11 October 2023
ESMA50-2085271018-3349

ESMA TRV Risk Analysis

Financial Innovation

Decentralised Finance in the EU: Developments and risks

ESMA Report on Trends, Risks and Vulnerabilities Risk Analysis

© European Securities and Markets Authority, Paris, 2023. All rights reserved. Brief excerpts may be reproduced or translated provided the source is cited adequately. Legal reference for this report: Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/77/EC, Article 32 'Assessment of market developments, including stress tests', '1. The Authority shall monitor and assess market developments in the area of its competence and, where necessary, inform the European Supervisory Authority (European Banking Authority), and the European Supervisory Authority (European Insurance and Occupational Pensions Authority), the European Systemic Risk Board, and the European Parliament, the Council and the Commission about the relevant micro-prudential trends, potential risks and vulnerabilities. The Authority shall include in its assessments an analysis of the markets in which financial market participants operate and an assessment of the impact of potential market developments on such financial market participants.' The information contained in this publication, including text, charts and data, exclusively serves analytical purposes. It does not provide forecasts or investment advice, nor does it prejudice, preclude or influence in any way past, existing or future regulatory or supervisory obligations by market participants. The charts and analyses in this report are, fully or in part, based on data not proprietary to the European Securities and Markets Authority (ESMA), including from commercial data providers and public authorities. ESMA uses these data in good faith and does not take responsibility for their accuracy or completeness. ESMA is committed to constantly improving its data sources and reserves the right to alter data sources at any time. The third-party data used in this publication may be subject to provider-specific disclaimers, especially regarding their ownership, their reuse by non-customers and, in particular, their accuracy, completeness or timeliness, and the provider's liability related thereto. Please consult the websites of the individual data providers, whose names are given throughout this report, for more details on these disclaimers. Where third-party data are used to create a chart or table or to undertake an analysis, the third party is identified and credited as the source. In each case, ESMA is cited by default as a source, reflecting any data management or cleaning, processing, matching, analytical, editorial or other adjustments to raw data undertaken.

ISBN 978-92-95202-95-5, DOI 10.2856/588145, EK-03-23-190-EN-N

European Securities and Markets Authority (ESMA)
Economics, Financial Stability and Risk Department
201-203 Rue de Bercy
FR-75012 Paris
risk.analysis@esma.europa.eu
ESMA - 201-203 rue de Bercy - CS 80910 - 75589 Paris Cedex 12 - France - www.esma.europa.eu
Cover photo: Image Microsoft 365

Financial Innovation

Decentralised Finance in the EU: Developments and risks

Contact: anne.chone@esma.europa.eu[1]

Summary

Decentralised finance (DeFi) has attracted attention from investors and regulators, as the latest and arguably most innovative development in the crypto area. This article assesses the development of DeFi, its distinctive features, and the risks it raises to ESMA's objectives, with a view to informing the future review of the markets in crypto-assets regulation (MiCA). It highlights that although investors' exposure to DeFi remains small overall, there are serious risks to investor protection, due to the highly speculative nature of many DeFi arrangements, important operational and security vulnerabilities, and the lack of a clearly identified responsible party. DeFi does not represent a meaningful risk to financial stability at this juncture, considering its small size, but this is something that requires monitoring as the phenomenon continues to evolve quickly. Looking at one specific type of DeFi application, namely decentralised exchanges, the article shows that they purport to eliminate important pain points in the trading of crypto-assets but bear their own flaws and challenges. While market integrity in DeFi and crypto-asset markets is still under-researched, due to important data gaps and the technicalities involved, the article shows that DeFi has spawned new market manipulation issues and techniques, such as maximal extractable value and flash loan attacks, that the industry needs to address.

[1] This article was written by Anne Chone, Zeno Benetti and Filippo Giuglini.

Introduction

Decentralised finance (DeFi), which seeks to provide financial services using blockchain or distributed ledger technologies in an open, decentralised and permissionless way, has seen significant development over the last few years. The phenomenon is still small globally and in the EU, but requires consideration because of the existing risks to investor protection, and possibly to financial stability. In addition to the lack of relevant data to assess the scope of the phenomenon and risks involved, DeFi also presents important challenges for EU regulators and supervisors because the existing EU regulatory framework, including the newly introduced markets in crypto-assets regulation (MiCA), revolves around the regulation of intermediaries and/or central authorities – all entities that DeFi purports to eliminate.[2]

This article sheds light on DeFi's innovative features, its potential benefits and specific risks EU regulators and supervisors should be aware of when dealing with the phenomenon, also in view of MiCA's future review. It starts with (i) an introduction to DeFi, from its origins to recent market developments; continues with (ii) the analysis of the potential benefits and risks of DeFi to users and the wider financial system; and zooms in on (iii) decentralised exchange protocols and (iv) the specific challenges that these protocols and DeFi's novel features raise for market integrity; followed by (v) concluding remarks.

Decentralised finance – Origins and key concepts

Sitting at the juncture of finance and blockchain technology, DeFi purports to provide financial services in an open and permissionless way, without traditional financial intermediaries being involved. To do so, DeFi leverages on blockchain technology and so-called smart contracts, i.e. self-executing pieces of codes that fulfil the terms and conditions of a transaction in an automated manner.

The concept of **smart contracts** is not new, and was introduced by computer scientist Nick Szabo in the early 1990s. Szabo referred to a smart contract as a 'set of promises, specified in digital form, including protocols within which the parties perform on these promises'. In 2014, Ethereum brought the concept to the next level by offering a blockchain-based platform 'allowing anyone to write smart contracts and decentralized applications where they can create their own arbitrary rules for ownership, transaction formats and state transition functions'.[3] Ethereum effectively bridged the world of crypto-assets and smart contracts and unleashed the development of new blockchain applications beyond currencies and payment. A forthcoming publication by ESMA will provide an overview of smart contracts, including a proposed classification. In 2016, the first (now defunct) decentralised exchange protocol, EtherDelta, was launched, followed by the first decentralised stablecoin, MakerDAO, in 2017. The phenomenon started to gain traction from mid 2020, when several DeFi protocols introduced token incentives programs for users.

DeFi is intended to serve the **same functions as traditional finance**, e.g. the transfer of monetary value, the pooling of funds, or the transfer of resources through time and space, and replicates existing financial services. What sets DeFi apart from traditional finance is the permissionless technological infrastructure on which it is built and its decentralised nature.

From a technological standpoint, DeFi has a **multi-layered architecture**, also known as the 'DeFi stack', that includes permissionless blockchains, smart contracts, DeFi protocols and decentralised applications (DApps), as illustrated in the appendix (Chart 8). The foundational layer, the 'settlement layer', is the permissionless blockchain where transactions are recorded and become immutable. On top of this settlement layer, comes the application layer, composed of smart contracts-enabled applications. These smart contracts-enabled applications can be further divided into three main groups, namely crypto-assets, DeFi protocols and DeFi compositions. A third layer comprises web or mobile device applications (DApps) providing user-friendly interfaces for users to access DeFi products and services from their computers or

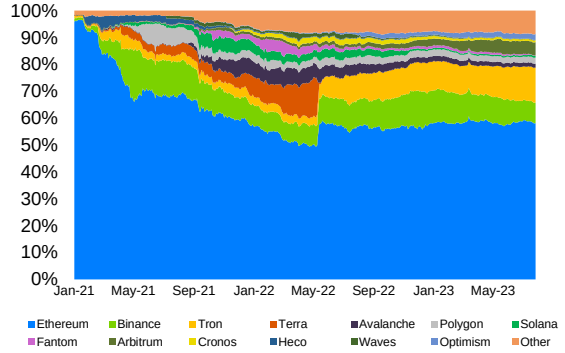
[2] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023. .EUR-Lex - 32023R1114 - EN - EUR-Lex (europa.eu)

[3] Ethereum white paper, 2014. Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform.

smartphones. It should be noted that the terms 'protocol' and DApp are often used interchangeably to refer to the protocol itself or the user interface.

This multi-layered technological architecture is an important feature of DeFi to the extent that it supports interoperability and **composability**, namely the ability of different protocols to work together and to be combined in different ways seamlessly (like Lego blocks). For example, a DeFi user can borrow Ether from Aave, deposit Ether into MakerDAO to mint Dai, and then use Uniswap to swap Dai for USD Coin — all without leaving the Ethereum ecosystem. Composability exists in many forms in the traditional world already. However, because DeFi is permissionless, it virtually allows anyone to build on the network, further increasing the possible activities and interoperability between them. On a less positive note, composability increases complexity and interconnectedness which brings with it new risks and regulatory challenges as discussed in the following sections. The majority of DeFi applications, representing about 60% of total value locked (TVL), currently leverage on Ethereum (Chart 1), although concurrent chains have started to emerge.

Chart 1
TVL breakdown by chain (%)
DeFi heavily reliant on Ethereum



Note: TVL per chain (in %) from January 2021 to June 2023. Terra's collapse explains its disappearance after May 2022
Source: DefiLlama, ESMA

Decentralisation in DeFi refers not only to the absence of intermediaries or central authorities for implementing financial services, thanks to the use of smart contracts as discussed above, but also to **decentralised governance structures**. Indeed, DeFi protocols purport to have decentralised governance structures, meaning that control and power over the protocol, such as how decisions on changes to the protocol are made, are decentralised. DeFi protocols use different mechanisms for that purpose, including novel decentralised autonomous organisations (DAOs). In its purest form, a DAO is entirely governed by its community and voting power is represented by governance tokens that may be acquired by virtually anyone. In practice however, even DAOs may involve some form of centralisation, e.g. because of concentrations of governance token holders or dependency on creators and foundational investors. In addition, the fact that elements of a DeFi protocol may be viewed as decentralised or subject to community vote does not mean that the protocol itself is fully decentralised.

Stablecoins, oracles and bridges are other core components of DeFi.

So-called **stablecoins** as their name suggests are crypto-assets that are meant to maintain a stable value relative to another asset, typically a fiat currency like the US dollar or the euro. Contrary to centralised finance, DeFi cannot support fiat currencies (since fiat currencies are not available 'on-chain'). Stablecoins are therefore essential to the operations of DeFi markets. They facilitate fund transfers between users and across protocols, are used as deposits and collateral in DeFi protocols and eliminate the need for multiple conversions to and from fiat money. This key role explains why their trading volume generally exceeds that of other crypto-assets.

Oracles enable smart contracts to access relevant external or off-chain data by means of queries. In other words, oracles allow data and content external to the blockchain (e.g. assets prices) to be incorporated into the DeFi transaction flow, enabling the execution of smart contracts.

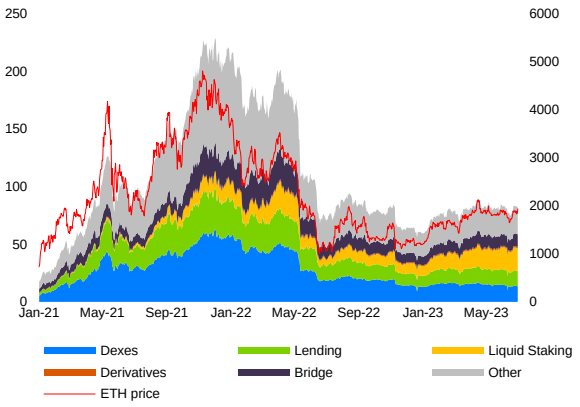
Bridges serve to connect two different blockchains, typically by creating a synthetic representation of a blockchain-specific crypto-asset (sometimes denoted as its 'wrapped' version) on a different blockchain. Bridges effectively solve one of the pain points within blockchains, which is the lack of interoperability between different chains. For example, wrapped Bitcoin is a form of Bitcoin that can be used on Ethereum. Many DeFi protocols have integrated bridges to let their users swap tokens from different protocols without having to leave the platform.

Market development: A rollercoaster

2021 saw an exponential growth of DeFi. TVL, i.e. the sum of the value of all assets deposited in a DeFi product, the most widely used metric to measure DeFi size despite its limitations, grew almost 20 times in about a year to a peak of USD 225bn in December 2021 (Chart 2), with decentralised exchanges (DEXs) and lending protocols leading the way.[4] The 2021 boom coincided with the surge in crypto-asset prices – Ether's price increased almost fivefold in 2021 to reach its all-time high in November 2021 – fuelled by speculation in an extremely low yield environment and investors' fear of missing out.

It was followed by an abrupt fall in 2022 amid rising interest rates and the global economic slowdown. In May 2022, the **collapse of Terra** and its contagion effect led to an almost 40% fall in TVL in several days and exposed important fragilities in DeFi markets (Box 1). Since then, TVL has fluctuated around USD 70-80bn (or USD 40-50bn discounting for double counting), less than a third of the historical peak.

Chart 2
TVL by DeFi protocol type
Sharp fall after exponential growth



Note: TVL per protocol type in USD billion (primary y-axis) and ETH price in USD (secondary y-axis), between January 2021 and June 2023. The category 'Others' include all other protocols categorised by DefiLlama, including collateralized debt positions, yield and yield aggregators, algo-stables, services.
Sources: DefiLlama, ESMA

Yet, the estimated number of DeFi users continues to grow, although at a slower pace, and some predict continued growth in the years to come, mainly as a result of the ongoing development of new DeFi use cases, the increasing adoption of crypto-assets by mainstream investors, and the continued emergence of new DeFi protocols.[5] The number of estimated users of DeFi protocols now exceeds 7.4mn, representing a 35% increase in a year, even if it only represents a tiny fraction (around 3%) of the total of Ethereum addresses.

Public sources list more than **2,800 DeFi protocols but the vast majority are very small** in size or not even active and the three largest protocols account for about 30% of DeFi TVL (Table 1). Beyond TVL, another useful metric to gauge the popularity of a protocol is the market capitalisation of its native token. There again, a handful of protocols stand out.

Table 1
Top 10 DeFi protocols by TVL
Three largest protocols represent c. 30% of TVL

Protocol	Native token	Type	TVL (bn)	Native token mkt cap (mn)
Lido	LDO	Staking	14.051	1.651
MakerDAO	MKR	CDP	6.090	0.621
AAVE V2	AAVE	Lending	3.765	0.901
Curve	CRV	DEX	3.740	0.616
Uniswap V3	UNI	DEX	2.781	3.718
Summer.fi	NA	Services	2.588	NA
Coinbase WETH	NA	Staking	2.131	NA
AAVE V3	AAVE	Lending	1.856	0.901
Rocket Pool	RPL	Staking	1.181	0.723
Liquity	LQTY	CDP	0.732	0.083

Note: Top ten DeFi protocols by TVL as of end June 2023, along with their native token, type, TVL (in USD billion) and native token market cap (in USD billion). None of these protocols is currently registered in the EU.
Sources: DefiLlama, Coingecko, ESMA

DeFi accounts for a small portion of crypto markets (DeFi TVL represents about 6% of the total crypto market capitalisation) but a few DeFi protocols rival their centralised finance equivalents in terms of usage or size. Trading volumes on Uniswap rival (and even exceed for

[4] One of the main limitations of TVL is double-counting due to the composability of DeFi, e.g. one asset deposited in one protocol may be used as collateral in another protocol. TVL also fluctuates with market prices and not only because of users depositing or withdrawing assets from DeFi protocols.

[5] Statista, 2023. Revenue in the DeFi market is projected to reach USD 16,960mn in 2023 and to show an annual growth rate of 19.60% resulting in a projected total amount of USD 4,700mn by 2027. DeFi – Worldwide | Statista Market Forecast.

certain crypto-assets) large centralised crypto exchanges. The Dai stablecoin powered by the MakerDAO protocol is the third largest stablecoin in size after Tether USDt and USD Coin.

DeFi promises benefits…

DeFi is still new, and whether it will deliver on its stated objectives, namely more efficient, transparent and open financial services, remains to be seen. The Bank for International Settlements (BIS) observes that DeFi activities do not finance activity in the real economy at this point, meaning that the ecosystem is mostly self-referential and used for speculation (BIS, 2023).

Conceptually, the use of smart contracts, because of the finality and trust attached to them, could reduce the need for traditional intermediaries and central counterparties as we know them today, with **potential benefits in terms of speed, security and costs** for financial transactions. DeFi protocols operate continuously, allowing worldwide transactions 24 hours a day, 7 days a week. DeFi transactions are recorded on chain, where they become immutable and traceable (albeit in a pseudonymous way) by virtually anyone, which can enhance transparency for users and supervisors.

DeFi could contribute to greater **financial inclusion** by allowing users to access products and services without an intermediary who may selectively restrict access.

Because the code underpinning DeFi protocols and applications is open source and DeFi is composable, DeFi may also facilitate the development of **innovative financial products**. Innovative products already made available by DeFi include perpetual futures, flash loans and autonomous liquidity pools. Perpetual futures are futures contracts that, contrary to traditional futures, have no expiry date, meaning that they can be held indefinitely, without the need to roll over contracts when they near expiration. Flash loans are uncollateralised loans whereby the actions of borrowing and repaying the loaned amount both happen in one single block on the blockchain. Flash loans purport to eliminate the risk of the borrower (or lender) defaulting on its obligations and the need to post collateral thanks to blockchain's atomicity, namely the fact that actions can be executed collectively in sequence in one block or fail collectively.[6] The term 'flash' denotes the speed with which the transactions are executed, often within seconds. Autonomous liquidity pools, such as those implemented by automated market makers on decentralised exchanges, provide instantaneous liquidity to users without an intermediary exchange being involved. Flash loans and decentralised exchanges are discussed in greater detail in the following sections.

… but comes with significant risks

Important risks to consumers

Yet, DeFi entails important vulnerabilities and risks. Because DeFi aims at replicating traditional financial services, it exposes users to the same types of risks, including market, liquidity, and counterparty risks. **Market and liquidity risks** are exacerbated with DeFi compared to traditional finance due to the highly speculative and hence volatile nature of many crypto-assets (ESMA, European Banking Authority and European Insurance and Occupational Pensions Authority, 2022). By way of comparison, the annualised 30-day volatility of Bitcoin or Ether has been on average 3.6 and 4.7 times higher respectively than that of the Euro Stoxx 50 between June 2021 and June 2023 (ESMA TRV No 2, 2023). These risks are compounded in the case of margin trading or derivatives because of the leverage involved.

Counterparty risk should in theory be lower or even non-existent in DeFi thanks to the use of smart contracts and atomicity. Yet, smart contracts are not immune to errors or flaws (see section on exploits). When it comes to DeFi lending protocols, in the absence of creditworthiness checks, they often require users

[6] Atomicity is a feature of blockchains in which actions can be executed collectively in sequence in one block or fail collectively. In the case of flash loans, if the borrower does not repay the capital, the conditions set out in the flash loan smart contract are not met, and the transaction is reversed, with the funds returned to the lender. In theory, atomicity eliminates counterparty risk and the need to post collateral since it guarantees that a transaction is either completed or reversed as if it never happened. Yet, blockchains and smart contracts are not immune to flaws and errors as discussed in the following sections.

to provide collateral assets of higher value than the granted loan – resulting in overcollateralisation. However, if the collateral value decreases below a certain threshold, the borrower is exposed to the risks of liquidation. Qin et al (2021) find that liquidation designs in major DeFi lending protocols incentivise liquidators to sell excessive amounts of discounted collateral at the borrowers' expense. Automated liquidations of leveraged positions on DEXs expose traders to the same risks.

DeFi is especially vulnerable to **scams and illicit activities**, since virtually anyone can create or interact with DeFi protocols without the need to identify oneself and go through 'know your customer' checks. DeFi development has progressed to the point where templates allow for the creation of a token in a matter of minutes without any programming knowledge or experience. Malevolent people can use the technology to anonymously create malicious decentralised applications, which have no other purpose than to deprive users of their money. By identifying and analysing Ponzi schemes on Ethereum, Chen et al (2019) estimate that before July 2017, as many as 507 smart Ponzi schemes were created (although they represented a tiny portion, around 0.03% of all Ethereum contracts). Another important source of risk for DeFi users is the lack of a clearly identifiable responsible party and the absence of a recourse mechanism if things go wrong.

Disintermediated access to a wider range of financial products can expose less sophisticated investors to **overly complex or risky products**. In the 2021 bull market, many DeFi protocols lured users with double-digit expected returns that basically extrapolated on indefinitely booming crypto-assets prices and used high leverage. When crypto-assets prices collapsed in early 2022, several protocols, including the Anchor protocol on the Terra blockchain (see Box 1) collapsed, which translated into severe losses for users.

There are important **operational, technological and security risks** that are inherent to DeFi and its underlying technology. These risks are typically found in any DLT-based system but are exacerbated in the case of DeFi, because of its multi-layered infrastructure, its composability and smart contracts functioning in an autonomous way. According to one blockchain analytics firm, in 2022, DeFi protocols as victims accounted for 82.1% of all crypto-assets stolen by hackers – a total of USD 3.1bn – up from 73.3% in 2021 (Chainalysis 2023). Bridge protocols in particular, because they act as huge, centralised repositories of funds backing crypto-assets bridged from one blockchain to another, are targets of choice for hackers. Five out of the ten largest exploits ever are attributable to attacks on bridges (Table 2) and of the USD 3.1bn stolen in 2022, 64% came from bridges.

Box 1

Terra's collapse exposed important fragilities

The Terra blockchain's most popular product was a stablecoin called UST. Before its collapse, UST was the fourth-largest stablecoin with USD 18bn in market capitalisation. Unlike other large stablecoins though, UST was an **algorithmic stablecoin**, meaning that it was not backed by traditional assets but rather maintained its parity with the US dollar through an algorithmic relationship with Terra's native token, LUNA. In Terra's case, this process was set up to work through UST's **mutually dependent pairing** with LUNA. Every time a UST token was minted, the equivalent of USD 1 in LUNA was burnt, and vice versa.

While the project attracted critics from the outset, being described as 'creating nothing out of nothing' and akin to a Ponzi scheme, Terra, including the Anchor protocol, became the **second largest DeFi project** with almost USD 40bn in TVL (Anchor lured investors into buying USDT by offering a 20% yield to users depositing their UST in the protocol).

In early May 2022, UST lost its peg following large UST sales in what looked like an attack against the Curve liquidity pool (Briola et al., 2023). UST holders could redeem their UST, which was worth less than USD 1 for one dollar worth of LUNA. As more users redeemed and the supply of LUNA rose, its value fell. In the following week, UST and LUNA holders rushed to the exit, resulting in a **death spiral** that sent the value of both tokens to zero.

Terra's collapse highlighted the fragility of algorithmic stablecoins and extremely **speculative** nature of certain DeFi protocols. It also highlighted the **high interconnectedness** within DeFi and crypto-assets more broadly. The collapse bankrupted many investors, erased more than USD 100bn in TVL and pulled down the entire crypto market with it: over USD 400bn in value was wiped out in terms of crypto market capitalisation. Indeed, when Terra's founder and the LUNA Foundation deployed more than USD 3bn to (unsuccessfully) support LUNA's price and defend the peg, they caused a downward pressure on the market and triggered a sell off of other crypto-assets. Meanwhile, attackers cashed in over USD 800mn estimated profits (Locke, 2022).

Table 2
10 largest DeFi exploits to date
DeFi exploits

Protocol name	Protocol type	Exploit type	Loss (USD mn)	Year
Ronin Network	Bridge	Consensus	624	2022
Poly Network	Bridge	Smart contract	611	2021
BNB Bridge	Bridge	Smart contract	586	2022
Wormhole	Bridge	Smart contract	326	2022
Euler Finance	Lending	Smart contract	197	2023
Nomad Bridge	Bridge	Smart contract	190	2022
Beanstalk	Stablecoin	Governance	181	2022
Wintermute	Mkt maker	Private key	162	2022
Cream Finance	Lending	Market design	130	2021
BonqDAO	Lending	Smart Contract	120	2023

Source: Rekt database, ESMA

Attacks on DeFi protocols essentially target **code vulnerabilities** (e.g. errors in the underlying smart contracts), and **access control points** (e.g. protocols' consensus mechanisms or governance frameworks), with a view to altering their functioning. Many DeFi protocols go live without any audit or due diligence and the public open-source nature of the underlying smart contracts leaves their code vulnerabilities exposed to malicious actors. Indeed, if a protocol becomes large enough, any flaw in its smart contract code is very likely to be found and exploited. Prominent examples of consensus and governance-related exploits include Ronin Network and Beanstalk in 2022. In the Ronin case, the attacker managed to compromise one of the Ronin Bridge signatures and gained the majority control needed to approve deposit and withdrawal transactions on the chain. For Beanstalk, an attacker exploited a flaw in the governance framework to put forward a proposal for a vote, buy a significant stake of governance tokens to acquire a super majority, vote the proposal in his favour and immediately execute it.

No sizeable financial stability risks

Crypto-assets markets, including DeFi, **do not represent meaningful risks to financial stability** at this point, mainly because of their relatively small size and limited contagion channels between crypto and traditional financial markets (ESMA 2022, ESRB 2023, Financial Stability Board (FSB) 2023). As of the end of June 2023, crypto-assets had a market capitalisation of around USD 1.1tn (around EUR 1tn, [7] equivalent to the assets of the Intesa Sanpaolo bank (which stood at USD 1.1tn or EUR 1tn as of April 2023, making it the EU's 12th largest bank by assets at that date)[8] or 3.2% of the total assets held by EU banks (an estimated USD 33.7tn or EUR 30.8tn as of December 2022).[9]

ESMA identified in an earlier article (ESMA, 2022) **two main risk transmission channels** between crypto and traditional financial markets, namely the exposure of traditional investors to crypto-assets and stablecoins but concluded that they did not represent a meaningful risk to financial stability at this point. Notably, the collapse of FTX in November 2022, the 'Lehman moment' [10] for the crypto industry, sent shockwaves across the entire crypto market – Bitcoin and Ether lost 15–20 % in 48 hours, several stablecoins temporarily de-pegged, several crypto-lenders went bankrupt and several DeFi protocols were also indirectly affected – but had no meaningful impact on traditional markets. Similarly, the collapse of the Terra/Luna DeFi protocol had no material spillover effects on traditional markets.

However, because DeFi intends to replicate the same functions as traditional finance, it shares the same vulnerabilities, including **liquidity and maturity mismatches, leverage and interconnectedness**, which could translate into systemic risks if the phenomenon were to gain significant traction and/or if interconnections with traditional financial markets were to become material. Stablecoins and lending protocols in particular can give rise to liquidity and maturity mismatches and in turn run risks, with potential

[7] Panetta, 2023. https://www.ecb.europa.eu/press/key/date/2023/html/ecb.sp230623_1~80751450e6.en.html

[8] S&P Global, 2023. https://www.spglobal.com/marketintelligence/en/news-insights/research/europes-50-largest-banks-by-assets-2023

[9] ECB, 2023. https://www.ecb.europa.eu/press/pr/date/2023/html/ecb.pr230622~a115bde6aa.en.html

[10] U.S. Treasury Secretary Janet Yellen likened the collapse of FTX to that of Lehman Brothers in 2008 at the New York Times DealBook Summit on 30 November 2022, but noted that it has not spilled over into the traditional banking sector.

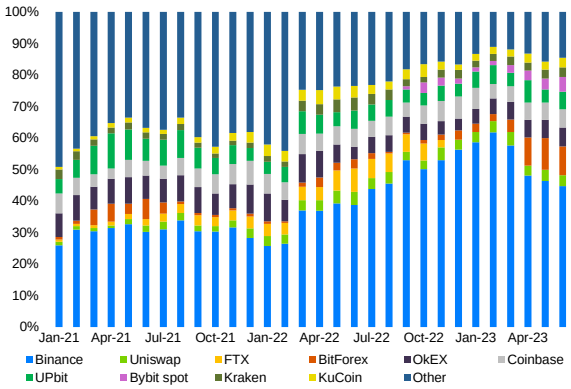
negative spillover effects on the wider financial system, e.g. through confidence effects. The combination of high leverage and automatic liquidation mechanisms which are not typically found in traditional finance, is another important source of risk, as it can increase procyclicality within crypto markets with potential negative externalities on the wider financial system. [11] DeFi's composability also translates into high interconnectedness within DeFi and crypto markets more broadly, which could have negative financial stability implications if contagion channels between crypto and traditional markets were to expand further.

While DeFi purports to provide financial services in a decentralised manner, it gives rise to new forms of **concentration risk**. DeFi activities are concentrated in a small number of protocols, which rely on a handful of blockchains as settlement layer (Chart 1). The failure of any of these large protocols or blockchains could reverberate across the whole system, also considering the complex web of interactions across smart contracts and protocols. It is also unclear whether and how DeFi protocols may be shut down in the event that they raise risks or behave in unexpected ways.

Decentralised exchanges address pain points…

Crypto 'exchanges' are instrumental to crypto markets as they bring together potential buyers and sellers, facilitate price discovery and support market liquidity. Crypto exchanges fall in two categories, namely **centralised exchanges (CEXs) and DEXs.** Public sources list more than 650 crypto exchanges globally, including more than 400 that would qualify as DEXs and a sizeable number that appear accessible to EU investors. [12] However, more than 80% of the reported spot trading volumes is attributable to the 10 largest exchanges, all being CEXs except one (Chart 3). Over the past year, Binance alone – the largest CEX – has represented a share of the spot trading volumes in crypto-assets ranging from 40% (June 2022) to 60% (February 2023), although its dominance is now receding.

Chart 3
Top crypto exchanges by market share
Binance's dominant position receding



Note: The graph shows the monthly relative trading volumes (in %) of the 10 largest exchanges (and of all others as an aggregate) between January 2021 and June 2023. The collapse of FTX explains its disappearence after November 2022. Of note, the above data is reported by the exchanges themselves and should therefore be considered with caution. Except for Uniswap, and disregarding the 'Other' category, all the exchanges featuring in the chart are centralised.
Source: Kaiko, ESMA

CEXs, as their name suggest, involve a central authority or operator, and function in a way that is comparable to traditional exchanges and fall beyond the scope of this article. [13] Unlike CEXs, **DEXs rely on smart contracts** for peer-to-peer trading (DEXs are one application of DeFi) and allow for **non-custodial** trading, meaning that they do not require users to entrust them with the control of their assets for trading. Because DEXs do not hold client assets, DEXs should mitigate the risk of theft via exchange hacking (that does not mean though that DeFi protocols, including DEXs, are immune to exploits as discussed above). They also reduce counterparty risk vis-à-vis the exchange operator and the risk of clients' asset misappropriation, as was the case with FTX, since the custody and exchange logic of the assets is processed and guaranteed by smart contracts.

[11] Several prominent crypto exchanges, e.g. Binance, BitForex, BitMEX or Bybit offer up to 100x or more leverage.

[12] Coinmarketcap.com

[13] One difference being that the listed assets are not necessarily denominated in fiat money such as the euro but maybe denominated in another crypto-asset, typically a stablecoin, e.g. Tether USD or USD Coin, hence the notion of 'trading pairs'. In the case of DEXs, because they do not support fiat money, the trading pairs are all 'crypto-to-crypto'.

On the downside, though, DEXs come with an inherent weakness; the fact that on-chain, smart-contract-enabled trades are slow. DEXs are still relatively new but have grown in popularity lately. In this regard, it should be noted that the collapse of FTX in November 2022 led to an increased awareness of potential conflicts of interests within CEXs. This, coupled with the regulatory uncertainty that characterises CEXs' operating environment, led to a slight decrease in CEXs' spot trading volume in the months following FTX's collapse, while that of DEXs' remained relatively stable.[14] Other motives driving DEXs growth include for users the absence of 'know your customer' checks and for issuers the absence of listing requirements for their crypto-assets, both things now commonly found at established CEXs. Uniswap, the largest DEX, processes daily spot trading volumes that rival those of large CEXs like OkEX or Kraken.

DEXs come mainly in two forms, namely, **'order book exchanges' and 'automated market makers'** (AMMs). Order book exchanges typically include both on-chain and off-chain components, where order books are maintained by centralised operators and the blockchain primarily serves as a settlement layer. The centralised entity helps connect buyers and sellers and can restrict access to the order book (to view and/or submit orders).[15] AMMs are more novel but now dominate (Table 3).

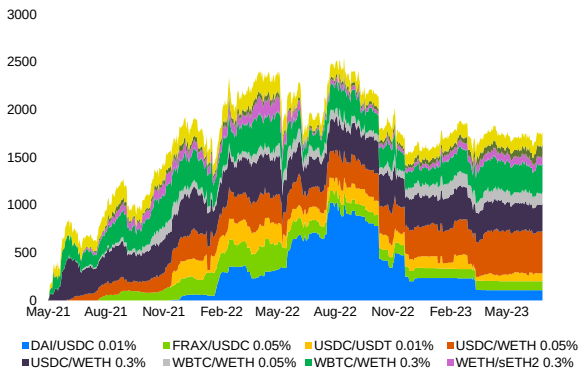
To get a sense of those crypto-assets that are the most liquid on DEXs, we looked at the largest liquidity pools available on Uniswap V3[16] (Chart 4). Unsurprisingly, stablecoins, such as Dai, USD Coin and Tether USDt, because of their key role in DeFi, are present in the largest pools, together with Ether. Bitcoin, considering its dominant market share in crypto-assets markets, is comparatively less prominent.

Table 3
Top 10 DEXs
Large DEXs are AMMs

DEX	Type	No. of crypto-assets	No. of trading pairs	Monthly volume (USD bn)
Uniswap	AMM	885	1744	34.24
dYdX(*)	Order	N/A	38	27.79
PancakeSwap	AMM	2326	3340	8.7
Curve	AMM	74	100	4.77
Maker PSM	AMM	N/A	NA	3.76
Dodo	AMM	7	121	3.05
Balancer V2	AMM	80	121	2.16
Raydium	AMM	255	578	0.68
Orca	AMM	88	207	0.413
Sushiswap	AMM	347	484	0.243

Note: 10 largest DEXs by volume traded in June 2023, along with their key features (i.e. order- or AMM-based type, number of crypto-assets traded, number of available trading pairs, and monthly traded volume (in USD bn) for June 2023). (*) For dYdX, available data show large variations in the reported figures across sources, suggesting limited reliability.
Source: Coingecko, CoinMarketCap, TheBlock, ESMA

Chart 4
Uniswap V3 TVL per top liquidity pool
Ether and stablecoins most widely traded



Note: TVL (in USD mn) for each of the top ten liquidity pools on Uniswap V3 as of June 2023, from May 2021 (when the Uniswap V3 protocol was first introduced) to June 2023.
Sources: Uniswap, ESMA

[14] For further insight regarding the trading volumes of CEXs vis-à-vis that of DEXs, see Murphy O Kane and Weert (2023) and the Chart 'DEX to CEX Spot Trade Volume (%)' at https://www.theblock.co/data/decentralized-finance/dex-non-custodial

[15] Daian et al. for example, highlights that EtherDelta used a design whereby the traders themselves performed order matching as follows: a trader selected an order in the order book and presented it to the smart contract with a signed counterorder. The smart contract executed the order and counterorder, clearing the order from the order book. In other designs, used by IDex and others, the exchange itself matches the orders off chain and submits order/counterorder pairs to the smart contract for processing.

[16] Uniswap has developed several decentralised exchanges protocols through time, known as Uniswap V1, V2 and V3. Uniswap V3 now concentrate most of Uniswap's trading activities, although Uniswap V1 and V2 continue to exist. A fourth version, Uniswap V4, is expected shortly. For further details on Uniswap V3 see Uniswap v3 Core.

Unlike order-book-based DEXs, AMMs can exist entirely on-chain. Instead of matching buy and sell orders, AMMs implement liquidity pools and determine price algorithmically through a hard-coded '**conservation function',** also known as the 'bonding curve'.

AMMs work as follows. Liquidity providers contribute (i.e. deposit) two crypto-assets (or more) (crypto-asset A and B) in the liquidity pool and receive a share in the liquidity pool in return (see Chart 9a in the appendix, token A and B stand for crypto-asset A and B respectively). Traders willing to trade (i.e. swap) crypto-asset A for B submit an order to the pool, specifying the input (A) and output (B) asset and one associated quantity x_a. The smart contract automatically calculates the swap rate between crypto-asset A and B based on the conservation function and executes the order accordingly. As the ratio of crypto-asset A to crypto-asset B increases, the liquidity pool price of crypto-asset A relative to crypto-asset B decreases (see Chart 9b in the appendix). At the same time, arbitrage traders should prevent the liquidity pool price from deviating significantly from the average market price. AMMs use different conservation functions, the most common being the constant product function.

… but create new forms of welfare losses

With AMMs, users obtain immediate liquidity without having to find an exchange counterparty and liquidity providers can earn a return on the assets that they deposit in the pool. Yet, AMMs expose users to 'slippage' and liquidity providers to 'impermanent loss'.

Slippage measures the deviation between the effective swap rate (between crypto-asset A and crypto-asset B) and the pre-swap spot exchange rate (between crypto-asset A and crypto-asset B). It is effectively akin to market impact in traditional markets, which is generally understood as the change in the price of an asset caused by the trading of that asset. While every trade encounters slippage, the slippage value depends on the trade size relative to the pool size (the smaller the trade relative to the pool, the smaller the slippage) and the exact design of the conservation function. With a view to preventing excessive slippage and to concentrating and hence enhancing liquidity, some protocols provide for pre-set slippage tolerance levels. However, this feature can be exploited for front-running purposes (see the paragraph on front-running).

Impermanent loss, also known as 'divergence loss', corresponds to the loss in value of the reserves in the pool compared to holding the reserves outside of the pool.[17] In short, liquidity providers bear an impermanent loss if they would have been better off keeping their crypto-assets in their wallet instead of depositing them in a liquidity pool. Impermanent loss is effectively the result of traders being able to arbitrage the pair in the liquidity pool at their advantage until the liquidity provider withdraws its crypto-assets from the pool.

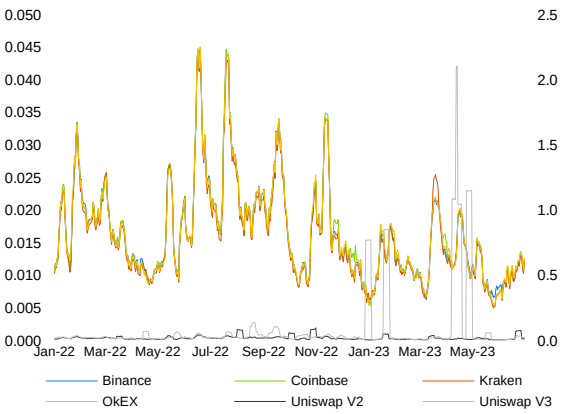
While impermanent loss is not illegal, liquidity providers may not understand the opportunity costs involved. Examining liquidity pools representing 43% of Uniswap V3's TVL in 2021, Loesch et al (2021) found that a majority of liquidity providers would have been better off holding their crypto-assets in their wallet. In certain pools, the percentage of users who lost more from impermanent loss than they gained in trading fees was as high as 70-75%. The only group that consistently made money when compared to holding their crypto-assets was flash liquidity providers who provided liquidity during one block.

Measuring efficiency in crypto-assets markets is a challenge because of important data gaps and the technicalities involved. Looking at the volatility of Bitcoin and Ether prices, available data point to a higher volatility on Uniswap compared to large CEXs, thereby suggesting lower liquidity on the exchange (Chart 5 and 6).

[17] Some consider the term 'divergence loss' more accurate as for the majority of AMM protocols, this 'loss' only disappears when the current proportions of the pool assets equal exactly those at liquidity provision (there is no divergence between the two), which is rarely the case.

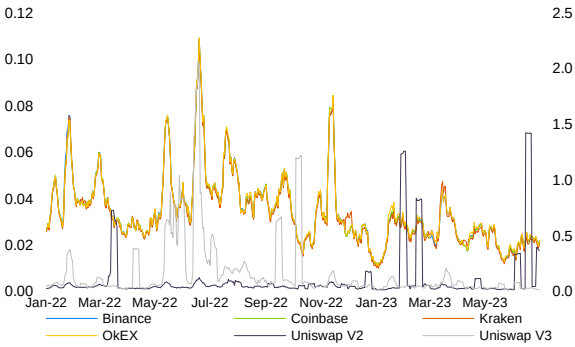
Yet, other data published by Uniswap suggest a higher market depth on the exchange (Chart 7).

Chart 5
ETH/BTC price volatility per exchange
Higher volatility on Uniswap versus CEXs



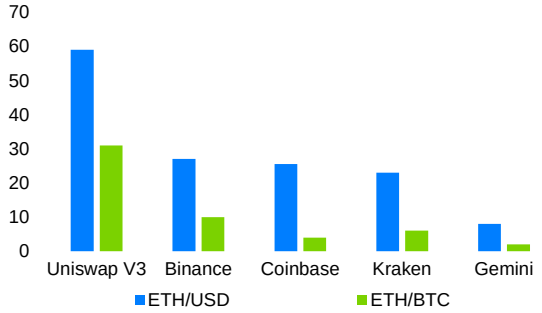
Note: Primary y-axis: 7-day average Parkinson volatility[18] for ETH/BTC on Binance, Coinbase, Kraken, and OkEX. Secondary y-axis: 7-day average Parkinson volatility for WETH/WBTC on Uniswap V2 and Uniswap V3 (January 2022 - June 2023). It is worth noting that ETH/BTC volatility is fairly similar across Binance, Coinbase, Kraken, and OkEX through time. However, it is signficantly higher on Uniswap V2 and V3, using WETH/WBTC as a proxy, with notable spikes especially on Uniswap V3.
Sources: Kaiko, ESMA

Chart 6
ETH/USD price volatility per exchange
Higher volatility on Uniswap versus CEXs



Note: Primary y-axis: 7-day average Parkinson volatility for ETH/USD on Binance, Coinbase, Kraken, and OkEX. Secondary y-axis: 7-day average Parkinson volatility for WETH/USDT on Uniswap V2 and Uniswap V3 (January 2022 - June 2023). It is worth noting that ETH/USD volatility is fairly similar across Binance, Coinbase, Kraken, and OkEX through time. However, it is signficantly higher on Uniswap V2 and V3, using WETH/WBTC as a proxy, with notable spikes.
Sources: Kaiko, ESMA

Chart 7
Market depth for ETH/BTC and ETH/USD
Indications of deeper market on Uniswap



Note: Average estimated market depth (in USD mn) for ETH/USD and for ETH/BTC within a -/+2% price change for the sample period from 1 June 2021 to 1 March 2022 as disclosed by Uniswap. While the chart suggests a superior market depth for both pairs for the only DEX featuring in it, namely Uniswap, compared to large CEXs, it is not necessarily reflective of the exact conditions of the trades (e.g. because of the implied costs).
Sources: Uniswap, ESMA

Relatedly, Hansson (2022) finds that most arbitrage profits are made immediately after the occurrence of price anomalies, indicating that decentralised markets adjust fast after a shock to the no-arbitrage price. Wang et al (2022) conducted a systematic investigation on cyclic arbitrages in DEXs using transaction-level data of Uniswap V2. They found that traders exploited more than USD 138mn in revenue from cyclic arbitrages over 11 months. However, they also found sizeable arbitrage opportunities were left unexploited, suggesting that DEX markets may not be efficient enough. The high volatility of Ether can also weigh on transaction costs, especially for smaller investors, and in turn affect liquidity conditions on DEXs, although causality is hard to infer (Organisation for Economic Co-operation and Development (OECD) 2022).

Market manipulation and the special case of DEXs

The highly volatile and speculative nature of many crypto-assets and the lack of clear

[18] Parkinson volatility is a metric which combines the high and low prices over a given period. For its calculation, the authors direct the interested reader to https://breakingdownfinance.com/finance-topics/risk-management/parkinson-volatility

regulatory frameworks globally provide a fertile ground for market manipulation. This market manipulation takes a variety of forms, some being well known from traditional markets and others more novel, sometimes originating from the inherent features of the underlying technology.

Wash trading can exist in traditional markets (and is considered unlawful) but in the case of crypto-assets is facilitated by the **pseudonymity** attached to blockchains. [19] Many crypto exchanges also inflate their traded volumes on purpose to attract new users and crypto-asset issuers. To perform wash trading, several users can collude and trade only amongst themselves, thereby misleading others into thinking that they are buying and selling, while they keep the same positions or do not take any market risk.

When it comes to DEXs, all transactions are publicised on chain, which provides some transparency. However, the identity of the owners of the accounts from and to which the transactions are made remains unknown. Several users can therefore collude, without the others knowing. A single user can also operate multiple accounts, something that is made particularly easy by the fact that **account creation is virtually cost-free** and does not require identity information on Ethereum for example.

While prominent crypto exchanges currently report strict anti-wash trading measures, Cong et al (2019) identified **wash trading on most unregulated crypto exchanges** representing as much as 77.5% of the total trading volume on average. These estimates translated into wash trading of over USD 4.5tn in spot markets and over USD 1.5tn in derivatives markets in the first quarter of 2020 alone.

Examining two of the first popular limit **order book-based DEXs** on Ethereum, namely IDEX and (now defunct) EtherDelta, Victor and Weintraub (2021) identified wash trading activities in excess of USD 159mn between September 2017 and April 2020 and common wash trading structures, which consisted mainly of one or two accounts. Surprisingly, because it would seem easy to prevent, self-trades occurred frequently. More than 30% of all crypto-assets on both exchanges had been subject to wash trading activity, and 10% of the tokens on EtherDelta had been almost exclusively wash traded over the period under review. While this study was limited to order-book based DEXs, similar issues can be expected with AMMs even if traders do not trade against each other but rather a pool.

Pump and dump schemes in crypto-assets markets are mainly achieved and organised through groups organised via **social media and platforms** like Twitter, Reddit, or Telegram, which target less sophisticated investors (Eigelshoven, Ullrich and Parry, 2021). One blockchain analytics firm reported thousands of online chat rooms in the deep and dark web as well as public chat channels on Telegram dedicated to pump and dump schemes, some with as many as four million subscribers in a single room. [20] Researchers at the Centre for Economic Policy Research identified a total of 4,818 different pump signals advertised on Telegram and Discord during a six-month period in 2018 that promoted more than 300 crypto-assets, suggesting that this phenomenon is widespread and often quite profitable (Hamrick et al., 2019).

These schemes tend to be conducted on **less sizeable crypto-assets** as a smaller group of traders can have an impact on their price. The scammers also recruit credulous participants on Twitter to help them pump the coins and use bots to amplify the phenomenon. Again, research on pump and dump schemes specific to DEXs is lacking at this point but the authors of this study expect that DEXs' growing popularity will create incentives for such schemes. Beyond outright pump and dump schemes, a recent example of the influence and reach of social media on crypto-assets markets was the temporary change of the Twitter logo for the Dogecoin symbol, which led to a massive surge in the coin price and trading volumes. [21]

[19] In the EU, Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 sets a comprehensive framework to preserve (traditional) market integrity.

[20] TRM, "Illicit Crypto Ecosystem Report: A Comprehensive Guide to Illicit Finance Risks in Crypto," (June 2023), available at https://www.trmlabs.com/illicit-crypto-ecosystem-report-2023#:~:text=TRM%20Labs%20data%20indicates%20that%20cryptocurrency%20wallets%20that%20receive%20victim,large%20transnational%20organized%20crime%20groups

[21] On 3 April 2023, Twitter temporarily changed the blue bird logo on its homepage and the loading screen to a cut-out image of the Dogecoin symbol. The market responded enthusiastically to the company's unexpected endorsement which investors perceived as a positive signal for the coin's

Front-running (and extensions of it, namely 'back-running' and 'sandwich-attacks'[22]) risk is exacerbated with DEXs because of the publicity of transactions and the computational steps needed to confirm a transaction. To compensate and incentivise the blockchain network's validators, each transaction entails a fee, which is levied regardless of the transaction success or failure. In Ethereum, gas fees (or simply 'gas') refers to the transaction processing fees charged by the Ethereum network. Every participant who monitors the mempool[23] can potentially front run unconfirmed transactions by sending an adaptative transaction with a higher amount of gas. This phenomenon is commonly known as **miner or maximal extractable value** (MEV)[24], i.e. the value that miners (or validators on Ethereum) can extract through ordering manipulation.

Daian et al (2020) report a **sizeable economy of arbitrage bots** profiting from opportunities provided by transaction ordering in DEXs. They further argue that MEV threatens blockchain's consensus layer security by incentivising attacks against the network. Auer et al. (2022) report that total MEV amounted to an estimated USD 550–650mn on just the largest Ethereum-based protocols between 2020 and 2022. Another study calculates the losses due to frontrunning attacks between May 2020 and April 2021 to have amounted to more than USD 100mn (Capponi et al, 2022). Park (2023) shows that all convex liquidity invariance pricing functions (of which the constant product rule is a special case) allow profitable sandwich attacks. Ideas to prevent some forms of front-running – such as keeping transactions encrypted while they are ordered or slippage or price impact limits – are being developed but do not fully resolve those issues and their implementation is not trivial.

More novel market manipulation techniques spawned from DeFi's innovative features include the use of **flash loans** for pump and dump attacks and the **manipulation of oracles**. While flash loans may serve legitimate purposes, e.g. profiting from arbitrage opportunities arising from individual price discrepancies across exchanges, they have been extensively used by attackers to exploit DeFi protocols. What makes flash loans particularly popular among attackers is the fact that they are virtually cost free, and difficult to track down, because of blockchain's pseudonymity and permissionless nature. Thanks to blockchain's atomicity[25], flash loans allow users to borrow crypto-assets with no collateral requirements, no credit checks, and no borrowing limit (other than the amount effectively made available for borrowing by depositors/liquidity providers). In a nutshell, attackers use flash loans to borrow large amounts of crypto-assets, which they can in turn use to shift demand and supply in the market (less liquid crypto-assets being natural victims) and/or manipulate oracles to their advantage. Examples of market manipulation through flash loans include Mango Markets (Box 2), Cream in October 2021 (USD 130mn loss), and Pancake Bunny in May 2021 (USD 3mn loss). [26],[27]

future. The price of Dogecoin increased by more than 30% within one hour and saw a surge in trading volume. For further details, see ESMA (2023).

[22] Back-running is similar to front-running except that the participant seeks to have their transaction executed immediately after a pending transaction A sandwich attack refers to a situation where an order is placed just before the victim transaction and another right after.

[23] The mempool refers to the pool of transactions sitting in memory waiting to be included in a block. It consists of transactions that are awaiting processing by the blockchain's miners or validators.

[24] MEV emerges on the blockchain in a few ways, including through DEX arbitrage, liquidations or sandwich trading. For further details, see Maximal extractable value (MEV) | ethereum.org

[25] Ibid 7

[26] C.R.E.A.M. Finance Post Mortem: Flash Loan Exploit Oct 27 | by C.R.E.A.M. | C.R.E.A.M. Finance | Medium

[27] Coinmarketcap, 2021. What Are Flash Loan Attacks? | CoinMarketCap

Box 2

Mango Markets

On 12 October 2022, Mango Markets reported an attack via an oracle price manipulation. It later appeared that the attack was performed by Avraham Eisenberg. According to the US Securities and Exchange Commission complaint, Eisenberg used two accounts to take both long and short perpetual futures positions on MNGO tokens (for around 488 million MNGO tokens, out of a total of 500 million in circulation). He subsequently performed a series of large purchases of low traded MNGO tokens at gradually higher prices. These operations artificially increased both the price of a MNGO token (to 0.91 from 0.03 when this all started) and the value of Eisenberg's long MNGO perpetual futures position. Finally, Eisenberg used this fictitiously overvalued position as collateral to borrow (and eventually withdraw) approximately USD 116mn worth of various crypto assets from the Mango Markets platform. While Mango exploit is typically reported as a flash loan exploit, it is not possible using publicly available information to pinpoint exactly when/where the attacker used flash loans but the authors' interpretation is that he did so to buy the necessary collateral for the perpetual futures (and maybe also to manipulate the price of MNGO tokens on the spot market).This example illustrates the series of steps that attacks typically need to follow and the complexity involved in tracing back the exact source of the attack and technique used.

Conclusion

While current overall exposures remain small, DeFi creates important risks to investor protection and has the potential to create negative externalities on the traditional financial system. New forms of market abuse are also facilitated by DeFi innovative features, something that the industry will need to address for DeFi to ever reach sustainable growth.

Effectively regulating and supervising DeFi is not easy, because of the technicalities involved and also the need to determine how the current rules may apply to a system that purports to eliminate those entities to which existing rules precisely apply. In addition, the ability of regulators (and investors) to understand DeFi and the risks involved is hampered by important data gaps.

In the EU, MiCA sets a new comprehensive framework for the regulation of previously unregulated crypto-assets but does not directly address DeFi. [28] Importantly, MiCA will be thoroughly reviewed going forward with a view to making sure that its provisions remain relevant in a fast-evolving market. First, ESMA will as of 2025 report annually on crypto-asset market developments. Second, the European Commission will report on the application of the regulation. A first report – coinciding with the full entry into application – will notably assess the development of DeFi and whether it deserves additional regulatory action. A second broader review will be provided after two years, leading to a full review after four years. These reports could where appropriate be accompanied by legislative proposals. The risks and challenges identified in this article are intended to help inform MiCA's future review.

Meanwhile, ESMA will continue actively monitoring DeFi developments, as DeFi activities and arrangements continue to evolve quickly and raise particular challenges and risks. ESMA will also continue contributing to international initiatives on the topic. Both the FSB's and and the International Organization of Securities Commissions' (IOSCO) work in particular are instrumental to fostering a common understanding and convergent approach to the phenomenon (FSB 2023, IOSCO 2023).

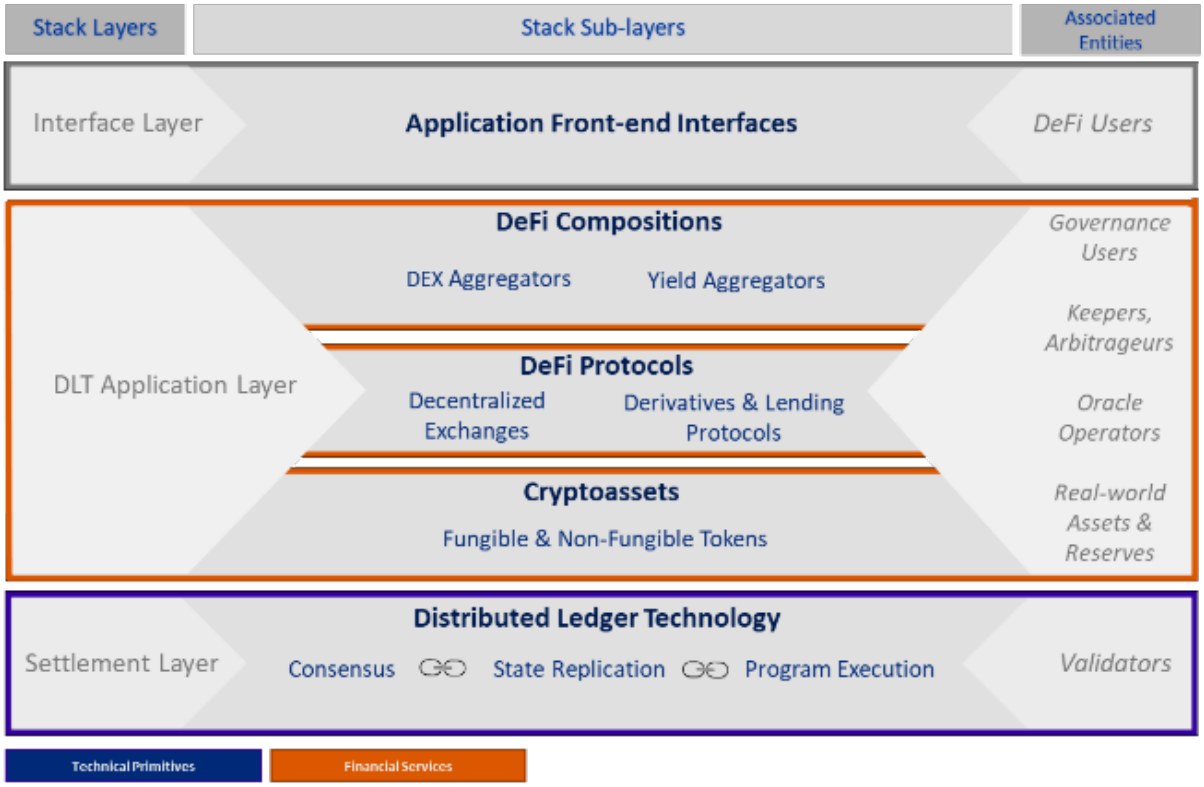
[28] Whether a given DeFi product or service may be exempted from MiCA depends on whether it meets the conditions set under Recital 22 of MiCA, which provides that '[...] Where crypto-asset services are provided in a fully decentralised manner without any intermediary, they should not fall within the scope of this Regulation'.

Appendix

Chart 8

The DeFi stack

A multi-layered architecture

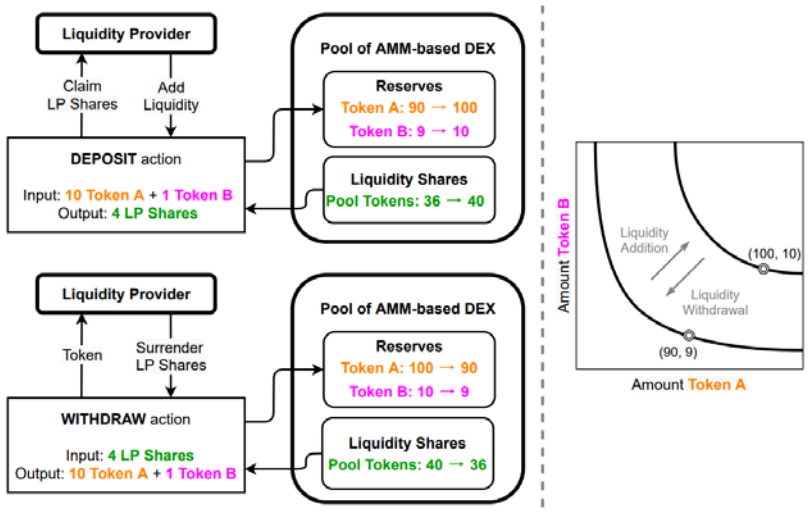


Note: Three layers, the settlement layer, the application layer and the interface layer compose the DeFi stack. Each layer is associated to off-chain entities: validators ensure that consensus is reached, fiat currencies are the reserves for many stablecoins, oracles import external/off-chain information, and keepers and arbitrageurs enforce incentive mechanisms. Protocol governance is composed of DeFi users with decision-making powers. End-users interact through interfaces with DeFi protocols.
Source:Reproduced from Schar 2021 and Auer et al. 2023

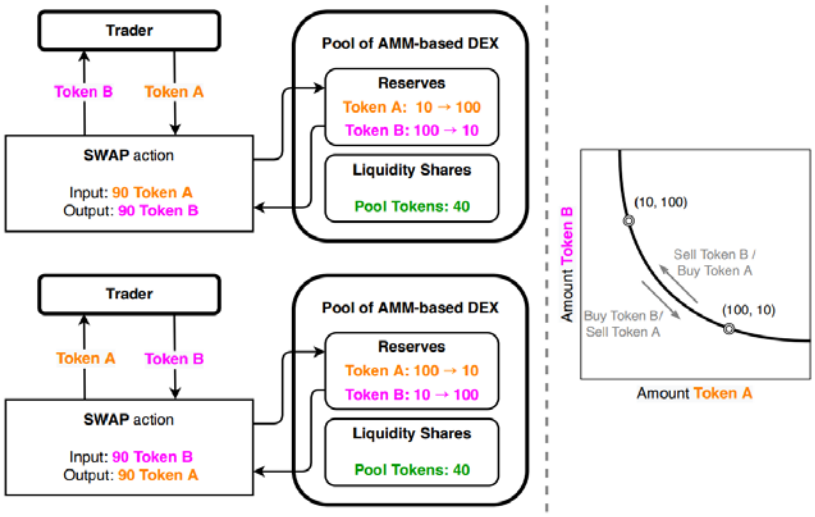
Chart 9

Stylised AMM mechanisms for liquidity providers and traders

(a) Liquidity provision and withdrawal mechanism



(b) Swap mechanism



Note: Liquidity provision or wothdrawal must respect the existing ratio between two reserve assets and has no impact on the swap price of the two assets in the pool. The way in which a given swap translates into a pool's reserve balance is defined by its conservation function. In short, when one reserve asset comes close to depletion, its price (denominated in the other reserve asset of the pool) becomes exponentially high.

Sources: Reproduced from Xu et al, 2023

Related reading

Auer, R., Frost, J. and Vidal Pastor, J. M., 2022. 'Miners as intermediaries: Extractable value and market manipulation in crypto and DeFi.', *BIS Bulletins*, No 58, Bank for International Settlements (Miners as intermediaries: extractable value and market manipulation in crypto and DeFi (repec.org)).

Auer, R., Haslhofer, B., Kitzler, S., Saggese, P. and Victor, F., 2023. 'The technology of decentralized finance (DeFi)', *BIS Working Papers*, No 1066 (The Technology of Decentralized Finance (DeFi) (bis.org)).

BIS, 2023. *The Crypto Ecosystem: Key elements and risks* (The crypto ecosystem: key elements and risks (bis.org)).

Briola, A., Vidal-Tomás, D., Wang, Y. and Aste, T., 2023. 'Anatomy of a stablecoin's failure: The Terra-Luna case', *Finance Research Letters*, Vol. 51, 103358 (Anatomy of a Stablecoin's failure: The Terra-Luna case - ScienceDirect).

Capponi, A., Ruizhe, J., and Wang, Y., 2021. *Allocative Inefficiencies in Public Distributed Ledgers* (Allocative Inefficiencies in Public Distributed Ledgers by Agostino Capponi, Ruizhe Jia, Ye Wang :: SSRN).

Chainalysis, 2023. *The 2023 Crypto Crime Report* (The Chainalysis 2023 Crypto Crime Report).

Chen, W., Zheng, Z., Ngai, E. C.-H., Zheng, P. and Zhou, Y., 2019. 'Exploiting blockchain data to detect smart ponzi schemes on Ethereum', *IEEE Access*, Vol. 7, pp. 37575–37586 (Exploiting Blockchain Data to Detect Smart Ponzi Schemes on Ethereum | IEEE Journals & Magazine | IEEE Xplore).

CoinMarketCap, 2022. 'What Are Flash Loan Attacks?' (What Are Flash Loan Attacks? | CoinMarketCap).

Cong, L. W., Li, X., Tang, K. and Yang, Y., 2019. 'Crypto wash trading', arXiv preprint ([2108.10984] Crypto Wash Trading (arxiv.org)).

Daian, P., Goldfelder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., Breidenbach, L. and Juels, A., 2020. 'Flash Boys 2.0: Frontrunning in decentralized exchanges, miner extractable value, and consensus instability', in Kellenberger, P. (ed.), *IEEE Symposium on Security and Privacy (SP)*, San Francisco, United States, pp. 910–927 (Flash Boys 2.0: Frontrunning in Decentralized Exchanges, Miner Extractable Value, and Consensus Instability | IEEE Conference Publication | IEEE Xplore).

ECB, 2023. 'ECB publishes consolidated banking data for end-December 2022' (ECB publishes consolidated banking data for end-December 2022 (europa.eu)).

FSB, 2023. *The Financial Stability Risks of Decentralised Finance* (The Financial Stability Risks of Decentralised Finance – Financial Stability Board (fsb.org)).

Eigelshoven, F., Ullrich, A. and Parry, D., 2021. 'Cryptocurrency market manipulation – A systematic literature review'. ICIS 2021 proceedings, Blockchain, DLT and Fintech track (AIS Electronic Library (AISeL) - ICIS 2021 Proceedings: Cryptocurrency Market Manipulation – A Systematic Literature Review (aisnet.org)).

ESMA, European Banking Authority and European Insurance and Occupational Pensions Authority, 2022. 'EU financial regulators warn consumers on the risks of crypto-assets' (EU financial regulators warn consumers on the risks of crypto-assets (europa.eu)).

ESMA, 2022. *Crypto-assets and their Risks for Financial Stability* (esma50-165-2251_crypto_assets_and_financial_stability.pdf (europa.eu)).

ESMA, 2023. *ESMA Report on Trends, Risks and Vulnerabilities*, No. 2, 2023 (ESMA50-1389274163-2681 TRV 2, 2023 Risk Monitor (europa.eu)).

ESRB Task Force on Crypto-Assets and Decentralised Finance, 2023. *Crypto-assets and Decentralised Finance: May 2023 – Systemic implications and policy options* (Crypto-assets and decentralised finance (europa.eu)).

Buterin, V., 2014. 'Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform', Ethereum white paper (Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform).

FSB, 2023. *The Financial Stability Risks of Decentralised Finance* (The Financial StabilityThe Financial Stability Risks of Decentralised Finance (fsb.org)).

Hamrick, JT and Rouhi, Farhang and Mukherjee, Arghya and Feder, Amir and Gandal, Neil and Moore, Tyler and Vasek, Marie, 2019. *'The Economics of Cryptocurrency Pump and Dump Schemes (December 2018)'*, CEPR Discussion Paper No. DP13404 (The Economics of Cryptocurrency Pump and Dump Schemes by JT Hamrick, Farhang Rouhi, Arghya Mukherjee, Amir Feder, Neil Gandal, Tyler Moore, Marie Vasek :: SSRN)

Hansson, M., 2022. *Arbitrage in Crypto Markets: An analysis of primary Ethereum blockchain data* (Arbitrage in Crypto Markets: An Analysis of Primary Ethereum Blockchain Data by Magnus Hansson :: SSRN).

IMF, FSB, 2023. *IMF–FSB Synthesis Paper: Policies for crypto-assets* (IMF-FSB Synthesis Paper: Policies for Crypto-Assets).

IOSCO, 2023. *Policy Recommendations for Decentralized Finance(DeFi): Consultation report,* CR/04/2023 (CR04/2023 Policy Recommendations for Decentralized Finance (DeFi) (iosco.org)).

Locke, T., 2022. 'Did a "concerted attack" cause Terra's UST to crash below $1? An exec behind the largest stablecoin and experts agree it's suspicious'. *Yahoo! News* (Did a 'concerted attack' cause Terra's UST to crash below $1? An exec behind the largest stablecoin and experts agree it's suspicious (yahoo.com)).

Loesch, S., Hindman, N., Welch, N. and Richardson, M. B., 2021. 'Impermanent loss in Uniswap v3', arXiv ([2111.09192] Impermanent Loss in Uniswap v3 (arxiv.org)).

Mones, D. and Taqi, M., 2023. 'Europe's 50 largest banks by assets, 2023'. *S&P Global* (Europe's 50 largest banks by assets, 2023 | S&P Global Market Intelligence (spglobal.com)).

OECD, 2022. 'Why decentralised finance (DeFi) matters and the policy Implications'. OECD Paris (Why Decentralised Finance (DeFi) Matters and the Policy Implications - OECD).

Murphy, O., Kane, O. and Van Wert, Y., 2023. 'Decoding the CEX landscape: An in-depth analysis of 2023 H1'. *Nansen Research Report* (https://research.nansen.ai/articles/decoding-the-cex-landscape-an-in-depth-analysis-of-2023-h1).

Panetta, F., 2023. 'Paradise lost? How crypto failed to deliver on its promises and what to do about it: Speech by Fabio Panetta, Member of the Executive Board of the ECB, at a panel on the future of crypto at the 22nd BIS Annual Conference' (Paradise lost? How crypto failed to deliver on its promises and what to do about it (europa.eu)).

Park, A., 2023. *Conceptual Flaws of Decentralized Automated Market Making* (Conceptual Flaws of Decentralized Automated Market Making by Andreas Park :: SSRN).

Qin, K., Zhou, L., Gamito, P., Jovanovic, P. and Gervais, A., 2021. 'An empirical study of DeFi liquidations: Incentives, risks, and instabilities', ACM Internet Measurement Conference (IMC '21), 2–4 November 2021, Virtual Event, United States. (An empirical study of DeFi liquidations | Proceedings of the 21st ACM Internet Measurement Conference).

Schar, F., 2021. 'Decentralized Ffnance: On blockchain- and smart contract-based financial markets', *Federal Reserve Bank of St. Louis Review*, Second Quarter 2021, Vol. 103, No 2, pp. 153–74 (Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets | St. Louis Fed (stlouisfed.org)).

TRM, 2023, *Illicit Crypto Ecosystem Report* (Illicit Crypto Ecosystem Report (trmlabs.com)).

Victor, F. and Weintraud, A. M., 2021. 'Detecting and quantifying wash trading on decentralized cryptocurrency exchanges' Proceedings of the Web Conference 2021 ([2102.07001] Detecting and Quantifying Wash Trading on Decentralized Cryptocurrency Exchanges (arxiv.org)).

Xu, J., Paruch, K., Cousaert, S. and Feng, Y., 2023. *SoK: Decentralized Exchanges (DEX) with Automated Market Maker (AMM) Protocols* ([2103.12732] SoK: Decentralized Exchanges (DEX) with Automated Market Maker (AMM) Protocols (arxiv.org)).

Wang, Y., Chen, Y., Wu, H., Zhou, L., Deng, S. and Wattenhofer, R., 2022. *Cyclic Arbitrage in Decentralized Exchanges* ([2105.02784] Cyclic Arbitrage in Decentralized Exchanges (arxiv.org)).

Publications Office
of the European Union