols. The below section provides an overview and summary of the risks considered as the key risks arising from the use of DeFi trading protocols, and so DeFi-wide risks are not included here.

Unregulated market risk	As DeFi trading protocols are currently not regulated, they could be exposed to a heightened risk of illicit activity, including market abuse, manipulation, fraud, or Anti-Money Laundering and Counter-Terrorist Financing (AML-CFT) risks. Further, for many participants (specifically those that might lack experience or an understanding of the functioning of blockchain protocols), DeFi trading protocols could be complex to understand due to the specificities of the models or technology used. This in turn can expose participants to unexpected risks of liquidity or losses, absent sufficient disclosure of the existence of such risks.
Liquidity and fair and orderly market risks	DeFi trading protocols could be affected by risks of market liquidity that indirectly impact the operation of a fair and orderly market, though such risks may materialise in a different manner compared to the way they do within traditional finance platforms. In DeFi trading protocols, liquidity strongly relies on the number of participants in the protocol. A swap of a large size (within an AMM smart contract for example) could have a significant impact of the exchange rate, influencing the probability of existing orders being filled, and thus in turn reducing the number of eligible participants. Further, should liquidity be withdrawn from a liquidity pool in a DeFi trading protocol, this would directly affect the relative price of the assets contained within, but could also lead to more lasting liquidity issues if prices remain stuck at certain levels. Larger scale 'runs' could also be witnessed, and may further amplify the scale of liquidity draw-downs. Finally, when relative prices diverge substantially, liquidity providers can also suffer losses if they withdraw their asset contribution from a pool.
Pricing model risk	While "oracles" could be used to correct potential differences in prices, the use of an external source to potentially correct price inaccuracies raises questions as to the soundness of the pricing model offered by DeFi trading protocols in the first place. Further, the sources of the data provided by some oracles is not always clearly indicated, and could thus lead to mis-pricing the assets contained within liquidity pools.

Price manipulation and front-running risks	Separately, the reliance on oracles can also lead to potential price manipulation, whereby the price provided by an oracle could be affected by manipulation taking place on the market where the data is sourced from, leading in turn to prices being impacted on the DeFi trading protocol. Liquidity-takers in a DeFi trading protocol could also be exposed to manipulation risk due to the execution of trades requiring validation by nodes on the blockchain in order for settlement to occur. While the liquidity taker is uncertain about the timing of the settlement of their trade, the transaction order they have submitted becomes public before it becomes priced, at point of settlement on the underlying blockchain. This time lag opens the door to malicious activity, as another participant could take advantage of it by placing their own trades around the transaction time[39]. By having access to information about an order before it is included in a block (i.e. before it is settled), attackers can thus take advantage of variations in assets prices. Such types of attacks have commonly been referred to as "sandwich" attacks[40].
Slippage risk	Slippage risk is a further risk that occurs more specifically on DeFi trading protocols, due to the lag experienced between the point in time when a trade order is confirmed in a smart contract, versus the time when the trade is settled on the blockchain. This time difference can lead to significant variations in order versus execution price, and potentially to significant losses experienced by participants. As a consequence, when trading on a DeFi trading protocol, participants may be brought to specify a slippage tolerance level, which is the maximum variation in price they are willing to accept.
Leverage risk	High forms of leverage can be present on DeFi trading protocols, especially where these are interconnected to lending or derivative protocols. Though loans in DeFi are typically over-collateralised, amounts borrowed can be re-used as collateral in other transactions and on other protocols (including potentially in relation to crypto-asset derivatives), and hence collateral can quickly depreciate in a context of widespread de-leveraging. Due to this, leverage risk can be of major concern to DeFi trading protocols that offer derivatives trading activities. The Bank for International Settlements (BIS)[41] in particular has also highlighted that, unlike TradFi, DeFi does not benefit from intermediaries acting as shock-absorbers, such as banks, and hence any contagion resulting from highly leveraged market activity could potentially be fatal to a DeFi trading protocol.
Governance risk	As described above in relation to risks pertaining to price manipulation and front-running, DeFi trading protocols do not prevent such risks despite a seemingly disintermediated and decentralised governance structure, as bad actors may still have an incentive to take advantage of the blockchain mechanism to make undue gains based on transaction data before it is registered on the blockchain.

[39] See: "bis.org - DeFi risks and the decentralisation illusion"
[40] See: "arxiv.org - SoK: Preventing Transaction Reordering Manipulations in Decentralized Finance"
[41] See: "bis.org - DeFi risks and the decentralisation illusion"

IV) New forms of governance: Decentralised Autonomous Organisations (DAOs) and governance tokens

1. DAOs: An Overview

When Vitalik Buterin, the founder of the *Ethereum* protocol, first described the concept of a Decentralised Autonomous Organisation (DAO) in 2014, he referred to it as an "entity that lives on the internet and exists autonomously, but also heavily relies on hiring individuals to perform certain tasks that the automaton itself cannot do"[42]. In the context of DeFi, DAOs represent a form of organisation through which the various stakeholders of a protocol (such as its users, developers, etc.) can organise themselves to perform tasks in relation to the protocol, including the ability to make decisions over its governance or functioning. In the case of DeFi protocols, the rules and design features of a DAO are typically written into a smart contract.

DAOs do not necessarily have a pre-set or defined legal form. They bring together a community of individuals or entities whom are granted a right to make decisions in relation to the underlying protocol they participate in. In practice, this takes place in the form of making proposals, or voting on such proposals, via the use of governance tokens (see section IV. 2 below for further details). While a protocol has users that participate in its economic activity, the corresponding DAO structure will have members that participate in its governance, where the protocol's users are members of the DAO insofar as they are given governance tokens that allow them to participate in the governance of the DAO.

The votes of DAO members are a key aspect of the decision-making process regarding the organisation and functioning of a protocol, as they can (for instance) express their views on proposals pertaining to the development of new activities, the inclusion of new assets, or with regards to any proposed changes made to the protocol's governance rules themselves.

The structure of a DAO mirrors that of the protocol it governs in its decentralised aspects: its rules are written into the protocol, and as its members are distributed across the network, so is their participation. Hence DAOs themselves are referred to as decentralised organisations, and purport to remove the need for a centralised form of management. Votes are carried out on-chain to safeguard the transparency and immutability of the voting process. Results of a vote are registered on the blockchain and are publicly accessible, allowing all members to verify them.

Developers hold a key role within a DAO, being the ones that have developed the related protocol on the blockchain. They often are the founding members of the associated DAO and work closely with other members of the organisation, suggesting changes or improvements to the protocol, which are subsequently put to a vote from all members. Individual members can submit proposals, which are then discussed between members and developers. Where a proposal is accepted, the developers will then implement the code changes to the protocol. Further, developers play a key role in securing and stabilising the protocol, and are responsible for identifying or resolving software bugs or errors that could affect its security or operation, and for informing DAO members of such breaches.

More generally, a DAO refers to a form of organisation, rather than to a type of economic activity, and as such, different types of economic activities can be governed by a DAO (DAOs which can serve to govern the activities of a protocol – protocol DAOs – being one such example).

Beyond protocol DAOs, other types of DAOs include investment or venture DAOs (where members can pool their funds with a view to investing in projects), DAOs that are used for philanthropic or charitable goals (e.g. for the attribution of grants or non-profit funding), and community-driven or "social" DAOs, which bring together like-minded members on common topics of interest (e.g. social issues). As of the end of 2022, it was estimated that there were several thousands of DAOs, with some estimates placing their number close to 5,000[43].

[42] See: "blog.ethereum.org - DAOs, DACs, DAs and More: An Incomplete Terminology Guide"
[43] See: "bitkan.com - How many DAOs are there in the world?"

2. Governance tokens

Members of a protocol DAO will typically be provided with a token generated by the protocol. Where such tokens give rise to rights in relation to governing or making decisions in relation to the protocol, they are referred to as "governance tokens". In certain cases, such tokens can also be used as a form of remuneration for the users of the protocol.

Governance tokens can be obtained upon their initial distribution after the development of the protocol, or they can be obtained in exchange for work or services contributed to the functioning of the DAO (for instance, developers of a DeFi protocol might obtain governance tokens in exchange for their development work). Specifically in the case of DeFi trading protocols, governance tokens can also be distributed directly to liquidity providers as form of remuneration in exchange for the assets they bring to a liquidity pool.

Within protocol DAOs, governance tokens can be used in various forms of voting[44]. Voting mechanisms can be similar to, or vary from, those found within traditional organisations – depending on the structure of the mechanism, these can display similarities or differences compared to traditional shareholder voting structures. For instance, DAO voting structures such as quorum-based or relative majority voting allow for votes to be cast on the basis of the highest number of votes winning, with either a simple majority or a qualified majority being required for a proposal to pass. Other forms, such as quadratic, or "conviction" voting introduce further variables (such as a form of weighting to allow for smaller holders to be recognised against larger ones, or for votes that last the longest in time to gain more recognition). Finally, mechanisms such as "multi-signature" or indirect voting allow for votes to be delegated to other parties, either within the DAO (e.g. to a college of members) or outside of it.

Whilst governance tokens are specific and only issued for use in relation to a given DAO, they can be freely traded, either on DeFi protocols or within CeFi markets, giving them a speculative nature, similarly to other crypto-assets. Therefore, as governance tokens are exchanged, anyone can theoretically acquire membership (and thus voting rights) within the corresponding DAO, being able to potentially influence its governance without necessarily being a user of the underlying protocol.

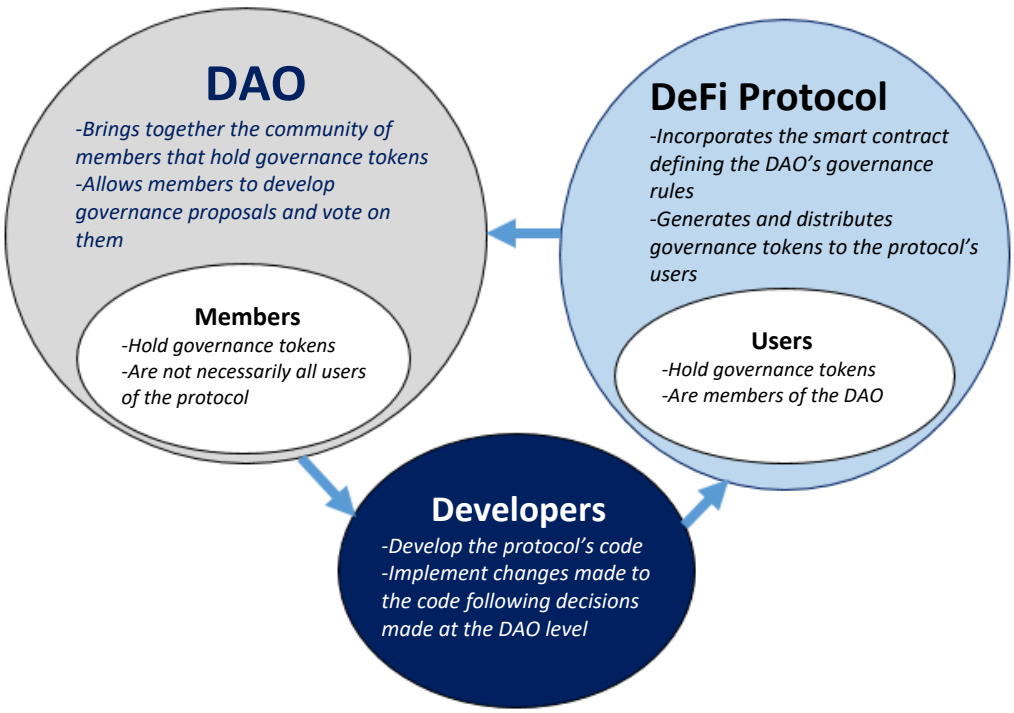


Figure 9 – Relationship between a DAO, a protocol, and its developers

[44] See: "medium.com - Voting Options in DAOs"

3. Risks and issues of protocol DAOs and of DeFi protocol governance

3.1. Uncertainty of legal form and economic models

Most jurisdictions currently do not have a legal framework that provides a legal form for DAOs[45]. In practice, DAOs can often have a "sister entity" however, which can itself be set up as a private company or as a non-profit organisation. Via the use of governance tokens, such entities may often exert a strong degree of influence over the DAO.

The legal liability of the structure used and of the various stakeholders involved can thus vary depending on the mode of organisation that is adopted. Further, while some DAOs operate as non-profit organisations, others can be for-profit, and are structured to receive fees for the activity of the protocol that they govern, or even hold reserve funds in the same way that traditional economic actors would. DAOs can thus also display different economic structures, in such a way that different economic incentives may prevail, thereby generating different risks depending on the way they are incentivised. As a consequence, where a DAO is not subject to any legislation or rules, its members may not be able to benefit from the legal protection or guarantees that might otherwise offer them protection in relation to incorporated structures.

Further, the location of a DAO could be difficult to establish due to its decentralised nature and structure. Due to issues of pseudonimity (see below), it may also be difficult – if not impossible – to identify DAO members, the absence of a home jurisdiction for a DAO further compounding the issue by hindering efforts to identify what legal framework or rules would apply to its members.

This can cause notable difficulties for legislators whose aim is to develop frameworks that would seek to offer further legal certainty to DAOs and their members.

In France, work is being undertaken by the *Haut Comité Juridique de Place* (HCJP – the Legal High Committee for financial markets of Paris) with regards to the governance and structuring of DAOs, in order to provide clarification on the legal framework that could apply to them under French law.

3.2. Governance and pseudonymity risks

As the identity of users on the blockchain is provided through components such as wallet addresses or transaction references, the blockchain is considered to be "pseudonymous" by nature in its functioning[46], i.e. making the identification of individuals impossible on the basis of such data alone. This leads to clear concerns in relation to regulatory risks with regards to identification around the ownership of assets, the origin and destination of funds, as well as AML, know-your-customer (KYC) or fitness and propriety risks.

Due to such pseudonymity, the risks of bad governance of DAOs could be significant. Specifically, such pseudonymity makes it difficult to understand who may exert control over a DAO, as several pseudonymous actors could in fact be the same actor, or represent the same interest, increasing the possibility of conflict of interest or collusion.

Finally, the pseudonymity of participants in a DAO could render any form of legal or regulatory action against them difficult if not impossible, further creating incentives for "bad" actors to participate in DAOs.

It should be noted however that since pseudonymity is principally a feature of permissionless blockchain protocols, this risk would likely be more present in the context of such protocols, rather than in relation to permissioned blockchains (see discussion point 1 above), which would be more readily able to implement requirements around the identification of participants.

[45] To date, certain jurisdictions have worked on developing legal frameworks regarding the treatment of DAOs, including the United States (in the states of Delaware, Utah, Vermont, and Wyoming), as well as Switzerland, Jersey, Guernsey and the UK.

[46] See: "europa.eu - Decentralized finance: Information frictions and public policies : approaching the regulation and supervision of decentralized finance"

3.3. (De)centralisation and degree of control

One difficulty observed in relation to DAOs is that of assessing the effective degree of control exerted by participants over its governance. Indeed, certain actors could concentrate control over a DAO and over the related protocol, thus giving the organisation a *de facto* centralised governance model.

Depending on the specific setup of a DAO with regards to who is eligible to hold governance tokens, whether those who develop the code of the protocol can hold tokens, or how the voting is carried out, the degree of decentralisation may vary.

In practice, levels of decentralisation vary strongly between DAOs. One study shows strong discrepancies in degrees of control, with certain structures displaying very concentrated vote distribution levels (less than 1% of token holders controlling up to 90% of voting power), whereas others show a more equitable distribution[47].

Discussion point 7 – Decentralisation and degree of control

The effective degree of decentralisation is a key component that should be evaluated when determining the effective degree of control that is exerted over a DAO's governance, and thus over the underlying blockchain protocol that it governs.

In particular, estimating the number of governance tokens held by the developers of the protocol is one aspect to take into account when determining whether effective control is exerted over a protocol, whether by an individual or by a group of individuals. In certain cases, it should also be considered whether control can, or is, being exerted by third parties who may not be users of the protocol, or may not be linked to how it is effectively managed.

Similarly to traditional entities or organisations, the degree of control over a DAO can also be established on the basis of factual evidence. On the one hand for instance, control could be observed "de facto" in situations where an individual or group of individuals hold a significant proportion of the votes (without holding an effective majority), with the other votes being dispersed across the remaining holders. Meanwhile, situations of control "de jure" could also be established where an individual or group of individuals hold an absolute majority in votes.

[47] See: "blog.chainalysis.com - Dissecting the DAO: Web3 Ownership is Surprisingly Concentrated"

Conclusion

Through the publication of this paper, the *Autorité des Marchés Financiers* (AMF) aims to share its preliminary thinking on the subject of Decentralised Finance, by giving an overview of its ecosystem and the trends observed to date, while focusing more in-depth on certain areas, including DeFi on trading protocols and governance-related matters. This paper also seeks to raise certain points of discussion that could be useful for consideration in a regulatory context.

The emergence of DeFi as a new phenomenon and the crash of the Terra / Luna protocol in May 2022 have raised a number of questions regarding the maturity and viability of certain DeFi protocols. This has also pointed to a lack of clarity in the operation of such protocols, emphasising the need to have a clear framework with safeguards that would help enable better information-sharing and protect users of DeFi protocols, in order to foster trust in the ecosystem and the innovation it brings.

With DeFi still being at an early stage of development, yet evolving rapidly as a sector, legislation should be thought in a progressive and proportionate manner, taking into account on the one hand the benefits to innovation displayed by DeFi activities and governance models, while on the other considering the risks they pose to participants.

When defining a regulatory perimeter for DeFi, the "same activities, same risks, same regulation" approach should apply unambiguously, whilst taking into account the novel aspects displayed. DeFi poses a broader number of risks for regulators to consider beyond those mentioned in this paper, in particular anti-money laundering and counter-terrorist financing (AML-CFT) or know-your-customer (KYC) risks, mainly due to the issues of pseudonimity outlined under section IV.

Due to the cross-border nature and reach of DeFi activities, the AMF also supports the development of a global coordinated approach towards regulation to ensure a global level-playing field, which should both aim to protect investors and foster innovation.

In this context, the coming years may prove to be a crucial period for the DeFi sector, with a double challenge: allowing for the development of transparent and secure means to help grow the ecosystem and encourage innovation on the one hand, whilst providing adequate levels of investor protection on the other.

In France, the *Autorité de Contrôle Prudentiel et de Résolution* (ACPR) has made certain proposals for the regulation of DeFi which it has submitted for consultation[48]. At the EU level, the European Commission will have to assess developments relating to decentralised finance in crypto-asset markets and evaluate the need for the regulatory treatment of decentralised finance crypto-asset systems following the entry into force of the Markets in Crypto-Assets (MiCA) regulation. Work carried out by international bodies and organisations (such as IOSCO[49] and the FSB[50]) will also bring further clarity regarding guidance or recommendations made to jurisdictions in relation to the regulatory treatment of DeFi.

The AMF fully supports these initiatives, and intends to increase its engagement with stakeholders, both public and private, with a view to allow the emergence of a balanced regulatory framework that will help support the sound development of decentralised finance in the long run.

[48] See: "ACPR - "Decentralised" or "disintermediated" finance: what regulatory response?"
[49] See: "iosco.org - IOSCO Decentralised Finance Report (March 2022)"
[50] See: "fsb.org - The Financial Stability Risks of Decentralised Finance (16 February 2023)"