ESMA75-453128700-1391

EBA/Rep/2025/01

16/01/2025

Joint Report

Recent developments in crypto-assets (Article 142 of MiCAR)

Contents

Executive Summary

1. This report sets out the outcome of the analysis undertaken by the EBA and ESMA on specific elements covered by Article 142 of MiCAR and constitutes the EBA and ESMA's contribution to the production of the EC's report to the European Parliament and Council on recent developments in crypto-assets. The analysis has been informed by extensive research on DeFi and crypto lending, borrowing and staking.

2. The report is of analytical nature and does not set out any specific policy recommendations or legislative proposals to the EC or co-legislators. In addition, it makes use of terms proposed by the industry, such as "centralised" and "DeFi protocols", which should not be interpreted as a view of the actual level of (de)centralisation for the purposes of recital 22 of MiCAR.

3. The first chapter of the report is focused on DeFi, including the engagement of EU consumers and businesses into DeFi. It finds that DeFi remains a niche phenomenon, with amounts locked in DeFi protocols representing 4% of all crypto-asset market value at the global level. It also finds that EU adoption of DeFi, while above global average, is behind other developed economies (e.g. the US, South Korea). The report sets out the different types of businesses providing access to DeFi, namely DeFi application interfaces, self-custodial wallets, and centralised platforms, and finds that the preferred method of access to DeFi depends on the activity. Lastly, the chapter delves into risks associated with DeFi (mainly ICT risks, as requested by the EC, and ML/TF risks, due to their relevance) and assesses the implications of maximal extractable value (MEV) on DeFi markets.

4. The report finds that the number of DeFi hacks and the value of stolen crypto-assets has generally evolved in correlation with the DeFi market size. While historically the majority of DeFi hacks have stemmed from on-chain vulnerabilities (mainly through the exploit of smart contract vulnerabilities), recent attacks on DeFi appear to be more successful when exploiting off-chain vulnerabilities (e.g. compromising users' private keys). The report also finds that DeFi protocols present significant risks of ML/TF, with flows on decentralised exchanges representing 10% of spot crypto trading volumes globally. This is mainly due to the current absence of adequate AML/CFT controls, which means that users can transact in practice without being identified and verified. The risk is increased due to the cross-border nature of transactions as the funds or crypto-assets from potentially illegitimate sources can be transferred via DeFi without any obligations on the protocols to perform AML/CFT checks on such funds or crypto-assets and report them to Financial Intelligence Units. The report identifies some initiatives to apply KYC in DeFi protocols. In relation to MEV, the report concludes that these activities are widespread in DeFi because of the decentralised nature of the underlying blockchain. However, mitigating the negative externalities of MEV requires further consideration of technical solutions.

5. The second chapter sets out a description of the business models present in the market for the lending, borrowing and staking of crypto-assets. For each of the three types of services, the report analyses the main types and most typical features of the business models observed in the market, regarding both centralised and decentralised forms. The report finds that crypto lending, borrowing and staking services are offered by a number of CASPs in EU jurisdictions, which in some cases also offer regulated crypto-asset services. In provision of services under assessment, the report finds that users may receive insufficient information on conditions in relevant areas such as fees, interest rates paid or yields, changes to collateral requirements, the actions the service provider may take with regard to any assets used as collateral or placed in a staking account, or rights and liabilities in case of dispute or insolvency. The chapter then sets out the existing (limited) evidence of the engagement of EU

consumers and financial institutions with those services and sets out the specific risks associated with each of them. Finally, it assesses the risks associated with crypto lending, borrowing and staking, such as excessive leverage, information asymmetries, exposure to ML/TF risks, and systemic risks arising from re-hypothecation and collateral chains, procyclicality and interconnectedness.

Abbreviations

AML/CFT: Anti-Money Laundering and Countering the Financing of Terrorism

AMLD: Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing

API: Application Programming Interface

APY: Annual Percentage Yield

ART: Asset-Referenced Token

BIS: Bank for International Settlements

CASP: Crypto-asset service provider

CDD: Customer Due Diligence

DApp: Decentralized Application

DeFi: Decentralised Finance

DEX: Decentralized Exchange

DORA: Regulation (EU) 2022/2554 on digital operational resilience for the financial sector

EBA: European Banking Authority

EC: European Commission

ECB: European Central Bank

EMT: Electronic Money Token

ESMA: European Securities and Markets Authority

FSB: Financial Stability Board

FTR: Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets

ICT: Information and Communication Technology

IOSCO: International Organisation of Securities Commissions

KYC: Know-Your-Customer

LTV: Loan-to-Value ratio

MEV: Maximal Extractable Value

MiCAR: Regulation (EU) 2023/1114 on markets in crypto-assets

ML/TF: Money Laundering and Terrorism Financing

NCA: National Competent Authority

OECD: Organisation for Economic Cooperation and Development

PoS: Proof of Stake (consensus mechanism)

PoW: Proof of Work (consensus mechanism)

RAQ: EBA Risk Assessment Questionnaire

SSM: Single Supervisory Mechanism (of the ECB)

TVL: Total Value Locked

VPN: Virtual Private Network

1. Introduction

Background

6. Article 142 of the Markets in Crypto-Assets Regulation – hereinafter ‘MiCAR‘ (Regulation (EU) 2023/1114 on markets in crypto-assets)[1] mandates the European Commission (EC) to submit, by 30 December 2024, and after consulting the European Banking Authority (EBA) and the European Securities and Markets Authority (ESMA), a report to the European Parliament and Council on recent developments in crypto-assets. On the basis of Article 142 of MiCAR, the EC is mandated to assess a) the development of decentralised finance (DeFi) in crypto-asset markets and the appropriate regulatory treatment of decentralised crypto-asset systems without an issuer or CASPs, including an assessment of the need for and feasibility of regulating DeFi; and b) the feasibility and necessity of regulating the lending and borrowing of crypto-assets.

7. In a letter dated 9 February 2024, the EC requested that EBA and ESMA provide a contribution focusing on certain elements related to DeFi and the lending and borrowing of crypto-assets, including staking, by the end of October 2024[2]. The EC subsequently agreed to a postponement of the EBA and ESMA's contribution to its report. The EC's report should therefore not be expected to be published before early / mid-2025.

8. Recital 22 of MiCAR establishes that the Regulation should only apply to natural and legal persons and certain other undertakings and to the crypto-asset services and activities performed, provided or controlled, directly or indirectly, by them, including when part of such activities or services is performed *in a decentralised manner*. Where crypto-asset services are provided in a *fully decentralised manner without any intermediary*, they should not fall within the scope of MiCAR. MiCAR, however, does not specify how to interpret references to *fully decentralised*.

9. Recital 94 of MiCAR sets out that MiCAR should not and does not address the *lending and borrowing of crypto-assets*, including e-money tokens (EMTs), and therefore should not prejudice applicable national law. MiCAR does not provide a definition of *lending and borrowing of crypto-assets*, and, generally, the regulation of such activities has not been specifically addressed or introduced in EU Member States, although some of these activities may fall under provisions in existing national financial services law. The terms have been used in very limited cases in legislative, tax or regulatory publications in Member states.[3] Where defined, their use has been of limited nature, and mainly for analytical purposes.

[1] http://data.europa.eu/eli/reg/2023/1114/oj

[2] See Annex 1 for the letter

[3] For instance, a publication by the Ministry of Finance in Austria (https://www.bmf.gv.at/themen/steuern/sparen-veranlagen/steuerliche-behandlung-von-kryptowaehrungen.html), a Discussion Paper on DeFi (https://www.amf-france.org/en/news-publications/public-consultations/amf-discussion-paper-decentralised-finance-defi) and a Q&A by the AMF in France (https://www.amf-france.org/sites/institutionnel/files/private/2023-08/QA%20DOC%202020-07%20-%20Questions-réponses%20relatives%20au%20régime%20des%20prestataires%20de%20services%20sur%20actifs%20numériques_0.pdf), and a study on crypto apps by AFM in the Netherlands (https://www.afm.nl/~/profmedia/files/rapporten/2024/verkenning-cryptodienstverleners.pdf).

10. As a result of the above, this report uses the following definitions:

- ***Decentralised Finance (DeFi)***: a system of financial applications built on blockchain networks that aims to replicate some of the functions of the traditional financial system in a seemingly open and permissionless way, eliminating traditional financial intermediaries and centralized institutions. See Section 2.1.

- ***Crypto lending***: an activity consisting of a provider (lender) transferring a certain value of crypto-assets or funds to a user (borrower) in exchange for the user placing a certain value of crypto-assets or funds as collateral and a commitment that the borrower will return to the lender a value equivalent to the transferred value of crypto-assets or funds and potential additional interests on a future date (or in the event of some other trigger event) to the lender. See Section 3.1.

- ***Crypto borrowing***: an activity consisting of a user (lender) transferring a certain value of crypto-assets or funds to another user (borrower) in exchange for a commitment that the borrower will return to the lender an equivalent value of crypto-assets or funds and potential additional interests on a future date (or in the event of some other trigger event). See Section 3.1.

- ***Crypto staking***: the process of immobilizing crypto-assets to support the operations of Proof-of-Stake (PoS) and PoS-like blockchain consensus mechanisms in exchange for the granting of validator privileges that can generate block rewards. See Section 3.1.

Methodology and data sources

11. The report was carried out on the basis of extensive desk-based research by EBA and ESMA, as well as NCAs, using academic papers, findings of international standard-setters (FSB, BIS, OECD, IOSCO), analysis of websites and marketing communications by relevant market participants and online consumer forums.

12. Moreover, the EBA and ESMA used to all the extent possible the evidence gathered during 2024 via different methods, such as surveys or risk assessment dashboards and questionnaires to banks carried out in the 2022-2024 period by either EBA[4], ESMA[5] or the ECB (SSM)[6], and two joint EBA-ESMA surveys to NCAs throughout 2024[7]. The aim of the surveys was to collect information (mainly regarding on the relevance of the activities covered in this report at national level) and gather views of NCAs on risks, potential risk mitigation measures and on the scope of existing regulatory framework, including national law.

13. The EBA and ESMA also held diverse interactions with relevant stakeholders, including workshops, bilateral meetings and participation in discussions with market participants.

Limitations

14. The findings of this report rely on data sources and evidence, which to a large extent, face technical limitations and should therefore be considered with caution.

[4] See EBA Risk Dashboards in https://www.eba.europa.eu/risk-and-data-analysis/risk-analysis/risk-monitoring/risk-dashboard.

[5] See ESMA Risk Dashboards in: https://www.esma.europa.eu/esmas-activities/risk-analysis/risk-monitoring#RiskDashboard

[6] For instance, the ECB survey in summer 2022 on digital transformation and fintech covered all credit institutions directly supervised by the ECB: https://www.bankingsupervision.europa.eu/ecb/pub/pdf/Takeaways_horizontal_assessment~de65261ad0.en.pdf

[7] A survey on crypto lending, borrowing and staking, with 37 NCAs from 25 EU Member States, 2 EEA country and the ECB/SSM participating; and a survey on DeFi, with 30 NCAs, representing 21 EU Member States, 1 EEA country and the ECB/SSM participating.

15. Regarding the total value locked (TVL)[8] metrics that were used to measure the size of DeFi markets, the report faced technical limitations, as already captured by the BIS[9] and the FSB[10]. Scoping EU DeFi activities and the engagement of consumers and businesses with DeFi was technically difficult for several reasons. On-chain transactions are publicly visible, but many of these protocols remain anonymous or pseudonymous. DeFi protocols are inherently global and can be accessed virtually from anywhere in the world. Users can employ Virtual Private Networks (VPNs) and other tools to mask their IP addresses and locations, hindering efforts to track DeFi activity geographically[11]. Against this background, in order to gain insights into the size of DeFi markets in the EU, EBA and ESMA have relied on available anecdotal evidence, such as surveys and news articles, and on a set of proxies, such as downloads of crypto apps, Google Trends data or crypto/DeFi adoption indices (discussed in more detail in Annex 2).

16. This approach, which also affects the research on crypto lending, borrowing and staking, also bears limitations - e.g., inconsistent data, unclear methodologies followed by data sources and difficulty in differentiating DeFi-specific activities from broader crypto markets.

17. Regarding the engagement of EU consumers and businesses in centralised crypto lending, borrowing and staking, desk-based research provides limited information. Absent reporting obligations on providers, there are limited indications of their size and the number of market participants. Furthermore, information provided by NCAs was mainly based on market observations, rather than direct oversight/supervision, with NCAs not having concrete statistics on activities in their jurisdictions, except for registrations for the purpose of AML/CFT supervision.

Next steps

18. The EC is expected to consider the EBA and ESMA's analysis and findings in the production of its report to the European Parliament and Council on recent developments in crypto-assets under Article 142 of MiCAR.

19. The EBA and ESMA plan to continue monitoring the relevance of the activities covered in this report, mainly via conduct of desk-based research, collection of information via regular innovation monitoring exercises and analysis of available data

[8] Total Value Locked (TVL) measures the sum of the value of all assets deposited (i.e., 'locked') in a DeFi protocol.

[9] See https://www.bis.org/publ/bisbull66.pdf (page 2)

[10] See https://www.fsb.org/uploads/P160223.pdf (page 22)

[11] Even those responsible for operating DeFi protocols encounter difficulties when attributing location metadata to their users. They may be able to track the IP addresses of those users interacting with their own web interfaces or wallet apps but this doesn't capture volumes originating from third-party wallet plugins or API-based access (e.g., from a liquidity aggregator). As an example, for one large DeFi protocol, the volumes associated with their own interfaces represented only 15-20% of total volumes on the app.

2. Decentralised Finance (DeFi)

2.1 Analysis of the engagement of EU consumers and businesses with DeFi

20. This section begins with an overview of the DeFi market and the main DeFi protocols globally. It then assesses the development of DeFi in the EU, looking at the number of DeFi users, the most popular DeFi protocols and decentralised applications (DApps), and several proxies to gauge the engagement of EU consumers and businesses, such as the volume of euro-denominated transactions in the total of fiat-to-crypto transactions. The analysis reveals that scoping DeFi activities in the EU is challenging for several reasons, including the pseudonymity inherent to blockchains and the global nature of the phenomenon.

21. In sum, this section finds that DeFi remains a niche phenomenon worldwide and in the EU, with the equivalent of 4% of the total crypto-asset market capitalisation locked in DeFi protocols, and DeFi activities being concentrated in a handful of large protocols. The current number of DeFi users in the EU is estimated at 7.2 million but a fraction only (less than 15%) seems to engage in DeFi activities regularly, and the main use cases of DeFi appear to be staking, lending and borrowing and exchanging. Euro-denominated stablecoins remain negligible in size in DeFi markets, and evidence points to a very limited exposure of EU financial institutions' to DeFi.

2.1.1 An overview of DeFi markets

22. So-called decentralised finance (DeFi) commonly refers to a system of financial applications built on blockchain networks.[12] DeFi aims to replicate some of the functions of the traditional financial system in a seemingly open and permissionless way, eliminating traditional financial intermediaries and centralized institutions. The DeFi ecosystem has a multi-layered architecture that includes permissionless blockchains, self-executing code (or so-called smart contracts), protocols[13] and decentralised applications, known as 'DApps'.[14] For further details on DeFi's technological infrastructure and decentralised features, see ESMA (2023).

23. The most widely used indicator to measure the size of DeFi markets, despite its limitations, is total value locked (TVL), which is the sum of the value of all assets deposited (i.e., 'locked') in a DeFi protocol.[15] As of September 2024, TVL *adjusted* for double-counting stood at around EUR 78 billion, equivalent to about 4% of the total crypto-asset market capitalisation. For a

[12] Currently, there is no generally accepted definition of DeFi, or what makes a product, service, activity, or arrangement decentralised. The EU legislation does not provide for a legal definition of the term.

[13] 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.

[14] A dApp is a computer program whose back-end runs on the blockchain.

[15] 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 and therefore counted twice in TVL. TVL also fluctuates with market prices, e.g., a rise in TVL is not necessarily attributable to users depositing assets but may reflect an increase in assets valuation levels. In addition, TVL does not measure user activity, also bearing in mind that certain protocols, e.g., DEXs, require less assets than others to operate.

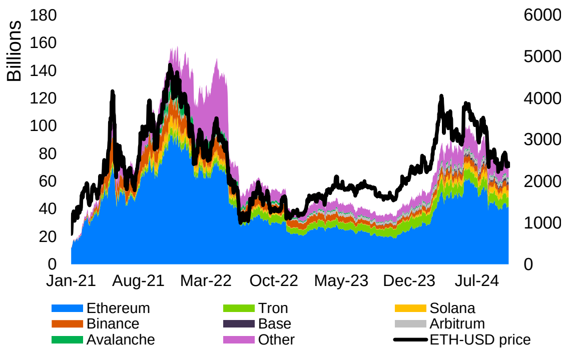
sense of the scale of composability in DeFi markets, TVL *including* double-counting stood at EUR 160 billion.[16] The rest of this section discusses adjusted TVL unless stated otherwise.

24. The first DeFi protocols were launched in 2016 but the phenomenon only started to gain traction from mid-2020. By 2021, the DeFi market experienced exponential growth, with TVL increasing to an all-time high of EUR 158 billion in December 2021 (Chart 1). This surge coincided with the boom of crypto-asset markets and ended abruptly at the beginning of 2022 with the global economic slowdown, rising interest rates and the subsequent collapse of Terra-Luna in May 2022.[17]

25. After a period of stagnation, TVL began to rise again from early 2024 to reach a new high of EUR 99 billion in May 2024, after which it started receding. Once again, this growth was concomitant with a strong rally in the broader crypto market.

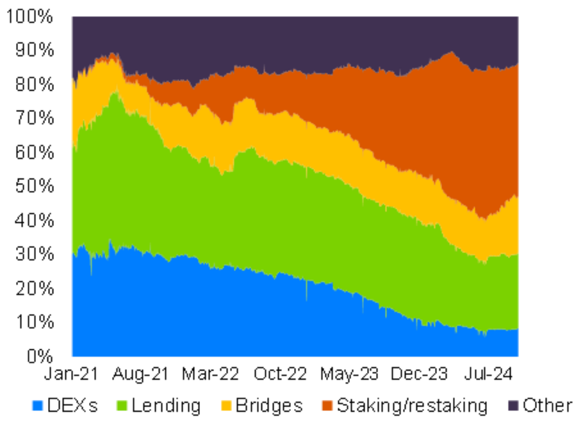
26. A majority of DeFi protocols (representing almost 60% market size by TVL) are deployed on the Ethereum blockchain (Chart 1), which contributes to the high correlation between the price of the blockchain's native asset, Ether (ETH), and TVL. This correlation is a result of a self-reinforcing mechanism by which an increase in ETH price typically boosts investor interest in DeFi and vice versa, also because a large portion of assets deposited in DeFi protocols are ETH or wrapped ETH.

Chart 1. TVL by chain



Note: TVL by chain (left-hand axis) (EUR billions) vs. ETH-EU price (right-hand axis) (Jan 2021 - Sept 2024)
Sources: DefiLlama, Kaiko, ESMA

Chart 2. TVL breakdown by protocol type



Note: TVL by type of protocol (relative)
Sources: DefiLlama, Kaiko, ESMA

27. As of September 2024, staking protocols were the largest by type of activity, representing 39% of the total TVL[18], which is almost double that of the next largest type: lending protocols (22%) (Chart 2).[19] The relative share of staking protocols has boomed from virtually nothing in January 2021 to 39% in September 2024. On the contrary, other segments in DeFi, such as decentralised exchange protocols (so-called DEXs), have seen their relative size shrink from 31% to 8%. The relative size of lending protocols in DeFi has remained fairly stable over the analysed period.

[16] Sources: DeFiLlama for TVL data; Coinmarket.com for crypto-asset market capitalisation data.

[17] For further details on Terra/Luna collapse, see ESMA, 2023. 'ESMA TRV Risk Analysis, Decentralised Finance in the EU: developments and risks', Oct. 2023.

[18] TVL including double-counting, as the available sources do not provide a breakdown of adjusted TVL by protocol type

[19] Please note that in contrast to Chart 1, which considers the adjusted TVL, namely the TVL corrected for double-counting, Chart 2 considers the non-adjustable TVL. The two charts are therefore not directly comparable. The non-adjusted TVL totalled EUR 160 bn as of end-September 2024, to be compared with EUR 78 bn for the adjusted TVL.

28. The increased relevance of staking in DeFi can be attributed to a series of events, including Ethereum's transition from a Proof of Work (PoW) to a PoS consensus mechanism in September 2022, more attractive yields, and, more recently, the growth of so-called liquid staking protocols. This phenomenon is discussed in more detail in section 3.1.

29. DEXs have seen their TVL remain fairly stable (between EUR 8 bn and EUR 15 bn since late 2022); this represents a declining relative share taking account of the growth of the overall DeFi market during that period. Innovations in the design of the DEXs have seemingly contributed to a reduction in the liquidity needed (and hence TVL) for DEXs to operate efficiently, suggesting that the stable TVL should not be interpreted as a lack of interest from users. For example, four out of the five most popular dApps are currently DEXs.[20]

30. Figures on the number of available DeFi protocols vary widely across sources, from 2,750[21] to as many as 17,000.[22] However, most of the protocols are very small in size or inactive. As of September 2024, the largest three DeFi protocols by TVL, namely Lido, Aave, and EigenLayer, had a combined TVL of EUR 46 billion, comprising 29% of the total TVL (Table 1).[23] Liquid staking and restaking protocols are among the largest, which is consistent with the recent boom in growth.

Table 1. Largest protocols by TVL as of September 2024

Protocol	TVL	Native token	Market cap	Type
Lido	23.3	LDO	0.9	Staking
Aave	12.1	AAVE	2.1	Lending
EigenLayer	10.6	EIGEN	0.7	Restaking
Ether.fi	5.8	ETHFI	0.3	Staking
JustLend	4.9	JST	0.29	Lending
Uniswap	4.6	UNI	5.8	DEX
Maker DAO	3.8	MKR	1.2	Lending / Stablecoin
Binance staked ETH	3.4	(WBETH)	N/A	Liquid Staking
Rocket Pool	3.0	RPL	0.2	Liquid Staking
Ethena	2.5	ENA	0.7	Basis Trading

Note: 10 largest DeFi protocols by TVL (EUR billions, corresponding to the sum of the different versions of the protocols across chains), native token, native token market cap (EUR billions), and type, as of end-September 2024. .
Source: DefiLlama, ESMA

31. Looking at DEXs protocols more specifically, Uniswap dominates by far, accounting for 40%-60% of the spot volume traded on DEXs since January 2021. DEXs currently account for around 10% of the spot volume traded of crypto-assets globally (with the remainder represented by centralised exchanges), in comparison with around 3% back in January 2021. The monthly volume traded on DEXs reached an all-time high of EUR 258 billion in November 2021 and peaked again at EUR 168 billion in March 2024, when crypto-assets prices surged.[24] For further details on DEXs and their functioning, see ESMA (2023).

[20] Source DappRadar.com, as measured by the number of unique active wallets interacting or performing a transaction with a DApp's smart contracts.

[21] https://blockchain-observatory.ec.europa.eu/document/download/205c457d-3e2e-4fe5-b3bc-4ef06c5b5396_en?filename=DeFi%20Report%20EUBOF%20-%20Final_0.pdf

[22] https://cointelegraph.com/news/simplifying-defi-how-an-intent-os-eases-on-chain-portfolio-management

[23] TVL including double counting as of end-September 2024.

[24] https://defillama.com/dexs

2.1.2 DeFi markets in the EU

32. Scoping DeFi activities in the EU and the engagement of EU consumers and businesses with DeFi is difficult for several reasons. First, while on-chain transactions are publicly visible, they remain pseudonymous, meaning that the real-world identity of the users involved remains hidden. Second, DeFi protocols and DApps are inherently global and can be accessed virtually from anywhere in the world. Because DeFi purports to eliminate financial intermediaries and centralised institutions and because individuals use self-hosted wallets to store and move their assets, there is, in principle, no censorship on who can access DeFi activities and products, meaning no single entity is capable of providing comprehensive location data on user activities. In addition, users can employ VPNs and other privacy tools to mask their IP addresses and locations, which further complicates efforts to track DeFi activity geographically.

33. Even those responsible for operating DeFi protocols encounter difficulties when attributing location metadata to their users. Protocols can typically only trace the origins of the volumes associated with their own web interfaces or wallet apps—which doesn't capture volumes coming from third-party wallet plugins or API-based access (e.g., from a liquidity aggregator). As an example, for one large DeFi protocol, the volumes associated with their own interfaces represented only 10-15% of total volumes on the protocol. And even here, the usefulness of the data is limited because it assumes that each wallet represents a unique user.

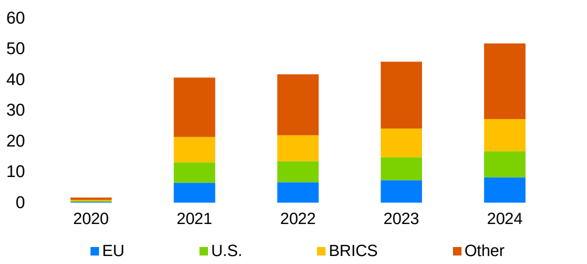
34. Against this background, in order to gain insights into the size of DeFi markets in the EU, the report relies on available anecdotal evidence, such as surveys and news articles, and on a set of proxies. While this approach bears limitations, it is considered that these proxies offer relevant insights into the size and scope of DeFi markets in the EU. The proxy indicators include: (i) crypto app downloads (including DeFi wallets), (ii) Google search trends, (iii) adoption indexes, (iv) euro-denominated transactions, and (v) time zone estimates. These proxies are discussed in more detail in Annex 2.

35. In aggregate, the evidence derived from these proxy indicators points to very low levels of DeFi activities in the EU. Overall, DeFi adoption in the EU appears higher than the world average, yet lower than that of comparable developed economies, most notably the US and South Korea.

Number of DeFi users in the EU

36. The data provider, Statista, estimates that there are 54 million DeFi users worldwide, including 7.2 million in the EU, representing 1.6% of EU citizens[25] (Chart 3). This is lower on a per-capita basis than the US with 7.5 million users (equivalent to 2.2% of the US population). These figures, derived from a variety of sources, are the only regional level data points specific to DeFi adoption that

Chart 3. Number of DeFi users globally



Note: Estimated number of DeFi users in different world regions. The figures are inferred via annual financial reports of key players, industry reports, third-party reports, publicly available databases, and survey results from primary research. BRICS include Brazil, India, Russia, and South Africa.
Sources: Statista, ESMA

[25] However, the comparison between DeFi users and EU citizens only provides limited visibility, as the assumption that one DeFi user corresponds to one EU citizen is technically limited, as explained throughout this report (see, for instance, paragraphs 32 and 33).

EBA and ESMA encountered.[26] Otherwise, a combination of surveys at the level of individual Member States provide some indicators of how large DeFi engagement could be (theoretically). The French crypto trade association, ADAN, extrapolated from a recent sample survey that 6.5 million (or 12% of the French population) held crypto-assets in 2024 (up from 9.6% in 2023), to be compared with 17% in the Netherlands and 16% in the UK[27]. With regards to DeFi, the same study implied that 21% of French population were familiar with the concept (but were not necessarily engaging in DeFi products or activities). Similarly, a consumer survey on crypto-assets carried out by the National Bank of Slovakia[28] found that 6.5% of Slovak Citizens owned crypto-assets in 2023. 16% of these crypto-asset holders had engaged in DeFi activities, but only half of them regularly.

37. Data on crypto app downloads reveals that the EU lags behind the US, UK, and South Korea in crypto app usage (see Annex 2). Data shows a trend for general-purpose crypto app downloads, with a lower than average download rate across the EU per 100,000 inhabitants compared to other developed countries. Google search trends for terms such as 'DEX' and the names of popular DeFi protocols also confirm that interest in DeFi is consistently lower among EU countries.

38. A custom-built index based on data published by the on-chain analytics provider, Chainalysis, provides a similar picture (Charts E and F, Annex 2): DeFi adoption aligns closely with general crypto adoption across countries. In the EU, countries such as France, Germany, and Italy exhibit higher levels of crypto and DeFi adoption, while Belgium, Croatia, and Ireland rank lower. Although some EU countries (e.g. France, Germany, Italy) surpass the global average in DeFi adoption, the EU trails behind the US, UK, China, and India.[29]

39. An analysis of euro-denominated transaction volumes further confirms this trend. Euro-denominated stablecoins account for a tiny share of the total volumes traded in DeFi markets, and in crypto-asset markets more generally. Of the trading in fiat-to-crypto pairs over the period under consideration (Chart G, Annex 2), euro represented 8% of total volume on average against other official currencies, which was dominated by US dollar (44%) and Korean won (37%). Using time zones to isolate transactions by geographical origin suggests that Europe and Africa account for lower volumes than Asia but are slightly ahead of the Americas with an estimated share of spot volumes on crypto exchanges of around 30% (Chart H, Annex 2) but these indications need to be considered with caution because of the important limitations involved. [30]

2.1.3 Exposure of EBA and ESMA scope financial institutions to DeFi

40. Absent reporting obligations, limited data is available to assess the exposures of EBA and ESMA scope financial institutions to crypto-assets, including DeFi.

41. According to available evidence from the EBA's Risk Assessment Questionnaire (RAQ), as of Q3 2024, a majority of surveyed EU banks do not engage in crypto-asset issuance or service

[26] Statista. (2024). *DeFi Market in Europe*. https://www.statista.com/outlook/fmo/digital-assets/defi/europe?currency=EUR..

[27] Adan. (2024). 'Web 3 and crypto in France and across Europe: continued adoption and growth of the sector', March 2024. The study leverages on a sample of 2001 respondents for France and two other samples of similar sizes for the Netherlands and the UK. Because of the potential sample selection biases, extrapolated figures need to be considered with caution.

[28] The survey was conducted for the National Bank of Slovakia (NBS) by the Focus agency in November 2023 from a sample of 1,535 respondents, using on-line polling and face-to-face interviews.

[29] Of note, Chainalysis data weighs crypto-activity against purchasing power per capita, which may contribute to higher scores for lower income economies.

[30] An important limitation relates to crypto-assets being typically available for trading 24 hours a day and 7 days a week globally, with the consequence that the time of a transaction may be loosely related to the geography of the user.

provision, with only less than 5% involved in any of those activities. However, approx. 10% EU banks are expecting to engage in crypto activities within the next two years or more, mainly offering the custody and administration of crypto-assets on behalf of clients, and a lower proportion, in the reception and transmission of orders on behalf of clients. Historical EBA RAQ data shows that the adoption of technologies related to crypto-assets is low among EU banks (< 30% of the sample), as compared to other technologies.

42. Consistent with EBA data, ECB surveys show that SSM banks have very limited activities related to crypto-assets, and that while there is some exploratory work taking place, adoption rates over the next three years are likely to be low. Moreover, only 1% of credit institutions supervised by the SSM are already engaged in the use of DeFi applications. The proportion of SSM scope credit institutions exploring, planning or testing them is approx. 7%.

43. The potential increased engagement by EU banks that can be derived from EBA and ECB data can be attributed in part to the regulatory clarity delivered by MiCAR and the CRD/CRR regarding the prudential treatment of banks' exposures to crypto-assets[31], and to increased client demand for services, in particular, custody and trading. At the same time, there are no indications of a potential significant increase in EU banks' engagement with DeFi in the near future.

44. Furthermore, ESMA research found that EU investment funds providing exposure to crypto-assets markets or the blockchain sector in a broader sense represent, as of February 2024, a tiny portion of the EU fund universe (0.02%) with a combined net asset value of a few billion euros only (between EUR 2bn and EUR 4bn dependent on the source).

45. As a result of the abovementioned information, and consistent with the fact that the successive booms and busts of DeFi markets had no spillover effects, including indirect ones, on EU financial institutions, EU financial institutions' direct exposures to DeFi is very limited so far. Nonetheless, the limited visibility over exposures suggests the need to continue efforts to enhance monitoring exposures, including indirect ones[32] (see ESRB, 2023).

2.2 Businesses providing access to DeFi

46. The use of DeFi by retail and institutional users is also dependent on firms providing access to DeFi activities, which is primarily facilitated through three types of services, which are sometimes offered in combination: development of DeFi application interfaces, self-custodial wallet provision, and centralised crypto trading platform provision. This section analyses the functioning of these services in facilitating users access to DeFi and their relevance as potential regulatory entry points into DeFi.

DeFi application interfaces

47. DeFi application interfaces provide intuitive front-end access to protocols, allowing users to engage in a variety of financial activities, such as lending, staking or trading through web-

[31] Regulation (EU) 2024/1623, amending Regulation (EU) No 575/2013 as regards requirements for credit risk, credit valuation adjustment risk, operational risk, market risk and the output floor (CRR III) introduced a transitional regime for the prudential treatment of crypto asset exposures, starting to apply from 1 January 2025 and until the Commission submits a legislative proposal to introduce a dedicated regime. In particular, Article 501d(2) sets outs the methodology for the calculation of own funds requirements for crypto asset exposures. Article 501d(5) mandates the EBA to develop draft regulatory technical standards (RTS) to specify the technical elements necessary for institutions to calculate their own funds requirements, including how to calculate the value of the exposures and how to aggregate short and long exposures to crypto assets. The EBA shall submit those draft RTS to the Commission by 10 July 2025.

[32] Experience in other jurisdictions has shown that absent direct exposures to DeFi, banks and other financial institutions could be indirectly exposed to crypto and DeFi markets via technology companies directly engaged with those markets.

based interfaces that do not require advanced technical knowledge or blockchain expertise. Interfaces help users automate actions without the need for third parties.

48. Interfaces are typically provided by the development teams behind decentralised exchanges protocols. At the same time, users also access DeFi activities via interfaces provided by instant messaging services providers; such as 'bots' available in Telegram channels, with actors behind those bots often not being easily identifiable.

Self-custodial wallets

49. Self-custodial wallets are an integral part of DeFi, as they allow users with sufficient technical knowledge to interact with DeFi protocols, either through their own interfaces or by connecting the wallet to external DeFi application interfaces. Unlike custodial wallets offered by intermediaries, self-custodial wallets give users control of their private keys.

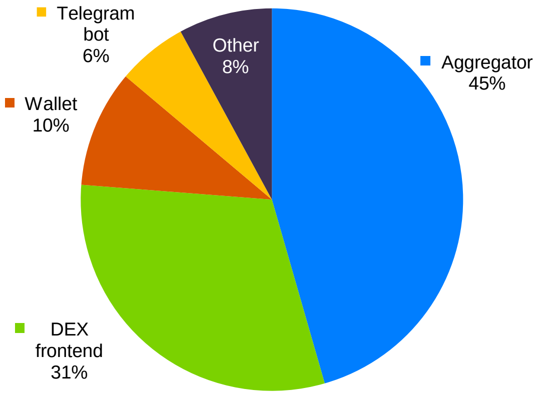
50. Self-custodial wallets facilitate seamless interaction with various DeFi activities, but users become responsible for securing their private keys or seed phrases. Loss of these keys typically results in the permanent loss of access to assets, in contrast to traditional banking systems where intermediaries provide custody of assets. Moreover, self-custodial wallets present regulatory challenges, as transactions made with them are anonymous or pseudonymous and their use is often not subject to AML/CFT requirements (see Section 2.3).

51. Moreover, the access to DeFi is also facilitated by protocols called 'aggregators', that lower the complexity for users who would otherwise need to navigate multiple platforms manually and allow them to optimise their yield-generating efforts by scanning multiple sources of placement opportunities in real time and to execute a transaction from a single interface[33]. DeFi aggregators are also increasingly incorporating cross-chain functionalities, enabling users to access liquidity and services across different blockchain networks. Evidence shows that aggregators have become particularly attractive for users with large transaction volumes: aggregators accounted for 45% of volume on DEXs while they 'only' accounted for 14% of DEX transactions (see Chart 4).

52. The utility of interfaces and self-custodial wallets is reflected in their popularity among users. For instance, users interact with DEXs mainly through the DEXs' front-end (41%), followed by Telegram bots (17%), self-custodial wallet providers (16%) and aggregators (14%) (see Chart 5).

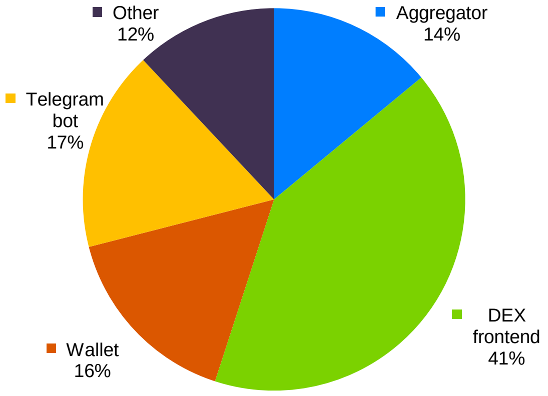
[33] Aggregators use sophisticated algorithms to split large trades across several DEXs, ensuring that users can execute orders with minimal slippage and at the best possible rates. This reduces costs for users but also improves liquidity utilisation across the DeFi ecosystem. For example, platforms such as 1inch and Paraswap provide users with access to aggregated liquidity from multiple DEXs, including Uniswap, SushiSwap, and Curve, offering a seamless experience for decentralised trading.

Chart 4. DEX volumes by type of interface



Note: Type of DeFi application interface by share of volume (Oct 2024) based on a 7-day average
Sources: Messari, Dune Analytics

Chart 5. DEX transaction counts by type of interface



Note: Type of DeFi application interface by share of transactions (Oct 2024), based on a 7-day average
Sources: Messari, Dune Analytics

Centralised trading platforms

53. Centralised trading platforms also play an important role as facilitators of user access to DeFi activities and, in particular, in bridging traditional finance and the crypto-asset ecosystem through a traditional set of tools, such as apps and websites. Some of those platforms provide their clients alternative tools, such as dedicated apps built by platforms that allow users to set up and use self-custodial wallets to access a variety of DeFi activities, which remain connected, to a certain extent, to their account and custodial wallet in the platform. Such tools enable fiat-to-crypto (on-ramp) and crypto-to-fiat (off-ramp) exchanges and transactions, and facilitate user access to DeFi activities (e.g. to earn yields via lending, borrowing and/or staking protocols). As a result, the role of centralised trading platforms as providers of access to DeFi could become relevant with respect to the interconnectedness between DeFi and regulated financial intermediaries.

2.3 ICT risks associated with DeFi

54. The complex technical architecture underlying DeFi markets can be associated with novel or enhanced ICT risks, as evidenced by the results of EBA and ESMA surveys to NCAs. In particular, a majority of NCAs showed concerns about cybersecurity risks, with potential exposure on consumers relying on self-hosted wallets to the loss or theft of their crypto-assets and to the unlawful or harmful disclosure of sensitive personal data. This section analyses the available data on the relevance of ICT incidents, and the main sources of ICT vulnerabilities in DeFi.

55. In sum, this section finds that the number of DeFi hacks and the value of stolen crypto-assets has generally evolved in correlation with the DeFi market size. While historically the majority of DeFi hacks had stemmed from on-chain vulnerabilities, recent attacks on DeFi appear to be more successful when exploiting off-chain vulnerabilities. In particular, the value stolen from DeFi protocols due to the compromise of private keys corresponds to slightly above 50% of all crypto-asset thefts in DeFi and a large majority of all price manipulation attacks were associated to attacks on oracles[34].

[34] Oracles are tools that provide external data feeds to smart contracts, connecting DeFi protocols with external sources of information.

56. This section also concludes that DeFi protocols present significant risks of ML/TF, mainly due to the lack of AML/CFT entry points, anonymity or pseudonymity, the cross-border nature of transactions and the risk that funds or crypto-assets from illegitimate sources are processed in DeFi.

2.3.1 The relevance of hacks and thefts in DeFi

57. Since 2021, the theft of crypto-assets has occurred in DeFi markets more than in any other segment of crypto-asset markets (Chainalysis, 2024). Evidence shows that the number of DeFi hacks and the value of stolen crypto-assets (see Chart 6) has generally evolved in correlation with the DeFi market size (already analysed in Section 2.1.1). As a result, the number of hacks and the value of thefts increased in 2021 and 2022, with attackers stealing approximately USD 2.5 billion and USD 3.1 billion (approx. 2% of total market size of DeFi), respectively, from protocols. DeFi hacking dropped in value and number in 2023, in correlation with the contraction of DeFi markets, with the average size of the value extracted by incident however increasing.

Chart 6:Number and value of crypto thefts in DeFi hacks

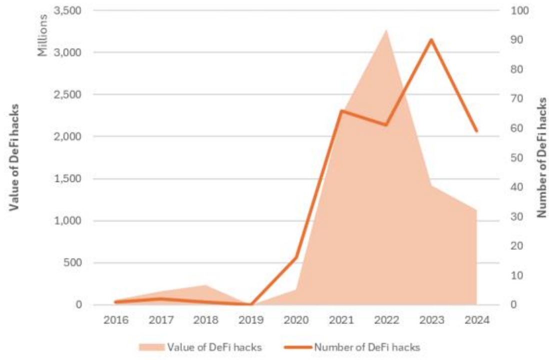
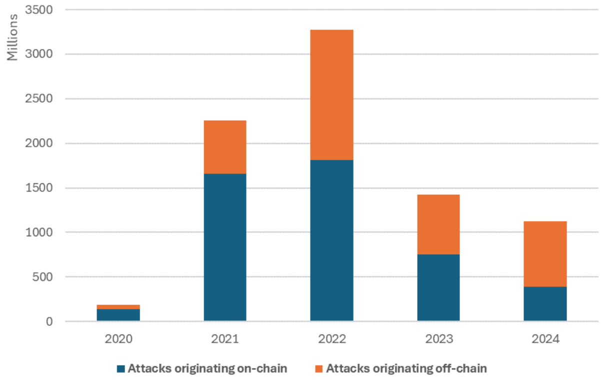


Chart 7: Value of thefts in DeFi protocols by category of attack



Sources: EBA, Defillama

58. The stagnation of the DeFi market but increase in value of DeFi hacks in 2023 confirmed the loss of the previous correlation between DeFi market size and value of DeFi hacks. While the overall value of DeFi hacks declined, there were occasions of large hacks of DeFi protocols in 2023 and 2024[35].

59. The types of attacks and hacks on DeFi protocols are diverse and evolve constantly. They can be grouped into attacks originating on-chain (e.g. smart contract exploitation, price manipulation, governance attacks or scams), and those originating off-chain[36] (e.g. private key compromise, phishing or other types of off-chain attacks). While historically the majority of DeFi hacks have stemmed from on-chain vulnerabilities (see Chart 7 above), recent attacks on DeFi appear to be more successful when exploiting off-chain vulnerabilities. Regarding the DeFi segments analysed in Section 2.1.1, according to data from Halborn (2024), lending

[35] For instance, in March 2023, Euler Finance, a borrowing and lending protocol deployed on Ethereum, experienced an attack that led to $197million in losses, in July 2023, the Curve Finance attack stole $73.5 million from the protocol, in September 2023 an attack on Mixin stole $200million in crypto-assets, and in July 2024 WazirX suffered $234.9million in losses.

[36] It must be noted that while both categories present ICT concerns to DeFi market participants, attacks originating off-chain may also be associated to vulnerabilities present in centralised contexts in crypto-assets.

protocols are the most attacked type of DeFi protocols[37] (see Section 3.1 for more details on DeFi lending), while bridges accumulate the highest loss[38].

2.3.2 ICT risks associated to technical features of DeFi

60. This section presents an analysis of the main ICT risks associated to the specific technical features DeFi (see Annex 4 for brief technical explanations on the key features).

The open-source nature of DeFi software

61. DeFi protocols rely heavily on open-source software[39], which is used in many other sectors and is generally considered to improve efficiency and interoperability, foster technical transparency and even facilitate cyber risk mitigation[40]. However, open-source code, which is not always audited, or audited without the existence of a robust standardisation framework, such as for certification, which may come at the expense of safety, potentially exposing DeFi protocols to attention from malicious actors.

62. The management of vulnerabilities in open-source software can be complex even after they are identified, as any delay in patching can open a window for malicious actors to exploit the vulnerability. Coordinating regular security audits for open-source code can also be challenging, as projects may lack formal processes for ensuring continuous security reviews and there may not be a clear responsible for conducting audits.

Dependence on blockchain networks

63. DeFi protocols are deployed on blockchain networks, called the Layer 1 (see Annex 2), with some deployed on one single network and others in multiple [41]. DeFi protocols depend on the blockchain infrastructure on which they are deployed, including on their technical limitations and security guarantees[42] to ensure the integrity of their operations.

64. Disruptions to the blockchain network caused, for instance, by poorly designed/planned updates, outages, congestion or consensus failure can affect the cost, functioning and performance of the services provided in DeFi protocols. While this risk can also affect crypto platforms operated by CASPs, the automaticity of DeFi protocols can enhance forced liquidations and losses to DeFi users in quicker manner than in centralised settings.

65. On the other hand, some DeFi protocols rely on so-called Layer 1 and Layer 2 scaling solutions, which aim to upgrade the L1 blockchain to allow the processing of more transactions per second, reduce latency or lower transaction costs (see Annex 4 for technical explanations). While scalability may be beneficial for DeFi users for many reasons, L1 and L2

[37] The most common causes of attacks on DeFi lending protocols are price manipulation attacks, followed by smart contract exploitation and, to a lesser extent, the compromise of private keys.

[38] Bridges accumulate a very high number of attacks in proportion to the number of protocols, with the most common causes of attacks being smart contract exploitation and compromised private keys.

[39] Open-source software includes, among others, smart contracts (SCs), blockchain networks, oracles, bridges, user interfaces, decentralized governance arrangements.

[40] For instance, bug bounty programs encourage the community to help identify and report vulnerabilities before they can be exploited, creating a positive feedback loop for cyber risk and security mitigation.

[41] For instance, Uniswap is deployed in Ethereum and Polygon, or Aave in Ethereum, Polygon and Avalanche.

[42] Layer 1s are ultimately responsible for ensuring that transactions are recorded, settled and processed in a secure, tamper-resistant manner, based on a pre-defined consensus mechanism.

scaling solutions can also introduce further ICT risks in DeFi systems. They require careful planning, coordination, and testing to ensure the changes do not disrupt operations[43].

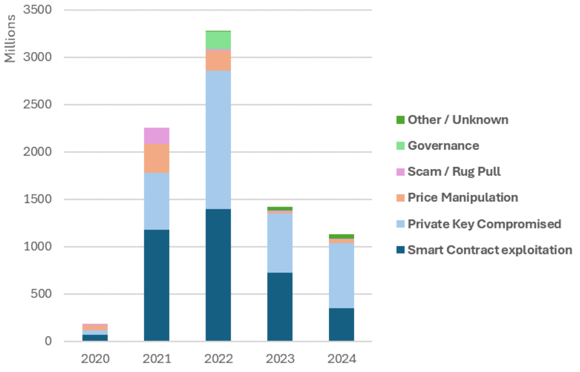
66. Moreover, some scaling techniques may result in a lower number of network nodes contributing to the functioning of a L1 or validators contributing to the security of the L1. As nodes are key actors in preserving the security guarantees of blockchain networks, a decline in their number can reduce the defence of the network against attacks, as they may struggle keeping up with larger and/or faster networks. As a result, DeFi protocols deployed in those L1s could see their security weakened and become more vulnerable to attacks.

67. Layer 2 scaling solutions move transactions off chain, instead of settling them on chain, for the benefit of users in terms of speed and cost. But, the operations of a L2 still rely on the L1 they are built on (and aim to scale), including on their security guarantees. As a result, disruptions on the L1 could affect a L2, and ultimately the DeFi protocols deployed on L2s. Moreover, L2 solutions are reliant on the interoperability between blockchains networks. This often requires the use of cross-chain bridges (see more on bridges on paragraphs 75-76), which may introduce additional risks. As a result, technical issues or malicious attacks not adequately mitigated or managed by L2s can disrupt services provided by DeFi protocols.

Smart contract-related risks

68. Smart contracts, as self-executing pieces of computer code, carry potentially ICT vulnerabilities because of their technical nature. While code carries ICT risks also in centralised settings and other sectors, the relevance of smart contracts in DeFi is prevalent. Smart contract exploitation is, together with private key compromise, the most frequent vulnerability exploited by attackers (see Chart 8). Smart contract exploitation may also carry legal risks (e.g. if a transaction is wrongly recorded), which could be increased in DeFi due to an often unclear or absent recourse for users.

Chart 8. Value of thefts in DeFi protocols by type of attack (2020-2024)



Sources: EBA, Defillama

69. Since 2022, the value stolen from DeFi protocols exploiting vulnerabilities in smart contracts has been on a decreasing trend, while other types of attacks on DeFi protocols have in parallel increased in relative terms. This may suggest that protocols, especially those operating for a longer time, may have improved smart contract security due to improved security audits (more on smart contract auditing in Section 2.4). Still, as of 18 October, there have been 34 DeFi hacks so far in 2024 that exploited smart contract vulnerabilities, with losses worth $346 million[44]. Among them, approx. 20% of value theft corresponds to flash loan attacks, with smart contract exploitation being the most frequent type of attack (see Annex 5).

[43] It is vital that all nodes contributing to the operations of a L1 or L2 on which a DeFi protocol is built use the same latest version of software, as otherwise consensus errors can occur and lead to incidents. For instance, Trail of Bits (2022) found that, as of June 2022, 21% of Bitcoin nodes were running an old version of the Bitcoin Core client that was known to be vulnerable. If such a proportion of nodes was to use old versions of software used in Ethereum, the operations of many DeFi protocols could risk facing disruptions.

[44] Based on EBA and ESMA analysis of data in https://defillama.com/hacks

70. Some of the typical causes of smart contract exploitation are a) math errors in formulae, b) logic or programming errors[45], c) configuration (e.g. address of a token's smart contract) errors, d) missing or weak access control (e.g. it is left for anyone to be called), e) re-entrancy[46], or f) missing or improper input verification or validation[47]. The latter is the most common and the one accounting for highest monetary losses (25.5% and 25.7%, respectively) (Holborn, 2024) . Smart contract security can also be compromised by the external elements with which it interacts[48], such as, infrastructure and interface layers, issues posed by Layer 2 components (see Section 2.3.1), code compilers[49], composite smart contracts[50] or oracles (see Section 2.3.3). As a result of the composability of smart contracts, vulnerabilities in one smart contract can spread across many DeFi protocols. Vulnerabilities can also arise from the fact that many protocols are so-called 'forks' of other protocols, inheriting the vulnerabilities in the smart contracts and code used in those other protocols and potentially spreading them further.

'Oracles'

71. Oracles are tools that provide external data feeds to smart contracts, and therefore, play a critical role in connecting DeFi protocols with external sources of information. They do it relying on multiple external providers of, for instance, market prices, decentralised identities, GPS device data, random number generating functions or weather conditions.

72. Oracles typically receive data from external providers and transmit such data to DeFi protocols via APIs, which then use them as the reference data for their operations. By doing so, oracles may become points of failure in the ICT value chain of a DeFi protocol. If oracles fail to provide accurate data (e.g. because they use data from the wrong sources), DeFi protocols could make decisions based on erroneous data, leading to, for instance, improper asset valuations or incorrect/unfair liquidations in lending protocols.

73. Oracles can face price manipulation attacks. Oracles can be compromised due to flaws in their design or through the manipulation of their data sources. There can also be latency and delay issues with oracles, with their reporting of data via APIs suffering delays. Oracles can become unresponsive due to a downtime, with nodes potentially obtaining a different view of the data depending on the exact time in which they receive it. Furthermore, as oracles are deployed in both L1s and L2 scaling solutions, oracles may need to bridge data securely from a L1 to different L2s, which adds technical complexity.

74. However, according to Defillama, although a large majority of all price manipulation attacks were associated to attacks on oracles, between 2023 and October 2024, price manipulation attacks accounted for 1% of all value stolen in DeFi hacks (see Chart 9).

[45] Human errors can affect SCs used by developers of DeFi protocols similarly to any other developers in centralised crypto services or other sectors. Humans may not always fully be able to anticipate all possible future states, scenarios, or outcomes. It may also be difficult to identify and implement all necessary updates to the SCs in a timely manner to address emerging risks.

[46] Reentrancy is a vulnerability that allows an attacker to re-enter a function multiple times before the first function call is finished. As a result, an attacker can lead the smart contract to unexpected behavior (e.g. reordering of transactions), leading it to a drain of assets.

[47] This is a vulnerability that occurs when a smart contract fails to adequately verify and validate the input data (the route parameter to an address) supplied by users or external sources before processing them. It can have significant security implications.

[48] SCs often rely on other SCs or applications for code development – i.e. code developers re-use the code scripted by other developers (or themselves) for other SCs. According to Trail of Bits (2022), the Ethereum SC ecosystem makes heavy use of code re-use. From a sample of 1,586 SCs deployed to the Ethereum blockchain in October 2021, they found that 90% of SCs were at least 56% similar to each other, and about 7% were completely identical. Similarly, Chen et al (2021) found that code reuse in SC is frequent.

[49] The source code of a smart contract requires a compilation phase, in order to be translated into a machine language that enables it to be executed on the blockchain. Compiler tools, particularly if they are not kept up to date, can introduce vulnerabilities into the machine code produced, which can be exploited by attackers.

[50] Smart contracts interact with third-party smart contracts, which can be considered as external components.

Cross-(block)chain 'bridges'

75. So-called bridges are used to 'transfer' crypto-assets across different blockchains. The interaction across networks is complex, and bridges rely on smart contracts that are more complex to design, hence this type of code may more likely contain bugs or vulnerabilities that attackers can exploit. Moreover, bridges can be vulnerable to complex attack vectors, such as double-spending (i.e. an attacker spends the same asset on two blockchains), replay attacks (reusing a transaction from one blockchain in another blockchain), downtime or congestion.

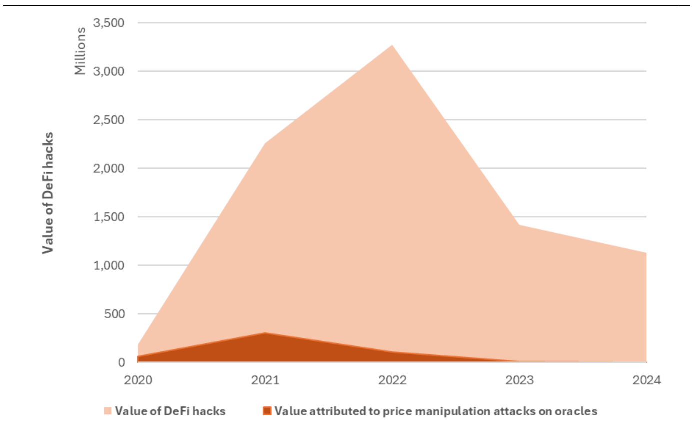
76. Attacks on DeFi bridges have been notable, targeting code vulnerabilities and access control points, i.e., they resulted in the theft of over USD 1.3 billion only in 2022[51].

2.3.3 Other features of DeFi that may increase ICT vulnerabilities

Governance arrangements

77. Decentralized or distributed, and often token-based, decision-making processes in DeFi may increase ICT risks. Governance in DeFi is typically facilitated through Decentralized Autonomous Organizations (DAOs), with rules and governance procedures typically written into smart contracts. Governance token holders often vote on proposals of 'community' members that can influence operations of a DeFi protocol.

Chart 9. Value of DeFi hacks attributed to price manipulation attacks



Sources: EBA, Defillama

78. As explained by the OECD (2022), in practice, there are a number of limitations to governance through DAOs based on governance token holding. Many DeFi projects suffer from low voter participation rate in decisions[52], leaving important decisions dominated by a few active participants, which increases the likelihood that poorly designed or malicious proposals are passed without sufficient scrutiny.

79. Furthermore, malicious actors can attack DeFi protocols by accumulating governance tokens to pass proposals (i.e. so-called 51% governance attacks)[53]. However, governance token ownership can be concentrated in a very small number of holders, who can be related to the core software development team (e.g. labs or foundations), venture capital investors, founders, or can just be investors who bought large amounts of tokens in the market ('whales'). Those actors can take decisions that may be detrimental to users of the protocol, if they hold economic incentives[54], or some simply retain veto or other control rights (e.g.

[51] https://www.chainalysis.com/blog/cross-chain-bridge-hacks-2022/

[52] Voter turnout in governance proposals for governance token holders in DAOs tends to be often under 10% of eligible voters. In DeFi lending protocols Aave and Compound, turnout is often between 3-5% for relevant decisions.

[53] A 51% governance attack refers to an attack on a protocol based on the accumulation of more than 50% of governance tokens by one single entity or user, which could allow the attacker to approve changes to the protocol that benefits the attacker (in detriment of the protocol and its users).

[54] See e.g. governance attacks in Compound and Balancer: https://research.despread.io/compound-finance-governance-attack/

‘multisig wallets’[55]) over discussions around protocol changes. But that concentration can also increase the difficulty of undertaking a 51% governance attack.

80. As a result, the existence of potentially opaque centralised governance arrangements could potentially threaten the integrity, security and functionality of DeFi protocols.

Box 1. ICT risks associated with the use of DeFi protocols and DORA

To understand to which the extent requirements established under the Digital Operational Resilience Act (DORA)[56] sufficiently address the range of ICT risks associated with a potential use of DeFi by entities in scope of DORA, albeit considering that their engagement is so far minimal (see Section 2.1.3), the EBA and ESMA carried out a survey of NCAs in July 2024.

The majority of responses suggested that while DORA provides a solid framework to enhance the digital operational resilience of regulated financial entities, some risks associated with the engagement with DeFi protocols may require further attention due to the lack of ‘entry points’ in DeFi contexts. Specifically, DORA applies to regulated financial entities such as credit institutions, insurance companies, CASPs or issuers of ARTs. If these entities were to adopt or integrate DeFi activities (e.g. as briefly explained in Section 2.2, should CASPs facilitate their users’ access to DeFi), they may need to ensure compliance with operational resilience and ICT risk management requirements under DORA. However, absent such engagement from regulated financial entities, there may not be relevant addressees for the purposes of DORA applicability where DeFi market participants operate in a fully decentralised manner.

In particular, DORA scope financial entities engaging with DeFi should consider, among others, DORA requirements in relation to:

(a) ICT risk management[57], which includes taking into account elements of increased complexity and risk, when implementing ICT risk management arrangements[58] to ensure resilience, continuity and availability of ICT systems.

(b) ICT third-party risk management, including the identification and assessment of all relevant risks in relation to contractual arrangements, undertaking all due diligence on perspective ICT third-party service providers, and the assessment of ICT concentration risks.

(c) ICT-related incidents, including establishing mechanisms for prompt detection of ICT-related incidents and anomalous activities, implementing appropriate arrangements to effectively respond to all ICT-related incidents, and reporting and notification of major ICT-related incidents[59] for major operational or security payment-related incidents.

[55] Those with access to multisig wallets (which require the signature of 3 out of 5 wallet owners to approve a decision) may control key aspects of a DeFi protocol, such as treasury management, upgrades, emergency interventions or handling security incidents.

[56] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (http://data.europa.eu/eli/reg/2022/2554/oj)

[57] See also the Joint ESAs draft RTS on ICT Risk Management Framework and on simplified ICT Risk Management Framework, developed under Article 15 and Article 16(3) of DORA as complementary to the requirements set out in DORA: https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/operational-resilience/regulatory-technical-standards-ict-risk-management-framework-and-simplified-ict-risk-management

[58] See ESA’s Draft RTS on ICT Risk Management Framework and on simplified ICT Risk Management Framework. The arrangements include among others ICT security policies, procedures, protocols and tools (including comprehensive policy on encryption and cryptographic controls), ICT operations security (particularly vulnerability and patch management), ICT incident and response procedures, and ICT business continuity policy and recovery plans.

[59] See also the Joint ESAs draft technical standards on major incident reporting (https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/operational-resilience/joint-technical-standards-major-incident-reporting) and the Joint ESAs draft RTS on criteria for the classification of ICT-related incidents (https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/operational-resilience/regulatory-technical-standards-criteria-classification-ict-related-incidents).

(d) Digital operational resilience testing[60].

(e) Information and intelligence sharing in relation to cyber threats and vulnerabilities.

The engagement of regulated financial entities with DeFi can occur in many forms: (i) they may engage with DeFi protocols on their own account; (ii) they may provide their clients access to DeFi (e.g. via apps and self-custodial wallets that allow users to transfer crypto-assets to addresses of DeFi protocols) or access DeFi on behalf of their clients; or (iii) they may run protocols on-chain to provide crypto-asset services or MiFID II services.

While the DORA requirements above apply to all regulated financial entities, each type of engagement with DeFi would involve a different set and scope of ICT services. Running a protocol on-chain, in particular, may require a broader set of ICT services, such as blockchain node infrastructure services, oracles, cloud, hosting and storage services, Layer 2 scaling services or cross-chain communication services. Other types of engagement may not require a regulated financial entity to directly engage with those ICT services (e.g. it may provide self-custodial wallets for clients to operate in DeFi ecosystems).

However, since DORA follows the principle of technical neutrality to ensure it is future-proof, all DORA requirements should be complied with by regulated financial entities engaging with DeFi ecosystems. Unregulated entities or ICT services providers operating in a fully decentralised manner may be part of the DeFi network in which a regulated financial entity operates. This does not exempt a regulated financial entity from compliance with DORA. This may be particularly relevant with respect to DORA requirements in relation to ICT risk management (Chapter II of DORA). Moreover, where ICT third-party services providers are identifiable, DORA requirements on ICT third-party risk (Chapter V of DORA) would apply to financial entities.

Regardless of the above, as noted in section 2.1.3, currently EU financial institution engagement in DeFi is extremely limited.

Anonymity or pseudonymity

81. In DeFi, many users operate with anonymity or pseudonymity. They use self-custodial wallets, instead of trusting the custody of their crypto-assets to a third party. This gives DeFi users autonomy and full control of their assets and activity and enhances their privacy (i.e. to their own individual data), but it also exposes them to the risk of losing control or access to their private keys (i.e. to their held crypto-assets). Preserving private keys securely is crucial – i.e. if they are lost or stolen, the users lose access to their crypto-assets.

82. The compromise of private keys is the main source of hacks in DeFi since 2022 (see Chart 10). Considering all attacks on DeFi between 2023 and October 2024, the value stolen from DeFi protocols due to the compromise of private keys corresponds to slightly above 50% of all crypto-asset thefts in DeFi. Moreover, while the method to steal private keys is most often unknown (see Chart 11), as it can happen off-chain due to human errors, there are indications of attacks becoming more sophisticated and innovative recently. Attackers increasingly deploy phishing[61] campaigns and have also undertaken social engineering campaigns[62].

83. Not necessarily implying a compromise of private keys, but being triggered by the anonymity or pseudonymity in DeFi ecosystems, other fraudulent activities also target user funds or

[60] See also the Joint ESAs RTS specifying elements related to TLPT: https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/operational-resilience/joint-regulatory-technical-standards-specifying-elements-related-threat-led-penetration-tests

[61] For instance, the WazirX attack that resulted in £234.9 million losses in July 2024 occurred due to a phishing campaign.

[62] For instance, in October 2024 a social engineering attack on Tapioca DAO resulted in $4.7 million losses.

crypto-assets, such as 'rug pulls'[63], 'pump-and-dump schemes'[64] or 'pig butchering'[65], in addition to hacking or denial-of-service (DoS) attacks. While the value of crypto-assets stolen from DeFi protocols via some of those schemes remains very low in total and relative terms in DeFi[66], some NCAs in the EU have issued warnings about their growing relevance[67]. According to Defillama, DeFi protocols (and users) have seen USD 211.9 million stolen via scam and rug pull schemes, with at least 20 instances of scams, mainly 'rug pulls', in DeFi protocols between 2020 and October 2024 (see Chart 8 above).

84. Furthermore, anonymity or pseudonymity in DeFi can facilitate the obfuscation of funds or crypto-assets (see section 2.3.4 on ML/TF risks associated with DeFi), as fraudulent activities are not easy or are impossible to trace and fraudsters held accountable. Combining anonymity and limited traceability, victims often have limited recourse in recovering lost assets. Potentially, the absence of accountability can contribute to higher frequency and severity of attacks on DeFi protocols.

85. Finally, the anonymity or pseudonymity of DeFi users may hinder transparency around token concentration and membership in governance arrangements.

Chart 10. Value of thefts in DeFi by attack type (2023-2024)

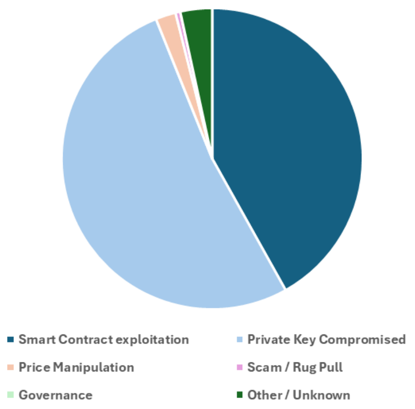
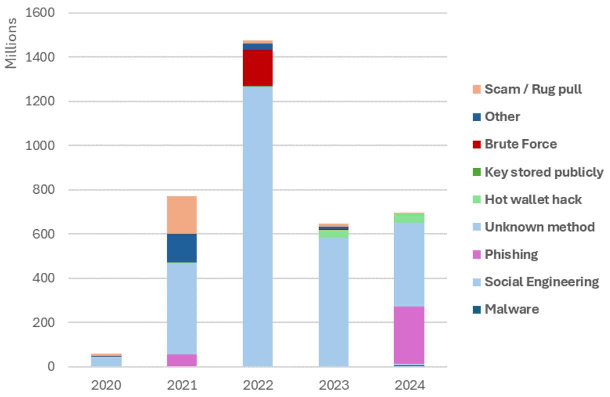


Chart 11. Value of thefts via attacks off chain



Sources: EBA, Defillama

2.3.4 ML/TF risks associated with DeFi

Box. 2 ML/TF risks associated with the use of DeFi protocols and EBA GLs on ML/TF risk factors

In the amended Guidelines on ML/TF Risk Factors[68], the EBA highlighted the transactions to and from self-hosted addresses and DeFi platforms that offer services in a fully decentralised manner

[63] A rug pull is a scam where the developer(s) of a token or a protocol hypes a project to attract investor funds, only to suddenly shut down or disappear, taking investor assets with them. They are particularly prevalent in DeFi (Chainalysis, 2021) and in so-called 'meme tokens' – i.e. investors are victims of rug pull scams in 62% of meme tokens, according to Li et al (2023).

[64] A pump and dump scheme involves artificially inflating the value of a token with marketing or whale activity to attract more buyers.

[65] A 'pig butchering' scheme is where scammers initiate and develop relationships with victims and pressure them to invest in fake investment platforms that enable the scammer to steal invested funds. These scammers encounter victims on dating apps, social media websites, or even text messages sent to appear inadvertently sent to the wrong number.

[66] According to Chainalysis, based on 2023 data, the total value of tokens that can qualify as pump and dump schemes account for just 1.3% of total Ethereum DEX trading volume. See: https://www.chainalysis.com/blog/crypto-crime-2024-pump-and-dump/

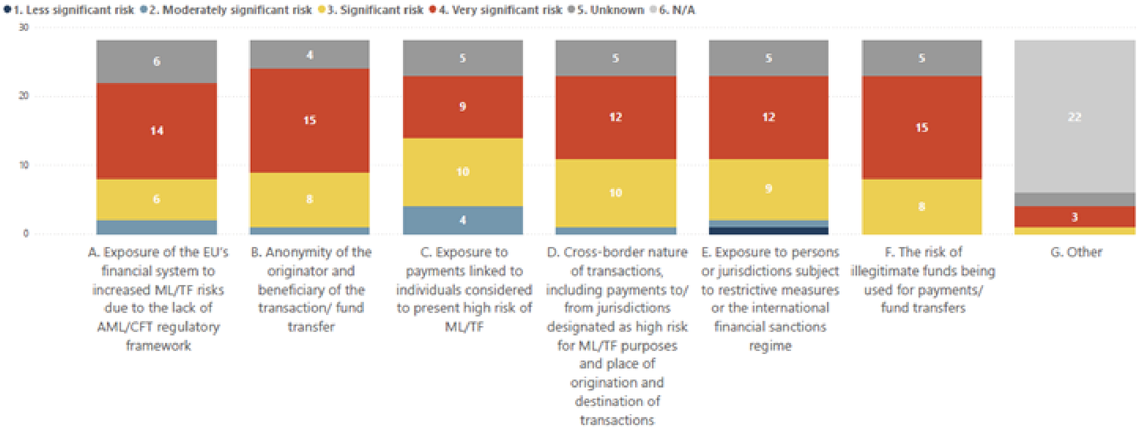
[67] In October 2024, the Dutch Authority for the Financial Markets (AFM) issued a warning against crypto pump-and-dump schemes: https://www.afm.nl/en/sector/actueel/2024/september/pump-en-dump

[68] Guidelines (EBA/GL/2024/01) amending Guidelines EBA/2021/02 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ('ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849.

without any intermediary as factors that may expose CASPs to an increased ML/TF risk. This is due to their unregulated nature, as both fall outside the remit of the Directive (EU) 2015/849[69] (AMLD) and the Regulation (EU) 2023/1113[70] (FTR). This means that customer due diligence (CDD) requirements (e.g. identification and verification of self-hosted address owners or users on DeFi platforms) do not apply to these fully decentralised platforms, increasing ML/TF risks.

86. Illicit actors, including cyber criminals, fraudsters and terrorist organisations, can take advantage of the technical nature and absence of AML/CFT checks in DeFi to launder illicit proceeds of crime or raise funds or crypto-assets to finance criminal activity[71]. Those actors use DeFi activities to obfuscate the movement of funds or crypto-assets or to move illicit funds or crypto-assets through various techniques and services, including a) exchanging crypto assets for other crypto assets that are easier to use in DeFi protocols or are less traceable (e.g. 'privacy coins'), b) using bridges, c) transferring crypto-assets through so-called 'mixers'[72], or d) placing crypto-assets in liquidity pools as a form of layering. DeFi protocols may be used to complicate the traceability of flows. The share of illicit funds or crypto-assets going to DeFi protocols has grown over time. However, overall, centralized exchanges remain the primary destination for funds or crypto-assets sent from illicit addresses[73].

Chart 12. ML/TF risks associated with the provision of financial services and activities via decentralised platforms



Sources: EBA-ESMA joint survey to NCAs

87. Based on EBA and ESMA surveys, EU NCAs generally consider DeFi activities to present *significant* and *very significant* ML/TF risks (see Chart 12). In particular, the NCAs highlighted the lack of applicable AML/CFT regulatory framework and implemented AML/CFT controls, which facilitate the anonymity or pseudonymity of DeFi users, as no CDD obligations apply to DeFi protocols. This, coupled with the cross-border nature of transactions and the ease to process funds or crypto-assets, means that funds or crypto-assets from potentially illegitimate sources can freely flow through DeFi protocols without being detected or reported to FIUs or law enforcement agencies. Moreover, some NCAs highlighted potential ML/TF risks associated with the use of DApps to obfuscate asset flows and hide the real origin of funds or crypto-assets.

[69] Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012, and repealing Directive 2005/60/EC and Commission Directive 2006/70/EC.

[70] Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849 (recast)

[71] See, for instance, the risk assessment by the US Treasury: https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf

[72] They allow users that deposit assets in an account to move them to omnibus accounts and withdraw them into separate accounts.

[73] See the 2024 Chainalysis Crypto Crime report: https://go.chainalysis.com/crypto-crime-2024.html

88. Some NCAs also warned that there is a greater susceptibility to the use of highly volatile crypto-assets in DeFi, since it enhances their appeal for movement and conversion. As a result, the purpose or nature of many crypto-assets used in DeFi may be purely illicit.

89. As a consequence, and despite the size of EU DeFi markets being relatively small (see Section 2.1.2), it is important to monitor developments and innovations in DeFi products and services, as they can enhance the interconnectedness between centralised (including traditional finance) and decentralised crypto-assets ecosystems if left unregulated, and ultimately exposing the EU financial sector to significant ML/TF vulnerabilities. Furthermore, level playing field and technological neutrality consideration point to a need to align expectations for risk mitigation between DeFi markets and more traditional financial contexts with respect to the viability of anonymous transactions.

2.4 Mitigation and monitoring of risks associated with DeFi

90. Considering the assessment of the ICT risks associated with DeFi, the blockchain / crypto / DeFi industry has been adopting measures or initiatives that aim to mitigate risks, following self-regulatory approaches. This section identifies some of those initiatives and provides considerations on how ICT risks associated with DeFi could be mitigated. It also sets out potential risk mitigating measures for ML/TF risks. In particular, embedded supervision of DeFi based on public data still appears to face many challenges. However, existing initiatives appear to be more advanced in other areas, such as for building a harmonized framework for the standardization of smart contracts, for the certification of DeFi protocols, and for the reporting of serious ICT incidents to relevant authorities and conducting of post-incident reviews, based on the approach set out by DORA.

91. **Standardisation and auditing of software used in DeFi, including smart contracts**. Initiatives to standardise the ICT security environment of software used in DeFi could facilitate and harmonize the auditing of code used in DeFi protocols[74], a practice that is already quite extended in DeFi. Standards could cover areas such as coding, software design, secure development, or use of reference data sources. There are already a number of specialized smart contract security audit firms, mathematical auditing firms specialized in the assessment of correctness of smart contracts, 'bug bounty' platforms that promote the crowdsourcing of audits and bug reporting in exchange for rewards, and firms offering automated auditing tools that can be integrated into workflows. The range of audit methods used by those firms seems sufficiently wide and the state of the art is advanced to provide some guarantee of safety. Therefore, existing best practices, standards and audit methods could serve as a basis of a potential harmonized framework.

92. **Certification of DeFi protocols following a product-based regulatory approach**. To address the risks associated with governance arrangements in DeFi, protocols could be considered products in the sense of traditional product regulation and be subject to a certification regime. It is not fully clear which entity could be responsible for the certification of the protocol if DeFi activities are undertaken in a fully decentralised manner. Regardless, combining the potential existence of harmonized standards and a framework for the auditing of software, the certification of DeFi protocols could cover security, user expectations on the compliance of the provided service, and governance standards, on the basis of

[74] The development of standards on code used in DeFi software could also help competent authorities improve their ability to assess the degree of decentralisation of providers of regulated activities. The standardisation of smart contracts and related code could help assess, among others, whether there is a self-executing software with programmable actions or whether there is a central entity retaining edit or other control permits (e.g. administrator keys), or whether there are special inherent or immutable rights (e.g. remuneration flows towards a specific address controlled by a specific central authority) embedded into the code or not.

documentation and post-market monitoring requirements. In particular, the ACPR and AMF have set up a dedicated working group in France to explore the different possibilities of introducing such a certification framework[75].

93. **Enhancing the security of oracles**. The use of multiple sources of data and blockchain node operators, and the implementation of multi-layered systems that cross-verify data from various data sources and oracles could improve the integrity, accuracy and security of data fed by oracles to DeFi protocols. While existing oracle providers already use multiple sources of data to mitigate price manipulation risks, DeFi protocols could implement safeguards in smart contract codes, real-time monitoring and early warning tools to detect abnormal data fluctuations or inconsistencies from oracles, to trigger emergency measures, including pausing critical functions or shift to alternative oracles. The development of a certification framework for oracles could harmonise and facilitate the implementation of those aspects by DeFi protocols.

94. **Enhancing the security of bridges**. Conducting regular security audits and stress tests of bridge protocols could help identify potential vulnerabilities in smart contracts or the operational mechanisms underlying the protocols. Moreover, DeFi protocols connected to bridges could implement cross-chain monitoring tools to ensure that crypto-assets are properly locked and minted or burned during transfers between blockchains to identify anomalies.

95. **Introducing disaster recovery and incident response mechanisms**. Implementing 'circuit breaker' mechanisms[76] in DeFi protocols could help provide early responses to disaster events and ICT incidents, mitigating the damage of attacks or exploit. Moreover, DeFi protocols could be required (without clarity about who would be responsible for it) to report serious ICT incidents to relevant authorities, on the basis of the approach set out by DORA, and conduct thorough post-incident reviews after incidents. This could, for instance, contribute to understanding the methods used by hackers to compromise private keys, and reduce, as a result, the high proportion of unknown methods used still as of 2024. However. the feasibility of introducing disaster recovery and incident response mechanisms into DeFi protocols has yet to be further assessed.

96. **On-chain monitoring and identity verification**. DeFi protocols could further explore the use of blockchain analytics services to track and analyse transactions to detect suspicious activity and identify address linked to illicit activities. DeFi protocols could maintain records of addresses identified as illicit. Moreover, DeFi protocols could further explore KYC solutions[77] that could be implemented in, at least, selective cases, such as transactions above a certain value or above a certain leverage.

97. **Identification of DeFi protocols that qualify as CASP.** The FATF has noted[78] that regulators have started to successfully identify DeFi entities that qualify as CASPs and/or taken supervisory or enforcement action against such entities. Coordinated action between EU

[75] See: https://acpr.banque-france.fr/sites/default/files/medias/documents/20240325_revue_acpr_gt_certification_sc.pdf While the EBA and ESMA were not able to assess the outcome of the activities of the WG, they could, based on future outcomes, further assess the potential avenues to introduce a certification framework, if deemed necessary and found feasible.

[76] 'Circuit breakers' are automatic mechanisms built into smart contracts that can temporarily halt or restrict certain protocol operations automatically under predefined conditions, such as high volatility.

[77] There appear to be developments in blockchain technology that appear to bring potential solutions to the implementation of identity verification while preserving the privacy of DeFi users, in areas such as so-called zero-knowledge proofs (ZKPs), like zk-SNARKs and zk-STARKs, multiparty computation (MPC) and decentralized identity (DID) solutions.

[78] See the 2024 FATF Targeted Update on implementation of the FATF Standards on Virtual Assets (VAs) and Virtual Asset Service Providers (VASPs): https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2024-Targeted-Update-VA-VASP.pdf

supervisors, and cooperation with authorities outside the EU, could help perform market monitoring to assess and identify DeFi arrangements that could potentially qualify as CASP.

98. **Promoting user education**. Considering the complexity of technology underlying DeFi, promoting financial and digital education with DeFi-specific initiatives would contribute to raising awareness of risks by actual or potential DeFi users. Education initiatives could focus on the risks of participating in DeFi, including regarding the use of self-custodial wallets and could be accompanied by improvements in disclosures of relevant information by any businesses, including CASPs, facilitating access to DeFi.

99. **Real-time supervisory monitoring of DeFi protocols based on public data**. Supervisory authorities could further explore the potential advantages of implementing real-time supervisory monitoring of DeFi protocols based on public blockchain data, also known as 'embedded supervision' (Auer, 2022). Since the transparency and openness of blockchain networks facilitates real-time monitoring, supervisory authorities could use automated tools to monitor DeFi activities directly from blockchain data without relying on traditional supervisory reporting mechanisms. As a result, embedded supervision could offer novel approaches to mitigate risks associated with DeFi. However, the cost-benefit implications of embedded supervision of DeFi protocols should be further assessed and it seems unlikely to succeed in managing financial crime risks without identities verified by entities subject to supervision or checked against public sector operated digital identity registries.

Box 3. EC pilot project on the embedded supervision of DeFi

In 2022, the European Commission (EC) launched a pilot project[79] to study the potential of embedded supervision of DeFi institutions and activities. The project, led by Promontory IBM Consulting, in coordination with the EC, EBA, ESMA and EIOPA, finalised in mid-2024. The aim of the project was to develop an experimental technical solution that could allow supervisors to engage embedded supervision of DeFi applications by directly linking supervisory data requirements and tools to DeFi applications. In order to do so, the project aimed at identifying how and what data can be gathered from DeFi applications on the Ethereum public blockchain in real time, how this can be used for effective supervision of DeFi activity and, if not, what critical data may be missing.

The project analysed relevant DeFi protocols in four domains: lending and borrowing (Aave, Compound), exchanges (Uniswap, Curve Finance), insurance (Nexus Mutual, Unslashed), and aggregators or protocols providing a combination of services (1inch, MakerDAO). After selecting appropriate benchmarks of traditional financial supervisory reporting (e.g. MiFIR / MiFID, AML, Corep/Finrep, SFTR, EMIR, Solvency II), a unique repository of all benchmarks was built, organised by blocks of thematic analysis, which, were relevant, were identified as proxy areas to information available on DeFi protocols.

On the basis of a dedicated IT solution, selected benchmarks were mapped with public data available on the selected DeFi protocols. Apart from information related to the identification of persons and entities participating in DeFi, which is not met in DeFi due to the anonymous or pseudonymity nature of self-custodial wallets, the mapping demonstrated that public data on DeFi protocols meets essential data requirements. The pilot showed that the monitoring of liquidity pools based on public data offers a good starting point for macroprudential supervision efforts, as they can provide valuable insights into the risks and exposures of DeFi market participants. Because all the data of the liquidity pool, since its inception, remains available on the public ledger, a liquidity pool's balance sheet can always be reconstructed based on public data. Additional data can be manually extracted for supervisory purposes, if deemed necessary, from protocols' website, documentation and publicly available statistics offered by third-party providers. Finally, supervisors could create new datasets by making their own computations based on different data collected from public ledgers.

[79] See: https://ted.europa.eu/en/notice/-/detail/542418-2022

Nonetheless, the project concluded that embedded supervision of DeFi based on public data, considering available data and techniques, still faces a handful of challenges, namely:

(i) Quality of documentation available varies greatly with updates often not checked or assessed, documentation is highly technical and complex and is not sufficiently user-friendly.

(ii) Dataset formats are not standardized in DeFi, hence supervisors would assume heavy harmonization or standardization efforts, or even manual collection of some datasets.

(iii) While data availability is broad and market manipulation activities could be detected, investigations and micro-prudential supervision are complicated by the absence of personal identification information.

(iv) The complexity of price formation mechanisms, including formulas and often bots executing arbitrage options, requires specific expertise that is currently not widely available.

(v) While the monitoring of liquidity pools provides macroprudential insights (which could be tested under stress scenarios), the monitoring and assessment of financial stability risks is difficult to undertake without knowledge about interconnections between DeFi markets and financial institutions within the remit of EBA and ESMA.

In addition to the abovementioned challenges, the use of hot wallets by centralized crypto exchanges in DeFi might impact the transparency of on-chain activity and introduce additional challenges for potential embedded supervision based on public data. Exchanges aggregate multiple users' transactions into larger, single transactions that they then settle on-chain. As a consequence, external observers can only see the total transaction from the exchange's hot wallet, not the individual actions of each user. This hides the specific intent, scale, and nature of each user's transaction and of their direct connection with DeFi protocols, reducing transparency into the true nature of the activity happening on the blockchain and on specific DeFi protocols. The information hidden in DeFi protocols is only known by the centralised exchange (and is accessible by their supervisors, FIUs and law enforcement). As a result, embedded supervision based on public data would not be able to identify which users are over-leveraged or over-exposed to risky protocols, assets or users, without relying as well on traditional supervisory work on regulated entities. The involvement of regulated exchanges however ensures that verified identities can be associated with trades, and supports the genuine identification of concentration risks, and other risks such as financial crime.

2.5 Implications of Maximal Extractable Value (MEV) on DeFi

100. For the purposes of this report, MEV refers to *the maximum amount of value a blockchain miner, validator or another agent in the block-building value chain, can make by including, excluding, or changing the order of transactions during the block production process*. Any agent with transaction ordering rights is effectively in a privileged position to perform the extraction.[80, 81]

101. MEV finds its origins in the fact that most blockchains do not enforce constraints on the precise ordering of transactions within a block. MEV has existed since the advent of blockchains but came to prominence in 2020 with the growth of DeFi and the development of arbitrage bots designed to exploit the inefficiencies of DEX protocols. MEV is currently

[80] The term '*miner extractable value'* was originally coined by Daian et al. (2019), which defined it as '*the total amount blockchain agents can extract from manipulation of transactions within a given timeframe, which may include multiple blocks' worth of transactions*'. It has since evolved into '*maximal extractable value'* to reflect the fact that the phenomenon is not limited to miners in PoW blockchains but also applies to validators (and other agents) in PoS blockchains..

[81] IOSCO provides a more technical definition, referring to MEV as 'the exploitation of mempool data by persons or entities participating in a blockchain's consensus mechanism (i.e., miners, validators, or other participants) to maximize their profit by choosing and sequencing proposed transactions from the mempool and/or inserting other transactions that are added to a block to be appended to a blockchain'. IOSCO (2023). Note: Mempools consist of transactions that are waiting to be processed by the blockchain's miners/validator.

widespread and requires monitoring because of its negative externalities for DeFi users and the DeFi system.

102. MEV is virtually possible on any decentralised blockchain but is generally more lucrative in the case of complex transactions. Ethereum, and the complex web of smart contracts and DeFi protocols built on top, represents a target of choice for MEV extractors, whereas the Bitcoin blockchain only processes BTC transfers—not sophisticated financial transactions.[82] The sheer volume of transactions on Ethereum also attracts more MEV extractors. As highlighted above in the section 2.1, Ethereum is the dominant chain for DeFi activities, representing more than 60% of TVL in DeFi protocols.

103. The rest of this section therefore focuses on MEV as it is currently observed on Ethereum. The development of MEV on other chains and so-called cross-chain MEV, namely the MEV that can be captured across chains is not discussed in this report.[83] The section also assesses the scope of the phenomenon, and discusses its implications, including risks, both for users of DeFi activities and the DeFi ecosystem. Finally, it sets out the various MEV counter-measures that industry stakeholders and academics are developing, including their benefits and shortcomings.

Incentives to engage in MEV

104. MEV can be traced back to the fact that most blockchains do not enforce any constraints on the precise ordering of transactions within a block and in turn their execution. A key reason for this is that it is virtually impossible in a decentralised system to ensure a precise enough and non-manipulable timestamp of transactions. Decentralisation means that blockchains do not have a natural order of transaction execution in the absence of a pipeline creating a single queue. One or several validators (or other agents) can therefore manipulate the ordering of transactions in a way that nets them the highest profits.

105. Beyond decentralisation, other factors combine to contribute to the persistence of MEV in blockchains, namely economic incentives and the public nature of transactions. Validators (and other agents) are incentivized to maximize profits, and MEV provides an opportunity to gain extra revenue beyond the reward from validating or creating blocks. And since all transactions are publicly visible before they are included in a block in the public mempool, allowing for potential exploitation by malicious actors, e.g., through sandwich attacks or front-running (see Annex 3 for detail on these exploitation strategies)[84]. The public nature of the ledger is inherent to the original design of blockchains and the censorship resistance principle that goes with it.

106. Several industry-led initiatives underway aim to mitigate the negative externalities of MEV but they are complex to implement and may only address certain elements of the MEV value chain. Blockchain designs may also vary, and MEV techniques adapt accordingly, in turn calling for customised counter-measures.

Key agents and techniques

[82] Of the various smart contract blockchains, Ethereum has the most advanced on-chain market structure. EY (2023).

[83] As MEV opportunities become more competitive on Ethereum, MEV extractors seem to be increasingly moving to alternate chains, where similar MEV opportunities exist with less competition. With an increasing number of 'wrapped' versions of the same asset on different blockchains and the increasing popularity of Layer-2 solutions, expectations are that cross-chain MEV will expand in the future. See: Barragan (2022).

[84] Front-running is an exploit in which a malicious attacker takes advantage of the transparency of the transaction queue (mempool) and the way transactions are processed to prioritise their own transactions at the expense of others. A sandwich attack is an extension of this concept, which involves two transactions: one placed by the exploiter before the victim's transaction and one after. The front-running transaction manipulates the price in the exploiter's interest. The back-running transaction reaps the profit of the initial manipulation. See Annex 3 for more detail on these exploit strategies.

107. There are three main agents involved in MEV, namely users, validators, and MEV searchers and they can have contradicting interests, as MEV is ultimately a zero-sum game where profits accrued to one agent come at the expense of the other agents.

Table 2. Agents involved in MEV

Entity	Description
Users	Individuals or platforms that submit transaction orders on the network. Orders are placed in the public 'mempool' (a queue for transactions pending validation) in Ethereum's original design. Users pay transaction fees to validators, and those willing to have their orders executed first bid higher fees.[85]
Validators[86]	Entities (or miners in PoW blockchains) that contribute resources to validate transactions and earn fees. Validators prioritize transactions with higher fees, as these offer stronger incentives, though prioritizing high-fee transactions is not mandatory.
MEV Searchers	Agents identifying profitable opportunities by reordering, inserting, or omitting transactions. Searchers may work independently or in collectives and often pay up to 90% of their MEV revenue to validators due to high competition. They are skilled at "gas golfing" to minimize transaction gas costs and maximize efficiency.[87]

108. Until 2020 and the emergence of arbitrage bots and priority gas auctions[88], a single entity, the validator, effectively combined the functions of validator and MEV searcher on Ethereum. MEV counter-measures, in particular Flashbots' MEV-Geth and MEV-Boost, led to the emergence of new agents in the chain: block builders and relays, which are discussed below.

109. MEV techniques are constantly evolving and increasingly complex, which makes defining a taxonomy challenging. However, they can be grouped into three categories: (i) arbitrage, (ii) front-running and sandwich attacks, and (iii) liquidations. A fourth type, sometimes referred as long-tail MEV, is often used as a catch-all for the rarer types of MEV strategies not covered by the first three categories. See Annex 3 for more details on each of these techniques.

2.5.1 Scoping the MEV phenomenon and its consequences

Measuring MEV is a challenge

110. There are no commonly accepted standards or methodologies to measure MEV at this point. Measuring MEV invites complex questions about what constitutes 'extracted' value vs. legitimate arbitrage and the available data suffer from important limitations:

[85] Since August 2021, and the adoption of Ethereum Improvement Proposal (EIP) 1559, transaction fees on Ethereum, also known as gas fees, have two components: a base fee and a tip. The base fee is a standard charge that all users need to pay. It is calculated by the network based on network traffic and paid per unit of gas (a measure of the computation required for a transaction). The tip, or priority fee, is an optional extra payment that users can pay to speed up their transactions. Prior to EIP-1559, gas fees operated on a simple auction system, which led to highly volatile and unpredictable fees when the Ethereum network became busy.

[86] For the sake of simplicity, the report uses the term 'validator' to refer to proposers and validators indistinctly. In short, a proposer is a validator that has been randomly selected in every slot. His role is to create a new block and send it to other validators, who in turn vote to determine the validity of the block being proposed. For further details on the exact role of proposers and validators in Ethereum's PoS, see Proof-of-stake (PoS) | ethereum.org

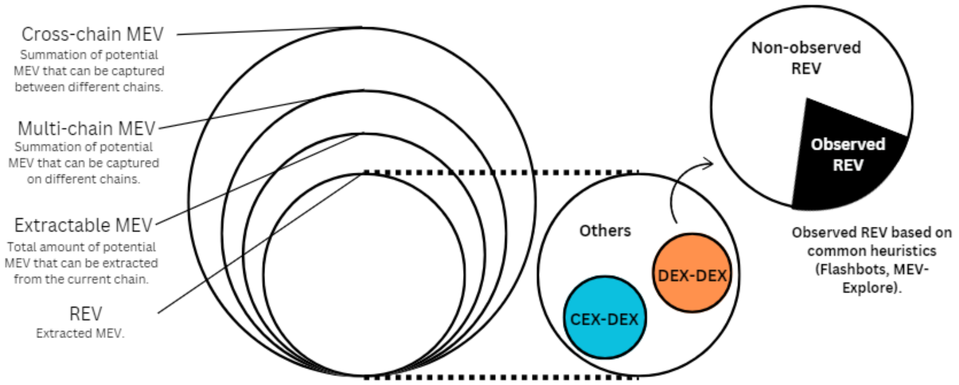
[87]A few well-known gas golf techniques include: using addresses that start with a long string of zeroes (e.g. 0x0000000000C521824EaFf97Eac7B73B084ef9306) since they take less space (and hence gas) to store; and leaving small ERC-20 token balances in contracts, since it costs more gas to initialize a storage slot (the case if the balance is 0) than to update a storage slot. Finding more techniques to reduce gas usage is an active area of research among searchers.

[88] Priority gas auctions is a term coined in the Flashboys 2.0 paper which refers to the high competition between arbitrage bots to have their transactions included in a block first. For further details on priority gas auctions and their negative consequences, see for example EY, 2023. 'An introduction to maximal extractable value on Ethereum', March 2023.

111. First, the distinction between MEV and 'mainstream' trading activities is often very difficult to identify. For example, bidding higher fees may be the expression of a user's intention to have its orders executed rapidly, not necessarily to front-run others. Sandwich attacks may also resemble market making activities. Second, MEV is difficult to detect because of the pseudonymity of blockchain interactions and the lack of a natural ordering of transactions. Sandwich attacks may go unnoticed when the front-running and back-running transactions are initiated from two distinct wallets or if multiple pseudonymous users collude.[89] Third, measuring aggregate MEV requires the collection of data from different sources (e.g., protocols, chains and oracles), which can also be hidden. Quin et al (2021) find 32% of sandwich attacks were relayed to miners privately. Many of these attacks also involved transactions with more than 200 intermediate sub-transactions embedded within.

112. A consequence of these challenges is that comparing MEV data across different sources often yields inconsistencies because of the diversity of approaches to measurement (Diagram 1). A historical analysis of the data is also unproductive because the measurement approaches have evolved over time alongside MEV techniques and as a consequence of Ethereum's transition to a PoS consensus in September 2022 (known colloquially as the 'Merge'). A more comprehensive discussion of the data sources and the limitations is available in Annex 3.

Diagram 1 – The different definitions of MEV


Cross-chain MEV
Summation of potential MEV that can be captured between different chains.
Multi-chain MEV
Summation of potential MEV that can be captured on different chains.
Extractable MEV
Total amount of potential MEV that can be extracted from the current chain.
REV
Extracted MEV.
Others
DEX-DEX
CEX-DEX
Non-observed REV
Observed REV
Observed REV based on common heuristics (Flashbots, MEV-Explore).

Note: Graphic comparison of different definitions for MEV.
Sources: ESMA, Galaxy Research.

113. Despite the data limitations, the MEV research and software developer, Flashbots[90], has estimated a dollar-value for gross extracted MEV from January 2020 to September 2022 at USD 675 million, mostly from arbitrage (99%), with Uniswap V2 and V3 accounting for around 80% of this extraction.[91] These MEV transactions seemingly affected nearly half (USD 328 billion) of the USD 666 billion traded on Ethereum's DEXs in 2022.[92]

114. Further studies, such as Qin et al. (2021), estimated USD 540 million in MEV was extracted from December 2018 to August 2021, with single profits reaching up to USD 4.1 million.

[89] Quin et al (2021) note that of the 750,529 sandwich attacks that they identified over 32 months between December 2018 and August 2021, 18% used different accounts to issue the front- and back-running transactions.

[90] Flashbots was formed in 2020 by Alexandre Obadia, Philip Daian and Stephane Gosselin as a non-profit organization with the objective to 'mitigate the negative externalities posed by MEV to stateful blockchains, starting with Ethereum'

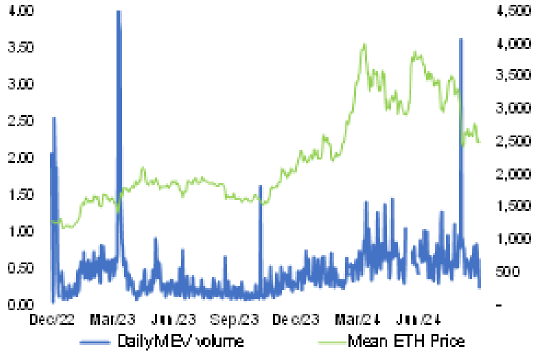
[91] See: Flashbots. MEV Explore (flashbots.net)

[92] See: https://x.com/EigenPhi/status/1630266577894375425 https://explore.flashbots.net/

Another source, Chorus One, estimated pre-Merge MEV profits from arbitrage and liquidations at USD 710 million, which is largely consistent with Flashbots' estimates.[93]

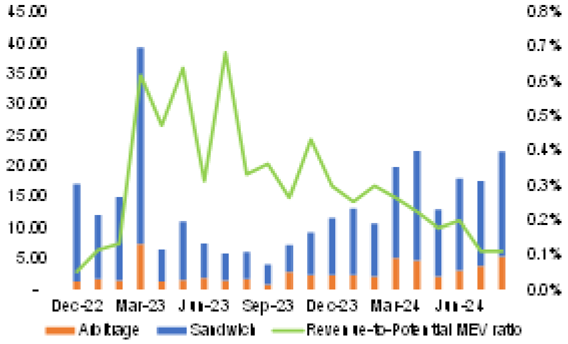
115. For more recent estimates, EigenPhi, an MEV data specialist, takes a more encompassing approach that considers not only the *actual* extracted MEV but also the *potential* extractable MEV, i.e., the total MEV that could be extracted in theory.[94] From December 2022 until August 2024, the cumulative extractable MEV on Ethereum according to EigenPhi's estimates totalled USD 290 billion, with huge daily variations (Chart 13). A tiny share, 0.3% on average, of this extractable MEV was extracted (Chart 14), for a total of USD 851 million in revenues and a cumulative profit, net of costs, of USD 393 million over the period.

Chart 13. Extractable MEV and Ether price



Note: On the left axis, daily MEV volume in Ethereum (USD bn), considering arbitrage activities and sandwich attacks. On the right axis, Mean daily spot price of ETH cryptocurrency (USD).
Sources: Eikon, EigenPhi, ESMA

Chat 14. Extractable MEV and extracted MEV



Note: On the left axis, monthly extractable MEV volume classified by technique (USD bn). On the right axis, the percentage of revenues relative to monthly extractable MEV volume.
Sources: EigenPhi, ESMA

116. By way of comparison, Flashbots estimated that the realised extractable value (REV)—or the portion of MEV that the block proposer receives—totalled 526,207 Ether between the Merge and early June 2024.[95] This is equivalent to around USD 1.1 billion, when considering the average Ether price over the same period. Sorella Labs estimates that since 2023, total profits from MEV on Ethereum totalled USD 1.04 billion *when including MEV from arbitrage between DEXs and CEXs*.[96] A high-level overview of these estimates is presented in Table 3.

Table 3. Estimated MEV profits (USD mn)

	Prior to the Merge	2023	2024
Flashbots Explore [1]	675	-	-
Flashbots Transparency Dashboard [2]	-	577	388
Chorus One [3]	1,920	-	-
EigenPhi [4]	94 (for 2022)	310	75
Sorella Labs [5]	-	554	487

[1] Gross extracted MEV from arbitrage and liquidations covering 9 protocols.
[2] REV profits accrued to proposers (computed as the difference in the proposer's balance before and after a block is proposed) from arbitrage and liquidations covering 9 protocols. Data for 2024 as of mid-June.
[3] Extracted MEV from arbitrage and liquidations (USD 710mn), and sandwich attacks (USD 1210mn).
[4] REV profits from arbitrage, sandwich attacks and liquidations. Data for 2024 as of August.
[5] REV profits from arbitrage, sandwich attacks, just-in-time liquidity, plus CEX-DEX transactions. Data for 2024 as of August.

117. The amount of extractable MEV tends to increase when valuation levels and transaction volumes for crypto-assets increase (Chart 13). For example, the peak observed in March 2023

[93] Distribution of MEV Surplus | Galaxy

[94] See: How EigenPhi Identifies MEV | EigenPhi Classroom (gitbook.io)

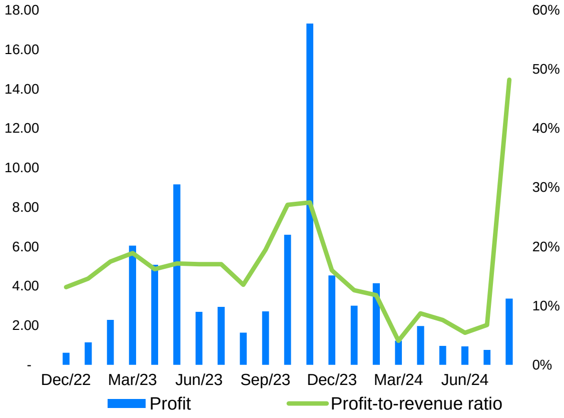
[95] Flashbots Transparency Dashboard. Data last updated as of 9 June 2024

[96] Sorella (sorellalabs.xyz)

coincided with the temporary de-peg of the stablecoin, USD Coin, following the collapse of Silicon Valley bank.[97] This is consistent with Wahrstätter et al. (2023) who find empirical evidence that moments of crisis amplify MEV revenue. According to their research, the FTX collapse and the USD Coin de-peg boosted MEV revenues by 400% and 1000% respectively for several days, when compared to the baseline. The same paper finds that MEV opportunities are not equally distributed on Ethereum where from September 2022 to May 2023 just 20% of MEV operations captured 72% of the total revenues.

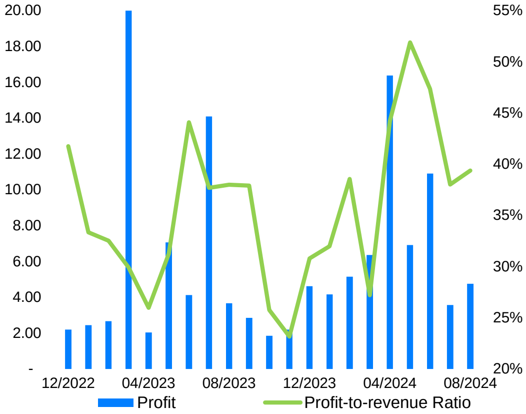
118. The MEV extractable by means of sandwich attacks has been significantly higher (by a ratio of 4 to 1 on average) than the MEV extractable by means of arbitrage since the Merge (Chart 15). However, looking at the extracted MEV, arbitrage has yielded higher profits on average and at a lower cost, although with higher variations through time (Chart 16).

Chart 15. Sandwich MEV: profit and profit-to-revenue ratio



Note: On the left axis, MEV monthly profits extracted with sandwich attacks (USD mn). On the right axis, profit as a percentage of the revenues of such activities.
Sources:EigenPhi, ESMA

Chart 16. Arbitrage MEV: profit and profit-to-revenue ratio



Note: On the left axis, MEV monthly profits extracted with arbitrage activities (USD mn). On the right axis, profit as a percentage of the revenues of such activities.
Sources:EigenPhi, ESMA

MEV creates negative externalities for users, but can also provide some marginal benefits

119. Because MEV is a zero-sum game, profit accrued to MEV extractors is necessarily at the cost of another agent in the block-building value chain, which in most cases is the end user of a DeFi platform. In short, MEV shifts wealth from ordinary users to MEV searchers and validators. MEV extractors—sometimes just an individual running a single algorithm or a trading bot—can accrue serious profits in a short timeframe. To illustrate, a bot specialising in MEV extracted USD 34 million over three months in May 2023 through a series of sandwich attacks.[98]

120. MEV increases competition for block space among players by incentivising them to bid higher fees to have their transactions executed in the next block, which can translate into higher execution costs for everyone. This happened in 2021, when MEV extraction ballooned with the development of arbitrage bots and priority gas auctions. In this case, bots spammed multiple orders with increasingly higher gas fees up to the point where their margin was eliminated, and simultaneously cancelled orders. MEV activities can also weigh on the efficiency of the blockchain by artificially inflating the volume of transactions, which causes network congestion and latency issues with negative outcomes for users.

[97] In March, the second largest stablecoin, USD-Coin (USDC), temporarily lost its peg when Circle, its issuer, revealed a USD 3.3bn exposure to failing Silicon Valley Bank (around 8% of its reserves at that time). It took it three days to recover its peg, after US authorities stated that SVB creditors would be repaid in full.

[98] Jaredfromsubway.eth's MEV bot rakes in millions of dollars in three months | The Block

121. At the same time, certain MEV extraction activities can help mitigate inefficiencies found in DeFi protocols. For example, arbitrage helps DEXs keep their prices synchronized with other DEXs and the wider market. Like in traditional finance, where arbitrage contributes to more efficient financial markets, this reduces market fragmentation and enhances market liquidity with positive outcomes for users.

122. Front-running and sandwich attacks are more problematic as they are intentionally designed to profit from ordinary users' transactions and would typically be considered unlawful (or potentially prohibited) in traditional markets. Still, they can have some indirect positive outcomes, e.g., faster execution, although this comes at the cost of worse prices. Further, MEV can accelerate liquidations, which means lenders are repaid more rapidly when borrowers fall below the specified collateralization ratio.

MEV poses risks to network security and decentralisation

123. In addition to the negative externalities for end-users of DeFi protocols, MEV has the potential to act as a force for centralisation, which is at odds with the value proposition of blockchain technology. MEV techniques have become increasingly sophisticated and require important skills and resources, e.g., high computing capabilities, which favours big players. This phenomenon could be self-reinforcing: the more MEV operators extract, the more resources they can re-invest in MEV strategies, crowding out smaller players in the block-building value chain. The resulting concentration of validation power could potentially introduce censorship and undermine network security. In this hypothetical scenario, a dominant validator could decide to delay or block the execution of certain transactions or several validators may collude to manipulate the blockchain's consensus.

124. Another risk to the security of the network stems from the incentives that MEV creates for validators to re-write the history of blocks, undermining blockchain integrity. Daian et al. (2019) have argued that if the available MEV exceeds block rewards, validators would have an interest in reorganising previous blocks to extract past MEV in what is known as a 'time-bandit attack'.

2.5.2 MEV counter-measures

125. Various industry-led initiatives are underway to address the negative externalities of MEV. These counter-measures can be placed in two broad categories depending on the externalities they intend to address.[99] The first category, which seeks to minimize the centralising effects of MEV, tends to see it as an integral part of decentralised systems and a necessary incentive for validators to maintain the network. Proponents of this approach are more concerned with maintaining decentralisation and system stability by making MEV extraction more accessible, efficient and decentralised; something that is sometimes referred to as 'democratising' MEV. The proposer-builder-separation (PBS) framework proposed by the Ethereum Foundation, which introduces a mechanism to decouple block-proposing from block-building, falls into this category.[100]

126. The second category comprises those measures aimed at eliminating (or at least reducing) harmful forms of MEV for end-users by making order manipulation virtually

[99] The approaches in each of the two categories can lead to different and sometimes contradictory outcomes. The first category, for example, may not have a primary objective of limiting losses to users but it can provide certain indirect benefits to users, e.g., lower network congestion.

[100] "Instead of the block proposer trying to produce a revenue-maximizing block by themselves, they rely on a market where outside actors that we call block-builders produce bundles consisting of complete block contents and a fee for the proposer, and the proposer chooses the bundle with the highest fee. The proposer's choice is reduced to picking the highest-fee bundle [...]" Vitalik Buterin, Proposer/block builder separation-friendly fee market designs, ETHEREUM RESEARCH: BLOG: ECONOMICS (June 4, 2021), source: [Proposer/block builder separation-friendly fee market designs - Economics - Ethereum Research (ethresear.ch)]

impossible. Examples include initiatives intended to enforce a deterministic order of transactions, e.g., a first-come, first-served order sequencing.

127. Each of the two paradigms for MEV counter-measures has its own flaws and limitations in their current state of development. And while there is no consensus on the *best* counter-measures at this point, the second approach focused on limiting consumer harm tends to be a focus of academics. However, it is the first approach that is being widely deployed in practice thus far. Notwithstanding the important technical challenges involved, the limited uptake of the second approach may be attributable to the lack of incentives for validators and other agents in the block-building value chain as it would effectively translate into lower MEV revenues for them.

128. More recent initiatives, which purport to capture the benefits of both approaches, are explored further in Annex 3. In contrast to the common refrain from industry stakeholders that MEV is a necessary component of blockchains, our analysis finds that MEV should not be considered as unavoidable. However, effective technical solutions to address the MEV problem are still an area of ongoing research.

Initiatives aimed at addressing centralisation issues

129. Although PBS is endorsed by the Ethereum Foundation as a viable MEV mitigator, it has yet to be formally enshrined in the consensus protocol (known as 'e-PBS'). With e-PBS, the relay would be performed in-protocol and the trust relationship between the builder and the block proposer would be guaranteed by Ethereum. To implement PBS, the Ethereum Foundation would be required to introduce a governance proposal to update the fork choice rule on the consensus layer (i.e., the 'Beacon Chain'). Before this can be done, the Foundation would also have to resolve several critical research and design questions.[101]

130. In the meantime, an out-of-protocol software known as 'MEV-Boost' is the next closest option for PBS implementation at present. Since MEV Boost is technically not embedded in the core Ethereum protocol (it is considered a 'sidecar' component), it requires a trusted relay to implement. MEV-Boost is developed by Flashbots as the post-Merge successor to their first iteration of the software, known as MEV-Geth.[102] The adoption rate of MEV-Boost has increased rapidly since its launch and recent estimates place the share of blocks built with MEV-Boost on Ethereum between 85% and 95% (Heimbach et al. (2023)). An illustration of how MEV-Boost works is available in Diagram 5 of Annex 3.

131. The MEV Boost instantiation of the PBS framework is intended to mitigate the negative externalities of MEV in three ways:

(i) It reduces the risk of time-bandit attacks (Daian et al. (2019)) because validators are not directly focused on optimising MEV[103];

(ii) It reduces centralisation at the protocol level because even smaller validators can accrue MEV revenues[104];

[101] PBS could in principle be instantiated as part of the core Ethereum protocol, into what is known as enshrined-PBS but this poses several challenges, many of which are active research questions.

[102] Rpc.flashbots.net. Mev-boost overview. Overview | Flashbots Docs April 2024.

[103] PBS reduces MEV's effect on consensus by removing MEV extraction from the purview of validators. Still, this does not exclude validators totally from MEV-related income, as builders must bid high to get their blocks accepted by validators. Nevertheless, with validators no longer directly focused on optimizing MEV income, the threat of time-bandit attacks reduces. MAXIMAL EXTRACTABLE VALUE (MEV) (gate.io)

[104] The use of a relay and a commit-reveal scheme removes the need for builders to trust validators. This lowers the barrier for solo validators to benefit from MEV (otherwise, builders would have an incentive to favour large pools with good reputation and conduct

(iii) It makes transaction censorship at the protocol level difficult as validators can act as protectors against censorship by builders[105].

Benefits and limitations of initiatives aimed at addressing centralisation issues

132. Anecdotal evidence suggests that MEV-Boost (and its predecessor MEV-Geth) lowered network congestion and hence gas fees on Ethereum by moving MEV-related activity off-chain. Capponi et al. (2024) argue that PBS reduces and even eliminates centralisation among validators by enabling them to access blocks from the highest-bidding builders regardless of their size. This is consistent with the stated objective of PBS. However, the same paper finds an emerging trend towards centralisation within the builder market, with benefits accruing to those builders who possess advanced capabilities for identifying lucrative MEV opportunities. These advanced capabilities allow certain builders to secure order flows at lower costs, making their blocks more competitive.106 Capponi et al. (2024) also observe that PBS transforms incentives in the builder market towards generating and securing more MEV. This leads to an overall increase in the total MEV and in turn potentially greater harm to ordinary users.

133. Heimbach et al. (2023) observed that the top three builders: Flashbots, builder0x69, and beaverbuild,[107] consistently accounted for more than half of all blocks produced between 15 September 2022 and 15 March 2023.[108] Centralisation is even more prominent in the case of relays (although it has been trending downward).[109] The Flashbots relay is the largest, consistently accounting for more than half of all blocks proposed in the PBS framework from November 2022 onwards and accounting for more than half of all (including non-PBS) blocks between November 2022 and January 2023.

134. Centralisation at the level of builders or relays does not have the same negative consequences for the integrity of the network as it would at the validator level because builders and relays do not influence the protocol's voting mechanism for validating transactions. However, it can introduce censorship issues. For example, Flashbots in 2022 announced they would censor transactions from blacklisted Tornado Cash and Heimbach et al. (2023) show that relays who advertise themselves as OFAC-compliant effectively discriminate between compliant and non-compliant blocks. In addition, centralisation creates single points of failure, which raises operational risks, e.g., in case a prominent relay or builder suffers a glitch or a cyber-attack or simply misbehaves.[110] Proposals to address risks of censorship include so-called inclusion lists, which are designed to enforce inclusion

off-chain deals with them). Similarly, validators do not have to trust builders. The validator's fee still processes even if the proposed block is unavailable or declared invalid by other validators. In the latter case, the block is simply discarded, forcing the block builder to lose all transaction fees and MEV revenue.

[105] PBS and censorship resistance, Proposer-builder separation | ethereum.org.

[106] It is worth noting in that respect that Flashbots invite searchers to co-locate with Flashbots Builders (and use FlashBots Builder) to optimise their latency.

[107] Builder0x69 seemingly originated from a former mining pool but EBA and ESMA lack further details on the organization; EigenPhi links Beaverbuild with the HFT firm Symbolic Capital Partners. See: Ethereum centralization: a single builder accounts for over half of August blocks - Ledger Insights - blockchain for enterprise but EBA and ESMA lack further details on the organization.

[108] A more recent and comprehensive list of builders on Ethereum is available here (see 'builders' section): https://mevboost.pics/. Titan Builder and RSync-Builder are currently the two largest builders.

[109] Heimbach et al. (2023) highlighted a Herfindhal-Hirschmann index fluctuating between 0.80 and 0.32 for relays between October 2022 and March 2023, to be compared with 0.67 and 0.21 for builders. An industry with a HHI index above 0.25 is said to have high concentration, while a HHI between 0.15 and 0.25 indicates moderate concentration.

[110] There should be a strong incentive for a relay to act faithfully, otherwise builders and validators would use another relay. The same holds true for builders. However, possible misbehaviour cannot be discarded.

of certain transactions that might be at risk of censorship but require that some honest validators observe the transactions. [111]

Initiatives intended to make order manipulation infeasible

135. In traditional finance, fair-ordering is usually understood as first-come-first-served and straightforward to implement thanks to the existence of an intermediary who manages an orderbook based on transactions timestamps. But as discussed previously, in the absence of a central intermediary, blockchains do not have a 'natural' time-based ordering. Instead, transactions originate from any of the network's distributed nodes (sometimes simultaneously) before they enter a common queue known as a mempool. While a large body of literature has developed around the concept of fair ordering on blockchains, practical deployments are still limited so far.[112] Solutions currently under development follow the principle that the ordering of transactions should be determined independently of the contents of the orders. The envisaged solutions fall into two categories: time-based ordering and blind ordering.

136. **Time-based ordering**, as presented by Kelkar et al. (2020), requires the ordering of transactions received by a sufficiently large fraction of honest nodes to be preserved. Where this is not possible for practical and technical reasons, the authors concede it can be done on a block-ordering basis. Another method would involve nodes maintaining synchronised local clocks to confirm a common timestamp for all incoming transactions.

137. **Blind ordering** typically involves a commit-and-reveal protocol, which receives user commitments (a request to include a transaction in a block) along with some metadata (e.g., the transaction fee). The commit-and-reveal function can be instantiated through to a trusted layer such as time-lock encryption or a hardware-based 'trusted execution environment' (TEE). Once this step is achieved, validators determine an ordering based on the commitments, then the protocol opens the commitments, and the transactions are executed.

138. Fair-ordering solutions are purpose-built to mitigate the risk of harmful order manipulation for users, but they introduce other shortcomings. Blind ordering is generally considered weaker than time-based ordering because it may not fully eliminate the risk of front-running. For example, the leakage of ancillary information (i.e., metadata such as gas price or address) may still be sufficient to run an attack. An important drawback of timed-based ordering is that it creates a speed race between users, and hence creates incentives to co-locate computing for execution and node consensus, similar to high-frequency trading in traditional finance. Fair-ordering solutions can also introduce centralisation depending on the exact framework used to order transactions.

[111] See for example Fork-Choice enforced Inclusion Lists (FOCIL): A simple committee-based inclusion list proposal - Proof-of-Stake / Block proposer - Ethereum Research (ethresear.ch)

[112] For more on transaction fairness definitions in blockchains, see Li R., Hu X., Wang Q. and Duan S., 2023. 'Transaction fairness in blockchains, revisited', available at: Transaction Fairness in Blockchains, Revisited (iacr.org)

3. Lending, borrowing and staking of crypto-assets

139. This Chapter aims to provide an overview of the EBA and ESMA's understanding of the main categories of business models of crypto lending, borrowing and staking activities, an approximation to the dimension of the engagement of EU consumers and financial institutions with those activities, and assesses the potential risks associated to them.

140. The lending, borrowing and staking of crypto-assets take many forms in practice. Overall, they can be divided into centralised or DeFi settings, as both have gained significance in crypto markets. Centralised lending and borrowing providers became the centre of crypto market failures during 2022 (see more on the failures of Celsius and Voyager in Annex 8). DeFi lending has recently been the subject of research by international bodies, such as the BIS (see Aramonte et al, 2022, Cornelli et al, 2024 or Heimbach and Huang, 2024) or the OECD (see Brodesky and Nassr, 2023), as well as by monetary authorities such as the ECB (Born et al, 2022) or the Bank of Canada (Chiu et al, 2023). Finally, staking has become the main use case in DeFi, and has become the subject of relevant innovations, such as liquid staking and restaking, worth analysing and monitoring.

3.1 Business models of crypto lending, borrowing and staking

141. To analyse the lending and borrowing services provided by EU-based entities and estimate of the size of EU markets, this section sets out the typical business models identified in EU-based providers of crypto lending and borrowing services.

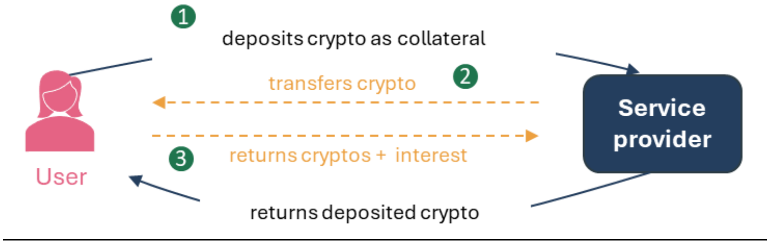
3.1.1 Lending of crypto-assets

142. Crypto-asset lending refers to the activity consisting of a *provider (lender) transferring a certain value of crypto-assets or funds to a user (borrower) in exchange for the user placing a certain value of crypto-assets or funds as collateral and a commitment that the borrower will return to the lender a value equivalent to the transferred value of crypto-assets or funds and potential additional interests on a future date (or in the event of some other trigger event) to the lender*[113] (see Diagram 1 below for a generic representation of crypto lending services). The provision of crypto lending services can be intermediated by centralised entities or DeFi protocols.

Centralised crypto lending services

143. Centralised crypto lending activities are those provided by either specialised crypto-asset lending platforms or CASPs who offer the lending of crypto-assets as part of a wider range of

Diagram 2: Pictorial representation of crypto-asset lending services



[113] Crypto lending may resemble securities and commodities lending.

services. They offer those services to retail customers, institutional clients or both.

144. Crypto lending most often relies on over-collateralisation, rather than creditworthiness checks from lenders – i.e. customers place crypto-assets or funds as collateral in an account held at the service provider to obtain the loan, usually of a higher value than the loan. The collateralisation ratio typically varies per crypto-asset used as collateral and the crypto-asset received in the loan, with riskier or more volatile crypto-assets being subject to higher collateralisation requirements.

145. Lenders typically compete in "loan-to-value" (LTV)[114] ratios offered in their marketing communications. The LTV ratio acts as a minimum requirement, with crypto borrowers often placing higher collateral ratios than those required by lenders, to mitigate potential collateral liquidation risks. LTV typically ranges from 20% to 80%, with a higher LTV (e.g., 80%) meaning the borrower has more debt relative to the collateral.

146. Regarding the range of crypto-assets accepted as collateral in crypto loans, they can consist of a large number of crypto-assets, but a majority of lenders accept mainly the crypto-assets with the most liquid markets (BTC, ETH) and the stablecoins with the largest market capitalisation and most liquid markets (USDT, USDC). Moreover, a few lenders also accept utility tokens issued by the service provider itself (or an affiliated entity) as collateral for crypto loans. This is normally offered on the basis of stricter LTV requirements (between 20% and 66%), as compared with other crypto-assets.

147. To cover against the volatility of crypto collateral, some lenders include liquidation mechanisms in their services. Such mechanisms rely on a specific LTV value, typically approx. 85%[115], which, if reached, triggers the liquidation of the loan in favour of the lender. Liquidations fees (approx. 2% of the loan amount) are charged on borrowers. When their loans are at risk of liquidation, borrowers are often given a 'grace period' to post more collateral to avoid the triggering of the liquidation mechanism, although to avoid liquidation, borrowers normally over collateralise their loan even above the required LTV ratio. Similarly, some lenders also offer their customers the possibility to release excess collateral when the collateralised assets of a crypto loan increase their value over a certain rate (e.g. 10%). In such cases, borrowers can release a portion of the collateral initially placed for the crypto loan, and use to back other crypto loans, or for any other purposes.

148. In centralised lending, loans typically have a length varying between 1 to 36 months, with borrowers required to return the loaned assets at maturity (with some lenders charging a repayment fee of approx. 0.25%).

149. The revenue model for lenders normally includes fixed interest rates to be paid by borrowers at the end of the loan term or variable rates for loans without a predetermined term. Interest rates typically range from 8% to 15%, and can vary depending on the term, denomination, LTV and degree of customer loyalty level. Some rates, however, are offered at higher level than 15%, with a few lenders offering, for specific crypto-assets and during specific periods, rates that go beyond conventional usury levels[116]. Moreover, some crypto lenders charge loan origination fees (ranging from 1.5% and 2.5%) and/or early repayment fees (approx. 2.5%). Crypto lenders may also earn revenues through market-making activities on collateral assets.

[114] Loan-to-value (LTV) refers to the ratio of the loan amount to the value of the asset (collateral) used to secure the loan.

[115] However, a service provider was found to be applying multiple thresholds, after which automatically email notifications are sent to users to inform them about the worsening of the LTV of their loan and approximation to the liquidation threshold.

[116] According to information publicly available in some providers' websites, the EBA and ESMA have identified annualised interest rates above 21%, which go as far as 81%, for the most volatile crypto-assets.

DeFi lending services

150. Crypto lending activities are also provided via DeFi protocols. DeFi lending, as centralised lending, also relies on over-collateralisation[117] and no intermediary in DeFi governance arrangements undertakes creditworthiness checks on specific DeFi market participants[118]. The possibility to undertake unrestricted leverage-based strategies has been one of the key drivers for the attractiveness of DeFi lending activities (OECD, 2022). DeFi lending allows investors to follow strategies that consist of either taking a long position[119], when the expectation is that volatile crypto-asset prices will rise, or a short position[120], in the opposite market sentiment (Carey and Melachrinos, 2022).

151. There are two main types of DeFi lending protocols: collateralized debt position (CDP) and collateralized debt markets (CDM).

152. A **collateralized debt position (CDP)** is a mechanism under which borrowers are able to take out loans from DeFi protocols by locking up crypto collateral they own in a smart contract, minting or borrowing new assets (typically, stablecoins) against that collateral. In CDP-based DeFi lending, the list of eligible collateral crypto-assets can be quite broad, including, as in centralised crypto lending, the crypto-assets with the most liquid markets (e.g. BTC, ETH), as well as other crypto-assets – e.g. governance tokens of the protocol as collateral, on the basis of stricter LTV requirements (between 20% and 66%[121]).

153. In **collateralized debt markets (CDM)**, borrowers lock up collateral to take out loans, but instead of minting or borrowing new assets (e.g. stablecoins) directly from the protocol (like in CDP), they borrow assets from other users (lenders) who deposit their assets into the DeFi lending protocol. That is, CDM-based DeFi protocols intermediate (in automated ways via smart contract-based protocols) between potential borrowers and lenders.

154. There are two types of CDM-based DeFi protocols. On one side, **Peer-to-Peer (P2P) lending** protocols, that match prospective borrowers and lenders. In this case, a borrower creates a loan request in the protocol, specifying the amount they would like to borrow, the type of collateral they hold, the interest rate they offer to pay and the term of the loan they seek. Lenders can search for loan requests and choose the loan they find attractive or matches their interests. Once a lender chooses an offer, the borrower deposits the collateral assets into the smart contract deployed and indicated by the protocols, and the lender sends the assets of the loan to the same smart contract, which redirects them to the borrower.

155. On another side, **pooled lending** protocols (also called 'peer-to-pool lending') do not require direct interaction between borrowers and lenders, but instead, intermediate loans via

[117] While there are a few DeFi protocols allowing users to access 'flash loans', which are uncollateralized because the loan and its repayment are executed within the same transaction in a blockchain, these are not covered in this report, due to their rather small relevance in DeFi markets. According to Defillama, the TVL of all uncollateralized lending protocols accounts for 12.94 million USD.

[118] Even though the EBA and ESMA observe that some companies and DeFi protocols are developing solutions to automate checks of the history of transactions of a blockchain address, and hence, of the credit worthiness of a DeFi user, mainly via so-called zero-knowledge proof techniques. There are also proposals to create KYC pools between institutional crypto borrowers and participant lenders. However, overall these solutions are still not gaining sufficient traction in the market, and the largest DeFi lending protocols are still not implementing such solutions.

[119] A long position strategy consists of depositing a volatile crypto-asset as collateral and borrowing a less volatile crypto-asset (e.g. a stablecoin). The less volatile crypto-asset can then be exchanged for the volatile crypto-asset in an exchange services provider, and the user can again borrow crypto-assets, increasing their leverage. If the price of the volatile crypto-asset increases, the user makes a profit; if the price declines, the user incurs a loss, and potentially a liquidation.

[120] A short position strategy consists of depositing a non-volatile crypto-asset and borrowing a volatile asset, with the user making a profit if the price of the volatile crypto-asset declines (Brodesky and Nassr, 2022).

[121] According to EBA and ESMA's desk-based research, including the websites of relevant DeFi lending protocols.

'liquidity pools' (LPs). The DeFi protocol sets up a LP for each specific crypto-asset, with specific conditions defined for the pool of each asset. Pooled lending models have become the most popular in DeFi (see Box 4 below for more details on pooled lending models in DeFi).

156. In all DeFi lending models, if the value of the collateral drops below a certain threshold (similar to LTV ratios in centralised lending), the protocol triggers a liquidation system to repay the loan and protect the protocol from under-collateralized loans[122]. Typically, the liquidation is automatically activated[123], and protocols typically offer the collateral in auction[124] [125]. In all cases, the borrower whose assets were liquidated is subject to liquidation fees.

<u>Box 4. Pooled lending in DeFi</u>

Lenders deposit amounts they hold of a specific asset into its corresponding LP (see more on DeFi borrowing in paragraphs 153-155), and borrowers can place an order in the protocol's smart contract to borrow from the LP. In order to do so, the borrower must deposit required collateral (LTV ratios often range between 20%, for the most volatile crypto-assets, and 90%, typically only for stablecoins) in the pool's smart contract.

The list of crypto-assets on which LPs are set up is quite broad, with pooled lending protocols normally doing so for the most liquid assets, such as BTC, ETH or the stablecoins with the largest market capitalisation. However, pooled lending protocols also often offer LPs for their own governance tokens or for the governance tokens issued by other DeFi lending protocols. LPs for governance tokens may be particularly fragile, due to their volatile nature and potential sudden loss of value. To facilitate the liquidity and interoperability of DeFi markets, they also offer LPs for 'wrapped tokens'[126].

Each LP normally offers a variable 'borrow APY' and a variable 'supply APY', with APYs determined algorithmically based on market conditions of supply and demand[127]. See Annex 6 on interest rates (e.g. APYs) paid by borrowers in a few DeFi (pooled) lending protocols.

The revenue model for DeFi lending protocols is based in the interest rate spread between the rate paid by borrowers and the rate paid by the protocol to lenders. That spread often ranges around 0.20% and 2% for the largest LPs, but it can be as large as 25% for few smaller LPs (see Annex 6).

In addition to interest rate spread, DeFi lending protocols may obtain revenues from charging borrowers origination and withdrawal fees (often ranging between 0.1% and 0.5%) or liquidation fees, when liquidation is automatically activated (they typically vary based on the type of assets, and often range from 5% to 15%). Additionally, due to the existence of LPs for governance tokens, including those issued

[122] When their loans are at risk of liquidation, crypto borrowers can post more collateral to the smart contract where the loan was executed, to avoid the triggering of the automatic liquidation mechanism. As explained in BIS (2022), to avoid forced liquidation, borrowers in fact normally add more crypto-assets to their accounts than the minimum required, leading to a higher effective collateralisation ratio than the prescribed minimum by the protocols. Conversely, some protocols offer their customers the possibility to release excess collateral, when the collateral of a crypto loan increases their value over a certain rate (e.g. 10%). In such cases, borrowers can release a portion of the collateral initially placed for the crypto loan, and use it to back other crypto loans.

[123] The liquidation threshold often ranges between 40% (for the most volatile crypto-assets) and 95% (typically only for stablecoins).

[124] Protocols incentivize 'liquidators' (anyone who can detect and take action) to liquidate loans. But, as any blockchain network participant may liquidate default positions, but spotting liquidation opportunities can be technically challenging, competition can be costly and earnings can be limited. Recently market participants have set up 'bots' that can automate the task of spotting liquidation opportunities and quickly executing the liquidation. According to Xu et al (2020), while liquidations are typically associated to a few market events, there is a trend of rising amounts of liquidated collateral in DeFi lending. With the use of bots, liquidation efficiency appears to be high - e.g. approx 60% of liquidations are executed in the same block as the one triggering the liquidation, while 85% of liquidations occur only after 2 blocks, and 95% after 16 blocks.

[125] However, Iin P2P lending, the lender retains some flexibility in deciding when to trigger the liquidation, with even the liquidation conditions being open to negotiations and customization during the lending agreement phase.

[126] Wrapped tokens allow non-native tokens to be used on different blockchains, by "wrapping" tokens that are native to one blockchain (e.g. BTC in Bitcoin) as synthetic or tokenized representations in other blockchains (e.g. WrappedBTC in Ethereum). Additionally, in certain blockchain network, such as Ethereum, the standard for the creation of tokens requires crypto-assets to follow a specific format for their easy integration with DeFi protocols. As a result, even tokens that are native to one blockchain (e.g. ETH in Ethereum) are wrapped (e.g. WETH, to make it compatible with ERC-20).

[127] When borrowing demand is high, interest rates are increased to incentivize more lending, and vice versa.

by the DeFi lending protocol itself, the governance tokens can become another source of revenue for protocols, as their issuance can attract liquidity providers (lenders) and borrowers to the market, driving growth and increasing the value of the tokens. Furthermore, DeFi protocols can own their own liquidity – i.e. rather than relying solely on external liquidity providers (lenders), the protocol may also be a liquidity provider itself and collect a significant share of the rates generated from the liquidity provision (lending). The EBA and ESMA note that, according to evidence[128] one single DeFi lending protocol's fees largely dominate the DeFi lending market, accounting for well above 50% of all fees obtained in the market for at least the period between 2022 and 2024.

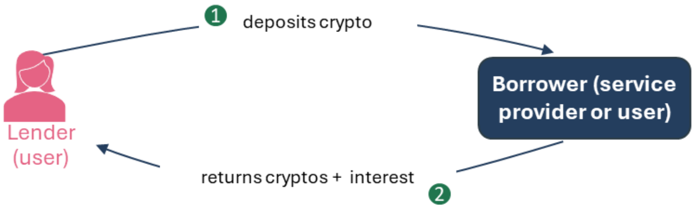
3.1.2 Borrowing of crypto-assets

157. Crypto-asset borrowing refers to the activity consisting of *a user (lender) transferring a certain value of crypto-assets or funds to a another user or the provider (borrower) in exchange for a commitment that the borrower will return to the lender a value equivalent to the transferred crypto-assets or funds and potential additional interests on a future date (or in the event of some other trigger event)*[129]. The provision of crypto borrowing services can be intermediated by centralised entities or via DeFi protocols, which often attract users in search for yields on their crypto-asset holdings (see Annex 7 for a list of other DeFi activities attracting users with yields).

Centralised crypto borrowing services

158. Centralised crypto borrowing activities are those provided by either specialised crypto-asset platforms or crypto-asset services providers who offer their users to earn yields on their holdings of crypto-assets[130] as part of a wider range of services. Crypto borrowing activities are provided to either retail customers, institutional clients or both.

Diagram 3: Pictorial representation of crypto-asset borrowing services


1
deposits crypto
Lender (user)
Borrower (service provider or user)
returns cryptos + interest
2

159. Centralised crypto borrowing is typically offered either with the provider acting itself as the direct counterparty to the user's loan (see Diagram 3 above), or the provider matching lenders with interested borrowers. When the provider acts as an intermediary, it may do so on its own or via a third party acting as a provider which ultimately connects the lender with interested borrowers (see Diagram 4 below). Both the provider or the third party acting as an intermediary may connect with borrowers that are their customers or may even do so via DeFi protocols[131].

160. Where a third-party acts as the intermediary, it is responsible for the assessment of the creditworthiness of borrowers. In exchange, they typically charge commission fees to lenders, representing a portion of the total rewards obtained from borrowers (typically ranging between 15% and 30%). Interest paid to lenders typically ranges from 4% to 16% for lending stablecoins and from 5% to 13% for lending other crypto-assets.

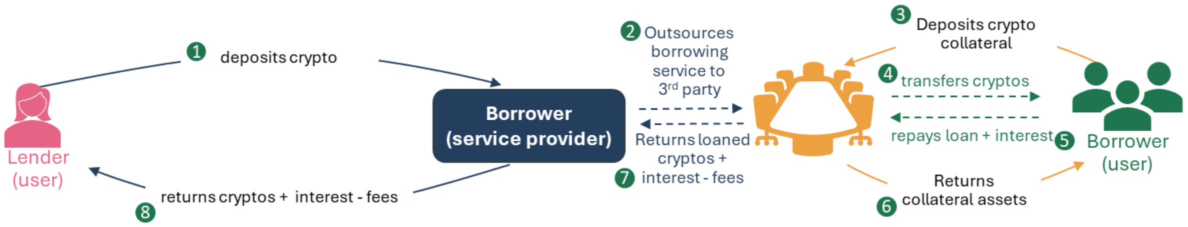
[128] See https://defillama.com/fees?category=Lending or https://tokenterminal.com/terminal/markets/lending

[129] The structure of crypto borrowing services may resemble those offered by credit institutions in the EU with deposit accounts.

[130] Such services are often called "earn", "custody lending" or simply "borrow" services.

[131] In such cases, the lender may not directly participate in DeFi, which is only used by the intermediary to find interested borrowers.

Diagram 4: Pictorial representation of crypto borrowing when a 3rd party connects lenders with borrowers


1 deposits crypto
Lender (user)
Borrower (service provider)
2 Outsources borrowing service to 3rd party
Returns loaned cryptos + 7 interest - fees
3 Deposits crypto collateral
4 transfers cryptos
repays loan + interest 5
Borrower (user)
Returns 6 collateral assets
8 returns cryptos + interest - fees

DeFi borrowing services

161. DeFi borrowing activities are provided by the same protocols that facilitate pooled lending, as analysed in Box 4. The same way those protocols lend users crypto-assets if they deposit crypto collateral in a liquidity pool, protocols allow DeFi users to deposit their crypto-asset holdings in liquidity pools to lend them to other users and earn interest in exchange[132]. In doing so, lenders become liquidity providers in DeFi. In fact, lenders can often create LPs and earn interest on a wide range of crypto-assets, as long as they have a liquid and deep market.

162. Each LP normally offers lenders a variable ‘borrow APY’, with APYs determined algorithmically based on market conditions of supply and demand[133], and they are usually differentiated between a ‘base APY’ and a ‘rewards APY’. The base rate is the interest rate that a user (lender) earns purely from lending their assets on the protocol, without any additional incentives or bonuses. The rewards rate is instead an additional yield offered to lenders (and sometimes borrowers) as an incentive to participate in the protocol, typically paid out in the form of governance tokens, with the aim to attract liquidity and participation.

163. DeFi borrowing therefore can attract new users thanks to protocols’ promise or claim to users about future earnings (see Annex 6). “Search for yield” is a key determinant of liquidity provision in DeFi, especially for retail users[134] (Cornelli et al, 2024) and potential high rates promised to lenders have been an important driver of DeFi lending and borrowing activity (Born et al, 2022), given the low interest rate environment and search for yield by investors (see Annex 6 for a comparison between yields in DeFi and traditional finance).

3.1.3 Staking activities

164. This section begins by defining and scoping the various methods of staking. It examines the risks stemming from each of these staking methods and the corresponding disclosure practices by entities offering staking activities. Next it looks at the developments referred to as “liquid staking” and “restaking” and the resulting interconnectedness between staking and other value-added activities, which can offer new opportunities for liquidity and yield but also may contribute to systemic risk when interacting with composable DeFi services.

Key features

165. The term ‘staking’ is often used in crypto-asset markets, interchangeably with terms such as “earn” and “yield farming”, to refer to a number of different activities. However, for the

[132] Those services should not be confused with non-custodial staking, which is analysed in Section 3.4.

[133] See: https://defillama.com/yields

[134] The ‘low-for-long’ interest rate environment may have pushed retail investors to ‘search for yield’ by depositing crypto to obtain interest in DeFi. But, as a result, retail investors may ‘fly to safety’ more quickly than institutional investors as interest rates normalise.

purposes of this report, the term 'staking' refers to "*the process of immobilizing crypto-assets to support the operations of PoS and PoS-like blockchain consensus mechanisms in exchange for the granting of validator privileges that can generate block rewards*", as set out by a Commission Q&A on staking and MiCAR published in June 2024[135][136]. In this sense, only the native tokens of PoS or PoS-like blockchain can be used to contribute to the network's consensus and security protocols, and therefore be staked[137]. Staking operates differently on each blockchain. On Ethereum, the activation of a single validator node involves running the specific software and staking of the 32 ETH required to operate it[138][139]. Active validator nodes then have multiple (potential) roles: first, each block is "attested to" by a number of validators nodes who attest to the validity of blocks gain rewards. Validators are also selected to propose blocks at random, meaning that the greater percentage of the total validating power a person operates, the more likely that person will be selected to propose blocks. Since proposing blocks offers the chance to receive additional rewards, validators are incentivised to operate multiple nodes. Nodes that become inactive or misbehave (e.g., by proposing invalid transactions) suffer financial penalties[140]. This scheme incentivises validators on Ethereum to operate several (high uptime) nodes but it also encourages the concentration of staking power among fewer node operators.

166. Although Ethereum does not natively support staking for below this threshold – and in fact encourages solo staking[141], a series of solutions have developed, giving those with the technical expertise and resources access to a broader base of capital through 'delegated staking' while also allowing those who lack such resources to participate (as delegators). This development has increased staking, which now has a market cap valued at USD 562 billion (of which Ethereum and Solana staking respectively account for USD 85 billion (18%) and USD 66 billion (13%) respectively as of November 2024[142][143]).

167. Delegated staking includes a variety of different business models, each with their own technical and economic characteristics (e.g. technical requirements, financial investment, interface, fees, offer of a liquid staking token). That said, staking services can be broadly categorised as follows:

168. **Validator-as-a-service (VaaS)**, also referred to as 'staking-as-a-service' refers to entities that facilitate access to staking to persons who have the capital necessary to operate a node on their own but may not have the technical means.[144] On Ethereum, a user with 32 ETH required for the operation of a node simply delegates these 32 ETH to the VaaS provider.

169. In **pooled staking** persons who do not have the technical or financial means to operate a validator node can participate in staking pools. In most cases, this involves depositing any amount of the native PoS token of a blockchain into a corresponding liquidity pool, the

[135] ESMA. (2024). *Q&As on MiCA*. https://www.esma.europa.eu/publications-data/questions-answers/2067

[136] Industry stakeholders consulted by the EBA and ESMA showed broad support with the use of that definition, further noting that staking is mainly seen as a technical activity designed to maintain the security of the blockchain, as opposed to a financial activity.

[137] Terms such as NFT staking and BTC staking are therefore incompatible with this definition.

[138] At the time of writing this report, worth approx. EUR 70,000.

[139] Other blockchains, such as Tezos or Avalanche, have different token thresholds or mechanisms, each designed to balance decentralization, security, and scalability in a way that suits the needs of their respective networks.

[140] See below in section on penalties and slashing

[141] Ethereum, Home stake your Eth. See: https://ethereum.org/en/staking/solo/

[142] Staking Rewards. *Proof of Stake assets overview*. See: https://www.stakingrewards.com/assets/proof-of-stake

[143] Interesting to note: while 67% of Solana is staked, only 29% of Ethereum is.

[144] The term also appears to be commonly used in the industry to refer to what can also be called custodial staking (typically provided by a crypto trading platform. Source: Staking as a service | ethereum.org

contents of which are linked to network staking contracts. Each pooled staking provider offers different technical and economic characteristics (interface, fees, use of a liquid staking token).

Centralised staking services. Many centralised providers, including crypto trading platforms, have developed a user-friendly conduit to participate in staking without the risk of safekeeping one's own crypto-asset keys. The centralised trading platform may operate its own validator nodes, or it may use a third-party operator of validator nodes (see 'validator-as-a-service' above). There are typically no thresholds for minimum capital to access the service.

Custody

170. One distinguishing characteristic of these staking models is whether the service involves custody or not, which is not a straightforward determination in crypto. Indeed, control over crypto-assets is ensured by possession or knowledge of the private key associated with a wallet. Possession or knowledge of private keys is the lynchpin for custody because, fundamentally, staking is the attribution of 'signing keys' associated with each staked crypto-asset to a node (in exchange for block rewards). Signing keys allow for participation in consensus, whereas 'withdrawal keys' allow for moving a crypto-asset between wallets or SCs.

171. Applying this standard for custody across the various models of staking allows for greater differentiation between the services. Self-stakers retain both sets of keys, non-custodial staking services (such as pooled staking) involve a transfer of signing keys to a third-party (while retaining the withdrawal keys) and custodial staking services involve transferring both sets of keys to the provider[145]. Staking services across each of these categories come with a variety of risks. For the purpose of this report, the focus is on those that are common to all, and which interrelate with existing CASP services under MiCAR or with lending or borrowing.

Distribution of staking rewards

172. Delegated staking involves the use of third-party node operators or protocols who typically compete on the basis of the share of staking rewards distributed to delegators (after fees). In the case of centralised staking providers, the fee and reward schedules vary significantly, not only across providers but also across tokens, based on market and network conditions. For example, the terms and conditions of some centralised staking providers suggest that only the consensus layer rewards are passed on to the delegator once the fee has been subtracted—not the execution layer rewards.

173. As of October 2024, the average APY on self-staking at the protocol level for Ethereum and Solana was around 3.46% and 6.73% respectively, with other networks offering considerably higher APYs (Table 4). Using data from Staking Rewards to compare these base rates with the end-user reward APYs offered by various staking providers we see yields ranging from 2.29% to 5.09% on Ethereum and 5.94% to 7.74% on Solana respectively (i.e., in some cases higher than the baseline network reward).[146] A longer discussion on staking rewards and the process of 'unstaking' is available in Annex 9.

Table 4: Staking reward rates by network

	Ethereum	Solana
Baseline	3.46%	6.73%
Min	2.29%	5.94%
Max	5.09%	7.74%

Source: Staking Rewards (APY)

[146] Staking Rewards (2024)

Liquid staking

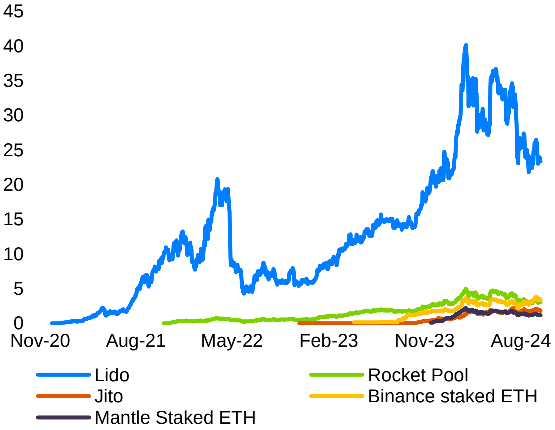
174. Liquid staking is a type of pooled (delegated) staking protocol that has witnessed massive TVL growth, particularly since the Ethereum Merge and subsequent network upgrades. Although there are different variations, in its simplest form, liquid staking involves the deposit of a user's native staking assets into a liquidity pool in exchange for 'liquid staking tokens' (LSTs) representing a certificate of ownership of the underlying staked asset. The LSTs can then be reinvested while allowing users to simultaneously earn yields from the rewards generated by their staked assets. See Annex 9 for the different liquid staking models.

175. As of October 2024, liquid staking TVL across all blockchain protocols was valued at USD 44 billion (Chart 18), with nearly 80% of the total share staked in Ethereum-based protocols. Of the USD 35 billion staked in these protocols, 70% of the market share (USD 25 billion) was staked in Lido (Chart 17). Total TVL in liquid staking increased 131% year-over-year (from USD 19 to 44 billion).

176. Demand for liquid staking is driven in part by the desire of stakers to offset potential losses due to increased vulnerability to volatility where tokens are immobilised. Indeed, since staking requires users to immobilise or 'lock' their assets onto a node for extended periods of time, this leaves users with unrealised losses when the loss of value of the asset outstrips the rewards they are receiving for their participation in staking. An unencumbered LST provides opportunities for additional returns through its use in DeFi protocols, e.g., as collateral, without relinquishing ownership of the underlying staked asset (and hence the possibility to redeem or unstake those assets). Liquid staking rewards are discussed in more detail in Annex 9.

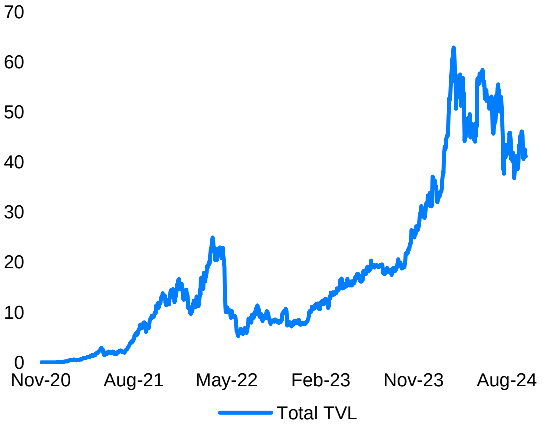
177. Liquid staking can be conducted either directly through a liquid staking provider or via centralised trading platforms who typically either 1) offer their own liquid staking token or 2) stake with a liquid staking provider on behalf of the delegator.

Chart 17. TVL of top five liquid staking protocols (USD)



Note: Historical growth of the top five liquid staking protocols by TVL (USD bn) as of Oct 2024 (any chain)
Sources: DeFiLlama

Chart 18. Total TVL of all liquid staking protocols (USD)



Note: Total TVL across all liquid staking protocols (any chain) in USD bn
Sources: DeFiLlama

Leveraged (liquid) staking

178. The emergence of LSTs has allowed for the development of leveraged staking strategies through the use of DeFi lending services. Research by Xiong, X. et al.[147] and Alexander, C.[148] highlights the development of strategies that involve the use of LSTs as collateral to obtain (over-collateralised) loans denominated in the original native staking asset on lending and

[147] Xiong, et al. (2024)

[148] Alexander (2024)

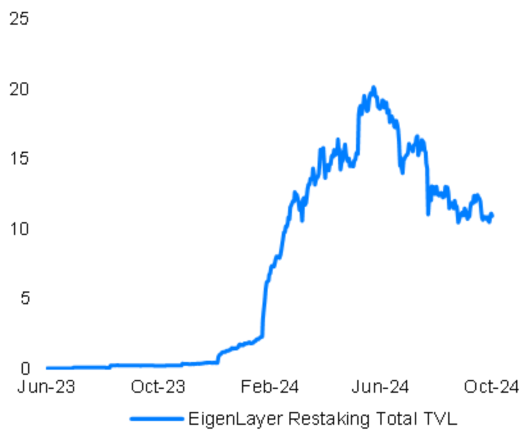
borrowing protocols. These borrowed native staking assets are subsequently staked in liquid staking protocols—a process that can be repeated multiple times. This cycle of leveraging can significantly amplify staking yields, but also introduces new risks, such as increased exposure to market volatility and liquidity risks when LSTs deviate from their underlying value.

179. While these leverage risks are discussed in more detail in section 3.3.2, leverage that involves liquid staking may introduce a special type of systemic risk in the scenario of a sharp devaluation of the LST (or a 'de-pegging' event). This is not an entirely theoretical risk. The temporary de-peg in 2022 of the most prevalent LST, Lido's stETH, demonstrates how illiquidity or sharp market corrections can lead to mass liquidations.[149] A cascade of liquidations can trigger broader instability across interconnected DeFi ecosystems and could also threaten the orderly functioning of the underlying blockchain as people unstake their assets to maintain healthy collateralisation ratios or limit losses. Moreover, the use of LSTs in leveraged positions complicates the risk management of these DeFi protocols, making them more vulnerable to adverse events outside of their control.[150]

Restaking and leveraged restaking

180. A related emerging phenomenon is 'restaking', which involves staking LSTs (or Layer 1 blockchain governance tokens) via specialised protocols to support actively validated services (AVS)[151] (instead of PoS blockchains), whose consensus mechanisms also requires staking. For a sense of scale, the largest of the restaking services is currently EigenLayer with EUR 11 billion as of October 2024 (Chart 19).

Chart 19. TVL over time of restaking on EigenLayer (USD)



Note: Total TVL of EigenLayer in USD bn
Sources: DeFiLlama

181. As compared to leveraged (liquid) staking, the observed "loop" is widened, and involves (i) the staking of tokens and receipt of liquid staking tokens (ii) the restaking of those liquid staking tokens on an AVS and the receipt of liquid restaking tokens (LRTs) and (iii) the use of LRTs as collateral to obtain (over-collaterised) loans denominated in the original native token, and (iv) the subsequent staking of the borrowed tokens, and so on.

182. The risks previously described are intensified. Notably, because the introduction of LRTs in the process involves both (i) adding on top of the layer of risk of the LST de-pegging from its value as compared to the original native token, the risk of the LRT de-pegging from its value

[149] The de-pegging of stETH occurred in mid-2022, primarily due to market fears surrounding liquidity constraints following the collapse of the Terra/Luna ecosystem. While stETH is typically pegged 1:1 to ETH, during this period, the price of stETH deviated significantly from ETH due to a sell-off sparked by concerns over centralized liquidity and macroeconomic pressures. This led to cascading liquidations in DeFi lending protocols, such as Aave and Maker, where stETH was used as collateral. The temporary loss of the peg highlighted the risks associated with over-leveraging in liquid staking environments, especially when liquidity is constrained, and market sentiment turns negative.

[150] To mitigate such risks, some DeFi platforms have introduced mechanisms such as dynamic collateral ratios, risk-based governance, and automated liquidation protections. Additionally, advancements in smart contract auditing and real-time risk assessments are being developed with the aim of preventing systemic shocks.

[151] Actively validated services (AVS) is a concept coined by the restaking protocol, EigenLayer, to mean any DLT-based module with its own distributed validation semantics for verification. E.g., data availability layers, new virtual machines, keeper networks, oracle networks, bridges, threshold cryptography schemes, and trusted execution environments. AVS are typically either secured by a native token or are permissioned. Source: EigenLayer (2023)

as compared to the LST and the original native token and (ii) because the variety of AVSs that may be secured via restaking could imply that an LRT is more likely to de-peg than an LST, leaving those restaking at risk of considerable losses. Furthermore, certain stakeholders have expressed concern with regards to the risks such strategies may impose to the underlying networks (and in turn to stability in DeFi markets) (see Buterin, 2023).

3.2 EU market for crypto lending, borrowing and staking

183. A majority of NCAs identify providers of lending, borrowing and/or staking services in their jurisdictions: 16 NCAs (out of 37) identified crypto lending and/or borrowing providers, and 23 identified staking providers. Many of the identified entities offer their services in multiple jurisdictions, taking into account the 'border-less' nature of blockchain technology, which allows providers to quickly extend their services across border (subject to local regulation).

184. 16 entities were identified as providing in EU jurisdictions at least two types of services among crypto lending, borrowing and staking. Moreover, 11 entities were identified as offering lending, borrowing and/or staking services as part of a range of services that also included other regulated crypto-asset services[152], including asset management or exchange services. Those entities could be thought of as 'multifunction crypto-asset intermediaries' (MCIs) (FSB, 2024). Two NCAs also identified entities specialised in offering crypto staking or lending services only, with the latter being an entity to whom lending and borrowing services are outsourced by other centralised customer-facing providers.

185. To-date, credit institutions in the EU appear to have very limited or no engagement with crypto lending, borrowing and staking services, and only about 5% of SSM credit institutions appear to be exploring, planning or testing the engagement with such services[153]. Absent reporting obligations on providers, there are very limited indications on the engagement of EU consumers in those activities. According to the analysis presented in Section 2.1, the size of global DeFi markets is estimated to be of EUR 78 billion, with approx. 18% (i.e. EUR 14.04 billion) belonging to lending and borrowing protocols and 39% (i.e. EUR 28.08 billion) to staking protocols. As the EU appears to account for approx. 13% of crypto and DeFi users globally, the EU market for DeFi lending and borrowing could be estimated to be of EUR 1.8 billion, and for DeFi staking of approx. EUR 3.6 billion[154].

3.3 Potential risks associated with crypto lending, borrowing and staking

186. Notwithstanding the above, a broadly common set of potential risks can be identified, to a greater or lesser extent, across different structures facilitating crypto-asset lending, borrowing and staking (see Section 3.1). Some of these risks can be more pronounced in the

[152] That is, entities that may need to become authorized as 'CASPs' under MiCAR starting from 30 December 2024, are currently registered as VASPs under national AML or ad hoc regimes, or are authorized providers under national prudential crypto regulation.

[153] Credit institutions often cite that their low engagement with crypto lending, borrowing and staking is related to the unclear regulatory framework, including on the prudential treatment of exposures to crypto-assets involved in lending, borrowing and staking. However, as explained in Section 2.1.3,, Regulation (EU) 2024/1623 has introduced a transitional regime for the prudential treatment of crypto asset exposures, starting to apply from 1 January 2025, which should help clarify the prudential treatment of crypto lending, borrowing and staking. Therefore, credit institutions' low engagement may rather be associated to the conservative approach adopted by international standard setters and EU legislators.

[154] This numbers are still very small relative to the size of traditional financial markets. For instance, Euro area banks' loans to households account for EUR 6,665.7 billion. That is, the total DeFi market for lending, borrowing and staking in the EU would account approximately for 0.08% of euro area bank loans to households.

context of decentralised models, albeit some other risks have the potential to be reduced in them. Other risks can be more pronounced either in crypto lending and borrowing or in crypto staking. Considering that these activities are not expressly regulated by MiCAR, based on NCA feedback, only 5 respondent authorities (representing 4 EU / EEA Member States) indicated that some of these services (primarily lending) are regulated to some extent in their jurisdictions.[155] The following sections identify the potential risks.

3.3.1 Potential risks that are common to lending, borrowing and staking

Consumer protection

187. As observed historically with regard to crypto-asset activities, marketing materials may provide misleading information on the opportunities and risks relating to crypto-asset lending, borrowing and staking.[156] Similarly, disclosures (if any) relating to the risks involved in crypto-asset lending, borrowing and staking may not adequately explain the risks facing users (including consumers). In particular, users may receive **insufficient information** on conditions such as (a) pricing and fees they may incur, (b) interest rates paid or rewards/yields users may obtain, (c) changes to collateral requirements, including the basis on which additional collateral may be required to be posted, (d) the actions the service provider may take with regard to any assets used as collateral (including regarding any ability to rehypothecate the assets) or placed in a staking account, or (e) rights and liabilities in the case of assets placed in a pool or staked, including in the event of dispute or insolvency (see Annex 10 for examples of T&Cs of providers). Even where risks are disclosed in terms and conditions, they may be explained with sophisticated language that requires a high level of financial, legal and technical literacy.

188. Collectively, this means that consumers may struggle to understand the full implications of their crypto lending, borrowing and staking activities, and the risks to which they may be exposed, such as over-indebtedness. Consequently, crypto lending, borrowing and staking may pose **high consumer protection risks**. However, to-date, surveyed NCAs report that they have not received a large number of complaints (or complaints addressed to other organisations responsible for consumer protection in their jurisdictions), partly in view of the largely unregulated nature of the activities. Indeed only 4 respondent NCAs indicated they were aware of complaints.

189. Consumer protection risks may be heightened in the context of **limited financial education or digital literacy** (activities involving crypto-assets have historically been regarded as 'high risk' due to volatility in prices and other risks highlighted in several ESA warnings).[157]

Legal risks

[155] Two NCAs indicated that the activities may be carried out by VASPs and thus be subject to AML/CFT measures, pending the application of Title V MiCAR; another NCA indicated that if a loan is denominated in official currency and offered to consumers the loan would be deemed a consumer loans and the lender would require registration as a consumer credit provider with the NCA.

[156] For instance, one NCA reported a case of a service provider who was intermediating crypto loans by connecting users with borrowers via a third-party intermediary. The third party faced financial difficulties and decided to deny lenders the option to get their loaned assets back. Consumer complaints explained that the service provider's marketing communications were not clear regarding the risks they could face. In fact, while the NCA expected lenders to have been attracted by high interest rates, this was not even the case (rates offered were rather low), with this contributing even further to the lack of understanding of risk implications from lenders.

[157] For the ESAs' most recent warning, on the factors consumers should 'know and check' before investing in crypto-assets see: www.eba.europa.eu/sites/default/files/document_library/Publications/Warnings/2022/1028326/ESAs%20warning%20to%20consumers%20on%20the%20risks%20of%20crypto-assets.pdf.

190. Users may face legal risks, including as a result of potential co-mingling of assets, a lack of dispute resolution/recourse mechanisms should things go 'wrong', a lack of clarity with respect to the applicable governing law and a lack of access to direct or indirect redress mechanisms. Moreover, in some jurisdictions, the unclear legal status of crypto-assets (e.g. as property) and/or of smart contracts can complicate the enforcement of claims and impact the recovery of funds or crypto-assets, including in an insolvency.

Market risks

191. Users participating in lending, borrowing and staking are exposed to crypto-asset price fluctuations that can impact their returns or collateral value. This volatility poses liquidation risks for borrowers and can lead to rapid changes in the value of staked or placed assets. While market risks are also present in traditional financial markets, they can contribute to enhancing market risks in lending, borrowing and staking. In lending and borrowing, market risks can also be increased due to interconnectedness and procyclicality in the crypto-asset market[158].

Operational and ICT risks

192. ICT risks associated with DeFi are summarised in Section 2.3, and apply both to the decentralised and centralised models of lending, borrowing and staking of crypto-assets. Regardless of the context, users can face significant fraud and theft risks (e.g. hacking centralised entities, stealing the users' private keys, fraud schemes, scams) and traditional cyber risks (e.g. hacking, phishing).

ML/TF risks

193. ML/TF risks associated with lending, borrowing and staking (regardless of whether these services are centralised or decentralised) are broadly the same as those associated with crypto-assets in general (see Box 5 below) and with credit activity in particular.

Box 5. ML/TF risks associated with crypto lending, borrowing and staking

Consistent with the EBA's ML/TF Risk Factor Guidelines, ML/TF risks[159] associated with crypto lending, borrowing and staking can be grouped under four main risk factors:

(i) **Anonymity or pseudonymity of customers**. Without robust CDD measures in place, users can transact without disclosing their true identity or without having their identity being verified by the service provider or intermediary based on reliable information or documentation.

(ii) **Transactions involving illegitimate funds or crypto-assets**. Regardless of whether fiat currency or crypto-assets are used to provide or repay the loan or stake crypto-assets, the lack of scrutiny by the service provider of the source of these funds or crypto-assets exposes the financial system to significant vulnerabilities.

[158] For example: a crypto-asset borrower borrows on Day 1 10 crypto-assets with a market value of 100 EUR, with 10 of the same crypto-assets to be returned to the lender on Day 5. On Day 2 the borrower sells the crypto-assets for 101 EUR. On Day 4 the borrower looks to buy crypto-assets in order to meet the contractual requirement to return crypto-assets to the lender on Day 5. However, the market price has gone up in the meantime and the borrower has to pay 110 EUR for the crypto-assets. In this case, the borrower has suffered a loss of 9 EUR. By way of another example, a crypto-asset lender requires a borrower to post collateral of 120% for a loan of 100 crypto-assets. The borrower defaults on the loan. However, in the meantime, the value of the collateral has fallen and, on liquidation, is worth only 80% of the loaned amount meaning the lender suffers a loss of 20% on the value of the loan due to the decline in the market value of the collateral.

[159] Moreover, In July 2023, the EBA published an Opinion on ML/TF risks where it confirmed its findings from the 2021 Opinion on ML/TF risks that crypto-assets are susceptible to high risk of ML/TF. This is due to continuous growth of the crypto-assets market within recent years and, the development of novel crypto-related business models (including tumbling and mixing services or anonymity-enhanced coins) that were not accompanied by a commensurate investment in AML/CFT compliance.

(iii) **Unclear purpose of the transaction**. The lack of understanding by the lender of the real purpose of the loan may result in that loan being used for illegitimate purposes. For example, the proceeds of the loan could be used to finance terrorist activities.

(iv) **Exposure to high ML/TF risk jurisdictions**. Considering the cross-border nature of crypto-asset services, some users can be located in jurisdictions with deficient AML/CFT frameworks or in high-risk third countries designated as such by the EC in accordance with Article 9 of the AMLD. This means that, without proper monitoring systems in place or robust identification and verification checks, users from high-risk jurisdictions can transfer funds or crypto assets, which may be illicit or purchased with illicit funds or crypto-assets, across the world without being detected.

194. The ML/TF risks can be reduced where lending, borrowing or staking services also involve some of the CASP services regulated under the MiCAR or other applicable frameworks. In such cases, the providers are also obliged entities under the AMLD[160] and therefore are required to perform adequate CDD checks (see Box 6). CASPs regulated in third countries where the AML/CFT framework is as robust as in the AMLD, may also contribute to reducing risks.

195. Nonetheless, while CDD checks may give some level of protection against ML/TF, their impact may often be limited. As crypto-assets are continuously transferred between users and DeFi protocols, it may be difficult or, in some cases, impossible, to establish the legitimacy or true ownership of funds or crypto-assets used in transactions. Transactions in DeFi may involve providers based in countries where no AML/CFT regulation or supervision are applied or where serious deficiencies have been identified e.g. by the FATF.

Box 6. ML/TF risks associated with crypto lending, borrowing and staking and the existing AML/CFT regulatory framework

AML/CFT rules and standards are applicable to credit and financial institutions in the EU, which are required to identify, assess and manage ML/TF risks associated with their business, according to the AMLD provisions. With the publication of the FTR, the scope of the AMLD was extended to apply to CASPs that provide services according to MiCAR. This change took effect on 30 December 2024.

Lending, borrowing and staking are not explicitly captured under the definition of crypto-asset services set forth in MiCAR. This means that different AML/CFT rules will apply to the same services depending on who provides them (CASPs vs non-CASPs), leaving gaps in the EU's defences against ML/TF risks and creating a unlevel playing field between providers. Where lending, borrowing or staking are provided as ancillary services by CASPs, they will be required to assess the level of exposure to ML/TF risks of these services and put in place measures to mitigate these risks. In contrast, where these lending, borrowing or staking activities are carried out by a services provider that does not fall under the scope of MiCAR, such providers will have no AML/CFT obligations (unless otherwise in scope of the AMLD).

3.3.2 Potential risks that are specific to crypto lending and borrowing

Leverage

196. Crypto-asset lending can contribute to building up of leverage in the market (i.e. a user may borrow crypto-assets, lend them out and, with the proceed of the loan, seek to borrow more). Over time ,the level of leverage may become high (see Azar et al, 2022), absent limits on lenders, including large institutional lenders (such as, CASPs) acting on their own account.

[160] Those providers that fall outside the scope of the AMLD have no obligations pursuant to EU law to manage these risks or put in place any risk mitigating measures. In some jurisdictions, these services or service providers may be governed by the national AML/CFT legislative frameworks. However, based on the NCAs' survey responses, the EBA and ESMA understand that such national provisions apply only to a small number of services provided via centralised platforms.

Since the majority of lending is carried out by a small number of accounts (see Xu et al, 2020), this may also pose potential concentration risks, which can ultimately increase risks arising from excessive leverage in stressed market conditions.

197. Crypto borrowers can often use different market making activities that lead them to **rehypothecation** (i.e. lending out assets placed by borrowers as collateral), leading to '**collateral chains'**[161] in crypto-asset markets. As a result, institutional crypto borrowers often hold very high 'debt-to-equity' (D/E) ratios[162]. Highly leveraged market making activities based on crypto lending contribute to vulnerabilities of crypto-asset market participants to market movements. Absent reporting obligations on collateral assets, leverage can introduce risks not only for borrowers, but also potential systemic risks in crypto markets.

198. Moreover, some crypto lending and borrowing services include utility tokens among accepted collateral assets. This has the potential to increase leverage risks of crypto lending markets, due to the collective effects of a) the potential low underlying or intrinsic value, b) their ties to the platform's own ecosystem, which creates a feedback loop of borrowing against a potentially volatile, platform-specific asset, and c) the potential that the indirect interconnectedness between crypto lenders using utility tokens may amplify risks via cascading effects of liquidations and/or price declines.

System-wide risks: Interconnectedness, procyclicality and concentration risk

199. The use of collateral can pose risks of contagion via the **interconnectedness** arising from common asset holdings and **procyclicality**. This is for two reasons: (i) the amount of lending that can take place depends on the total value of assets eligible for collateral, and (ii) declines in the value of collateral assets can trigger liquidations. The latter can further depress prices leading to a classic 'doom loop', not only in terms of amount of lending, but also as a result of the wider impact of falling asset prices. That may ultimately lead to wider asset sell-offs[163].

200. Procyclical effects can be compounded by market **concentration**, evident both in centralised and decentralised lending markets, with any tightening in lending activities in a highly concentrated market having a disproportionate impact across the wider market.

Credit and liquidity risk

201. Frequently, no creditworthiness checks are carried out by lenders before providing a crypto-asset loan – i.e. the counterpart cannot assess **credit risk**. Importantly, lenders and borrowers often do not have information to assess the 'riskiness' of their decisions and to price the loan on a risk-sensitive basis. This means that higher overall rates may be charged to borrowers absent a more customised/risk-sensitive approach and that lenders can face situations where they need to accept a loss (because the amount returned is lower than the loan).

202. Credit risk is typically mitigated via collateral requirements, and the lender can liquidate collateral to cover the impact of any loan default. Due to over-collateralisation requirements, subject to market conditions at the time, the liquidation of assets held as collateral may mean that the lender does not suffer a loss. At the same time, the activation of liquidation introduces risks to borrowers, with the rigidity of the operation of smart contracts further

[161] Borrowers can use the borrowed amount to use it as a collateral in an ulterior loan, and do that in several instances.

[162] According to desk-based research by EBA and ESMA, some institutional crypto borrowers surpass the 170% D/E ratio, with the ratio increasing between 2022 and 2024.

[163] As described by Aramonte et al, 2022: (i) in 'booms' collateral value increases, collateralisation ratios fall, and loan volumes expand; (ii) in 'busts' positions are liquidated as prices and collateral values decline sharply, suppressing lending activity; (iii) effects may be further amplified when borrowed crypto-assets are used as collateral for additional loans, giving rise to "collateral chains".

enhancing procyclicality in stress conditions (see Chiu et al, 2023), as well as the lack of recourse for borrowers.

203. Borrowers and lenders may also face **liquidity risk**, for example, where a person has lent out crypto-assets long, but has borrowed short, and market conditions are such that it is not possible to repay short term obligations (see Azar et al, 2022).

204. Moreover, if centralised crypto lenders and borrowers co-mingle those services users' crypto-assets with those of users of other services (mainly custody and administration of crypto-assets), such co-mingling of crypto-assets belonging to the CASP (borrowed from users) and crypto-assets belonging to the user (under custody and administration) may raise risks to users in the case of **dispute or insolvency,** if a shortfall of assets vs claims on those assets occurs (see Dell'Erba, 2024). This risk may be increased if intermediaries have the ability to **rehypothecate** crypto-assets and some of those assets (or equivalent value) are lost due to losses on loans. Often the way in which the return to be paid to clients for crypto-assets borrowed from them is made is not clear.[164]

205. Finally, custody risks may also arise in the event of the failure of the custodian, and, for example, co-mingling of assets and insufficient record-keeping and/or legal clarity as to the identity of persons with a right to claim against those assets. This risk may be enhanced in the event of market concentration (i.e. reliance on relatively few custodians).

3.3.3 Potential risks that may be increased in DeFi lending and borrowing

Systemic risks

206. A key concern associated with DeFi lending and borrowing is that collateral chains in DeFi can potentially come with enhanced **systemic risks** via three channels: a) effects of cascade liquidations across multiple DeFi protocols, b) deleveraging spirals when assets are liquidated, and c) systemic liquidity crunches.

207. DeFi lending and borrowing services also pose **market concentration risks**, which can compound the procyclical lending and borrowing markets. According to available data[165], while there are around 440 DeFi protocols currently offering DeFi lending and borrowing services, 13 protocols distribute 86% of the total market, and the two largest ones, as of October 2024, account for 52% of total TVL for DeFi lending and borrowing.

208. Finally, the inclusion of governance tokens among accepted collateral in DeFi lending protocols, in similar way to utility tokens in centralised lending, may enhance leverage risks, particularly where protocols offer them as rewards for users (lenders or borrowers)[166].

Consumer protection concerns and financial inclusion

[164] https://www.afm.nl/~/profmedia/files/rapporten/2024/verkenning-cryptodienstverleners.pdf (in Dutch, page 11)

[165] See https://defillama.com/protocols/Lending

[166] In particular, such practice may potentially introduce wrong way risks in DeFi. For example, Xu et al (2020) found that some DeFi lending protocols were offering governance tokens as rewards to borrowers, just for the sake of participating in borrowing activities. As a result of that reward, borrowers became particularly interested in the positive growth of the value of governance tokens. Researchers found that jumps in crypto lending and borrowing volumes were associated with the launch of governance tokens under such schemes, with users incentivized to increase their borrow position as long as the borrowing cost does not exceed the value of their (governance) token earnings. They concluded that such scheme may lead to a drop in the degree of collateralization in the DeFi lending markets. This may be the case because, as users have incentives to borrow as much as possible as long as governance token rewards compensate borrowing costs, market dynamics lead them to a race to the bottom for collateralization, with user maximizing leverage. This would lead to a more fragile market, and in case the value of governance tokens drops quickly, many users would be in liquidation risk. In such a scenario, the protocol could face systemic risks, as liquidations could have cascading effects on others.

209. While DeFi proponents may often claim that DeFi permits a higher degree of financial inclusion compared to traditional financial services, DeFi may in practice constitute a barrier to enter lending and borrowing services**.** The complexity of DeFi protocols and their non-custodial nature make access to those services practically difficult, if not outright unsuitable, for retail participants and therefore unsuitable to promote financial inclusion (OECD, 2024).

210. The requirement to provide collateral to access crypto lending may also add complexity that results in an exclusionary effect for some users.

211. Moreover, as DeFi protocols often lack standardised disclosures, users may be able to access sophisticated financial services without **sufficient information** on the risks involved compared to regulated centralised crypto lending and borrowing offered by regulated providers. As a result, consumer protection risks may be heightened in DeFi, as the complexity of the technology underlying DeFi protocols requires particular attention to **financial and digital literacy**.

3.3.4 Potential risks that may be increased in crypto staking

Volatility and market risks

212. In staking, as there is often a lock-up and unbonding period of several (tens of) days, users may be vulnerable to significant changes in the valuation of their crypto-assets, should they be unable to trade them during periods of market volatility due to the lock-up period. Such risk may not be adequately disclosed to users.

213. In liquid staking, market volatility risk can be both mitigated and amplified. In particular, it can be amplified when the market value of the liquid staking token declines, with the user losing value. They may also be mitigated since the receipt of a liquid staking token means that instead of unstaking, a user can trade the liquid staking token and potentially prevent losses that might have occurred before the staked asset could be unstaked.

Penalties and Slashing

214. Validator penalties and slashing are a built-in part of certain PoS blockchains (see Annex 9). In the case of staking-as-a-service questions may arise as to how prevalent risks relating to these penalties/slashing are[167], in particular to what extent are these passed on to clients and to what extent are the risks adequately disclosed.

215. It appears to be a practice in the market, at least among known centralized providers, to provide a layer of contractual protection to delegators in case of penalties and slashing. In practice, this means guaranteeing that the provider will take on the risk and replace lost assets in certain situations – however the level of legal certainty and situations covered depend across providers.

Custody risks

216. Finally, custody risks may arise in crypto staking in the event of the failure of the custodian, the co-mingling of assets, or insufficient record-keeping and/or legal clarity as to the identity of persons with a right to claim against those assets. This risk may be enhanced in the event of market concentration (i.e. reliance on relatively few custodians).

[167] Slashing does not appear to be a frequent occurrence. Indeed, studies suggest that on Ethereum for example, as of February 2024, 0.04% of all active validators had been slashed.

4. Key findings

On DeFi:

217. Since its early days in 2016 when the first DeFi protocol was launched, the report finds that DeFi has grown to reach EUR 77 bn in TVL as of September 2024. Still, it remains a niche phenomenon, equivalent to 4% of the total crypto-asset market capitalisation, and DeFi activities are concentrated in a handful of large protocols.

218. Assessing the scope of DeFi in the EU is challenging due to the technical limitations, anonymity or pseudonymity and the global nature of DeFi protocols. The report estimates the current number of DeFi users in the EU at 7.2 million but less than 15% of DeFi users appear to have either bought or sold crypto-assets on DeFi on average per month in 2024, suggesting that a significant portion of DeFi users are not engaging in DeFi activities regularly.

219. DeFi adoption in the EU appears higher than the world average but lower than comparable peers, such as the US. The share of the Euro in crypto transactions did not exceed 8% on average since December 2022 (versus 44% for the US Dollar), and the use of euro-denominated stablecoins remain negligible in size in DeFi markets (in line with their general small size), although EU users may also be trading in DeFi using stablecoins denominated in other currencies.

220. Available evidence points to a very limited direct exposure of EU financial institutions' to DeFi, also considering that the successive booms and busts of crypto-asset and DeFi markets had no meaningful spillover effects, including indirect ones, on those institutions.

221. Within DeFi markets, crypto lending, borrowing and staking, account for more than 50% of all total value locked (TVL).

222. The number of DeFi hacks and the value of stolen crypto-assets has generally evolved in correlation with the DeFi market size. While historically the majority of DeFi hacks have stemmed from on-chain vulnerabilities (mainly through the exploit of smart contract vulnerabilities and price manipulation attacks), recent attacks on DeFi appear to be more successful when exploiting off-chain vulnerabilities (e.g. compromising the private keys that give access to non-custodial wallets).

223. In particular, among all attacks on DeFi during 2023 and up to October 2024, the value stolen from DeFi protocols due to the compromise of private keys corresponds to slightly above 50% of all crypto-asset thefts in DeFi. Moreover, a large majority of all price manipulation attacks were associated with attacks on oracles.

224. DeFi presents significant risks of ML/TF, mainly due to the current absence of an AML/CFT regulatory framework and controls and to the cross-border nature of transactions. Flows on decentralised exchanges represent 10% of the spot volume traded of crypto-assets globally, and such flows through decentralised exchange may exceed EUR 100 billion a month. This means that funds or crypto-assets from potentially illegitimate sources can be processed on protocols by users who are not identified or verified and can therefore act anonymously or pseudonymously without being detected. The risk is slightly reduced, even though not fully mitigated, when transfers are processed via centralised platforms or regulated exchanges subject to AML/CFT requirements.

225. Regarding different alternatives explored that could (partly) mitigate ICT risks associated with DeFi, the embedded supervision of DeFi based on public data is found to face significant limitations, based on available data and techniques. However, existing initiatives to mitigate ICT and ML/TF risks appear to be more advanced in other areas, such as in the standardization of smart contracts, the certification of DeFi protocols, and the reporting of serious ICT incidents to relevant authorities and conducting of post-incident reviews, based on the approach set out by DORA.

226. MEV activities are widespread in DeFi, mainly because most blockchains, including Ethereum, do not enforce constraints on the precise ordering of transactions within a block. Estimates for cumulative MEV profits on Ethereum vary across sources between USD 0.7bn and USD 1.9bn prior to Ethereum's move from PoW to the PoS consensus mechanism and between USD 0.4bn and USD 1.1bn after the move to PoS.

On crypto lending, borrowing and staking:

227. The report defines and analyses centralised and decentralised forms of crypto lending, borrowing and staking services. Regarding crypto-asset lending services, all forms are characterised by over-collateralisation, liquidation mechanisms, and a wide range of crypto-assets accepted as collateral. The report finds that centralised crypto lending offers loan-to-value ratios between 20-80%, with liquidation thresholds typically at around 85%. The report finds that interest rates paid by borrowers typically range between 8 to 15% but finds evidence of rates offered at a higher level. On the other hand, centralised crypto borrowing, the subject of significant market failures, is found to be attracting users in search for yield on their crypto-assets, with interest paid to lenders ranging from 4-16%.

228. DeFi protocols offering lending and borrowing services, most typically relying on 'liquidity pools', which appear to work based on a rather narrow interest rate spread (the difference between rates charged to borrowers and rates paid to lenders), often ranging between 0.20-2%. However, DeFi protocols appear to benefit from additional revenue streams, such as withdrawal fees, liquidation fees, increases in values of governance tokens and market-making activities. Finally, the DeFi lending market appears to be highly concentrated.

229. On staking, the report finds that there are a variety of business models in the market, with custody being a key feature distinguishing the different models. In general, staking rewards offered to validators vary considerably across blockchain networks (3 - 45%), while rewards that can be expected by delegating stakers for one same staked token can further vary depending on the fees charged by the provider(s) with which they stake that token.

230. The report finds that crypto lending, borrowing and staking services are offered by a number of crypto-asset services providers in EU jurisdictions. A majority of identified providers offer multiple of those services, and many also offer regulated crypto-asset services, such as exchanges, with at least 16 offering at least two types of services among crypto lending, borrowing and staking. Moreover, 11 entities were identified as offering lending, borrowing and/or staking services as part of a range of services that also included other regulated crypto-asset services, such as asset management or exchange services.

231. The report finds information asymmetries regarding those activities, with users receiving insufficient information on conditions around relevant areas such as fees, interest rates paid or yields obtained, changes to collateral requirements, the actions the service provider may take with regard to any assets used as collateral or placed in a staking account, or rights and liabilities in case of dispute or insolvency. The report finds that information on those aspects

is often not clear or misleading in marketing communications and lenders' websites and apps, and that disclosures are insufficient to prospective lenders and borrowers, hindering their ability to properly identify and assess all potential risks they may incur. Moreover, the report finds that over-collateralisation in crypto lending and borrowing, combined with procyclicality present in DeFi, may lead to rehypothecation, ultimately leading to collateral chains. The risk for potential excessive leverage is enhanced in DeFi settings and where lending services are used to fund staking. DeFi lending and borrowing also appears to face market concentration risks.

232. Finally, the assessment of ML/TF risks associated with the lending, borrowing and staking of crypto-assets concludes that such activities present ML/TF risks which, in light of the fragmented or non-existent AML/CFT legislative frameworks governing them and providers, may remain unmanaged and unmitigated.

Annex 1. EC letter to EBA and ESMA

Date: 09/02/2024

Subject: Call for contributions under Article 142 of MICA

<u>(1) DECENTRALISED FINANCE</u>

(a) Analysis of the engagement of European consumers and businesses with DeFi

Given the pseudonymous nature of transactions in DeFi and the general data gaps in this market, ESMA and EBA may also make assessments based on third party data sources, including approximate ones. The analysis should provide an overview, to the extent possible, of both the engagement of EU retail investors and regulated entities with DeFi services, as well as of notable EU businesses providing DeFi services. The focus should be on lending and trading protocols, yield farming protocols and aggregate (composite) protocols.

(b) Businesses providing access to DeFi services (access intermediaries)

An analysis of the undertakings that provide access to DeFi protocols that underpin DeFi services, in particular those based in the EU. To our knowledge, there are at least 3 types of businesses providing access to DeFi protocols:

(i) standalone DeFi application interfaces that provide user-friendly connectivity to the functionalities of DeFi protocols;

(ii) self-custodial wallets that provide direct access to DeFi protocols within the wallet front-end;

(iii) centralised trading platforms that provide access to DeFi protocols within their ecosystems.

The assessment should include an analysis of the technical solutions and business models for providing DeFi connectivity of a representative sample of undertakings, and any additional services that are directly complementary to the service of accessing and using a DeFi protocol. These businesses should be assessed as potential regulatory entry points to mitigate risks to clients using DeFi protocols.

(c) Specific IT risks associated with the use of DeFi protocols

Due to its open-source nature, sometimes inadequate IT resilience standards and the fact that crypto-assets are often bearer instruments that can be stolen, DeFi has been subject to numerous hacking attacks. In this context, ESMA and EBA should analyse which elements of DeFi present particular IT vulnerabilities and to reflect on possible mitigation measures. The analysis should also include an assessment of whether and to what extent the application of Regulation (EU) 2022/2554 (DORA) rules can mitigate some of the specific risks associated with DeFi, should a CASP be identified in the context of a DeFi service. Where no such CASP can be identified (full decentralisation), ESMA and EBA should assess the feasibility of certifying smart contracts as a means to mitigate risks for clients, building on the work of the French ACPR.

(d) Monitoring risk in DeFi protocols based on public data

Based on an assessment of the data output of a representative sample of DeFi protocols, ESMA and EBA should provide views on the extent to which protocol activity, and in particular build-up of risks, can be monitored by supervisors or access intermediaries through publicly available data, whether online or on-chain. This should take into account the findings of the DeFi Pilot on embedded supervision, which is currently being finalised by an external contractor for DG FISMA.

(e) How MEV affects the DeFi ecosystem

MEV (maximal extractable value) is a widespread practice on the Ethereum blockchain, and can potentially occur on any permissionless blockchain where validators use their ability to order transactions within a block in order to maximise their profit.

To do this, validators often make use of public information about pending transactions in the so-called public mempool. ESMA and EBA should assess how widespread MEV is across blockchains, and what mitigants exist or are being considered to mitigate client harm (e.g. price slippage) resulting from such activities.

In conducting the analysis, ESMA and EBA should consider that MEV appears to be a necessary consequence in a blockchain protocol that allows validators to reorder transactions as part of its rules and incentive mechanisms. This is in contrast to traditional markets, which typically operate under a strict time/price prioritisation of transaction execution. MEV should therefore be seen as a feature of certain permissionless blockchain ecosystems, the negative consequences of which should be better understood.

(2) BORROWING AND LENDING OF CRYPTO ASSETS

(a) An analysis of the EU market for the lending and borrowing of crypto-assets, both through centralised entities and DeFi protocols.

To the extent possible, this should include a data-driven analysis of the lending and borrowing services provided by EU-based CASPs/VASPs and estimates of the size of the market. Particular attention should be paid to retail participation in lending and borrowing markets.

(b) Specific risks associated with the borrowing and lending of crypto assets

We would welcome ESMA's and EBA's views on any material risks posed to retail clients by the activity of lending and borrowing crypto assets. In particular, the analysis should include views on how leverage is facilitated through the activity of lending and borrowing crypto assets and whether this poses risks similar to those in traditional finance. This should include a comparison of the risks associated with the lending and borrowing activities of centralised platforms and those associated with DeFi protocols.

(c) Staking activities

Staking activities in the wider sense of the notion means locking up of crypto assets for the purpose of obtaining yield on investments. This can cover a wide variety of activities.

ESMA and EBA should however focus in their analysis on staking services provided by centralised trading platforms (staking-as-a-service), where the platform uses the tokens entrusted to it by the client to generate yield for that client. ESMA and EBA should assess how such staking services inter-relate with borrowing and lending services provided by that same platform, and indeed other services regulated by MICA, most notably custody of crypto-assets. The assessment should in particular cover staking-as-a-service related to securing the blockchain protocol, and provide insights into how yield is distributed between the platform and the client, what disclosures are made to clients when providing the services, and what are the rights of clients in case of adverse events such as token slashing.

Additionally, the assessment should also examine the risks of staking liquid staking tokens for the purpose of maximising yield. As far as we know, this activity takes place mainly in DeFi and has similarities to the rehypothecation of collateral in traditional finance, leading to increased leverage in the system. It is important to better understand these practices, as they can increase vulnerabilities of the blockchain network as a whole.

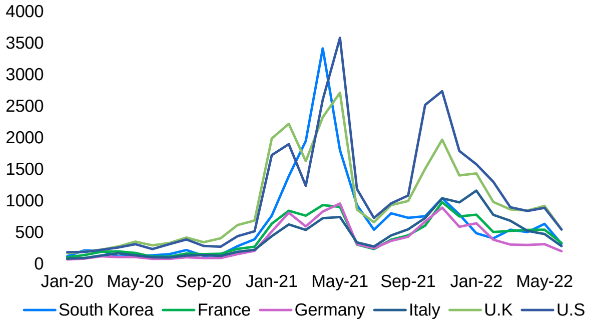
Annex 2. Proxies for EU DeFi adoption

Downloads of crypto apps in the EU

Available data suggest that the EU lags the US, the UK and South Korea regarding the use of crypto apps[168] (Chart A). In the EU, the number of crypto app downloads[169] fluctuated between 400 and 1000 per month per 100,000 inhabitants between January 2021 and May 2022. Although the number of downloads tends to spike when crypto-assets prices surge, EU consumers seem less sensitive to the cyclical hype surrounding crypto-assets as the number of downloads in the region tends to remain more stable over time.

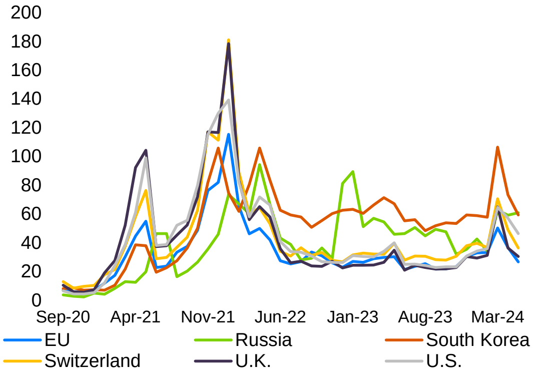
Data on MetaMask downloads (Chart B) shows a comparable low incidence across the EU and other countries like the US and the UK, ranging from 20 to 180 downloads per 100,000 inhabitants between January 2021 and May 2024. MetaMask is a popular crypto wallet that allows users to manage their crypto-assets and interact with DApps on Ethereum and other compatible networks. Therefore, data on the use of MetaMask more closely reflects DeFi adoption among retail users than general crypto apps. Consistent with the above observations on crypto apps, downloads of MetaMask tend to increase when crypto prices are high, as was the case mid- and late-2021 for example.

Chart A. Crypto apps - downloads per country



Note: Monthly downloads per 100,000 inhabitants.
Sources: Sensor Tower, Auer et. al (2022), ESMA

Chart B. MetaMask – downloads by country



Note: Monthly downloads per 100,000 inhabitants in different countries (September 2020 to May 2024)
Sources: Statista, ESMA

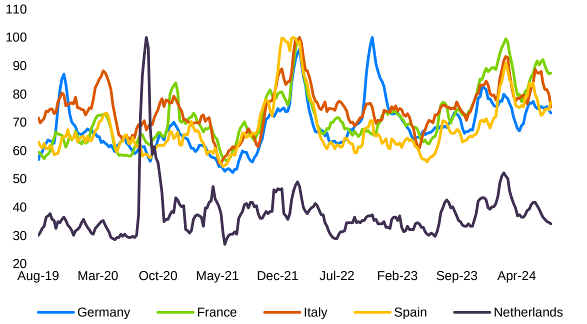
Consumer interest in DeFi based on Google Trends data

Google Trends data also suggests that EU consumers' interest in DeFi increases when crypto-assets prices are high (Chart C). Google Trends data also suggests that the interest of the population at large for DeFi-related terms varies across EU member states, with higher values in countries such as the Netherlands and Ireland (Chart D). This interest is consistently lower than in other countries outside the EU.

[168] That is, mobile apps facilitating crypto-assets services.

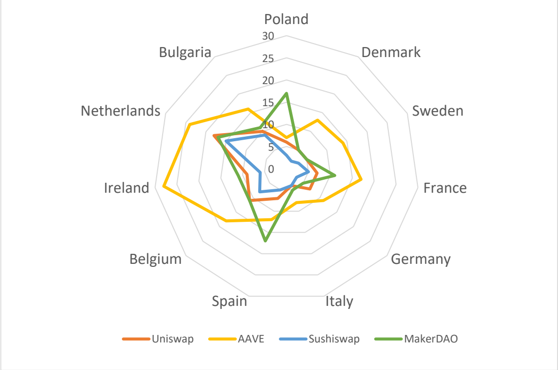
[169] To select the sample of crypto-apps, Auer et al. (2022) rely on the list of crypto exchanges from the CCData "All Exchanges General Info" application programming interface (API) endpoint. Thus, they find a match with the Sensor Tower database for 187 of these exchanges (out of 296). Lastly, they complement this selection with a list of 26 apps identified as crypto exchange apps by Sensor Tower directly.

Chart C. Interest over time for the term 'DEX'



Note: Interest over time for the term 'DEX'. Numbers represent search interest relative to the highest point on the chart for the given country over the specified period. A value of 100 is the peak popularity for the term. A value of 50 means that the term is half as popular. A score of 0 means that there was not enough data for this term. Normalised rolling monthly avearge of orginal weekly values.
Sources: Google Trends, ESMA

Chart D. Interest for popular DeFi protocols across EU countries



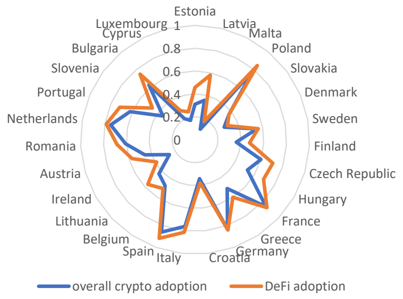
Note: Interest across EU member states for a set of landmark DeFi protocols ('Uniswap', 'AAVE', 'Sushiswap', and 'MakerDAO') as measured by Google searches. A country where the term claims its peak interest is assigned a value of 100 (not visible in the spider diagram). A country where the same term claims only half (10%) the interest is assigned a value of 50 (10). Values as of September 2024
Sources: Google Trends, ESMA

Indexes of DeFi adoption in the EU

Using the Chainalysis Crypto Adoption Index[170], which measures crypto adoption for individuals and a customised 'DeFi version'[171] of it, illustrates how DeFi adoption generally coincides with crypto adoption, as our customised index and the original Chainalytics index exhibit similar scores in each country (Chart E).

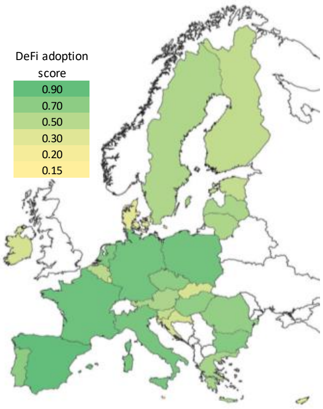
Crypto and DeFi adoption rates tend to be comparatively higher in France, Germany, Italy, the Netherlands, Poland, and Spain, and lower in Belgium, Croatia, Finland, and Ireland (Chart F). When compared to the rest of the world, DeFi adoption in many EU countries appears to be higher than the world average. Yet, for the EU as a whole, it is lower than in the US, the UK, China, Russia, India, South Korea, Turkey, and Brazil.

Chart E. Crypto Adoption Index (original vs. 'DeFi' version)



Note: 'Original' version of the Chainalysis Global Crypto Adoption Index (2023).
Source: Chainalysis, ESMA

Chart F. 'DeFi version' of Crypto Adoption Index



Note: Customised 'DeFi' version of the Chainalysis Global Crypto Adoption Index (2023).
Source: Chainalysis, ESMA

[170] The Chainalysis Crypto Adoption Index was designed to identify countries where "the most people are putting the greatest share of their wealth into cryptocurrency". The index is composed of five sub-indexes, each of which is based on a country's usage of different types of crypto-assets services. the country scores are scaled to range from 0 to 1, with a score closer to 1 denoting a higher adoption rate. For more details, see https://www.chainalysis.com/blog/2023-global-crypto-adoption-index/

[171] EBA and ESMA computed a customised version of the index (hereinafter 'DeFi adoption index') to measures DeFi adoption (rather than crypto adoption in general) using the two sub-indexes focusing on DeFi adoption specifically.

The geographical location of Ethereum nodes[172] was also analysed, due to its potential as an indication of crypto and DeFi adoption. Indeed, running an Ethereum node is associated with a high level of engagement with the Ethereum ecosystem, and areas with a high concentration of Ethereum nodes suggest an active and engaged blockchain community, among which there may be a significant portion of DeFi users. The geographical location of the Ethereum nodes indicate that a significant portion operate from the EU (only behind the US). Of the 6,245 Ethereum nodes active in September 2024, 14.78%, were in Germany, followed by France (4.69%) and Finland (4.34%).[173] The above numbers may suggest that EU market participants, particularly Germany, play an active role in the Ethereum network, but it should be noted that the geographic distribution of Ethereum nodes is mainly associated with the location of the technical 'infrastructure' on which DeFi activity is occurring. Therefore, the number of Ethereum node operators remains an imprecise proxy for actual DeFi engagement.

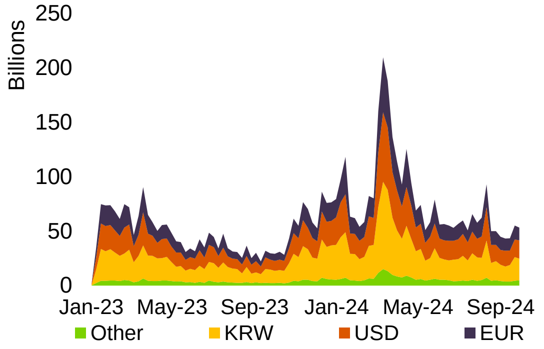
Fiat-to-crypto transaction volumes and geography of transactions based on timestamp

The volume of euro-denominated crypto transactions gives an indication of the volume of transactions likely to originate from EU individuals and businesses (this indicator is relevant for crypto activities in general though, not DeFi specifically). Since December 2022, the weekly volume of crypto-assets traded against the euro has fluctuated between a low of EUR 1.4 billion (in January 2023) and a high of EUR 7.9 billion (in March 2024). On average, over the considered period, this represents 8% of the total volume of crypto-assets traded against official currencies, compared to 37% for the Korean Won and 44% for the USD (Chart G).

Another proxy used to estimate the share of EU individuals and businesses in crypto transactions is the time at which the transaction occurred during the day. On that basis, crypto-asset transactions can be assigned to three world regions: the Americas, Europe and Africa, and Asia.

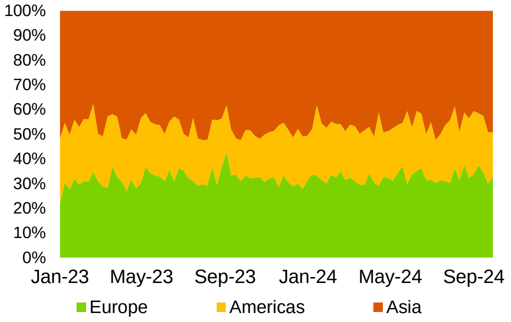
The results, shown in Chart H, suggest that Asia has the largest share of crypto trading (45% on average for the period considered), followed by Europe and Africa (30%), and the Americas (25%). These results contrast with the findings of the analysis of fiat-to-crypto transactions above, as they indicate a significantly higher appetite for crypto-trading among European investors. However, allocating a geography to a transaction based on its time has limitations. This is especially true for crypto-assets, as they are typically available for trading throughout the day from different locations.

Chart G. Fiat-to-crypto transactions by official currency (EUR bn)



Note: spot volume traded against different fiat currencies (EUR billion) (Jan 2023 - Sept 2024)
Sources: Kaiko, ESMA

Chart H. Weekly crypto volumes traded by region (in %)



Note: Estimated share of spot volume traded in different world regions (weekly) (Jan 2023 - Sept 2024)
Sources: Kaiko, ESMA

[172] An Ethereum node is a computer that participates in the Ethereum blockchain by maintaining a copy of the blockchain's data and processing transactions.

[173] Ethereum Node Tracker | Etherscan

Euro-denominated stablecoins

Stablecoins are instrumental to crypto-asset markets and DeFi due to their frequent use in trading and for liquidity provision in DEXs and lending protocols.[174]

While USD-denominated stablecoins have seen widespread adoption, accounting for nearly 90% of the total market capitalisation of stablecoins and for over 70% of the total volume of crypto-assets traded, euro-denominated stablecoins remain marginal in size and volumes traded.

Because euro-denominated stablecoins are still in their infancy, it seems likely that many EU users favour more established and widely used USD-denominated stablecoins instead. The use of euro-denominated stablecoins therefore appears as a likely underestimate of DeFi adoption in the EU.

[174] https://www.ecb.europa.eu/press/financial-stability-publications/macroprudential-bulletin/html/ecb.mpbu202207_2~836f682ed7.en.html

Annex 3. MEV techniques, data limitations, and counter-measures

MEV Techniques in detail

Arbitrage opportunities arise when the price of an asset on one exchange deviates from another exchange, e.g., because of a large trade on a given exchange. Arbitragers profit from this opportunity by purchasing the asset on the exchange offering the lower price and selling it on the exchange offering the higher price. In doing so, they contribute to closing the price gap between the two exchanges, while earning a profit. Arbitrage is not unique to blockchains and is widespread in traditional markets, where it contributes to efficient markets.

In the case of crypto-assets markets, arbitrage can be performed between centralised (CEXs) and decentralised exchanges (DEXs) (CEX-to-DEX arbitrage) or in-between DEXs (on-chain arbitrage). DEXs effectively rely on arbitrageurs to keep the prices of their AMMs in line with competing AMMs and off-chain oracles prices.

Front-running attacks happen when malicious actors take advantage of an information and submit an order ahead of the original ones, allowing them to "cut in line". In traditional markets, front-running refers to the practice where a broker or trader executes orders for their own account, taking advantage of advance knowledge of pending orders from their clients and is generally considered illegal. With blockchains, orders pending validation are publicly available in the mempool.[175] Attackers can monitor the mempool for profitable transactions and send the same transaction with a higher fee, causing theirs to be processed first (‘displacement’ attack).

Another type of front-running attack is when the attacker floods the network with high-fee transactions, thereby preventing the execution from the original order (‘suppression attack’). The latter is expensive for the attacker who must use a large amount of blockspace to reach the block capacity limit (Torres et al. 2021). Of note, because pending orders are publicly available, making front-running accessible to virtually everyone, some argue that on-chain front running (and sandwich attacks) should not be likened to front-running in traditional markets. Yet, like traditional front-running it creates important losses to users.

Sandwich attacks (sometimes also known as insertion attacks) are another variant of front-running attacks. In the case of a sandwich attack, the exploiter places two transactions, one before the victim’s transaction and one after. The front-running transaction manipulates the price in the attackers’ interest. The back-running transaction reaps the profit of the manipulation. There are two main scenarios for a sandwich attack on DEXs:

(i) ‘liquidity taker vs taker’ attacks: a classic example is when a user (a taker) wants to trade a large amount of crypto-asset A for another crypto-asset B. The attacker places a front-running transaction (a swap order of B in exchange for A with a higher fee) before the large transaction is executed. This activity causes the price of B to go up for the original trader, resulting in higher costs. The attacker profits by selling B at an increased price in a back-running transaction.

(ii) ‘liquidity provider vs taker’ attacks: in that case the attacker (the liquidity provider) manipulates the price of B relative to A by removing liquidity from the pool prior to the original transaction of the user (the taker) being executed. The lower liquidity translates into more slippage and therefore higher costs for the user. The attacker then re-adds

[175] This is true where transactions happen on-chain. The situation is different in the case of centralised exchanges, which operate a central order book in a similar way to traditional exchanges.

liquidity to restore the original pool balance and swaps asset B for A at a more lucrative price.

Liquidations. This technique consists in exploiting liquidations on lending protocols, as explained in Section 3.1 of the report. The liquidator repays the borrow position and receives a portion of the collateral larger than the amount repaid, which creates MEV opportunities. Searchers compete to determine which borrowers can be liquidated and be the first to submit a liquidation transaction in order to cash in the 'extra' collateral amount. In addition, if liquidated liquidation, users have to pay a liquidation fee, which goes to the searcher in that case.

Long-tail MEV include using event-driven strategies or exploiting specific design features within the system. Examples include front running a fraud prover and claiming the reward for successfully proving fraud, MEV strategies involving non-fungible tokens, or time-bandit attacks. Time-bandit attacks rewrite the history of blocks to capture MEV opportunities in those blocks, which threatens blockchain's integrity as discussed further down.

MEV data are sparse and need to be considered with caution

Available MEV data are sparse, often deviate from one source to another and should therefore be considered with caution.

Flashbots estimates the total gross extracted MEV between January 2020 and September 2022 to USD 675mn.[176] This is likely to be an underestimate though, as the data cover a limited number of protocols and includes arbitrage and liquidations, but not sandwich attacks.[177] Liquidations (1% of extracted MEV) were negligible in size compared to arbitrage (99%). Unsurprisingly because of their dominant market share among DEXs, Uniswap V2 and V3 concentrated almost 80% of the MEV extracted. Balancer, another DEX protocol, represented 19% of the MEV extracted, with the balance (~1% of total extracted MEV) split across several other protocols.

According to Flashbots estimates, the percentage of block gas used by MEV transactions fluctuated between 0.5% and 1.5% in most cases, with a few spikes to up to 3.5%, suggesting that MEV transactions represented a small fraction of transactions at the time. However, Barczentewicz and Gomes (2024) highlighted that according to one estimate, in 2022, the volume traded on DEXs on the Ethereum blockchain was USD 666 billion. At the same time, the volume of crypto-assets involved in MEV extraction was equivalent to USD 328 billion, meaning that nearly 50% of all trading volume was affected in some way by MEV extraction.

Another source, Chorus One, estimated MEV from arbitrage and liquidations to USD 710mn prior to the Merge, which is consistent with Flashbots' estimates.[178] According to the same source, sandwich attacks totalled USD 1,210mn, bringing the total extracted MEV to USD 1,920mn prior to the Merge.

Qin et al. (2021) estimated the value of MEV extracted from arbitrage, sandwich attacks, and liquidations on Ethereum to USD 540mn over 32 months between December 2018 and August 2021.[179] This profit was divided among 11,289 addresses, with the highest single profit reaching USD 4.1mn, equivalent to more than 600 times the Ethereum block reward.

[176] Cumulated gross profit from January 2020 until September 2022 when Ethereum transitioned from PoW to PoS. Source: MEV Explore (flashbots.net).

[177] The data cover the following 9 protocols: Aave, Balancer, Bancor, Compound, Cream, Curve, Uniswap V2, and Uniswap v3 and 0x.

[178] Distribution of MEV Surplus | Galaxy

[179] For the sandwich and arbitrage, Quin et Al. inspected all the trades performed on Uniswap V1/V2/V3, Sushiswap, Curve, Swerve, 1inch, and Bancor, spanning over 49,691 cryptocurrencies and 60,830 on-chain markets. For liquidations, they collected every liquidation event settled on Aave V1/V2, Compound, and dYdX.

Other initiatives aimed at reconciling users and validators' needs and objectives

Other initiatives aim at capturing the best of both approaches but have not been deployed or not at a large scale yet. The following paragraphs outline the key features of three of them but this list is in no way meant to be exhaustive as again MEV counter-measures remain an area of active research.

Some initiatives focus on mitigation techniques at the application design level. Some DEXs for example aim to address the MEV problem by allowing users to set an **optimal slippage**. Users of DEXs set a tolerance slippage to account for unexpected price changes at the time they trade. Using a low slippage run the risk of transaction failures, but setting a high slippage attracts attackers to reap the difference between the slippage and the actual price (e.g., through sandwich attacks). Heimbach and Wattenhofer (2022) propose an algorithm to calculate the optimal slippage that balances the cost of transaction failures and sandwich attacks.

MEV-share, an open protocol developed by Flashbots that builds on MEV-Boost, protects users by requiring that a portion (90% by default) of the extracted MEV is returned to them.[180] MEV-share allows users to selectively share data about their transactions with searchers who bid to include the transactions in bundles. To do so, MEV-share introduces a new entity, the Matchmaker. In short, the Matchmaker is responsible for forwarding information on the transactions from the users to the searchers (the level of information shared being dependent on the user's privacy preferences), simulating the bundles submitted by the searchers and forwarding the bundle that accrues the most value to the builder. A limitation of MEV-Share is its reliance on the Matchmaker as a trusted intermediary. In addition, MEV-Share does not really address the trade-off between the inclusion-time of a transaction and MEV protection. Indeed, the more information a transaction reveals, the more lucrative it becomes for builders and validators to work to finalize it, as it allows them to extract more MEV profits.

Babel et al. (2024) recently introduced the concept of **Protected Order Flow** (PROF). To prevent order manipulation and at the same time support the timely inclusion of transactions in blocks, PROF creates bundles of privately input transactions whose inclusion is profitable for block builders. PROF consists of two components, namely the PROF sequencer and the PROF merger, and leverages on the fact that Ethereum blocks are seldom full. The PROF sequencer ingests user transactions (routed to PROF, which maintains their privacy) and sequence them into a bundle according to pre-specified rules (e.g., these rules can represent different forms of fair ordering). The PROF merger takes the winning block (i.e., in a PBS framework the most profitable block already constructed by builders) and appends to it the transaction bundle provided by the PROF sequencer. Validators can then decide on whether they want to add or not the appended block to the winning block. Because validators are seeking profit, the idea behind PROF is that they will choose the incrementally higher revenue of a PROF-appended block. This will in turn ensure the timely inclusion of PROF transactions.

MEV Boost: An illustration

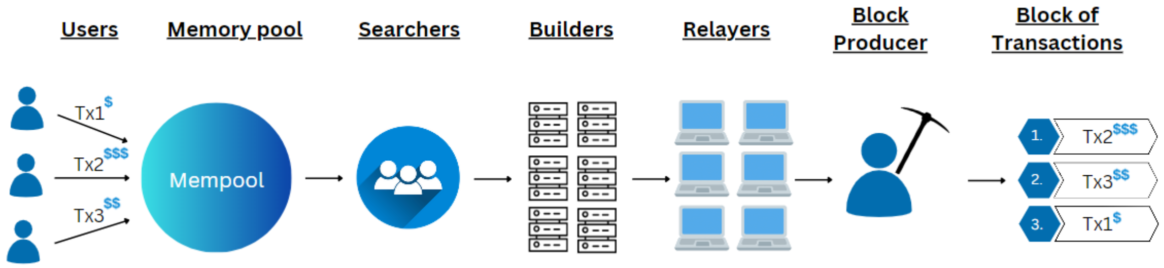
In summary, MEV-Boost enables validators[181] to outsource the task of finding MEV opportunities and building the most profitable block to other parties: searchers and block builders, who take MEV-related activity off-chain. Block construction begins with searchers who identify profit opportunities by sequencing collection of transactions into bundles. Block builders create blocks

[180] For further details on MEV-Share, see Introduction | Flashbots Docs and MEV-Share: programmably private orderflow to share MEV with users - The Flashbots Ship - The Flashbots Collective

[181] For sake of simplicity, the report uses the term 'validator' to refer to proposers and validators indistinctly. In short, a proposer is a validator that has been randomly selected in every slot. His role is to create a new block and send it to other validators, who in turn vote to determine the validity of the block being proposed. For further details on the exact role of proposers and validators in Ethereum's PoS, see Proof-of-stake (PoS) | ethereum.org

from these bundles. Validators select the most profitable blocks (from their transaction fee), without seeing the contents of the blocks. Relays act as trusted mediators between block builders and validators.[182]

Diagram 5. MEV-Boost supply chain



Notes: Ethereum MEV-Boost supply chain.
Sources: ESMA, Chainlink.

(i) Users can submit their transactions through Flashbots' private transaction pool;

(ii) Searchers compete to find the most profitable ordering of transactions, sequence them into bundles and bid for their inclusion in the next block using Flashbots' sealed-bid auction;[183]

(iii) Block builders use the bundles received from the searchers to construct the most profitable block. Using MEV-Boost middleware, they then send an 'execution payload header' (i.e., a cryptographic commitment to the block's contents and total value) to validators via a relay for signing;

(iv) Relays maintain the privacy of a block's contents until a validator commits to proposing it for inclusion in the network;

(v) Validators communicate with relays to get the most profitable block header, which they attest to it by signing with their public key.

[182] Builders trust the relay to not release their blocks in any other circumstance and run the auction with integrity, while proposers trust the relay to ensure that the winning block is valid and will be released in a timely manner. Relays also play an important role in mitigating the risk of DOS attacks by block builders. Prior to MEV-Geth, it would have been possible for a searcher to DOS attack a miner by sending bundles filled with low value transactions costing more to execute than the value extracted

[183] In this system, searchers submit their transaction bundles along with a bid for block space. These bids are sealed, meaning that no one else can see the bid amounts. Block builders then evaluate these bundles using a first-price auction mechanism, where the highest bid wins. A bundle consists of an array of valid Ethereum transactions, a block height, and optionally, a timestamp range over which the bundle is valid. Bundles allow searchers to specify the exact order of transactions. When a bundle is submitted, it is executed atomically, meaning either all transactions in the bundle are executed, or none are. A key difference with the previous Price Gas Auctions is also that non-executed transactions revert off-chain which reduces network congestion and costs for searchers.

Annex 4. Key features of the technical architecture underlying DeFi

Layer 1 blockchains (L1s)

L1s serve as the base infrastructure on which DeFi protocols are built and operate. Examples of L1s are Ethereum, Binance Smart Chain (BSC), Polkadot, Avalanche, Cardano or Solana. They provide the foundational components that DeFi protocols rely on to offer financial services. The key functions of L1s are: a) to settle transactions; b) to ensure that transactions are processed and recorded in a secure, tamper-resistant manner, following a consensus mechanism such as PoW or PoS; and c) to provide the execution environment for SCs, such as the Ethereum Virtual Machine (EVM).

L1 scaling solutions

Layer 1 scaling solutions are modifications or upgrades to the L1 of a blockchain network to improve its scalability – i.e. its ability to handle more transactions per second (TPS), reduce latency, and lower transaction costs. When successful, L1 scaling solutions may offer improved user experience and lower transaction fees. The following are some of the most common types of L1 scaling solutions:

(i) *Sharding*, which consists of dividing a L1 network into smaller segments called shards. As each shard processes and settles its own transactions and smart contracts, this solution reduces the load on a network node and increases TPS. Example: Ethereum implemented sharding in its Ethereum 2.0 project (upgrading the network to a PoS consensus mechanism).

(ii) *Implementing changes in the consensus mechanism* to increase TPS and lower transaction costs. Example: due to congestion problems and high transaction fees in PoW, Ethereum transitioned to PoS, EOS uses Delegated Proof-of-Stake (DPoS), Solana uses Proof-of-History (PoH) or Stellar uses Proof-of-Agreement (PoA).

(iii) *Increasing the size of block of transactions*, which helps reduce congestion and increase TPS. Example: Bitcoin Cash increased the block size from 1MB to 8MB.

(iv) *Reducing the time it takes to create a new block*. Example: while Ethereum block time is approx. 12 seconds and Cardano's 20 seconds, Solana's block time is 400-800 milliseconds.

L2 scaling solutions

Layer 2 scaling solutions (L2s) are solutions designed to improve the scalability of L2s by processing transactions off chain while still relying on the L1 blockchain for the final settlement (and security). By processing transactions off the L1 blockchain and periodically 'reporting' them to the L1, L2 solutions aim to increase transaction speed and reduce user fees. The following are some of the most common types of L2 scaling solutions:

(i) *State channels*, that allow two or more network participants to open a private channel to conduct a series of off-chain transactions, only recording the final settlement of the channel on the L1. Examples: Lightning Network in Bitcoin, or Raiden Network in Ethereum.

(ii) *Rollups*, that bundle multiple transactions and execute them off-chain, then submitting a compressed proof of transactions to the L1. There are two main types: a) *optimistic rollups*, which assume transactions are valid by default and only check for fraud if challenged during a challenge period before posting on the L1 – e.g. Arbitrum, Optimism or Base (by Coinbase) on Ethereum, and b) ZK-rollups, that use so-called zero-knowledge (cryptographic) proofs to verify the validity of transactions before they are posted on the L1 – e.g. Loopring on Ethereum.

(iii) *Sidechains,* to increase transaction speed and reduce transaction costs. Example: due to congestion problems and high transaction fees in PoW, Ethereum transitioned to PoS, EOS uses Delegated Proof-of-Stake (DPoS), Solana uses Proof-of-History (PoH) or Stellar uses Proof-of-Agreement (PoA).

(iv) *Others:* nested blockchains that involve a L1 and a series of L2 chains or hybrid rollups that use a combination of different types of L2 scaling solutions.

<u>Oracles</u>

Oracles are systems or services that provide off-chain data to smart contracts deployed on a L1 network or a L2 solution. Oracles act as intermediaries that collect, verify, and transmit external data to smart contracts so they can perform specific functions based on real-world information. There are four main types of oracles: a) price oracles, which feed real-time price data of all types of assets, b) event oracles, that provide information about real-world events, such as weather conditions or sports results, c) randomness oracles, that provide a source of randomness to lottery or gaming systems, or d) cross-chain oracles, which facilitate communication of information across L1s and/or L2s. Example: Chainlink is the leading oracle provider, with services in Ethereum, Binance Smart Chain (BSC), Polygon, Avalanche, Fantom, Arbitrum, Optimism or Base – accounts for 45.65% of Total Value Secured (TVS) by all oracles in all blockchains and 68.57% of TVS in Ethereum[184].

<u>Cross-chain bridges</u>

Cross-(block)chain bridges are systems that enable the transfer of assets, data, or tokens between two or more blockchain networks (either between L1s or between L1s and L2s) by allowing users to "bridge" assets from one chain to another, increasing the interoperability between different blockchain ecosystems. The bridging typically consists of locking an asset on the source chain and minting an equivalent asset on the destination chain. When the user wants to return the asset to the source chain, the bridged asset is burned, and the original asset is unlocked. Bridges offer DeFi users the possibility to a) transact with lower fees - e.g. bridging an Ethereum asset to a L1 or L2 with lower transaction fees, b) access assets from other blockchain networks – e.g. a BNB chain users can operate with stablecoins issued in Ethereum only, or c) interact with DeFi protocols in other blockchain networks – e.g. a lending protocol on Solana can access liquidity providers from Ethereum.

[184] See: https://defillama.com/oracles

Annex 5. Case study: ICT risks associated to 'flash loan attacks'

A flash loan is a type of uncollateralised, instant loan facilitated by some DeFi lending protocols (see more on the different types of DeFi lending protocols and services in Section 3.1), which allow DeFi users to borrow crypto-assets without collateral as long as they repay back the loan within the same block of transactions settled in the blockchain. This unique type of loan provides DeFi users the opportunity to access crypto-assets without collateral, potentially in connection with complex trading strategies, such as arbitrage, collateral swaps, or refinancing. As a result, DeFi users can profit from temporary price differences across DeFi protocols or restructure positions in a single transaction.

However, flash loans have also consistently been a source for hacks and attacks on DeFi protocols. According to evidence, approx. 20% of value theft from DeFi protocols corresponds to flash loan attacks (see Chart A). Among those attacks, smart contract exploitation is the most frequent vector of attack (see Chart B). Smart contracts are most frequently exploited for flash loan attacks via re-entrancy techniques, as well as the exploitation of diverse math or logic errors related to swaps, incentive rewards or donation functions. Regarding flash loan attacks executed via price manipulation, these occur largely via the exploitation of price feeds provided by oracles.

Chart A. Proportion of thefts in DeFi due to flash loan attack

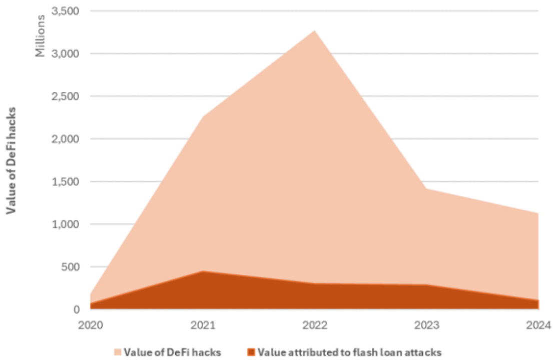
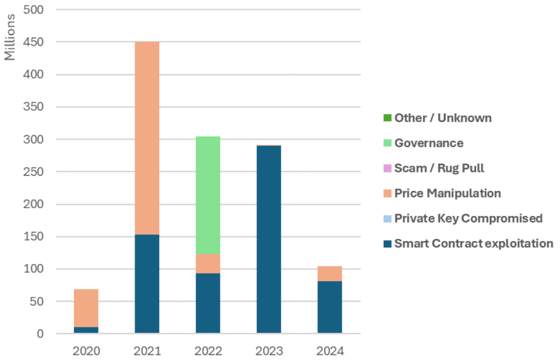


Chart B. Value of thefts via flash loan attacks by attack vector



Sources: EBA, Defillama

Annex 6. DeFi lending: rates paid by borrowers and to lenders

Interest rates paid by borrowers in DeFi lending protocols

The daily average interest rates paid by borrowers ranges between 2.30% and 2.51% for the period between August 2023 and August 2024. However, according to evidence gathered by the Banque de France (2024), borrow rates for the main stablecoins in DeFi lending protocols appear to range closer to 5% historically (between 2020 and the start of 2024), with a significant increase above 5% during the start of 2024. The Banque de France concluded that rates on DeFi lending protocols are volatile and appear surprisingly[185] disconnected from interest rates in traditional finance.

Regarding the period analysed by the EBA and ESMA, the borrowing rates have evolved with a similar pattern across the four crypto-assets, including during rate spikes that lasted brief periods. That is, while borrow rates offered in DeFi lending protocols may be disconnected from rates in traditional finance, they appear to be connected to the rest of the DeFi markets.

	USDT	USDC	WBTC	WETH
Daily Average	2.30%	2.32%	2.35%	2.51%
Daily Min	0.04%	0.12%	0.00%	0.00%
Daily Max	9.92%	14.22%	17.51%	17.83%

Moreover, the daily maximum interest rate paid by borrowers was as high as 17.83% during the analysed period. However, as explained by the Banque de France and as observed during desk-based research, they can be as high as 80%, especially for crypto-assets with smaller liquidity, if there is an imbalance between borrowers and lenders. Moreover, although rates paid have by borrowers followed a similar pattern for the four crypto-assets, the EBA and ESMA analysis found that two of them (USDT and WETH) have suffered one additional phase of volatility that the others have not during the analysed period. This, however, appears not to have dissuaded interest of potential borrowers.

The evidence also points towards wrapped tokens being associated to higher volatility, with minimum rates paid borrowers reducing to zero or close to zero often, but maximum rates also increasing further than those paid by borrowers for loans on stablecoins. This may occur due to several factors: a) as wrapped tokens are tied to highly volatile assets and the value of such assets fluctuates, the demand for wrapped tokens in lending protocols suffers more dramatic shifts; b) borrowing rates in DeFi protocols are often determined by algorithms based on demand and supply, and as wrapped tokens are typically more associated to speculative activities (e.g. margin trading, leveraged positions), their markets may suffer liquidity constraints and demand may suffer more sudden changes; and c) as of 2024, the size of LPs for wrapped tokens still tends to be smaller compared to LPs for stablecoins, which means that the former cannot absorb demand fluctuations as good as the latter.

[185] While DeFi protocols could be expected to 'compete' with borrow rates offered in traditional finance (e.g. US Fed or ECB lending rates), the rates offered by DeFi protocols appear to fluctuate in response to different market movements, such as booms and busts in specific crypto-assets or crypto markets. However, EBA and ESMA note that if crypto markets, and especially DeFi markets were to grow in the EU, DeFi borrowing rates could potentially become more closely connected to traditional financial markets in the EU.

Interest rates paid to lenders in DeFi. The EBA and ESMA also analysed interest rates paid to lenders in DeFi, using data between August 2023 and July 2024. The data shows that rates paid to lenders in DeFi vary widely between rates close to zero and up to 21%. However, the daily averages range between 2.20% and 2.34% for the analysed crypto-assets, although lenders appear to have been able to obtain rates above 5% quite often during the analysed period. Moreover, there is evidence of a certain correlation between the strength of the DeFi lending and borrowing market and the demand for crypto-assets from DeFi lending and borrowing protocols that are available to pay higher rates to depositors.

	USDT	USDC	WBTC	WETH
Daily Average	2.20%	2.30%	2.34%	2.29%
Daily Min	0.03%	0.13%	0.03%	0.05%
Daily Max	11.45%	10.61%	21.05%	11.32%

By comparing the lending and borrowing rates, it can be observed that there is a very marginal space for profit for the protocol across all the crypto-assets. For instance, the daily average rate obtained by DeFi protocols for lending USDT to DeFi users is 2.30%, while the daily average rate they pay to users lending DeFi in the protocol is 2.20%. In the case of USDC, the gap is even smaller, with protocols obtaining 2.32% and users getting 2.30%.

Comparison of lending and borrowing rates with rates in traditional finance

As shown above, crypto borrowers in DeFi pay, on average, rates on the range of 2.30 – 2.50%, while crypto lenders in DeFi get on average, rates between 2.20 – 2.30%. However, during certain periods, crypto lenders are able to get above 5% on their crypto-assets in DeFi.

During the same period analysed by EBA and ESMA, US Savings rates stayed relatively stable at 0.46% and the Deposit Certificate Rate ranged from 5.25% to 5.5%. ECB deposit facilities have moved between 1.50% and 4% during the same period[186]. That is, rates paid by DeFi protocols to crypto lenders stayed within the range between the Savings Rate and the Certificate of Deposit Rate in USD, and close to ECB rates. Consequently, DeFi rates provided customers similar rates to savings deposits. However, DeFi users may prefer, for different reasons, to retain their crypto-assets in DeFi protocols.

The case for borrowing in DeFi is different. During the period analysed, mortgage rates in the US ranged from 6.40% to 7.80%, and credit cards rates ranged from 21.20% to 21.60%. In the EU, bank interest rates in loans to households for consumption[187] have ranged between 5% and 8%, and the rates in loans for house purchasing[188] have ranged between 1.3% and 4%. That is, the rates paid by crypto borrowers in DeFi protocols is often lower than the borrowing rates in traditional finance.

Data source: Kaiko data on AAVE (versions: 1,2,3), Compound and Maker on Ethereum.

Methodological note on "Daily Weighted Rate Average": on a daily basis there are multiple transactions for lending and borrowing. There is separate calculation of the rate between Lending and Borrowing for each token. The daily weighted average rate is calculated with the following formula: Weighted Average = $\frac{\sum(Amount)}{\sum(Rate \times Amount)}$

[186] https://www.ecb.europa.eu/stats/policy_and_exchange_rates/key_ecb_interest_rates/html/index.en.html

[187] https://data.ecb.europa.eu/data/datasets/MIR/MIR.M.U2.B.A2B.A.R.A.2250.EUR.N

[188] https://data.ecb.europa.eu/data/datasets/MIR/MIR.M.U2.B.A2C.AM.R.A.2250.EUR.N

Annex 7. Other DeFi activities attracting users with yields

In addition to DeFi lending and borrowing as analysed in Section 3.1, there are a diverse range of services in DeFi offering users the possibility to earn yields based on different strategies or methods. While they may be smaller in size, the EBA and ESMA consider it is worth monitoring their evolution if the size of DeFi markets were to grow in the future.

- ‘yield farming’ or ‘liquidity mining’ protocols offer DeFi users to earn yield from numerous types of crypto-assets on various blockchains, by using algorithms to automate the transfer of crypto-assets from one protocol to another to maximize yield.
- ‘yield aggregators’ offer DeFi users the possibility to earn yield from various DeFi protocols.
- ‘flash loans’ offer DeFi users uncollateralized, instant loans that must be borrowed and repaid within the same transaction (see Annex 5 on the relevance of flash loans as means for attacks on DeFi protocols).
- ‘leveraged farming’ protocols offer DeFi users to undertake yield farming with borrowed crypto-assets.
- ‘NFT lending’ protocols offer DeFi users to deposit their Non-Fungible Tokens (NFTs) as collateral for crypto loans.
- ‘RWA lending’ protocols offer DeFi users to deposit so-called real-world assets (RWAs) as collateral for crypto loans.

Additionally, the term staking has also been used to refer to other yield-generating activities, which have nothing to do with PoS consensus mechanism. Also commonly referred to as “DeFi staking” or even “stacking”, these are activities whereby a user is provided with an opportunity to obtain a return on their crypto-assets. However, by principle, those activities differ from staking in a number of ways, namely: a) they are not linked to the PoS consensus mechanism (e.g. some are linked to the Bitcoin network, which runs on a PoW consensus mechanism), and b) validators are not involved, so they are simply a centralized or decentralized offer of yield, that can, depending on their characteristics, be comparable to a savings account or to crypto lending.

Annex 8. Failures in centralised crypto borrowers

Celsius

Celsius was a platform that allowed users to deposit crypto-assets in the platform in exchange for earning interest (it also offered lending services against crypto collateral). However, in June 2022, due to a combination of factors linked to liquidity issues, risky practices, and market volatility, Celsius froze all withdrawals, swaps and transfers on its platform, citing "extreme market conditions". This signalled severe liquidity issues within the platform’s operations, and ultimately led to the filing for bankruptcy in the US, revealing billions in liabilities and an inability to meet user obligations - i.e. Celsius reported liabilities of approx. $5.5 billion, including around $4.7 billion owed to users who had deposited funds or crypto-assets on the platform, but assets only valued at about $4.3 billion, leading to a shortfall of $1.2 billion.

The business model of the lending and borrowing services provided by Celsius consisted of taking in short-term deposits (assets) from users (lenders) and lend or invest them in riskier, longer-term projects (liabilities or loans to borrowers). To earn the high yields that were promised to users, Celsius would invest in high-risk projects or facilitate loans to borrowers that were allowed to use volatile crypto-assets as collateral for the loans.

But, following a broader market downturn in 2022, triggered by the failure of Terra/Luna, Celsius users increased their requests to withdraw the assets they deposited in Celsius. As Celsius had locked such assets in risky long-term or illiquid investments, it could not meet user requests.

Voyager Digital

Voyager Digital was a platform that, among other services (e.g. trading and brokerage), allowed users to deposit crypto-assets in the platform in exchange for earning interest. Voyager attracted users with promotions of high yields. On the other side of their business, Voyager was extending loans to high-risk projects and entities. When several of Voyager’s counterparties suffered significant losses as a consequence of the Celsius bankruptcy and the Terra/Luna collapse, Voyager faced a severe liquidity crisis. In particular, Voyager had extended a $650 million loan to Three Arrows Capital (3AC), a crypto hedge fund that declared bankruptcy in June 2022. 3AC became unable to repay the loans extended by Voyager.

In July 2022, suspended all customer withdrawals and ultimately filed for bankruptcy in the US. Voyager’s reliance on a single borrower (3AC), on which insufficient due diligence had been carried out, made it vulnerable to contagion risks.

Annex 9. Staking rewards and 'unstaking'

Penalties and Slashing

In order to function correctly, a blockchain needs validators to remain online and perform their validator duties. In order to incentivize good behaviour, most blockchains have built-in penalties which range in severity depending on the type of behaviour they expect to prevent: a) smaller penalties are applied to incentivize validators not to go offline more than they should – or to perform their validator duties as (often as) they should, and b) more severe penalties can be applied in case of actively nefarious activities or errors such as double signing. To incentivize validator nodes not to try to behave nefariously by engaging in activities such as double-signing. These "punishments" vary across blockchains, and can include the possibility of not gaining the expected reward but also losing part of its stake, of being suspended or of no longer being selected to build blocks. In terms of how this takes place in practice, interrogated providers indicate that penalties will be deducted from future rewards.

Distribution of staking rewards

There are several types of rewards obtained by validator nodes in the lifecycle of the blockchain on which they operate. On Ethereum for example, there are consensus layer rewards, which are new tokens minted by the network and execution layer rewards, which include transaction gas fees paid by users for the fulfilment of their transactions (including any priority fees) and realized MEV (see relevant section of this report). These rewards are all determined by the network and are paid directly to the "withdrawal address" or wallet set by the validator node.

The total amount of tokens minted and the portion attributed to each validator node for the purpose of consensus rewards appears to continuously evolve to reflect the total supply of the relevant governance / native token and the amount of active validators in the network.

In the case of delegated staking, rewards will depend on the fees retained by the providers:

(i) When using "validators-as-a-service", it seems that in most cases, the rewards accrued are the full rewards minus the fee (generally expressed in percentages) subtracted by the third-party node operator

(ii) When using a staking pool, the reward received corresponds to the delegator's percentage stake in the liquidity pool, minus any fee (generally expressed in percentages) subtracted by the liquid staking provider and/or third-party provider.

(iii) When using a centralised trading platform, the reward that can be expected by a delegator is therefore the staking reward, after subtraction of the fee (generally expressed in percentages) retained by the relevant staking providers, namely, as relevant, the third-party validator node operator and/or custody provider.

However, it should be noted that the terms and conditions of some centralised trading platforms suggest that only the consensus layer rewards are passed on to the delegator once the fee has been subtracted, not the execution layer rewards.

As of October 2024, the staking rewards currently set by Ethereum and Solana are 3.46% and 6.73% respectively, with some other networks offering considerably higher APYs still. Using validator-as-a-service, APYs across staking service options offer yields ranging options on 2.29% and 10.25% on Ethereum and 5.94% and 7.74% on Solana respectively (i.e. in some cases more than the network reward).

Indeed, according to EBA and ESMA desk-based research, at some of the main centralised providers, fees charged appear to vary significantly, not only across providers but also across tokens with one same provider and within that same token, based on market and network conditions.

Historically, as mentioned above, the rewards were periodically distributed directed to the withdrawal address "registered" in the network (and then, in the case of delegated staking, passed on as per the relevant service agreement). However, it appears that this is no longer systematically the case since development of liquid staking.

Liquid staking rewards

Liquid staking rewards are accrued by delegators in three ways[189]:

(i) Reward-bearing: The first is identical to the process mentioned above, i.e. new units of the staked token get distributed periodically to the delegated staker. In this case, the value of the LST is generally expected to remain 1:1 as compared to the staked token it represents and if the delegator chooses to unstake, the LST is burned and the delegator retrieves full use of the staked token (after unbonding). The same amount of the staked token can be recuperated after unstaking.

(ii) Rebasing: However, it appears that increasingly, rewards are not distributed to the delegated staker in this way. Here, it seems that instead of earning rewards, the rewards are reflected in an increased value of the LST, which is then valued at 1 LST = 1 staked token + percentage of the rewards earned). When unstaking, the delegator may redeem the staked tokens on the basis of the comparative value of the LST to the staked token (and should in that sense receive the rewards at that point in time (unless the market value of the LST changes).

(iii) Dual token: Finally, in the dual token model, two LSTs are for each staked token, one whose value is pegged to the staked token, and the other that varies in price depednign on staking returns – in a way, a hybrid of the other two models listed above.

Unstaking

"Unstaking" is subject to the unbonding period determined by the network and which may be long and unpredictable. It may also be subject to a maximum amount to be unstaked by the individual delegator, as well as across the provider's delegators. It should also be noted that unstaking there may require the payment of fees, the amount of which may be difficult to anticipate. Where these are large, this may have a considerable impact on the total return related to staking. In addition, forums frequently used by retail crypto-asset clients also suggest other obstacles, such as needing to have the same amount of *non-staked* tokens to mirror the number of tokens to be unstaked, difficulties in withdrawing all of their staked tokens, and the understanding of the return obtained. Furthermore, it remains unclear when the delegator start receiving rewards (when the validator nodes become active, in theory) and whether rewards continue during the unbonding period (this might differ from service to service).

[189] Swell (2023)

Annex 10. Examples of unfair or unclear T&Cs by providers

On interest rates paid or rewards/yields obtained

Providers *do not guarantee that the lender will receive lending rewards and that the applicable percentage of lending rewards (i) is an estimate only and does not constitute a guarantee, warranty or representation of any sort", (ii) "may change at any time for reasons within or outside of the service provider's control, and (iii) there is no guarantee that a return will be made, no security regarding the loaned crypto-assets is given and the loan will be non-recourse*.

On changes to the list of eligible collateral assets

The service provider may (but shall not be obliged to) notify customers of any changes to the list of eligible collateral, may, in its sole and absolute discretion, with or without notice to the customer, vary the collateral requirements at any time (…) and may also stipulate that such collateral requirements shall apply to existing loans, shall be entitled to deposit, pledge, rehypothecate, invest, loan, stake on chain and generally deal with and transfer any collateral in its sole discretion, or may deposit in its general account or any other account, any of customers' collateral and may commingle such collateral with the digital assets, currencies and properties of the service provider or of some other persons.

On actions the service provider may take on collateral assets or staked assets

If (the service provider) determines that additional eligible collateral is required (due to own-initiative collateral requirements), the user shall, upon demand, deposit additional eligible collateral immediately or within a specified period of time (which may be less than 24 hours). Notwithstanding any such demand for additional eligible collateral, the service provider may at any time exercise its rights" to declare the user's default and immediately, without prior notice to the user, suspend, cancel, terminate or liquidate the user's account and loan.

On rights and liabilities in the event of dispute or insolvency

The service provider *has no obligation or ability to return the crypto-assets from the third-party lending provider in the event of default, and all lending through the lending product will be on an unsecured basis meaning that the service provider will not collect or hold collateral from third-party lending provider, nor maintain any collateral account for the retail client's benefit*.

References

Alexander, C., 2024. Leveraged Restaking of Leveraged Staking: What are the risks? SSRN (https://dx.doi.org/10.2139/ssrn.4840805)

Aramonte, S. et al., 2022. *DeFi lending: intermediation without information?*, BIS Bulletin, No 57, July 2024. (https://www.bis.org/publ/bisbull57.pdf)

Auer, R., 2022. *Embedded Supervision: How to Build Regulation into Decentralised Finance*, CESifo Working Paper No. 9771. (http://dx.doi.org/10.2139/ssrn.4127658)

Babel, K., Jean-Louis, N., Ji, Y., Misra, U., Kelkar, M., Yapa Mudiyanselage, K., Miller, A., Juels, A., 2024. *PROF: Protected Order Flow in a Profit-Seekeng World*, Cryptology ePrint Archive. (PROF: Protected Order Flow in a Profit-Seekeng World).

Banque de France, 2024. *Interest rates in decentralised finance*, April 2024 (https://www.banque-france.fr/en/publications-and-statistics/publications/interest-rates-decentralised-finance)

Barczentewicz, M. and Gomes A., 2024. *Crypto-Asset Market Abuse Under EU MiCA* (Crypto-asset market abuse under EU MiCA :: SSNR).

Barczentewicz, M., Sarch A., Vasan N., 2023. *Blockchain Transaction Ordering as Market Manipulation* (Blockchain Transaction Ordering as Market Manipulation (2023) 20 Ohio State Technology Law Journal 1-87)

Barragan, J., 2022. '*The fundamentals of cross-chain MEV*' (The Fundamentals of Cross-Chain MEV | Blocknative).

Binance, General Risk Warning, points S and Z (https://www.binance.com/en/risk-warning)

Bitpanda, Staking (https://www.bitpanda.com/en/staking)

Born, A. et al., 2023. *Decentralised finance – a new unregulated non-bank system?*, July 2022, ECB Macroprudential Bulletin. (https://www.ecb.europa.eu/press/financial-stability-publications/macroprudential-bulletin/focus/2022/html/ecb.mpbu202207_focus1.en.html)

Brodesky, A. S. and Nassr, I. K., 2023. *DeFi liquidations: volatility and liquidity*, OECD Working Papers on Finance, Insurance and Private Pensions, No 48, July 2023. (https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/07/defi-liquidations_89cba79d/0524faaf-en.pdf)

Buterin, V., 2021. 'Proposer/block builder separation-friendly fee market designs', EthResearch (https://ethresear.ch/t/proposer-block-builder-separation-friendly-fee-market-designs/9725).

Buterin, V. 2023. *Don't overload Ethereum's consensus*. Vitalik Buterin's website (https://vitalik.eth.limo/general/2023/05/21/dont_overload.html)

Capponi, A., Jia, R. and Wang, Y., 2023. *MEV and Allocative Inefficiencies in Public Blockchains* (MEV and Allocative Inefficiencies in Public Blockchains :: SSNR).

Carey, R. and Melachrinos, A., 2022. The long and short of Aave, Kaiko Researc, December 2022. (https://blog.kaiko.com/the-long-and-short-of-aave-d61d5c14ad43)

Chainalysis, 2021. *The biggest threat to trust in cryptocurrency: rug pulls put 2021 cryptocurrency scam revenue close to all-time highs*, December 2021. (https://www.chainalysis.com/blog/2021-crypto-scam-revenues/)

Chen, E., Toberoff, A., Srinivasan, S. and Chiplunkar, A., 2023. 'A Tale of Two Arbitrages'. Frontier Research (A tale of two arbitrages | Frontier Tech).

Chiu, J. et al., 2023. *On the fragility of DeFi lending*, Bank of Canada, Staff Working Paper 2023-14, February 2023. (On the Fragility of DeFi Lending - Bank of Canada)

Coinbase, 'What is EIP-1559' (What is EIP-1559? | Coinbase).

Coinbase, Coinbase User Agreement, point 3 (https://www.coinbase.com/en-fr/legal/user_agreement/ireland_europe)

Coinbase, Staking Risks, Coinbase Help (https://help.coinbase.com/en/coinbase/coinbase-staking/staking/staking-risks)

Copeland, T., 2023. 'Jaredfromsubway.eth's MEV bot rakes in millions of dollars in three months.' *The Block* (Jaredfromsubway.eth's MEV bot rakes in millions of dollars in three months (theblock.io)).

Cornelli, G. et al., 2024. *Why DeFi lending? Evidence from Aave V2*, BIS Working Papers, No 1183, July 2024. (https://www.bis.org/publ/work1183.pdf)

CoW DAO. 'Batch Auctions', CoW protocol documentation (https://docs.cow.fi/cow-protocol/concepts/introduction/batch-auctions#:~:text=CoW%20Protocol%20collects%20and%20aggregates%20intents%20off-chain%20and).

Crypto.com, *Crypto.com Staking* (https://crypto.com/fr/staking#staking-faq-section)

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).

Dell'Erba, M., 2024. *Disrupting Shadow Banking or Crypto Shadow Banking*, Technology in Financial Markets: Complex Change and Disruption, Oxford, February 2024. https://doi.org/10.1093/oso/9780198873617.003.0005

Eigenlayer, 2023. *EigenLayer: Restaking and Cryptoeconomic Security*. https://docs.eigenlayer.xyz/assets/files/EigenLayer_WhitePaper-88c47923ca0319870c611decd6e562ad.pdf

EigenPhi, last update in 2024. Market Overview: MEV Scan Daily Report (https://eigenphi.io/mev/ethereum/dailyReport).

ESMA, 2023. 'ESMA TRV Risk Analysis, Decentralised Finance in the EU: developments and risks', Oct. 2023.

ESRB, 2023. '*Report on crypto-assets and decentralised finance: systemic implications and policy options'*, European Systemic Risk Board (ESRB), Task Force on crypto-assets and DeFi, May 2023 (https://www.esrb.europa.eu/pub/pdf/reports/esrb.cryptoassetsanddecentralisedfinance202305~9792140acd.en.pdf?853d899dcdf41541010cd3543aa42d37)

Ethereum, 2024. ‘Proof-of-stake (PoS)’, Ethereum Developers(Proof-of-stake (PoS) (ethereum.org)).

Ethereum, 2024. ‘Proposer-builder Separation’, Ethereum Roadmap (https://ethereum.org/en/roadmap/pbs/).

Ethereum, 2024. *Staking*. (https://ethereum.org/en/staking/)

EY, 2023. ‘An introduction to maximal extractable value on Ethereum’ (An introduction to maximal extractable value on Ethereum | EY).

Ferreira Torres, C., Camino, R., State, R., 2021. *Frontrunner Jones and the Raiders of the Dark Forest: An Empirical Study of Frontrunning on the Ethereum Blockchain*, ResearchGate (Frontrunner Jones and the Raiders of the Dark Forest: An Empirical Study of Frontrunning on the Ethereum Blockchain).

FSB, 2023. *The Financial Stability implications of multifunction crypto-asset intermediaries*, November 2023. (https://www.fsb.org/uploads/P281123.pdf)

Flashbots, 2022. Flashbots Builders, Flashbots Docs (https://docs.flashbots.net/).

Flashbots, last update in 2022. MEV-Explore v1 (https://explore.flashbots.net/).

Flashbots, last update in 2024. Flashbots Transparency Dashboard (https://transparency.flashbots.net/).

Galaxy, 2023. ‘Distribution of MEV Surplus’, Galaxy Insights Research (Distribution of MEV Surplus (galaxy.com)).

Halborn, 2024. *Breaking down the Top 100 DeFi hacks (2016 – 2023)*, August 2024. (https://www.halborn.com/reports/top-100-defi-hacks)

Heimbach, L. and Huang, W., 2024. *DeFi leverage*, BIS Working Papers, No 1171, March 2024. (https://www.bis.org/publ/work1171.pdf)

Heimbach, L., Kiffer, L., Ferreira Torres, C., Wattenhofer, R., 2023. *Ethereum's Proposer-Builder Separation: Promises and Realities,* arXiv (Ethereum's Proposer-Builder Separation: Promises and Realities (arxiv.org)).

Heimbach, L., Wattenhofer, R., 2022. *Eliminating Sandwich Attacks with the Help of Game Theory,* arXiv (Eliminating Sandwich Attacks with the Help of Game Theory)

IOSCO, 2023. *Final Report with Policy Recommendations for Decentralized Finance (DeFi)* (FR14/23 Final Report with Policy Recommendations for Decentralized Finance (DeFi)).

Juels, A., 2020. ‘Fair Sequencing Services: Enabling a Provably Fair DeFi Ecosystem’, Chainlink Blog (https://blog.chain.link/chainlink-fair-sequencing-services-enabling-a-provably-fair-defi-ecosystem/#introducing-the-fair-sequencing-service-fss).

Kelkar, M., Zhang, F., Goldfeder, S., Juels, A., 2020. *Order-Fairness for Byzantine Consensus,* Cryptology ePrint Archive (Paper 2020/269 Order-Fairness for Byzantine Consensus).

Li R., Hu X., Wang, Q., Duan S., Wang, Q., 2023. *Transaction Fairness in Blockchains, Revisited,* Cryptology ePrint Archive. (Paper 2023/1034 Transaction Fairness in Blockchains, Revisited).

Li, T., et al, 2023. *The dark side of DeFi: evidence from meme tokens*, July 2023. (https://chuyi-sun.github.io/repo/papers/meme_token.pdf)

MEV-Boost Pics, last update in 2024. MEV-Boost Dashboard (https://mevboost.pics/).

Neuder, M., Chitra, T., 2024, *The Risks of LRTs*. Ethereum Research (The risks of LRTs - Proof-of-Stake / Block proposer - Ethereum Research)

OECD, 2022. *Why Decentralised Finance (DeFi) matters and the policy implications*, OECD, Paris. (https://www.oecd-ilibrary.org/why-decentralised-finance-defi-matters-and-the-policy-implications_109084ae-en.pdf)

OECD, 2024. *The Limits of DeFi for Financial Inclusion: Lessons from ASEAN*, OECD Publishing, Paris, https://doi.org/10.1787/f00a0c7f-en.

Qin, K., Zhou, L., Gervais, A., 2021. *Quantifying Blockchain Extractable Value: How dark is the forest?,* arXiv (Quantifying blockchain extractable value: How dark is the forest? (arxiv.org)).

Saint Olive M., and Jagdev, S., 2024. *Understanding Slashing in Ethereum Staking: Its Importance & Consequences*, Consensys (https://consensys.io/blog/understanding-slashing-in-ethereum-staking-its-importance-and-consequences)

Sorella Labs, last update in 2024. MEV over time. Sorella Labs Dashboard (https://sorellalabs.xyz/dashboard).

Staked, 2024. Staking Rewards. (https://staked.us/rewards/)

Staking Rewards, 2024. (https://www.stakingrewards.com/)

Swell, 2023. Liquid Staking Token Wars: Reward-Bearing vs Rebasing v Dual Tokens (https://www.swellnetwork.io/post/reward-bearing-vs-rebasing-tokens)

Trail of Bits, 2022. Are Blockchains Decentralized? Unintended centralities in distributed ledgers, June 2022. (https://assets-global.website-files.com/5fd11235b3950c2c1a3b6df4/62af6c641a672b3329b9a480_Unintended_Centralities_in_Distributed_Ledgers.pdf)

Wahrstätter, A., Zhou, L., Qin, K., Svetinovic, D. and Gervais, A., 2023. *Time to Bribe: Measuring Block Construction Market*, arXiv preprint ([2305.16468] Time to Bribe: Measuring Block Construction Market (arxiv.org)).

X. Chen, P. Liao, Y. Zhang, Y. Huang and Z. Zheng, 2021. "Understanding Code Reuse in Smart Contracts," IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER), Honolulu, HI, USA, 2021, pp. 470-479. (https://ieeexplore.ieee.org/document/9425939)

Xiong, X., Wang, Z., Chen, X., Knottenbelt, W., Huth, M., 2023. Leverage Staking with Leverage Staking Derivatives : Opportunities and Risks, arXiv ([2401.08610] Leverage Staking with Liquid Staking Derivatives (LSDs): Opportunities and Risks)

Xu et al, 2020. *Liquidations: DeFi on a knife edge*. (https://doi.org/10.1007/978-3-662-64331-0_24).

Yang, S., Zhang, F., Huang, K., Chen, X., Yang, Y., Zhu, F., 2022. *SoK: MEV Countermeasures: Theory and Practice,* arXiv. (SoK: MEV Countermeasures: Theory and Practice (arxiv.org)).