

Read, Oliver

Working Paper

Decentralised finance: Growth, risks and regulation of a shadow financial system with crypto-assets

wifin Working Paper, No. 18/2025

Provided in Cooperation with:

RheinMain University of Applied Sciences, Wiesbaden Institute of Finance and Insurance (wifin)

Suggested Citation: Read, Oliver (2025) : Decentralised finance: Growth, risks and regulation of a shadow financial system with crypto-assets, wifin Working Paper, No. 18/2025, RheinMain University of Applied Sciences, Wiesbaden Institute of Finance and Insurance (wifin), Wiesbaden

This Version is available at:

<https://hdl.handle.net/10419/328275>

Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

Terms of use:

Documents in EconStor may be saved and copied for your personal and scholarly purposes.

You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.

If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.

WIFIN WORKING PAPER 18/2025

Decentralised Finance: Growth, Risks and Regulation of a Shadow Financial System with Crypto-assets

Oliver Read

10 October 2025

Decentralised Finance: Growth, Risks and Regulation of a Shadow Financial System with Crypto-assets

Oliver Read

*RheinMain University of Applied Sciences
Wiesbaden Business School
Bleichstr. 3
D-65183 Wiesbaden
E-Mail: oliver.read@hs-rm.de*

10 October 2025

Abstract: Decentralised Finance applications aim to replicate existing financial products and services from the highly regulated Traditional Finance (TradFi) system using the distributed ledger technology and smart contracts. An open, multi-layered and composable architecture has facilitated the deployment of many DeFi projects leading to a growing complex network of interacting DeFi protocols. The size of the DeFi market has grown to several hundred billion USD in Total Value Locked by users in DeFi protocols. Important use cases include decentralised lending and borrowing, decentralised exchanges and crypto staking. The DeFi sector is effectively becoming a shadow financial system with crypto-assets. DeFi innovators praise decentralisation and disintermediation of financial products and services as beneficial. On the contrary, regulators and policymakers issue warnings on consumer risks and financial stability risks. Awareness has increased following a string of crypto-related collapses and failures during the Crypto Winter 2022–2023. The emerging consensus is that the DeFi market needs to be supervised, but how? The traditional approach to regulate a few centralised entities and financial intermediaries does not work. Thus, a range of regulatory responses and approaches is being discussed. In the European Union the path has been partly laid by the Markets in Crypto-assets Regulation (MiCA) as the text itself contains mandatory steps to address developments of the DeFi market.

Keywords: crypto-assets, crypto staking, Crypto Winter, DAO, decentralised autonomous organisation, decentralised exchanges, decentralised finance, decentralised lending, DeFi, DeFi protocols, distributed ledger technology, governance token, MiCA, regulation, smart contracts, stablecoins, Total Value Locked, TradFi, TVL

JEL classification: F30, G15, G18, G28, O33, O38

I. Introduction

Crypto-asset markets have experienced a rapid development in recent years: Bitcoin, cryptocurrencies, initial coin offerings, stablecoins, non-fungible token, crypto exchanges, crypto lending and borrowing... Innovators in the crypto-asset sector have launched and deployed applications that copy or adapt features from the highly regulated traditional financial sector to the less regulated crypto-asset sector. Familiar concepts underpinning traditional financial transactions – carried out with fiat money, financial securities or other underlying assets – can be applied and adapted to transactions with crypto-assets. Anyone active in the crypto-asset network can perform transactions, without any special permission, in this new shadow financial system. Traditional financial intermediaries like banks, insurance companies, centralised exchanges or central counterparties are not required for this financial system to work. Hence, it may be described as “decentralised” (British spelling, preferred in this paper) or “decentralized” (US spelling).

The term Decentralised Finance or Decentralized Finance (DeFi) emerged a few years ago in order to describe the idea of replicating existing financial products and services from Traditional Finance (TradFi) with crypto-assets, e.g., transfer of monetary value, pooling of funds, transfer of resources through time and space. DeFi applications are supposed to perform these functions in a decentralised nature and using a permissionless technological infrastructure (ESMA 2023, p. 3). Crypto-asset markets have developed networks of complex interrelationships, between infrastructures, intermediaries and market participants, similarly to the TradFi system (ARNER ET AL. 2025, p. 185).

There is a growing number of publications on the topic of DeFi or elements of the DeFi market, particularly since 2020. The academic research papers by Meyer/Welpe/Sandner (2021) and Meyer/Welpe/Sandner (2022) give a first systematic literature review on DeFi. By now the pool of sources has expanded by many more new publications.

The approach for this working paper consists in analysing publications on DeFi ranging from 2000 to September 2025, with a focus on the subtopic of regulation. For this purpose, relevant reports and policy papers published by standard-setting bodies and recognised international organisations as well as academic research papers on DeFi that are available open access, were selected. This working paper brings aspects and points of view from many high-quality sources together in a way that was not available in the academic literature.

This paper is structured in nine sections. Following this introductory section I, the foundations of DeFi are laid out in section II. Section III walks through important DeFi use cases, here decentralised lending, decentralised exchanges and crypto staking (centralised and decentralised). Section IV looks at the recent DeFi market growth. Section V presents the benefits and risks attributed to the DeFi sector in a number of publications. Section VI reports about collapses and failures related to the DeFi market during the so-called Crypto Winter 2022–2023, which made clear, that there are significant risks lurking. Section VII puts the focus on regulatory responses and approaches concerning the DeFi sector at the international level. Section VIII outlines the current situation on regulating DeFi in the European Union (EU) following the entering into force of the Markets in Crypto-assets (MiCA) regulation in June 2023. This paper closes with an outlook in section IX.

II. Foundations of Decentralised Finance

II.1 Definition of Decentralised Finance

There is neither a legal nor a commonly accepted definition of DeFi, hence this working paper refers several sources. Table 1 displays a sample of definitions found in various high-quality sources. The Financial Stability Board (2023) defines DeFi quite broadly as a set of alternative financial markets, products and systems that operate using crypto-assets and smart contracts built into distributed ledger or similar technology (FINANCIAL STABILITY BOARD 2023, p. 42). For Zetzsche/Arner/Buckley (2020), DeFi means the decentralised provision of financial services through a mix of infrastructure, markets, technology, methods and applications. In their view, DeFi incorporates one or more of the following elements: decentralisation, distributed ledger technology (DLT) and blockchain, smart contracts, disintermediation, and open banking (ZETZSCHE/ARNER/BUCKLEY 2020, p. 173-174).

Source	Definition
Zetzsche/Arner/Buckley (2020)	Decentralized provision of financial services through a mix of infrastructure, markets, technology, methods and applications. Decentralized provision of financial services means, in turn, provision by multiple participants, intermediaries, and end-users spread over multiple jurisdictions, with interactions facilitated, and often in fact enabled in the first place, by technology.
Schär (2021)	An open, permissionless, and highly interoperable protocol stack built on public smart contract platforms, such as the Ethereum blockchain. It replicates existing financial services in a more open and transparent way.
Aramonte et al. (2021)	Financial applications run by smart contracts on a blockchain, typically a permissionless (i.e. public) chain
IOSCO (2022b)	Provision of financial products, services, arrangements and activities that use distributed ledger technology in an effort to disintermediate and decentralize legacy ecosystems by eliminating the need for some traditional financial intermediaries and centralized institutions

OECD (2022)	Provision of financial products and services built as decentralised applications on the blockchain. DeFi promises to replicate various activities in the traditional financial system in an open, decentralised, permissionless and autonomous way.
Financial Stability Board (2023)	A set of alternative financial markets, products and systems that operate using crypto-assets and ‘smart contracts’ (software) built into distributed ledger or similar technology

Table 1: Sample of Decentralised Finance definitions. Source: Own representation adapted from Zetzsche/Arner/Buckley (2020), p. 173-174; Schär (2021), p. 153; Aramonte et al. (2021), p. 23; IOSCO (2022b), p. 1; Financial Stability Board (2023), p. 42; OECD (2022), p. 18.

DeFi applications have the following characteristics: blockchain-based, protocols relying on smart contracts, non-custodial, community-driven and composable (OECD 2022, p. 18; FINANCIAL STABILITY BOARD 2023, p. 5).

- Permissionless public blockchains provide a ledger on which transactions are recorded and become immutable.
- The non-custodial nature means that no central authority or intermediary can gain access to or control the digital assets of the network participants.
- Community-driven means that the network community can contribute in some way, e.g., in case of open-source DeFi protocols the user could himself further develop the computer code underlying the protocols.
- Composable means that existing components of DeFi networks can be combined to create new applications.
- Smart contracts were introduced in 2015 on the Ethereum blockchain, where they play a significant role (BENEDETTI/PIAZZA 2024, p. 1). They are not contracts in a traditional legal sense, but are designed to execute a contract between two transacting parties. For example, a vending machine can be seen as a smart contract between a vendor and someone buying an item from the machine (DEUTSCHE BUNDESBANK 2021, p. 33). Smart contracts are defined as immutable computer programs that run deterministically on the blockchain and execute automatically, interacting with other accounts on the blockchain (BENEDETTI/PIAZZA 2024, p. 6). They effectively replace the trust between parties required in TradFi transactions.

Gogel et al. (2021) compare DeFi and TradFi concerning eleven aspects, including among others differences in investor protection (Table 2).

Aspect	Decentralised Finance	Traditional Finance
Custody of assets	Held directly by users in non-custodial wallets or via smart contract-based escrow	Held by a regulated service provider or custodian on asset owners' behalf
Units of account	Denominated in digital assets or stablecoins	Typically denominated in fiat currency
Execution	Via smart contracts operating on the user's assets	By intermediaries
Clearing and settlement	Writing transactions to the underlying blockchain completes the settlement process	By service providers or clearing houses
Governance	Managed by protocols developers or determined by users holding tokens granting voting rights	Specified by the rules of the service provider, marketplace, regulator and/or self-regulatory organisation
Auditability	Open-source code and public ledger allow auditors to verify protocols and activity	Authorised third-party audits of proprietary code or potential for open-source code that is publicly verified
Collateral requirements	Over-collateralisation generally required	Either no collateral or collateral less than or equal to the funds provided
Cross-service interaction	Any service may integrate with any other service on the same blockchain, and potentially across chains	Limited
Access and privacy	Identity verification requirements under discussion by anti-money laundering regulators	Identity checks conducted by service providers
Security	Vulnerable to hacks and other technical and operational risks of smart contracts	Vulnerable
Investor protection	Users assume all risks as a default, although private redress arrangements such as DeFi insurance offer some protection against losses	Government-mandated disclosure and consumer protections, anti-fraud enforcement, exposure limits, and insurance schemes

Table 2: Decentralised Finance versus Traditional Finance. Source: Adapted from Gogel et al. (2021), p. 4-5.

II.2 Multi-layered Architecture of Decentralised Finance

DeFi can be represented as a multi-layered architecture with every layer having a distinct purpose. The layers built on each other (or stacked) create an open and composable infrastructure that allows anyone to build on. Schär (2021) defines a conceptual framework with five hierarchical layers: settlement, asset, protocol, application, and aggregation layer (Table 3) (SCHÄR 2021, p. 155-156).

Number	Layer	Definition
1	Settlement layer	Consists of the blockchain and its native protocol asset (e.g., BTC on the Bitcoin blockchain and ETH on the Ethereum blockchain).
2	Asset layer	Consists of all assets that are issued on top of the settlement layer. This includes the native protocol asset as well as any additional assets that are issued on this blockchain.
3	Protocol layer	Provides standards for specific use cases, usually implemented as a set of smart contracts and can be accessed by any user.
4	Application layer	Creates user-oriented applications that connect to individual protocols. The smart contract interaction is usually abstracted by a web browser-based front end, making the protocols easier to use.
5	Aggregation layer	Aggregators create user-centric platforms that connect to several applications and protocols. They usually provide tools to compare and rate services, allow users to perform otherwise complex tasks by connecting to several protocols simultaneously, and combine relevant information in a clear and concise manner.

Table 3: Decentralised Finance layers. Source: Adapted from Schär (2021), p. 155-156.

In the literature there are slightly different versions of this so-called DeFi stack (including IOSCO 2022b, p. 4; ESMA 2023, p. 17). The sources often include a graphical depiction as a stack. The settlement layer, containing the underlying blockchain like Ethereum, is the base lying at the bottom of the stack. Multiple layers are built on top. End-user applications are located at the top layers of the stack.

The DeFi ecosystem is seen as a complex web of interconnections involving multiple actors like protocol creators, developers, so-called decentralised autonomous organisations (DAOs) and institutional and retail end-users. Some of the DeFi features already mentioned (permissionless blockchain, smart contracts) play an important role in the corresponding layers (FINANCIAL STABILITY BOARD 2023, p. 5):

- Permissionless blockchains provide a ledger on which transactions are recorded and become immutable on the settlement layer.
- Smart contracts and DeFi protocols are located in the protocol layer. Smart contracts fulfil the terms and conditions of a transaction in an automated manner. DeFi protocols combine smart contracts and user interfaces and contain the terms, conditions, and standards by which DeFi products and services are offered.
- Decentralised applications (dApps) allow users to interact with smart contracts via a set of graphical interfaces and other components. These are located in the application layer.

II.3 Centralisation versus Decentralisation of Decentralised Finance

DeFi applications aim to provide financial products and services without centralised entities. The contracting processes are digitised and automated. This is supposed to give users much greater anonymity and in future improve efficiency by reducing intermediation layers (ARAMONTE ET AL. 2021, p. 23). However, in a number of situations, projects in the crypto ecosystem cannot be characterised by decentralisation and disintermediation (ARNER ET AL. 2025, p. 186). DeFi applications can in fact show centralisation akin to TradFi.

Aramonte et al. (2021) even speak of a “decentralisation illusion”. In their view, the need for governance makes some level of centralisation inevitable and structural aspects of the system lead to a concentration of power. The blockchains and applications they support, which are designed to run autonomously, could be described as being decentralised. Nonetheless, it appears impossible to write computer code spelling out what actions to take in all contingencies in advance. Thus, a certain degree of centralisation allows the DeFi project developers to deal with “algorithm incompleteness” (ARAMONTE ET AL. 2021, p. 27).

The 2022 Decentralized Finance Report issued by the International Organization of Securities Commissions (IOSCO) casts doubt on the claim that the DeFi market is a peer-to-peer marketplace with no centralised insiders in control. A few central actors of a DeFi project can often retain control for example through the distribution of so-called governance tokens (IOSCO 2022a, p. 1; IOSCO 2022b, p. 9). There is no definition of what causes a DeFi application to be considered decentralised, i.e., with no concentration of ownership, voting power or control as to the product or service, enterprise or user asset. Some DeFi platforms may actually have a certain level of centralisation, for example because the founders still retain control over certain aspects (IOSCO 2022b, p. 9).

The 2023 report “Financial Stability Risks of Decentralised Finance” published by the Financial Stability Board (FSB) identifies several factors that contribute to an increased decentralisation (FINANCIAL STABILITY BOARD 2023, p. 12):

- Custodial control: Users have self-custody of their crypto-assets, meaning they can make transactions using their assets without an intermediary.
- Execution control of a transaction: Users can execute a transaction within a protocol without being controlled or censored by any intermediary, hence transactions are immutable.
- Distribution of decision-making: DeFi protocols use various mechanisms to distribute governance roles amongst users, through the use of governance tokens and decentralised

autonomous organisation (DAOs). This allows users to propose and vote on changes to the DeFi protocol.

- Resilience against censorship: Resilience to malicious takeovers by bad actors, therefore mitigating against instances of collusion and censorship.

Table 4 shows features of a pure centralised versus a pure decentralised architecture.

Pure Centralised	Pure Decentralised
Governance decision and administrative privileges are reserved for centralised operators	Governance decision and administrative privileges are distributed to a dispersed network of independent users
Users of the protocol cannot make or propose changes to the protocol or access underlying information without it being disclosed	Users have equal access to information and ability to vote to change aspects of the protocol

Table 4: Pure centralised versus pure decentralised architecture. Source: Adapted from Financial Stability Board (2023), p. 12; IOSCO (2022b), p. 9-10.

In practice, decentralisation is not a binary feature. DeFi platforms are likely to be between both opposite poles. When looking at a particular DeFi application, it is important to identify what features and activities involve central actors or parties (IOSCO 2022b, p. 9). A DeFi project may have the potential to become more decentralised over the course of its development. It could start as a centralised project with the end goal of decentralising incrementally over time (IOSCO 2022b, p. 10; WORLD ECONOMIC FORUM 2021, p. 9).

Schuler et al. (2024) complain that the term DeFi lacks a clear definition and that there are ways in which centralised entities or individuals may have special privileges and exert control over a DeFi project. The authors make a distinction between genuine DeFi, Centralised Finance (CeFi) and on-chain CeFi:

- Genuine DeFi: DeFi project with an independent, neutral infrastructure;
- CeFi: traditional financial intermediaries with a custodial model, e.g., centralised exchanges or crypto banks;
- On-chain CeFi: centralised, custodial financial services that are blockchain-based.

Schuler et al. (2024) analyse possible “centralisation vectors” of DeFi projects using the conceptual framework of the DeFi stack (Table 5). Their suggestion is to identify on which layer the DeFi project is active, look for endogenous restrictions and privileges of the project itself, and determine whether there are dependencies on that layer that may lead to a “centralisation inheritance” (SCHULER ET AL. 2024, p. 241-242).

DeFi Layer	Centralisation Vector	Criticality
Settlement layer	Restrictions on network access	High
	No or limited availability of open-source clients to operate a node	Medium-high
	Restrictions in terms of access to transaction data or execution logic	High
	Very high hardware requirements to operate a full node	Medium-high
	Closed set of consensus relevant nodes	High
	Closed set of consensus relevant resources	Low-high
Asset and protocol layers	Restricted function	Low-high
	Upgradability (specific type of restricted functions)	Medium-high
	Account-based governance (for executing restricted functions)	High
	Token-based governance (for executing restricted functions)	Low-high
	Integration with other assets or protocols	Low-high
	External promises	High
Application and aggregation layers	Web-based applications	High
Non-custodial off-chain user interfaces	Provision via centralised servers	High

Table 5: Possible centralisation vectors of DeFi projects. Source: Adapted from Schuler et al. (2024), p. 241-242.

II.4 Governance Mechanisms in Decentralised Finance

Shah et al. (2023) explain that DeFi applications are built on an open-source principle and aim to give users permissionless access to their services. Theoretically, the decision-making power of the application should not be monopolised. However, sometimes decisions on changes need to be made to ensure the longevity and success of the DeFi platform. Many DeFi projects have shifted decision-making power away from a small team of founding members or one entity to stakeholder communities through so-called governance tokens (SHAH ET AL. 2023, p. 172).

A 2021 DeFi policy paper by the World Economic Forum (WEF) differentiates three forms of DeFi governance (WORLD ECONOMIC FORUM 2021, p. 9):

- Centralised governance: The operator controls and implements changes of the DeFi protocol directly.
- Partially decentralised governance: Governance token holders receive limited voting rights and may have power over a few parameters. Developers either may retain effective veto power through large governance token holdings or may have no formal obligation to implement proposed changes.
- Decentralised governance: Decision-making power goes to a community of token holders through the establishment of a decentralised autonomous organisation (DAO). DAO participants can vote on changes to the DeFi protocol and are aligned through token incentives and rules written into smart contracts. Governance decisions are executed as

blockchain transactions, enforced through the consensus mechanisms of the settlement layer.

According to the 2023 DeFi report by the Financial Stability Board, a DAO purports to be an entity governed by its community. The future of the entity should be determined entirely by the members of the community, for example through governance tokens. Voting power is typically proportional to the holdings of the DAO's governance tokens, which are in principle open to be acquired by anyone. In reality, voting control can be highly concentrated. The report shows that in well-known DeFi applications (Uniswap, PancakeSwap, Aave, Compound, Ampleforth) over 85% of the DeFi governance tokens is owned by the top 100 addresses or wallets. Furthermore, DeFi platforms could allow for a delegated decision-making authority to avoid situations where decisions would take long to be approved by the governance token holders (FINANCIAL STABILITY BOARD 2023, p. 13).

An important case demonstrating the shortcomings of DeFi governance is an attack or exploit on "The DAO", a decentralised crowdfunding platform implemented on the Ethereum blockchain with USD 150 million in value with the goal of funding decentralised application development. In 2016 before the investment stage, an attacker exploited a coding error or bug to drain 40% of the funds into a "child DAO". The developers of "The DAO" could not stop the withdrawal because the smart contract could not be altered. However, the majority of miners on the Ethereum blockchain agreed to implement a hard fork that effectively reversed the theft on the forked Ethereum blockchain. The rationale was to limit the damage to the reputation of Ethereum as platform for smart contracts. A minority faction stayed on the deprecated blockchain which became known as "Ethereum Classic". This case shows how supposedly immutable entries on the Ethereum blockchain can be cancelled retroactively, in order to confiscate stolen funds from an attacker (DEUTSCHE BUNDESBANK 2021, p. 34; WORLD ECONOMIC FORUM 2021, p. 15). In October 2020, an attacker used a so-called flash loan to buy USD 7 million of the governance token associated with the MakerDAO protocol and exercised its rights to vote on a governance proposal. In the aftermath, MakerDAO adopted restrictions to prevent this from happening again (WORLD ECONOMIC FORUM 2021, p. 17).

III. Use Cases of Decentralised Finance

III.1 Overview of Use Cases

Several DeFi use cases with different naming conventions are mentioned in high-quality publications (Table 6). The denominations vary slightly, because there is no globally established taxonomy for the use cases.

Source	Use Cases
Aramonte et al. (2021)	• Trading (funds transfer, asset trading, derivatives trading) • Lending (secured lending, unsecured lending) • Investing (investment vehicles)
Born et al. (2022)	• Credit • Trading • Payments • Insurance • Investment (assets and derivatives)
Brühl (2021)	• Payments • Savings/loans • Trading platforms • Capital markets
Financial Stability Board (2023)	• Decentralised lending and borrowing • Trading platforms • Asset management and yield farming • Derivatives and synthetic assets • Margin trading
Gramlich et al. (2022)	• Stablecoins • Decentralised exchanges • Lending and borrowing • Derivatives • Insurances • Asset management
IOSCO (2022b)	• Lending and borrowing • Derivatives/synthetics • Trading • Insurance or risk protection • Asset management and advisory activity • Clearance and settlement activity • Custody and custodians
World Economic Forum (2021)	• Stablecoins • Exchanges • Credit • Derivatives • Insurance • Asset management
Zetzsche et al. (2023)	• Cryptocurrencies • Clearing and settlement systems • Trading platforms • Investment funds • Crypto lenders

Table 6: Use cases of Decentralised Finance. Source: Own representation adapted from Aramonte et al. (2021), p. 23; Born et al. (2022), p. 5; Brühl (2021), p. 634; Financial Stability Board (2023), p. 13-16; Gramlich et al. (2022), p. 19-25; IOSCO (2022b), p. 11-14; Zetzsche et al. (2023), p. 29.

These are some of the most common DeFi use cases with examples of DeFi applications deployed:

- Decentralised cryptocurrencies including stablecoins: Bitcoin (BTC), Ether (ETH) and Tether (USDT) (ZETZSCHE ET AL. 2023, p. 29);
- Decentralised lending and borrowing: Aave, Compound Finance, JustLend, Venus and MakerDAO (ARAMONTE ET AL. 2021, p. 27; FINANCIAL STABILITY BOARD 2023, p. 13; ZETZSCHE ET AL. 2023, p. 29);
- Decentralised exchanges: SushiSwap, Dodo, Uniswap, PancakeSwap, Curve DAO, dYdX and KyberSwap (ZETZSCHE ET AL. 2023, p. 29);
- Decentralised derivatives: Yearn Finance and dYdX (BORN ET AL. 2022, p. 5; FINANCIAL STABILITY BOARD 2023, p. 15);

Crypto staking appears on none of the lists in the sources between 2021–2023, but since 2024 it has gained relevance in the DeFi market. The following subsections III.2 – III.4 cover three selected cases: decentralised lending and borrowing, decentralised exchanges and crypto staking.

III.2 Decentralised Lending and Borrowing

Borrowing and lending of funds is an important business of banks as financial intermediaries. Normally, the bank manages the spread between the interest rates it pays to short-term depositors and the interest rates it receives from borrowers on longer-term loans. The bank has to assess creditworthiness of borrowers and set interest rates with embedded credit spreads to account for default risk (GOGEL ET AL. 2021, p. 12).

By contrast, crypto lending platforms provide loans in crypto-assets from one user (lender) to another (borrower). Centralised service providers organise the crypto lending and charge a commission on each transaction to make a profit. Alternatively, decentralised lending is carried out by DeFi lending protocols running smart contracts whose functioning is administered by a DAO (ZETZSCHE ET AL. 2023, p. 52).

According to Zetzsche (2023), crypto lending protocols offer the following lending services (ZETZSCHE ET AL. 2023, p. 53):

- Peer-to-peer lending: Automatically matches borrowers and lenders one on one.
- Direct lending: The lending platform uses its own crypto-assets, previously transferred by users, to lend to the borrower.
- Pool lending: Users commit crypto-assets as funds to a pool from which other users can borrow. Users can deposit or withdraw crypto-assets from the pool by interacting via smart contracts. In return for locking in crypto-assets, the lenders receive tokens certifying their deposits. The tokens represent the claim of the lenders and reward the holder by distributing interest.

DeFi loan platforms require neither the borrower nor the lender to identify themselves. Everyone has access to the platform and can potentially borrow or lend to earn interest. DeFi loans are completely permissionless and not reliant on trusted relationships. (SCHÄR 2021, p. 164). Users have to link their wallet containing crypto-assets to the DeFi lending protocol and thus render it subject to the conditions of the lending algorithm (ZETZSCHE ET AL. 2023, p. 53).

DeFi loans are an essential component of the DeFi ecosystem. According to the 2022 policy paper by the Organization for Economic Co-operation and Development (OECD), DeFi lending accounted for more than half of the Total Value Locked (TVL) in DeFi applications as of June 2021 (OECD 2022, p. 27).

DeFi lending platforms, such as Aave, Compound and MakerDAO, work with pooled assets provided by lenders in exchange for interest. The identities of the participants are typically unknown. Most DeFi loans have no specified maturity, hence they are referred to as perpetual, and can be repaid at any time. (FINANCIAL STABILITY BOARD 2023, p. 13-14).

Because of the lack of a trusted counterparty relationship, a mechanism is necessary to ensure that loans are repaid and the lender is protected (FINANCIAL STABILITY BOARD 2023, p. 14; SCHÄR 2021, p. 164).

DeFi loans can be closed as transactions without collateral as so-called “flash loans”. Users can instantaneously borrow, execute a transaction, and repay the loan within the same blockchain transaction of the DeFi protocol like done in Aave and dYdX. The transactions required for the flash loan to be executed are in a single block. Either all or none of them are settled. This is referred to as atomic settlement. In case the borrower has not returned the funds (plus interest)

at the end of the transaction's execution cycle, the transaction will be invalid and any of its results (including the loan itself) are reverted. Flash loans can only be employed in applications that are settled atomically and entirely on-chain. They are an efficient instrument for arbitrage and portfolio restructuring with settlement on the blockchain. Flash loans can also be used by market manipulators and attackers ("flash attacks") to borrow large amounts of crypto-assets and manipulate prices simultaneously on different platforms or exploit governance vulnerabilities of protocols e.g., MakerDAO (FINANCIAL STABILITY BOARD 2023, p. 14; GOGEL ET AL. 2021, p. 12; SCHÄR 2021, p. 164).

Alternatively, DeFi loans can be fully secured with crypto-assets as collateral. The collateral is locked or held in a smart contract and can only be released once the debt is repaid. Lending platforms often require over-collateralisation by setting a collateral factor (typically up to 80% of the collateral value posted) in order to buffer against price fluctuations of the collateral (e.g., a volatile crypto-asset). If the collateral value falls below a specified ratio of the loan value, additional collateral has to be posted. This is the equivalent to a margin call known in TradFi (e.g., cash collateral posted by transaction parties in derivatives exchanges). Borrowers must maintain the collateral requirements continuously, often within minutes. If additional collateral is not provided, the collateral is automatically liquidated to pay back the debt. In some DeFi lending protocols a percentage of interest paid by borrowers can be allocated to a reserve pool as a protection mechanism to repay lenders when a liquidation fails to cover the value of the loan (known as a failed liquidation) (FINANCIAL STABILITY BOARD 2023, p. 14; GOGEL ET AL. 2021, p. 13; OECD 2022, p. 27; SCHÄR 2021, p. 164). Collateralised loan platforms exist in three variations: Collateralised debt positions, pooled collateralised debt markets, and peer-to-peer collateralised debt markets. Collateralised debt positions are loans that use newly created tokens, while debt markets use existing tokens and require a match between a borrowing and a lending party (SCHÄR 2021, p. 164).

Most DeFi lending platforms entice users to provide liquidity/funds in crypto-assets to the platform and reward them with tokens which are native to the platform. The rates at which users (i.e., lenders) are rewarded depend on the demand and supply of liquidity, rather than the creditworthiness of the borrower (OECD 2022, p. 27). Interest rates may be determined by the ratio of supply to borrowing or the utilisation rate (total loans divided by total deposits of the assets) (GOGEL ET AL. 2021, p. 12; GRAMLICH ET AL. 2022, p. 22). Lenders receive platform-native tokens representing their tokens plus the interest rate. Lenders receive and borrowers pay the same interest rate. Transactions fees may accrue to service providers (GOGEL ET AL. 2021,

p. 12). The interest rate function can be either linear, nonlinear (dYdX), or kinked (Compound and Aave), determining at which rate the interest rate increases or decreases (GRAMLICH ET AL. 2022, p. 22). For example, in the Compound DeFi lending protocol loans have an unlimited duration and the interest is not simply credited once a year or monthly, but always at the time of a new Ethereum block, i.e., approximately every 15 seconds. A liquidation penalty applies (BITKOM 2020, p. 12).

So far, interest rates in DeFi lending protocols tend to be higher than those available for TradFi lending (Table 7). High DeFi interest rates have been a driving factor for growth of the DeFi credit market especially in a prolonged low interest rate environment for fiat money (OECD 2022, p. 27).

Borrowing in %	DAI	ETH	USDC	USDT	WBTC	LINK	ZRX	BAT	COMP	TUSD	REP	CRV	UNI	SNX
Maker	0.67													
Compound	3.78	2.84	3.13	3.45	4.52	5.4	6.79	7.02	5.82	3.28	14.44			
Aave	3.97	0.59	3.38	12.74	0.76	0.57	101.67	3.51		2.61	0.34	6.92	1.19	10.87
dYdX	5.58	1.29	5.47									17.4	1.79	5.94
Cream	7.97	4.12	10.61	14.38	5.23	1.91			8.04					
Definer	3.21	1.77	2.59	2.93	1.21	7.18	4.34	4.50						
Lending in %	DAI	ETH	USDC	USDT	WBTC	LINK	ZRX	BAT	COMP	TUSD	REP	CRV	UNI	SNX
Maker	0.01													
Compound	2.37	0.18	1.77	2.15	0.38	0.57	0.76	0.84	0.69	1.95	0.00			
Aave	3.52	0.02	2.55	5.43	0.02	0.00	1.85	0.54		0.91	0.03	2.46	0.07	2.40
dYdX	1.42	0.08	1.33											
Cream	2.81	0.88	5.22	8.36	1.40	0.11			1.81			8.05	0.09	1.00
Definer	3.21	1.41	2.59	2.85	1.21	1.84	4.27	3.60						

Table 7: Snapshot of DeFi borrowing and lending rates on 3 August 2021. Source: Adapted from OECD (2022), p. 29-30, data from Infotheblock.com.

Aramonte et al. (2022) look at the rise of the DeFi lending market from a macroeconomic perspective. In their view, lenders have been attracted by high interest rates that often exceed

those on bank deposits or money market funds. Borrowers use DeFi lending to gain leveraged exposure to crypto-assets or adjust portfolios (ARAMONTE ET AL. 2022, p. 1). Two suggestions are made for substantial changes of the DeFi lending business (ARAMONTE ET AL. 2022, p. 5-6):

- DeFi lending should engage in large-scale tokenisation of real-world assets, otherwise it would remain a self-referential system fuelled by speculation. Representing assets such as buildings or capital equipment on the blockchain, so that it can serve as collateral underpinning loans, would be beneficial for small and medium enterprises, which have more limited access to finance.
- In order to serve the un- or underbanked, DeFi should abandon anonymity and use real names. Some initial steps are already being taken. One major DeFi platform launched a lending pool in which participants are required to disclose their identities. Others seek to create credit scores that embed details available off-chain.

There is empirical research on selected aspects of decentralised lending and borrowing including academic papers by Gudgeon et al. (2020), Qin et al. (2021), Heimbach/Huang (2024), and Cornelli et al. (2025).

Gudgeon et al. (2020) review the methodologies used to set interest rates on the DeFi lending platforms Compound, Aave and dYdX (Table 8).

Protocol	Interest Rate Model	Stable Interest Rate	Variable Interest Rate	Governance Token	Interest-bearing Derivative Token	Additional Functionalities
Compound	Kinked	No	Yes	Yes	Yes	
Aave	Kinked	Yes	Yes	Yes	Yes	Swap rates, flash loans
dYdX	Non-linear	No	Yes	No	No	Decentralised exchange, flash loans

Table 8: Comparison of DeFi lending protocols. Source: Adapted from Gudgeon et al. (2020), p. 4.

The authors provide an empirical examination of how interest rate rules have behaved since their inception in response to differing degrees of liquidity (GUDGEON ET AL. 2020, p. 1). Table 9 shows that the cryptocurrencies (or stablecoins) ETH, USDC and DAI account for the majority of loanable funds on the three DeFi lending protocols (GUDGEON ET AL. 2020, p. 5).

Nr.	Cryptocurrency	Compound	Aave	dYdX
1	ETH	76.58	4.80	19.41
2	USDC	31.54	4.12	6.58
3	DAI	24.82	0.95	4.64
4	SAI	36.94		
5	USDT		3.92	
6	BAT	0.95	0.08	
7	LEND		3.60	
8	LINK		12.21	

Table 9: Total amount locked of DeFi loans (median in million USD, since each market's inception until 7 May 2020) across Compound, Aave, dYdX. Source: Adapted from Gudgeon et al. (2020), p.

5.

Qin et al. (2021) did research on the breadth of the lending and borrowing markets on the Ethereum blockchain for the DeFi platforms Aave, Compound, MakerDAO, and dYdX, (over 85% of lending market). The authors systematise the prevalent liquidation mechanisms and provide a methodology to compare them. They measure various risks that liquidation participants are exposed to and quantify the instabilities of existing lending protocols (QIN ET AL. 2021, p. 1).

Heimbach/Huang (2024) examine DeFi leverage, defined as asset-to-equity ratio, using wallet-by-wallet data on major DeFi lending platforms. According to the authors, the overall DeFi leverage typically ranges between 1.4 and 1.9. The largest and most active users consistently exhibit higher leverage in comparison to the rest. Leverage is mainly driven by loan-to-value requirements and cost of borrowing, as well as crypto-asset market price movements and sentiments. Higher borrower leverage generally undermines lending resilience, particularly increasing the share of outstanding debt close to being liquidated (HEIMBACH/HUANG 2024, abstract).

III.3 Decentralised Exchanges

Many crypto-asset holders or investors would like to rebalance exposure according to their preferences and risk profiles and adjust portfolio allocations (SCHÄR 2021, p. 161). Crypto-asset trading platforms are marketplaces that allow users to exchange crypto-assets for one another or for fiat currency. The following distinction between crypto exchanges can be made: centralised exchanges (CEX) and decentralised exchanges (DEX) (FINANCIAL STABILITY BOARD 2023, p. 14).

In CEX, traders have to trust an operator to safeguard user funds, provide accurate price information, match buyers and sellers to process trades, settle transactions, and engage in transaction monitoring. This applies to exchanges that are purely fiat-based (e.g., NASDAQ), or mixed fiat- and crypto-based (e.g., Coinbase), or purely crypto-based (GOGEL ET AL. 2021, p. 10). CEX rely on order books i.e., a centralised party stores demand and supply orders and matches them. A buy order is paired with an opposing sell order for an equal amount and price (GRAMLICH ET AL. 2022, p. 21). On CEX, traders must first deposit assets with the exchange. They forfeit direct access to their assets and have to trust the exchange operator. Dishonest or unprofessional exchange operators may disappear with entrusted funds, may confiscate assets or may lose assets by getting hacked. CEX are a single point of attack and face the constant threat of becoming the target of malicious third parties (GRAMLICH ET AL. 2022, p. 21; SCHÄR 2021, p. 161).

By contrast, a DEX mitigates the trust requirement. Users don't have to rely on a single trusted entity. They remain in exclusive control of their assets until the trade is executed, instead of having to deposit their funds with a centralised party (FINANCIAL STABILITY BOARD 2023, p. 14; GRAMLICH ET AL. 2022, p. 21; SCHÄR 2021, p. 161). DEX can be accessed programmatically with noncustodial wallets. Transactions are automatically processed by smart contracts on a peer-to-peer basis or against a pool of capital (GOGEL ET AL. 2021, p. 10). Users cannot exchange crypto-assets for fiat currencies (FINANCIAL STABILITY BOARD 2023, p. 14). Trade execution happens atomically through a smart contract. Both sides of the trade are performed in one indivisible transaction, mitigating the counterparty risk. Depending on the exact implementation, the smart contract may assume additional roles, effectively making many intermediaries such as escrow services and central counterparty clearing houses (CCPs) obsolete (SCHÄR 2021, p. 160).

Two of the most prominent types of DEXs are order book exchanges and automated market makers (FINANCIAL STABILITY BOARD 2023, p. 14).

In order book exchanges, buyers and sellers communicate their order to a third party (relayer) or DEX operator, who posts it to the order book and publishes that information so that an interested counterparty (taker) can match it. Settlement occurs on-chain and order books are usually maintained off-chain (FINANCIAL STABILITY BOARD 2023, p. 14).

Automated market makers (AMMs) are autonomous protocols that perform the role of market makers, i.e., they make sure there is liquidity for crypto-asset trading pairs. A liquidity pool

holds both assets of a trading pair and acts as counterparty to trades. A holder of crypto-assets can lock up funds as liquidity for potential trades. Users that demand liquidity can tap the liquidity pools locked inside smart contracts. Pools are usually set up as trading pairs of crypto-assets on the basis of deposits made by any entity or person interested in providing liquidity in exchange for a fee. An algorithm determines the exact amount and price at which an order is executed depending on the ratio of the assets in the liquidity pool. When trading against this liquidity pool, that is supplying only one asset and receiving the other asset, the pool ratio shifts and the price moves. The price of any trade is determined algorithmically as a function of the ratio of available liquidity in the assets being traded (FINANCIAL STABILITY BOARD 2023, p. 14-15; GOGEL ET AL. 2021, p. 10; GRAMLICH ET AL. 2022, p. 22).

Uniswap is a DEX implemented as AMM protocol built on Ethereum. Uniswap users can provide liquidity for others who want to exchange tokens or they can exchange tokens against each other. Uniswap uses an algorithm in which the product of the liquidity pool token count in the two crypto-assets being traded always equals a constant. Buying tokens removes them from the liquidity pool, causing their price to increase in order to maintain the constant. Uniswap charges a trading fee, part of which is distributed to liquidity providers. In mid-2020, an anonymous developer forked the Uniswap software to create SushiSwap. It added a governance token, whereby the community votes on major changes to the protocol. A portion of trading fees across the platform are paid out to the token holders (BITKOM 2020, p. 13-14; GOGEL ET AL. 2021, p. 10).

In 2023 the developers and investors of Uniswap were subject to a securities class action in the US by investors who lost money by investing in scam tokens traded on the DEX. The US court in charge dismissed the claims on the basis that the developer of computer code for a software platform is not liable for third-party misuse. This defense strategy in court is labelled as the “decentralisation defence” (KOKORIN 2025, p. 6-7).

III.4 Crypto Staking

Crypto staking (whether centralised or decentralised) is defined as the process of locking up crypto-assets to support the operations of a blockchain network and receive rewards for doing so (ZETZSCHE ET AL. 2023, p. 64). Staking is regarded as a key mechanism used by Proof-of-Stake (PoS) blockchains to validate transactions. In a PoS network, validators confirm transactions and add them to the blockchain network and earn income. The likelihood of a validator being chosen to create the next block depends on his stake. In the Ethereum blockchain

the consensus mechanism was transitioned in September 2022 from Proof-of-Work (PoW) to PoS and a minimum of 32 ETH is required (ZETZSCHE ET AL. 2023, p. 64-65).

The 2025 Joint Report on recent developments in crypto-assets by the European Securities and Markets Authority (ESMA) and the European Banking Authority (EBA) defines staking as “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” (ESMA/EBA 2025, p. 43).

Delegated staking solutions allow users who lack technical expertise and resources to participate as so-called delegators in the rewards earned by validators in a validation process. Staking services can be categorised as follows (ESMA/EBA 2025, p. 43-44):

- Validator-as-a-service: The service provider facilitates access to staking to persons who have the capital necessary to operate a node on their own (for example 32 ETH), but may not have the technical means.
- Pooled staking: This allows persons without the technical or financial means to participate in the rewards of validators, by making a deposit of the native PoS token of a blockchain into a liquidity pool from a pooled staking provider.
- Centralised staking services: Participation in staking in a user-friendly manner can be offered for example by centralised crypto-asset trading platforms to its users.

Liquid staking is a type of pooled staking protocol where the user deposits a native staking crypto-asset into a liquidity pool in exchange for liquid staking tokens (LST) representing a certificate of ownership of the underlying staked asset. The user can simultaneously earn yields from the reward for the staked assets and reinvest the LST somewhere else. Liquid staking has become a very important DeFi application (ESMA/EBA 2025, p. 45).

IV. Market Growth of Decentralised Finance

IV.1 Growth Factors for Decentralised Finance

A whole DeFi ecosystem has developed over the recent years around DeFi applications which interact with many actors within the crypto-asset space as well as the real world (DEUTSCHE BUNDESBANK 2021, p. 35).

The 2022 IOSCO Decentralised Finance Report looks at the reasons for the significant growth in DeFi projects. According to the report, there are multiple incentive mechanisms that have

helped fuel participation. DeFi relies on the contribution of various stakeholders, each of whom has an important role to play in making the system work and expects to earn a profit. Stakeholders include (IOSCO 2022b, p. 28):

- creators and developers of a DeFi protocol,
- investors in the development group or protocol,
- protocol users,
- service providers, and
- blockchain networks.

According to IOSCO, the following factors have contributed to the growth of the DeFi ecosystem (IOSCO 2022b, p. 28):

- Early investors have recognised the opportunity to allocate capital to new technologies with return and risk profiles like in venture capital projects.
- Crypto-asset holders have recognised a market looking for liquidity for trading crypto-assets and so they perform market-maker and related services to DeFi protocols.
- TradFi and CeFi market participants are looking to diversify their activities and have extended to DeFi markets.
- Blockchain communities have encouraged the proliferation of DeFi projects on their platform in order to scale their network.
- Early adopters and proponents of crypto-assets see the DeFi market as a place where they can invest in products and services that align with their general outlook for this industry.

The IOSCO report draws a so-called “Big Picture” of DeFi in terms of three primary components (IOSCO 2022b, p. 29-34):

- Capital formation, development, and deployment: This relates to the stage of setting up and financing a DeFi protocol development group by investors until reaching deployment of the DeFi protocol. Early investors, founders and staff of the protocol development group may receive an allocation of governance or other tokens as compensation. Control over the DeFi protocol may be transferred to a separate group or entity. Other investors join later through the purchase of governance tokens. Code changes in smart contracts and in protocols may be subject to governance token holder voting.

- **Use and investment:** Centralised crypto-asset trading platforms working with banks or other financial institutions serve as fiat currency on- and off-ramps to DeFi protocols and provide custody and other solutions that enable participants to hold and use their crypto-assets. DeFi participants try to use their crypto-assets to earn additional returns. The DeFi market also attracts service providers e.g., oracles who get compensated by acting as data provider for off-chain information like stock prices.
- **Settlement:** DeFi protocols rely on a blockchain for transaction execution and settlement. Blockchain networks seek to attract DeFi protocols to deploy on their blockchain. They compete on a number of measures, including the speed and cost of transaction settlement. DeFi protocols may run on multiple blockchains, in which case cross-chain bridges are necessary.

In the IOSCO report, the multiple interactions and relationships between the various actors in the DeFi ecosystem are depicted in detail as a large boxes-and-arrows-diagramme “DeFi: The Big Picture” (IOSCO 2022b, p. 35), not copied into this paper to avoid any copyright issues.

IV.2 Financial Incentives in Decentralised Finance Platforms

According to the 2021 DeFi policy paper by the World Economic Forum, many DeFi services incorporate explicit financial incentives to promote market development, including the creation of liquidity and collateral. A list of incentive types follows (WORLD ECONOMIC FORUM 2021, p. 10):

- **Lock-up yields:** Pay interest or a share of trading fees for immobilising crypto-assets to serve as liquidity or collateral for a service.
- **Liquidity mining:** Pays interest in the form of tokens issued by the service itself, typically governance tokens.
- **Airdrops:** Reward wallet addresses with tokens to promote awareness of new crypto-assets.
- **Yield farming:** Optimises returns from liquidity mining and lock-up yields by automatically moving funds among services.
- **Liquidation fees:** pay market-makers a percentage of the value of under-collateralised loans that they successfully liquidate.

IV.3 Size of the Decentralised Finance Industry and Available Metrics

Zetzsche et al. (2023) see no uniformly accepted insights as to the actual size of the industry. The volume of fully decentralised services is considered small compared to TradFi. The industry value is estimated at several billion USD. The Total Value Locked (TVL) is a preferred metric to measure the size of the industry. TVL relates to the total value of all crypto-assets (expressed in USD) that are locked into a DeFi protocol on a particular blockchain. “Locked into” means that crypto-assets are locked for any duration by a smart contract operated by the protocol. This value is meant to represent the total amount of underlying supply that is secured by a specific application (IOSCO 2022b, p. 30; ZETZSCHE ET AL. 2023, p. 32).

DeFi Llama is a platform that aggregates the TVL of DeFi protocols. In November 2021, the TVL metric by DeFi Llama reached a peak of USD 206 billion (ZETZSCHE ET AL. 2023, p. 32). Any user can look up the development of the aggregated TVL on the website of DeFi Llama. In September 2025, the TVL metric is lower, but still significant at roughly USD 150 billion (Figure 1).

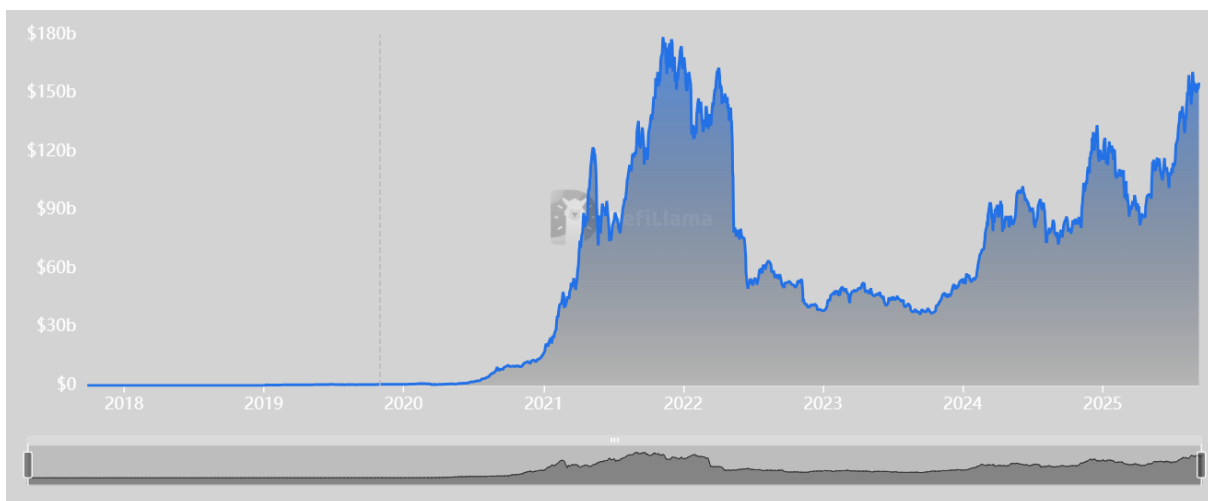


Figure 1: Total Value Locked on 9 September 2025. Source: defillama.com.

The 2023 ESMA report “Decentralised Finance in the EU: Developments and risks” contains a graph “Total Value Locked by DeFi protocol type”. The breakdown of the TVL by protocol type covers decentralised exchanges, lending, liquid staking, derivatives, bridge, and other (ESMA 2023, p. 6). A majority of the TVL comes from decentralised lending, decentralised and staking. This is in line with TVL numbers in the graph “Evolution of DeFi markets” in the 2023 FSB report (FINANCIAL STABILITY BOARD 2023, p. 34).

Most DeFi protocols use the Ethereum blockchain as settlement layer. The 2023 ESMA report shows a graph “TVL breakdown by chain” with 60% coming from the Ethereum blockchain (ESMA 2023, p. 5).

The 2025 Joint Report on recent developments in crypto-assets by ESMA/EBA highlights an interesting development. Staking protocols have become the largest by type of activity with 39% of TVL, followed by lending protocols 22% and decentralised exchanges 8%. The increased importance of staking may be attributed to Ethereum’s transition from a PoW to a PoS consensus mechanism and the growth of liquid staking protocols (ESMA/EBA 2025, p. 8-9).

The TVL of the top 10 DeFi protocols according to DeFi Llama is shown on Table 10.

	Name	Blockchains	Category	TVL in billion USD
1	Aave	17	Lending	40,2
2	Lido	5	Staking (Liquid Staking)	37,9
3	EigenLayer	1	Staking (Restaking)	19,0
4	Binance staked ETH	2	Staking (Liquid Staking)	14,4
5	Ethena	1	Basis Trading	13,1
6	Pendle	10	Yield	11,8
7	Ether.fi	1	Staking	11,1
8	Morpho	22	Lending	7,9
9	Spark	2		7,4
10	Babylon Protocol	1	Staking (Restaking)	6,2

Table 10: TVL of the top 10 DeFi protocols on 9 September 2025. Source: Own representation with data from defillama.com.

The 2022 Financial Stability Board report “Assessment of Risks to Financial Stability from Crypto-asset” contains an overview of available metrics and data gaps for DeFi (Table 11) including the TVL under the transmission channel “wealth effects”.

TVL numbers of several billion USD may appear very large and perhaps overemphasize the significance of the DeFi sector. The metric, whilst easy to follow, may overstate the size of the market in terms of “real capital” in fiat currency. It can be assumed that a significant part of the TVL numbers observed is inflated over time by attractive interest and yields generated only in a self-referential DeFi ecosystem. An interesting question would be, how much fiat money has been injected by investors into the DeFi ecosystem through investments and purchase of tokens. Then, assuming a potential bubble would burst at some point in time, how much capital would have been really lost in terms of fiat money previously injected?

Transmission Channels	Available Metrics	Data Gaps
Wealth effects	• Total value locked-in, gross, adjusted and net; realised volatility • Transaction volume of DEX • Wallet growth • Market capitalization and transaction volume of governance tokens • Transaction volume in DeFi lending • Lending rate in DeFi lending • Utilization rate of liquidity pool of DeFi lending and exchange • DeFi yield and return	• Share of retail vs. institutional participation • Number of dApps on a blockchain • Liquidity pools, DeFi stablecoins, derivatives (entities within the DeFi space, including types of financial institutions (specialized or traditional financial institutions) to understand linkages of DeFi with the rest of the financial system) • Metrics to measure leverage • Information on the governance tokens holders could be obtained to see to what extent the governance is decentralized (e.g., if the ownership of governance tokens is concentrated, that entity could be considered the actual developer)
Confidence effects	• Share of retail ownership of stablecoins • Number of clients in infrastructures that provide access to DeFi (e.g., trading platforms, wallet providers)	• Volume of crypto-asset fraud • Share of transactions in unbacked crypto-assets vs. stablecoins
Financial sector exposures	• Share of institutional ownership of crypto-assets • Share of assets invested in crypto-assets • Number of large financial service providers offering crypto-asset services • Volume of crypto-asset derivatives market • Open interest of derivative contracts • Correlations of crypto-assets with other asset classes • Share of transaction volume by transaction size	• Amounts and share of holdings of exchange traded funds that offer exposure to crypto-assets by investor type
Use in payments and settlements	• Price of key players (DOT, UNI, LINK) and delta over one week, one month, three months, six months, one year and 7-day average volume	• Number and value of transactions • Breakdown of counterparties: jurisdiction of the payers and payees, type of transactions (e.g., remittances, e-commerce, trading)

Table 11: Available metrics for DeFi. Source: Adapted from Financial Stability Board (2022a), p. 23-24, Annex 1, Table 3: Data issues for DeFi.

V. Benefits versus Risks of Decentralised Finance

V.1 Benefits of Decentralised Finance

Schär (2021) believes that the DeFi sector may increase the efficiency, transparency, and accessibility of the financial infrastructure. In his view, the system's composability would allow anyone to combine multiple applications and protocols, thereby creating new and exciting services (SCHÄR 2021, p. 168-169). The four main opportunities are explained in his paper as follows:

- **Efficiency:** While a large part of the TradFi system is trust-based and dependent on centralised institutions, DeFi replaces some of these trust requirements with smart contracts. The contracts can assume the roles of custodians, escrow agents, and central counterparties. Lower trust requirements may come with the additional benefit of reducing regulatory pressure and reducing the need for third-party audits.
- **Transparency:** DeFi applications are deemed as transparent insofar that transactions are publicly observable, and the smart contract code can be analysed on-chain. The observability and deterministic execution allow a high level of transparency. Financial data are publicly available and may potentially be used by researchers and users. DeFi applications may allow for the mitigation of undesirable events before they arise and help provide faster understanding of their origin and potential consequences when they emerge.
- **Accessibility:** DeFi protocols can be used by anyone. As such, DeFi may potentially create an open and accessible financial system. Infrastructure requirements are seen by Schär (2021) as being relatively low and the risk of discrimination as almost inexistent due to the lack of identities. If regulation demands access restrictions, such restrictions could be implemented in the token contracts without compromising the settlement layer's integrity and decentralisation properties.
- **Composability:** The shared settlement layer allows protocols and applications to interconnect. Any two or more pieces could be integrated, forked, or rehashed to create something new. Anything that has been created before can be used by an individual or by other smart contracts. Schär (2021) praises this flexibility which allows for an expanding range of possibilities and unprecedented interest in open financial engineering.

The opportunities highlighted above correspond to only one point of view on the benefits of DeFi applications by one academic author in an early publication from 2021. Table 12 lists purported benefits (or potentials or potential benefits or opportunities), as described in various

publications from the academic and practitioner sector, here Gogel et al. (2021) and Gramlich et al. (2022), as well as from standard-setting bodies and regulators, here OECD (2022) and ESMA (2023).

Source	Benefits
ESMA (2023)	Benefits • Reduce the need for traditional intermediaries and central counterparties with potential benefits in speed, security and costs for financial transactions • Greater financial inclusion by allowing users to access products and services without an intermediary • Facilitate the development of innovative financial products (e.g., perpetual futures)
Gogel et al. (2021)	Opportunities • Reduced friction and transaction costs for creation, distribution, trading, and settlement of financial assets • Increased standardisation and functional interoperability, allowing reuse and recomposition of financial primitives • Increased auditability and transparency of transactions through blockchain-based records • Improved accountability for decisions through software-based governance systems • Greater stakeholder control through non-custodial, disintermediated service provision • Improved market access by providing global, 24/7 availability of services and removing barriers such as bank account requirements • Faster settlement, reducing counterparty risks and freeing up capital • Greater inclusivity of financial services by making automated tools available to all, with transparent and non-discriminatory execution • Permissionless innovation, allowing the creation of novel products and services
Gramlich et al. (2022)	Potentials • Financial inclusion and independence • Innovative asset classes and funding opportunities • Fractional ownership • Open systems and interfaces • Catalyst for new ecosystems
OECD (2022)	Potential benefits • Blockchain-based ○ Efficiencies delivered by DLTs: faster, cheaper, frictionless value transfer ○ Automation of processes, user-to-smart-contract model, atomic transactions ○ Increased transparency, integrity of record-keeping ○ Allows for interoperability and composability • Fully decentralised ○ No need for trusted centralised intermediaries ○ Reduces concentration of service providers, increases diversity ○ Potential systemic benefits (risks associated with traditional financial intermediaries) ○ Absence of central point of failure or single attack point could enhance system resilience • Community-driven ○ Open-source code promotes innovation ○ Democratisation of financial service provision ○ Significant potential for network effects
Schär (2021)	Opportunities • Efficiency • Transparency • Accessibility • Composability

Table 12: Benefits of Decentralised Finance. Source: Own representation adapted from ESMA (2023), p. 7; Gogel et al. (2021), p. 7; Gramlich et al. (2022), p. 27-35; OECD (2022), p. 40-41; Schär (2021), p. 168-169.

V.2 Risks of Decentralised Finance

Although DeFi has been praised by many authors as providing potential benefits, it is acknowledged that it also presents numerous risks to investors and other market participants (IOSCO 2022b, p. 36).

Schär (2021) concentrates on the following six risks (SCHÄR 2021, p. 170-172):

- Smart contract execution risks: Coding errors may create vulnerabilities that allow an attacker to drain the smart contract's funds, cause chaos, or render the protocol unusable. The protocol is only as secure as the smart contracts underlying it.
- Operational security risks: Many DeFi protocols and applications that use admin keys allow a predefined group (usually the DeFi project's core team) to upgrade the contracts and to perform emergency shutdowns as precautionary measures. If the keyholders do not create or store their keys securely, malicious third parties could steal these keys and compromise the smart contract. The core team members may be malicious or corrupted by significant monetary incentives.
- Dependencies on other protocols: Some of the most promising features of the DeFi ecosystem are its openness and composability. These features allow various smart contracts and decentralised blockchain applications to interact with each other and to offer new services from a combination of existing ones. However, these interactions introduce severe dependencies. If there is a problem with one smart contract, it may potentially have wide-reaching consequences for multiple applications across the entire DeFi ecosystem.
- Reliance on external data: So-called oracles, that provide data not natively available, introduce dependencies on external sources and may lead to heavily centralised contract execution. To mitigate this risk, many projects rely on decentralised oracle networks with a large variety of data provision schemes.
- Illicit activity: Crypto-assets may be used by individuals who want to avoid records and monitoring. The network's pseudonymity may provide some privacy. On the one hand, pseudonymity can be abused by actors with dishonest intentions. On the other hand, privacy may be a desirable attribute for some legitimate financial applications. Schär (2021) thinks

that regulators should act with great care, trying to find reasonable solutions that allow them to step in where necessary without stifling innovation.

- Scalability: There is a trade-off between decentralisation, security, and scalability of a blockchain. While the Ethereum blockchain is regarded as relatively decentralised and secure, it has difficulties with the great demand for block space. High gas prices (transaction fees) and long confirmation times adversely affect the DeFi ecosystem.

Again, this is only the point of view by one author. Table 13 provides an overview of the risks (or potential risks or challenges) of DeFi applications, as described in the same sources that listed various benefits in the previous subsection. These publications were written on the basis of a logical structure of pros and cons.

Source	Risks
ESMA (2023)	Risks to consumers • Market and liquidity risks • Counterparty risk • Scams and illicit activities • Exposure of less sophisticated investors to overly complex or risky products • Operational, technological and security risks • Attacks on DeFi protocols targeting code vulnerabilities and access control points
Gogel et al. (2021)	Challenges • Scalability, throughput, and transaction fees for blockchain settlement platforms are significant limiting factors. Energy usage raises concerns about contributing to climate change. • Limited interoperability across blockchains and with traditional financial services. • Privacy considerations may be in tension with transaction transparency. • Immature governance as high-stakes decisions are made by small, inexperienced teams. Lack of accountability when developers are anonymous. • Hidden centralization of control and low thresholds for governance rights may give certain actors disproportionate power. • Regulatory questions and enforcement challenges in applying national legal requirements to decentralized global networks. • Immature technology is being used to manage high-value assets. Poor design choices and implementations have led to significant losses. • Extreme short-term returns during DeFi's early growth stage attract unscrupulous actors and warp user expectations. Limited usability impedes largescale adoption. • Potential for facilitation of financial crime such as money laundering.
Gramlich et al. (2022)	Challenges • Technical risks and security concerns • Scalability issues • Illiquidity • Transparency vs. privacy • Lack of harmonised regulation • Improper property and consumer protection laws • Inconsistent taxation and accounting rules • Recentralisation
OECD (2022)	Potential risks • Investor and consumer risks • Potential systemic risks • Anonymity and lack of anti-money laundering (AML) / know-your-client (KYC) • Regulatory and compliance risks • Challenges around governance • Technology and operational risks
Schär (2021)	Risks • Smart contract execution • Operational security • Dependencies • External data • Illicit activity • Scalability

Table 13: Risks of Decentralised Finance part 1. Source: Own representation adapted from ESMA (2023), p. 7-9; Gogel et al. (2021), p. 7; Gramlich (2022), p. 36-46; OECD (2022), p. 41-52; Schär (2021), p. 170-172.

Table 14 contains a list of the risks of DeFi applications found in publications that did not draw a list of benefits. The papers don't try to praise or evaluate DeFi applications from an economic perspective, they are aimed at regulators and policy-makers worldwide, who may be worried about the growth of the market and negative effects on consumers and the stability of the financial system.

Source	Risks
EBA/ESMA (2025a)	Potential risks associated with DeFi - Information and communication technology (ICT) risks - On-chain vulnerabilities (smart contract exploitation, price manipulation, governance attacks, scams) - Off-chain vulnerabilities (private key compromise, phishing, other) - recent attacks appear to be more successful when exploiting off-chain vulnerabilities - Money-laundering/Terrorist financing risks - Anonymity or pseudonymity, due to the use of self-custodial wallets, can challenge the enforceability of the regulatory framework - Can facilitate fraudulent activities and obfuscation of funds of crypto-assets - Consumer protection concerns - Need for high levels of digital/financial literacy to understand risks - Need to safeguard effectively private keys, with particular care regarding self-hosted wallet use - Opaque/complex products, services, and value chains with indications that risk disclosures may not be sufficient
FSB (2023)	DeFi vulnerabilities - Operational fragilities - Governance arrangements - Dependence of blockchain networks - Smart contracts - Oracles and bridges - Liquidity and maturity mismatches - Leverage - Interconnectedness, concentration and complexity - Composability - Critical functions, concentration and complexity - Other vulnerabilities - Market integrity - Cross-border regulatory arbitrage - Cryptoisation
IOSCO (2022b)	Key risks and considerations - Asymmetry and fraud risks - Market integrity risks including front-running (or similar frauds), flash loans, market dependencies, use of leverage, illicit activity risks - Operational and technology-based risks - Cybersecurity - Governance risks - Spill-over of risks to centralised/traditional markets
WEF (2021)	Risks - Financial risk: Depletion of funds due to the transactional behaviour of fellow users concerning the digital assets in the DeFi service. Associated risks: market risk, counterparty risk, liquidity risk. - Technical risk: Failures of the software systems supporting transaction execution, pricing and integrity. Associated risks: transaction risk, smart contract risk, miner risk, oracle risk.

	• Operational risk: Failures of the human systems for key management, protocol development or governance. Associated risks: routine maintenance and upgrades, code forks, key management, governance mechanisms, redress of disputes. • Legal compliance: Use of DeFi to engage in illicit activity or to evade regulatory obligations. Associated risks: financial crime, fraud and market manipulation, regulatory arbitrage. • Emergent: Macro-scale crashes or undermining of the financial system due to the interaction, scaling and integration of DeFi components. Associated risks: dynamic interactions, flash crashes or price cascades.
--	---

Table 14: Risks of Decentralised Finance part 2. Source: Own representation adapted from Financial Stability Board (2023), p. 16-24; IOSCO (2022b), p. 36-43; World Economic Forum (2021), p. 13-18.

A multitude of risks has been identified by a number of authors and organisations. These include risks already present in TradFi as well as new risks from DeFi.

A fundamental observation made in the 2022 IOSCO Decentralized Finance report is that DeFi seeks to obviate traditional intermediaries between parties to transactions. On one hand, disintermediation may allow for faster, cheaper and more efficient execution of transactions. On the other hand, disintermediation eliminates market participants that have acted as gatekeepers, performing central roles of ensuring investor protection and market integrity (IOSCO 2022b, p. 36).

- Some intermediaries, for example, provide investment advice to assist investors in understanding the potential benefits and risks of a particular investment.
- Others provide real-time information about investment products, companies and markets to reduce information asymmetries and allow investors to research potential investments.
- Intermediaries also impose structural constraints upon users, such as capital and liquidity controls, anti-money laundering (AML) / countering the financing of terrorism (CFT) protections and compliance, and targeted financial sanctions monitoring.
- They also can provide protections against losses as a result of bankruptcy and theft.

These are important investor and market protections that in the view of IOSCO seek to minimise fraud, reduce systemic risk and contribute to fair, efficient and equitable markets (IOSCO 2022b, p. 36).

The 2021 DeFi policy paper by the World Economic Forum delivers a taxonomy of DeFi risks. It breaks down the risks into five broad categorises (financial risk, technical risk, operational risk, legal compliance, emergent risks) which branch into several subcategories (Table 15). The

categories and subcategories are not mutually exclusive. DeFi failures may result from multiple risks in the taxonomy. Investors may lose money either unintentionally or due to deliberate attacks. Even undesired DeFi transactions may be effectively impossible to reverse. In some cases, the line between a legitimate trading strategy that takes advantage of an arbitrage opportunity and an improper exploit might be unclear (WORLD ECONOMIC FORUM 2021, p. 13).

Risks	Associated Risks	Definition or Explanation
Financial risk	Market risk	Possibility that asset value will decline over some time horizon due to market conditions, new information or traders' idiosyncratic Behaviour
	Counterparty risk	Possibility that a counterparty will default on its obligations to a financial instrument
	Liquidity risk	Possibility that there will be insufficient funds or assets available to realize the value of a financial asset
Technical risk	Transaction risk	Limitations or failures of the underlying blockchain network
	Smart contract risk	Deal with code that does not execute as intended
	Miner risk	Deals with the possibility that transaction processing entities behave maliciously towards certain transactions
	Oracle risk	Involves the potential that data external to the blockchain on which a DeFi contract relies is inaccurate or has been manipulated
Operational risk	Routine maintenance and upgrades	These may be more difficult to implement for decentralized services, or may create vulnerabilities, especially given the composability of DeFi
	Code forks	Options for groups seeking to alter elements of DeFi services, providing an "exit" option for minorities that prefer a different set of parameters
	Key management	Platforms identify users and their assets through cryptographic key pairs. Because DeFi services are non-custodial, they place the key management burden on their users in return for removing dependencies on centralized service providers.
	Governance mechanisms	Governance mechanisms for DeFi and other blockchain-based services raise complex potential risks
	Redress of disputes	Once a smart contract has executed, the output cannot be modified or reversed just because an individual actor, or a governmental authority, orders it to be
Legal compliance	Financial crime	Involves breach of anti-money laundering/countering the financing of terrorism (AML/CFT) restrictions, financial sanctions and similar legal regimes
	Fraud and market manipulation	Involve deliberate scams, misappropriation and other efforts to take advantage of investors
	Regulatory arbitrage or evasion	Failing to meet regulatory obligations by carrying out similar functions in a different technical manner
Emergent risks	Dynamic interactions	Dynamic interactions among a potentially endless number of interconnected DeFi components may produce risks that are not present in any individual service
	Flash crashes or price cascades	Unlike traditional markets, where primary dealers and brokers can manually intervene when defaults occur concurrently, the permissionless, algorithmic nature of DeFi means that it may not be possible to stop cascades

Table 15: Taxonomy of DeFi risks by World Economic Forum (2021). Source: Adapted from World Economic Forum (2021), p. 13-18.

The list of DeFi risks can be extended or customised for specific use cases like decentralised lending and borrowing. In January 2025, two factsheets were issued by EU regulators, one on “Decentralised Finance” by EBA/ESMA (2025a) and another one on “Crypto lending, borrowing and staking” by EBA/ESMA (2025b). These factsheets summarise the key findings in a Joint Report by ESMA/EBA (2025). The risks for crypto lending, borrowing and staking (centralised and decentralised) are listed in Table 16.

Consumer protection risks	• Marketing materials and disclosures may provide misleading information on opportunities and risks. • Users may receive insufficient information on (a) pricing and fees, (b) interest rates or yields, (c) changes to collateral requirements, (d) actions the provider may take, or (e) rights and liabilities. • Insufficient financial education or digital literacy of retail users on risks associated with these activities.
Consumer protection risks ... specific to crypto lending and borrowing	• Highly leveraged market making activities can lead to collateral chains. • Contagion risks via the interconnectedness arising from common asset holdings and procyclicality. • The absence of creditworthiness checks, and, as a consequence, of credit risk assessment. • Liquidity risks, risks of liquidation, and enhanced risks in cases of co-mingling of crypto-assets.
Specific to DeFi lending and borrowing	• Collateral chains can come with enhanced systemic risks via: a) cascade liquidations across multiple DeFi protocols, b) deleveraging spirals when assets are liquidated, and c) systemic liquidity crunches. • Market concentration risks. • Barriers to financial inclusion and insufficient information, due to heightened complexity.
Specific to crypto staking	• Market risks associated to significant valuation changes during lock-up or unbonding periods. • Market volatility risk amplification when the market value of liquid staking tokens declines. • Questions around to what extent penalties and risks are passed on to and disclosed to users. • Custody risks in the event of custodian failure, asset co-mingling and insufficient record-keeping.
Money Laundering / Terrorist financing risks	• Users can engage in lending and borrowing without disclosing their true identity or the identity being verified. • Limited scrutiny of purpose and source of funds could expose the financial system to vulnerabilities. • Without monitoring and checks, users from high ML/TF-risk jurisdictions could transact without being detected.
Other risks	• Operational and ICT risks. • Market risks (e.g., volatility enhances liquidation risks). • Legal risks.

Table 16: Risks of crypto lending, borrowing and staking. Source: Adapted from EBA/ESMA (2025b), p. 2.

V.3 Financial Stability Risks of Decentralised Finance

A key message of the 2023 DeFi report by the Financial Stability Board is that DeFi inherits and may repeat or amplify the vulnerabilities of the TradFi system like operational fragilities, liquidity and maturity mismatches, leverage, and interconnectedness. For instance, the automatic liquidation of collateral based on smart contracts, the use of oracles, or dependence on the underlying blockchain may lead to risks of fire sales or other spill over effects playing out differently than in TradFi. The amplification of known vulnerabilities comes from novel technological features, the high degree of structural interlinkages amongst the participants in DeFi and from non-compliance with existing regulatory requirements or lack of regulation. The Financial Stability Board takes the stance that the DeFi vulnerabilities don't represent a threat to global financial stability, but will require ongoing monitoring as the ecosystem continues to grow and evolve (FINANCIAL STABILITY BOARD 2023, p. 16). The extent to which the DeFi vulnerabilities can lead to financial stability concerns depends on the interlinkages and associated transmission channels between DeFi, TradFi and the real economy. At the time the standard-setting body saw little risk of a shock originating in the DeFi ecosystem having significant effects on the real economy due to the self-referential nature of the DeFi market. (FINANCIAL STABILITY BOARD 2023, p. 24)

In the 2022 Financial Stability Board report on how crypto-asset markets could impact financial stability, the organisation identified four potential transmission channels (FINANCIAL STABILITY BOARD 2022a, p. 1; FINANCIAL STABILITY BOARD 2022b, p. 4-10; FINANCIAL STABILITY BOARD 2023, p. 24):

- financial institutions' exposures to crypto-assets, related financial products and entities that are financially impacted by crypto-assets,
- confidence effects,
- wealth effects from the fluctuations in the market capitalisation of crypto-assets, and
- the extent of crypto-assets' use in payment and settlement.

The exposures of financial institutions to DeFi are particularly important for the first transmission channel, as problems in DeFi could be transmitted to TradFi. Confidence effects and wealth effects are more relevant for households and corporates heavily exposed to DeFi. If DeFi tokens, in particular stablecoins, were to become a widely used means of payment, then their systemic importance may substantially increase (FINANCIAL STABILITY BOARD 2023, p. 25).

The 2023 DeFi report by the Financial Stability Board identifies the following interlinkages and scope for spill overs:

- Financial institutions' exposures to DeFi: Banks' exposure to crypto-assets and DeFi is currently minimal. Some regulated financial institutions have invested directly in crypto-related companies, including companies that provide access to DeFi applications, exposing themselves to a potential loss of capital. Banks may also be exposed to DeFi through lending to DeFi counterparts, market-making / clearing services, facilitating activities in the DeFi ecosystem and DeFi lending to banks (FINANCIAL STABILITY BOARD 2023, p. 25-26).
- Households and firms: There is no comprehensive data on DeFi adoption by retail users. Available information indicates that household involvement in DeFi is currently minimal, suggesting limited linkages to date. Barriers to DeFi adoption at the retail level are its complexity, transaction costs, and the need to already be active in the crypto-asset ecosystem (FINANCIAL STABILITY BOARD 2023, p. 27).
- DeFi and payments: Some stablecoins are purportedly DeFi applications managed by DAOs, for example DAI. Stablecoins act as a substitute for fiat currency in the crypto-asset ecosystem. If they develop further, these could be additional sources of financial vulnerabilities, as they would likely increase the adoption of DeFi solutions by retail and corporate users as well as facilitate the adoption of crypto-assets as a means of payment (FINANCIAL STABILITY BOARD 2023, p. 27).

VI. Collapses and Failures Related to Decentralised Finance

VI.1 Attacks in the Crypto-asset Sector 2015–2022

According to Zetzsche et al. (2023), between 2015–2022 the crypto-asset sector saw a number of significant asset diversions. This undermined trust in the institutional stability of crypto platform models and protocols in general (ZETZSCHE ET AL. 2023, p. 33-34).

- In some of these instances, private keys were stolen through hacking the wallets of crypto custodians and exchanges while they were online.
- In others, the attackers hacked into the governance mechanism to adopt the means to control the protocols of the platform, allowing them to divert assets held by the platform.

- Further, attackers conned users into disclosing their private key, or took the private key from the user's wallet application, which were used to divert assets, or adopted thousands of tokens through flash loans to engage in arbitrage strategies against the platform.

According to ESMA (2023), attacks on DeFi protocols essentially target code vulnerabilities (e.g., errors in the underlying smart contracts), and access control points (e.g., protocols' consensus mechanisms or governance frameworks), with a view to altering their functioning. Many DeFi protocols go live without any audit or due diligence and the public open-source nature of the underlying smart contracts leaves their code vulnerabilities exposed to malicious actors. If a DeFi protocol becomes large enough, any flaw in its smart contract code is likely to be found and exploited. Prominent examples of consensus and governance-related exploits include Ronin Network and Beanstalk in 2022 (ESMA 2023, p. 9).

VI.2 The Crypto Winter 2022–2023

The Crypto Winter 2022–2023 denotes a period covering a series of major collapses and failures in the crypto ecosystem from May 2022 to March 2023 (Table 17).

Date	Event
May 2022	Terra-Luna stablecoin crash
November 2022	Bankruptcy of crypto exchange FTX
March 2023	Closure of Signature Bank
March 2023	Bankruptcy of Silvergate Bank

Table 17: Events of Crypto Winter 2022–2023. Source: Own representation adapted from Zetzsche et al. (2023), p. 33-41.

For Zetzsche et al. (2023), the Terra-Luna stablecoin collapse in May 2022 sparked a chain reaction resulting in a string of bankruptcies (Table 18), including the failure of the crypto exchange FTX, the closure of the crypto-friendly Signature Bank, and the failure of the crypto-friendly Silvergate Bank. These events show the lack of internal capacity on the side of crypto-asset intermediaries to deal with the risks related to their business models. The authors claim, if the crypto ecosystem would have been truly decentralised, such a chain reaction would not have taken place (ZETZSCHE ET AL. 2023, p. 36).

Date of Bankruptcy	Firm	Businesses Line
	Babel Finance	Crypto lender
July 2022	Three Arrows Capital (3AC)	Crypto investment fund
	Voyager Digital	
July 2022	Vault	Centralised crypto exchange
July 2022	Celsius Network	Crypto lender
July 2022	Zipmex	Centralised crypto exchange
August 2022	Holdnaut	Centralised crypto exchange, Crypto lender
	Compute North	Bitcoin mining
November 2022	FTX	Centralised crypto exchange, Crypto lender
November 2022	BlockFi	Centralised crypto exchange, Crypto lender
	Core Scientific Inc.	Bitcoin mining
	Genesis	Crypto lender
March 2023	Silverage Bank	Crypto-friendly bank
March 2023	Signature Bank	Crypto-friendly bank

Table 18: Bankruptcies since Crypto Winter 2022–2023. Source: Own representation adapted from Zetzsche et al. (2023), p. 37.

Crypto firms cite the negative price development in large crypto-assets as the main reason for their difficulties. Zetzsche et al. (2023) doubt that the price downturn in Bitcoin is the sole reason for the financial difficulties. Bitcoin miners such as Compute North and Core Scientific suffered from rising power costs and increased difficulty of mining Bitcoin. A combination of deficient accounting, lack of internal controls, deficient risk management (in particular lack of position limits and margin management) and outright mismanagement contributed to the bankruptcies (ZETZSCHE ET AL. 2023, p. 36).

VI.3 Crash of the Decentralised Stablecoin Terra-Luna

The 2023 DeFi report by ESMA sees the collapse of the Terra-Luna decentralised stablecoin system as having exposed important fragilities. TerraUSD (UST) was an algorithmic stablecoin. This means, the stablecoin was not backed by any assets, but it maintained its parity with the US dollar through an algorithmic relationship with Terra's native token, LUNA. At the time, UST was the fourth-largest stablecoin with USD 18 billion in market capitalisation. The algorithm was set up such that every time a UST token was minted, the equivalent of USD 1 in LUNA was burnt, and vice versa. Terra, including the DeFi lending protocol called Anchor, became the second largest DeFi project with almost USD 40 billion in TVL. Anchor lured investors into buying UST by offering a 20% yield to users depositing their UST in the protocol (ESMA 2023, p. 8).

According to ESMA (2023), in early May 2022, UST lost its peg following large UST sales in what looked like an attack against the Curve liquidity pool. UST holders could redeem their

UST, which was worth less than USD 1 for one dollar worth of the LUNA token. As more users redeemed and the supply of LUNA rose, its value fell. In the following week, UST and LUNA holders rushed to sell, resulting in a death spiral that sent the value of both tokens to zero (ESMA 2023, p. 8).

For ESMA (2023), the Terra-Luna collapse exposed the fragility of algorithmic stablecoins and extremely speculative nature of certain DeFi protocols. It also highlighted the interconnectedness within DeFi and crypto-assets more broadly. The collapse bankrupted many investors, erased more than USD 100 billion in TVL and affected the entire crypto-asset market. Over USD 400 billion in value was lost in terms of market capitalisation. When Terra's founder and the LUNA Foundation deployed more than USD 3 billion trying to support the price of LUNA and defend the peg, they caused a downward pressure on the cryptocurrency market and triggered a sell off of other crypto-assets. Attackers may have cashed in over USD 800 million estimated profits (ESMA 2023, p. 8).

VI.4 Bankruptcy of the Centralised Exchange FTX

FTX, one of the largest crypto-asset trading platforms, and a number of affiliated companies including Alameda Research, a crypto-asset hedge fund, filed for bankruptcy on 11 November 2022 (FINANCIAL STABILITY BOARD 2023, p. 27-28).

Zetzsche et al. (2023) see the FTX failure as a liquidity crisis that turned into a solvency crisis, similar to that of the investment bank Lehman Brothers in 2008. When a financial intermediary is unable to access sufficient liquidity to continue its business, this liquidity crisis will often turn into a solvency crisis triggering wider losses of confidence in the sector, and potentially a financial crisis. FTX was unable to secure additional funds and was forced to file for insolvency. The result is a range of insolvency actions in major jurisdictions and regulatory, investor and customer actions spread around the world (ZETZSCHE ET AL. 2023, p. 38).

According to the Financial Stability Board (2023), the full extent of the impacts of this failure, including on DeFi projects that were owned by FTX or depended on it for trading flows, may take time to become apparent given the lack of disclosure and transparency. The FTT token, an unbacked crypto-asset issued by the FTX group, does not appear to have been much used for collateral on DeFi platforms. The major DeFi platforms experienced some liquidations given the market turbulence, but so far to a lesser extent than during May/June 2022 (FINANCIAL STABILITY BOARD 2023, p. 27-28).

The failure of such a significant CEX could drive further adoption of DEXs, given the mismanagement of customer assets in the case of FTX. The Financial Stability Board (2023) claims, that after the FTX failure some DEXs increased their market share as compared to major CEXs. However, DeFi protocols are subject to various operational and governance issues that may limit their reach and appeal vis-à-vis CEXs (FINANCIAL STABILITY BOARD 2023, p. 27-28).

VI.5 Lessons Learned from the Crypto Winter

For Zetzsche et al. (2023), the incidents of the Crypto Winter confirm that institutional instability is widespread in the crypto-asset industry, notwithstanding the business models beyond crypto exchanges, including Bitcoin mining companies, stablecoin projects, crypto funds and crypto lenders, as well as crypto-friendly banks (ZETZSCHE ET AL. 2023, p. 40).

The irony inherent in the Crypto Winter 2022–2023 is the fundamental premise of a working paper by Arner et al. (2023). The authors state that the crypto-asset sector lost about USD 2 trillion in market value in only one year. They complain that Bitcoin, cryptocurrencies and DeFi were praised by many as an alternative to the failures of TradFi that culminated in the 2008 global financial crisis. Through a transparent technological framework, crypto was supposed to avoid the downsides of TradFi including conflicts of interest from many powerful intermediaries, information asymmetries, centralisation of functions and markets, control by a few large and often interconnected intermediaries, an abundance of poorly informed over-enthusiastic market participants, as well as agency, operational and financial risks, and fraud, manipulation and misconduct. Financial regulation and supervision for TradFi have evolved over centuries to seek to enhance financial stability, ensure adequate investor, depositor and consumer protection and other goals (ARNER ET AL. 2023, p. 2).

According to Arner et al. (2023), following the failure of FTX, the need for a global and coordinated approach to crypto regulation has become clear (ARNER ET AL. 2023, p. 2). The authors argue that for the crypto ecosystem to survive and thrive, appropriately designed regulation is essential and that such financial regulation must address the range of market failures, externalities and inefficiencies which have arisen in the crypto ecosystem (ARNER ET AL. 2023, p. 3).

VII. Regulatory Responses and Approaches

VII.1 Is Regulation of Decentralised Finance Needed?

The short answer to the question of this subsection is yes.

The 2021 DeFi policy paper by the World Economic Forum addresses the topic of regulation. The first step by regulators and policymakers is to identify the relevant objectives and associated categories of policy and regulation. Common goals for financial regulation include (WORLD ECONOMIC FORUM 2021, p. 21):

- protection of investors and other consumers,
- market efficiency and integrity,
- capital formation,
- financial inclusion,
- prevention of illicit activity,
- safety and soundness, and
- financial stability.

Each goal provides a distinctive logic for certain kinds of rules. For example, regulators focused on investor protection are typically concerned that custodians are not able to abscond with funds. The noncustodial nature of DeFi may alleviate some of these worries, while creating new ones (WORLD ECONOMIC FORUM 2021, p. 21).

DeFi activity spans many domains of financial regulation, including securities, derivatives, exchanges, investment management, bank supervision, financial crime, consumer finance, insurance, risk management and macroprudential oversight. A coherent overarching strategy is important and could be delegated to a cross entity taskforce or similar body. Some DeFi activity patterns will match established legal categories, others will not (WORLD ECONOMIC FORUM 2021, p. 21).

Zetzsche et al. (2020) already saw the need for regulating DeFi before the Crypto Winter 2022–2023. The authors warned that decentralisation has the potential to undermine traditional forms of accountability and erode the effectiveness of TradFi regulation and enforcement. They pointed out that where parts of the financial services value chain are decentralised, there would be a reconcentration in a different (but possibly less regulated, less visible, and less transparent) part of the value chain. DeFi regulation could, and should, focus on this reconcentrated portion

of the value chain to ensure effective oversight and risk control. Rather than eliminating the need for regulation, in fact DeFi requires regulation in order to achieve its core objective of decentralisation (ZETZSCHE ET AL. 2020, p. 1).

Arner et al. (2025) highlight the systemic risk in the crypto ecosystem. The emergence of concentration and interdependencies have created a web of “systemically important crypto institutions” and “systemically important crypto market infrastructures” in the crypto ecosystem. These take a variety of forms, spanning the range of crypto infrastructure, crypto intermediaries and crypto conglomerates (ARNER ET AL. 2025, p. 188). The authors recommend to move away from a micro-prudential approach, which focuses on individual firm or system stability to broader systemic risks arising from complex interrelationships, to a macroprudential approach to crypto regulations (ARNER ET AL. 2025, p. 209).

VII.2 Range of Policy Actions on Regulating Decentralised Finance

The 2021 DeFi policy paper by the World Economic Forum enumerates a range of policy actions that may be adopted by regulators and policymakers for DeFi (WORLD ECONOMIC FORUM 2021, p. 21):

- Forbearance: decision that no new regulations are needed;
- Warnings: issuance of warning to users/consumers;
- Enforcement: determinations that existing rules already cover the relevant actors and activities and have not been complied with;
- Opt-in: provide the option to become subject to regulations in return for certain protections, even though there is no legal requirement;
- Pruning regulations: eliminate regulatory requirements that are no longer essential in a DeFi context;
- Limited licence frameworks: the possibility of obtaining licences of limited scope or under size thresholds, with light-touch requirements;
- Prohibitive measures: prohibit certain activities in the DeFi sector;
- New licence types: address risks with new categories designed for DeFi;
- Issuing guidance or expectations: craft new frameworks, often with a public comment or consultation included before its official release.

According to the policy paper, an effective regulatory response to DeFi is likely to involve a combination of existing regulation, retrofitted regulation and new, bespoke regulation. An emerging body of law specific to crypto-assets is growing (WORLD ECONOMIC FORUM 2021, p. 21).

VII.3 Current Regulatory Responses and Policy Measures

For Garcia Ocampo et al. (2023), policymakers are considering their response to crypto-related risks. Potential lines of action, include banning specific activities, isolating crypto-asset markets from the TradFi system, regulating crypto-asset activities in a manner akin to TradFi and developing alternatives that improve the efficiency of the TradFi sector (GARCIA OCAMPO ET AL. 2023, p. 4).

Garcia Ocampo et al. (2023) present an overview of policy measures taken in 19 jurisdictions to address the crypto-related risks. For this purpose, crypto-asset initiatives are classified into three categories depending on whether they address the risks associated with

- centrally managed crypto-asset activities,
- community-managed crypto-asset activities, or
- users' direct exposures to crypto-assets and related activities.

Different types of policy measures across jurisdictions include bans, restrictions, clarifications, bespoke requirements and initiatives to facilitate innovation. As these measures tend to reflect the evolution of market developments, most current initiatives target centrally managed crypto-asset activities, with a particular focus on service provision (GARCIA OCAMPO ET AL. 2023, p. 4). See description of the policy measures in Table 19.

Classification	Description
Policy measures in relation to risks posed by centrally-managed crypto-asset activities	These initiatives aim to address risks associated with business models where ... - centralised entities, including traditional financial and other intermediaries, govern and/or operate the issuance of stablecoins, global stablecoins, security tokens and utility tokens. - traditional financial intermediaries operate a centrally governed DLT (i.e., private permissioned ledger). - centralised entities govern and operate service provision activities.
Policy measures in relation to risks posed by community-managed crypto-asset activities	These initiatives aim to address risks associated with business models where ... - native tokens created on public DLTs (i.e., public permissionless ledgers) by a community of participants who claim to be organised through decentralised arrangements. - DLT applications which enable financial functions such as exchange and lending through smart contracts to run in public DLTs and are governed by a community of participants that claim to be organised through decentralised arrangements. Applications with these features are commonly referred to as DeFi protocols.
Policy measures in relation to risks posed by users' direct exposures to crypto-asset and related activities	These initiatives aim to address risks associated with users' direct exposures to different types of crypto-asset and related activities, including both centrally and community-managed activities. These initiatives target both retail and wholesale users' direct exposures.

Table 19: Classification of policy measures on crypto, tokens and Decentralised Finance. Source:

Adapted from Garcia Ocampo et al. (2023), p. 12.

In particular for DeFi, the authors identified a number of regulatory responses in major jurisdictions including the EU and large European economies (Table 20).

	Rulemaking	Public Statements and Speeches	Discussion Papers and Consultations	Reports and Working Papers	Other
Canada				Yes	
European Union		Yes	Yes	Yes	Yes
France		Yes			
Germany		Yes		Yes	
Italy		Yes			
Japan				Yes	
Netherlands				Yes	
Singapore		Yes			
United Arab Emirates	Yes		Yes		
United Kingdom		Yes	Yes	Yes	
United States		Yes		Yes	Yes

Table 20: Regulatory responses and policy measures for DeFi. Source: Adapted from Garcia

Ocampo et al. (2023), p. 34.

In Germany, regulatory responses so far include public statements and reports. In 2022, the Federal Financial Supervisory Authority (BaFin) in Germany published a statement on its website informing that the complex and innovative DeFi business models always require detailed examination with regard to the relevant supervisory authorisation criteria. In BaFin's

view, since supervisory law is fundamentally designed to be technology-neutral, the use of smart contract and/or on-chain governance structures does not initially change the classification of the service in the existing supervisory framework. The decisive factor for the assessment is the classification of the underlying tokens. When tokens are offered to investors, any prospectus requirements must also be observed (BAFIN 2022).

VII.4 Challenges for Regulation and Rulemaking

Various sources, including Deutsche Bundesbank (2021), World Economic Forum (2021), OECD (2022) and Born et al. (2022), analyse the fundamental challenges for regulation and rulemaking posed by DeFi projects. The above publications arrive at similar conclusions in terms of difficulty to regulate DeFi with existing tools and approaches for TradFi.

Deutsche Bundesbank (2021) states that DeFi applications are often not captured by existing regulation, especially as the term decentralisation is sometimes interpreted in different ways. Even regulatory provisions that should otherwise be applicable often cannot be sufficiently enforced as there are no natural or legal persons to act as addressee, meaning no one can be held responsible or liable for any damages. It cannot be ruled out that providers attempt to obscure their actual central governance by referring to the decentralisation of an application in order to evade any regulation. Regulators are thus faced with the following issues (DEUTSCHE BUNDESBANK 2021, p. 42):

- What functions of DeFi applications and their underlying blockchains are covered by existing regulatory frameworks and which require regulation?
- What parties (e.g., developers, holders of governance tokens, users) can be subject to regulation? How can they be identified?
- Which jurisdiction is responsible for a DeFi application without a legal seat? Can an effective international framework be developed to prevent regulatory arbitrage?
- How can regulation be effective and, at the same time, sufficiently technology-agnostic as to allow for secure innovations?
- How can networks be identified whose agents only give the impression of decentralisation to evade regulation, for example?

In some cases, regulatory regimes already exist for the interfaces between decentralised networks and the TradFi system, such as centralised trading platforms. A particular focus here

is the purchase and sale of crypto tokens in exchange for fiat money, with regulation seeking to combat money laundering and terrorist financing (DEUTSCHE BUNDESBANK 2021, p. 42).

For Deutsche Bundesbank (2021), a clear framework which also includes participants in DeFi applications with core functions could provide legal certainty and thus protect the interests of consumers and investors. Regulation and the trust it can establish could thereby boost the appeal and acceptance of DeFi applications. At the same time, it would contribute to the stability of the system and, given the increasing degree of interconnectedness, ultimately also the financial system as a whole. In this context, regulators worldwide should collaborate to prevent opportunities for regulatory arbitrage so that existing risks are regulated equally, irrespective of the technology employed and different providers. This would create a level playing field for decentralised networks vis-à-vis conventional financial market agents. Regulation could be a precondition for sustainable growth as it is likely a necessary step in bringing DeFi applications to the attention of a broader set of users (DEUTSCHE BUNDESBANK 2021, p. 42).

The 2021 policy paper by the World Economic Forum points out that most financial regulatory regimes focus on those “carrying on business” in a certain regulated activity, “dealing”, “arranging” or “operating” some scheme or exchange or “issuing” an offer (or similar). The relevant government entity was clear and focused on who is in control of an operation. Similarly, there are exemptions for service providers that only provide infrastructure, data or other tools to enable others to layer on their financial services. Frameworks contemplate definable and centralised operators that are engaged in providing particular financial end products and services, but are not necessarily the underlying builders. In the DeFi context, however, there may be no central entity performing the relevant activities. The software developers and token holders may be easily identifiable, but not those occupying roles that are the traditional regulatory touchpoints. Even when operators can be identified, they may not be able to modify DeFi services or stop transactions because of the decentralised nature of the protocols. Smart contracts can interact with assets held by other smart contracts that are not directly associated with a particular user. Regulators need to assess who is responsible and when a locus of responsibility must be identified. This requires careful analysis (WORLD ECONOMIC FORUM 2021, p. 21).

According to the World Economic Forum (2021), legal regimes often include mechanisms for vicarious secondary “controlling person”, “responsible officer” or aiding-and-abetting liability on the basis of requirements such as knowledge or foresight of harmful consequences. If developers of a DeFi service or others associated with the DeFi business could have identified

and mitigated legal compliance risks, policy-makers will need to consider whether it is appropriate to mandate that they should have. However, regulating the creation of software raises important concerns of freedom of speech and administrability, which should be considered carefully. The borderless nature of blockchain networks and digital assets also poses challenges for DeFi regulation at the national or subnational level (WORLD ECONOMIC FORUM 2021, p. 21).

For the OECD (2022), some DeFi applications, or part of their activities, may represent regulated activities for which comprehensive frameworks are already in place aiming at preserving financial stability, protecting financial consumers, promoting investor protection and market integrity, and mitigating illicit finance risks. For example, the issuance of governance tokens has some characteristics of securities/investment contracts. Their issuance, promotion or trading in DeFi platforms could be considered non-compliant in many jurisdictions. When DeFi applications or activities currently fall outside of the regulated space in some jurisdictions, they raise risks that may be left unaddressed by existing rules. Additionally, anonymity or pseudonymity and lack of customer due diligence by many DeFi applications gives rise to risks of money laundering, terrorism financing, and other use of illicit funds, facilitating misconduct (OECD 2022, p. 58).

The policy paper by the OECD (2022) sees challenges that arise from the decentralised nature of DeFi systems and the sophistication of the technological innovation involved. Depending on the jurisdiction, some regulatory or supervisory gaps may exist. Some of the characteristics of DeFi may be incompatible with existing regulatory frameworks, particularly given that the current framework is designed for a system that has financial intermediaries at its core. As the existence of intermediaries is contrary to the very essence of DeFi, it can be difficult to identify parties involved that can be assessed or regulated, making it challenging to supervise DeFi constructs with the existing oversight architecture. Enforcement of existing regulation could also be difficult to apply given the absence of an identified accountable entity in some arrangements (OECD 2022, p. 58).

According to the OECD (2022), the absence of regulatory/supervisory access points in DeFi systems is one of the key policy questions that remains to be overcome. As a first step, there may be a need to recentralise DeFi in order to get some comfort from a regulatory and supervisory standpoint, without completely undermining decentralisation. Having one party accountable (e.g., developers of the protocol or other incentivised parties) can help balance between total absence of central controlling authority and full supervision. Similarly, regulatory

and supervisory access points need to be defined by the community even though they may sound against the ethos of DeFi markets. Many of the challenges to the supervision of DeFi could be mitigated through forms of centralisation, such as organised governance. DAO governance structures could serve as a potential control point for regulatory and supervisory purposes given their centralised characteristics such as the holding of the admin key or concentrated ownership of governance tokens. Similarly, holders of controlling shares of governance tokens or identified parties benefiting from the operation of DeFi services through profit sharing mechanisms or fees could be considered as potential regulatory access points. The legal basis for such access, which includes the ability to force a node operator to give regulators information or to cease its activities, is not guaranteed in all jurisdictions (OECD 2022, p. 58).

For Born et al. (2022), the lack of traditional centralised entry points for regulation and the opaque and anonymous nature of DeFi pose challenges for policymakers in terms of enforcement and effective regulation and supervision. The nature of DeFi may facilitate regulatory arbitrage and it may fall outside the regulatory perimeter. If DeFi protocols are not controlled by a central entity or such entities cannot be identified, it is not clear to whom regulation should apply. As some DeFi activities may already fall under current EU financial legislation, further steps will require a careful analysis to better disentangle actual regulatory gaps from lack of enforcement and DeFi trying to escape financial regulation through decentralisation and opaqueness (BORN ET AL. 2022, section “Regulation”).

According to Born et al. (2022), where regulatory gaps exist, the innovative ways in which DeFi provides financial services will require innovative ways of regulation to close regulatory loopholes. Where central entities are not available, tackling the “intersection” of DeFi and CeFi to regulate these new developments could be a consideration, DeFi protocols/code must be deployed, governed and upgraded, requiring human interaction. As a consequence, holders of governance tokens, DAOs and platform developers could be brought into the regulatory perimeter (BORN ET AL. 2022, section “Regulation”).

VII.5 Statements on Decentralised Finance by International Standard-Setting Bodies

Two international standard-setting bodies, namely the IOSCO and the Financial Stability Board, formulated action points in their respective DeFi reports from 2022 and 2023, regarding the way forward on dealing with DeFi risks.

The 2023 DeFi report by the Financial Stability Board enumerates the following “considerations” on DeFi, which can be read as at to-do list on DeFi risks:

- It should proactively analyse the financial vulnerabilities of the DeFi ecosystem as part of its regular monitoring of the wider crypto-asset markets. Its monitoring framework should be complemented with DeFi-specific vulnerability indicators. It also should explore the growth of tokenisation of real assets as it could increase linkages between crypto-asset markets/DeFi, TradFi and the real economy. (FINANCIAL STABILITY BOARD 2023, p. 2-3).
- It should explore approaches to fill data gaps to measure and monitor interconnectedness of DeFi with TradFi, with the real economy, and with the crypto-asset ecosystem (FINANCIAL STABILITY BOARD 2023, p. 3).
- It should explore the extent to which its proposed policy recommendations for the international regulation of crypto-asset activities may need to be enhanced to acknowledge DeFi-specific risks and facilitate the application and enforcement of rules. It could also consider potential policy responses to the risks stemming from DeFi’s interconnectedness with the broader financial system and the real economy. Potential policy responses may include, for example, regulatory and supervisory requirements concerning direct exposures of TradFi institutions to DeFi, as well as concerning other ways that such institutions may seek to become more integrated with DeFi (FINANCIAL STABILITY BOARD 2023, p. 3).
- It could also consider assessing the regulatory perimeter across jurisdictions to determine which DeFi activities and entities fall or should fall within that perimeter or outside of it. For activities and entities outside of the perimeter policies should be developed to achieve appropriate regulation of activities giving rise to similar risks. It may consider whether subjecting certain entry points of DeFi users (stablecoins and centralised crypto-asset platforms) to additional prudential and investor protection requirements, or stepping up the enforcement of existing requirements, could reduce the risks inherent in closer interconnections (FINANCIAL STABILITY BOARD 2023, p. 3).

The 2022 DeFi report by IOSCO states that to understand the regulatory implications from DeFi requires analysing the DeFi ecosystem as it exists currently, its interrelationship with centralised crypto-asset trading platforms and service providers and traditional markets and activities. The analysis should relate to the current status as well as how the ecosystem may continue to develop in the future. In the view of IOSCO, to develop a comprehensive understanding requires identifying and analysing

- the structural components of each type of DeFi financial product, service, arrangement and activity;
- what aspects of these may be decentralised and why;
- what are the roles of each of the components and participants involved at each of the different layers or levels, including incentives and motivations;
- how participants engage with the various components and each other;
- and the roles that centralized crypto-asset trading platforms and service providers play (IOSCO 2022b, p. 2).

According to IOSCO (2022b), the peer-to-peer nature of DeFi and the ability to create alternatives to traditional and centralised financial market infrastructures, products or services, can complicate the application of existing regulatory frameworks to DeFi market participants and activities, including those that govern issuers, offerings, products, intermediaries, and trading markets (IOSCO 2022b, p. 2). IOSCO complains that the DeFi market and its participants have operated either outside the scope of existing regulatory frameworks or, in some jurisdictions, in non-compliance with applicable regulations (IOSCO 2022b, p. 36).

The 2023 IOSCO final DeFi report contains nine policy recommendations (Table 21) to address market integrity and investor protection concerns arising from DeFi by supporting greater consistency of regulatory frameworks and oversight in member jurisdictions (IOSCO 2023, p. 1). One of IOSCO's goals is to promote greater consistency with respect to the regulation and oversight of crypto-asset markets, given the cross-border nature of these markets, potential for regulatory arbitrage, and significant risk of harm to retail investors. IOSCO is also seeking to encourage consistency in the way crypto-asset markets and securities markets are regulated within individual IOSCO jurisdictions, in accordance with the principle of "same activity, same risk, same regulation/regulatory outcome" (IOSCO 2023, p. 2).

Number	IOSCO Recommendation
1	Analyze DeFi Products, Services, Activities, and Arrangements to Assess Regulatory Responses A regulator should analyze DeFi products, services, activities, and arrangements, occurring or located within its jurisdiction, with a view to applying its Existing Framework or New Framework, as appropriate, to the offer of financial products, the provision of financial services, and the engagement in financial activities (or to products, services, and activities that behave like, or have been substituted by investors for, financial products, services, and activities), in accordance with the principle of “same activity, same risk, same regulation/regulatory outcome.” To do so, a regulator should aim to achieve a holistic and comprehensive understanding of such DeFi products, services, activities, and arrangements. A regulator should assess what technological knowledge, data, and tools the regulator needs to understand, and analyze DeFi products, services, activities, and arrangements, to inform regulatory responses (IOSCO 2023, p. 18).
2	Identify Responsible Persons A regulator should aim to identify the persons and entities of a purported DeFi arrangement that could be subject to its applicable regulatory framework (Responsible Person(s)). These Responsible Person(s) include those exercising control or sufficient influence over a financial product offered, financial service provided, or financial activity engaged in (or over products, services, and activities that behave like, or have been substituted by investors for, financial products, services, and activities) by the DeFi arrangement (IOSCO 2023, p. 21).
3	Achieve Common Standards of Regulatory Outcomes A regulator should use Existing Frameworks or New Frameworks to regulate, supervise, oversee, and address risks arising from DeFi products, services, activities, and arrangements in a manner consistent with IOSCO Standards. The regulatory approach should be functionally based to achieve regulatory outcomes for investor protection and market integrity that are the same as, or consistent with, those that are required in traditional financial markets (IOSCO 2023, p. 25).
4	Require Identification and Addressing of Conflicts of Interest In applying Existing Frameworks or New Frameworks, a regulator should seek to require Responsible Persons, as appropriate, to identify and address conflicts of interest, particularly those arising from different roles and capacities of, and products and services offered by, a particular provider and/or its affiliates. These conflicts should be effectively identified, managed and mitigated. A regulator should consider whether certain conflicts are sufficiently acute that they cannot be effectively mitigated, including through effective systems and controls, disclosure, or prohibited actions. This may include requiring more robust measures such as legal disaggregation and separate registration and regulation of certain activities and functions to address this recommendation (IOSCO 2023, p. 31).
5	Require Identification and Addressing of Material Risks, Including Operational and Technology Risks In applying Existing Frameworks or New Frameworks, a regulator should seek to require Responsible Persons, as appropriate, to identify and address material risks, including operational and technology risks. These risks should be identified and effectively managed and mitigated. A regulator should consider whether certain risks are sufficiently acute that they cannot be effectively mitigated and may require more robust measures to address this recommendation (IOSCO 2023, p. 32).
6	Require Clear, Accurate, and Comprehensive Disclosures In applying Existing Frameworks or New Frameworks, a regulator should seek to require Responsible Persons, as appropriate, to accurately disclose to users and investors comprehensive and clear information material to the products and services offered in order to promote investor protection and market integrity (IOSCO 2023, p. 37).
7	Enforce Applicable Laws A regulator should apply comprehensive authorization, inspection, investigation, surveillance, and enforcement powers, consistent with its mandate, to DeFi products, services activities, and arrangements, including their Responsible Persons, that are subject to Existing Frameworks and New Frameworks, including measures to detect, deter, enforce, sanction, redress and correct violations of applicable laws and regulations. A regulator should assess what technological knowledge, data and tools the regulator needs to enforce applicable laws (IOSCO 2023, p. 38).

8	Promote Cross-Border Cooperation and Information Sharing A regulator, in recognition of the cross-border nature of DeFi products, services, activities, and arrangements, should have the ability to cooperate and share information with regulators and relevant authorities in other jurisdictions with respect to such products, services, activities, and arrangements. This includes having available cooperation and information sharing arrangements and/or other mechanisms to engage with regulators and relevant authorities in other jurisdictions. These should accommodate the authorization and on-going supervision of regulated persons and entities and enable broad assistance in enforcement investigations and related proceedings (IOSCO 2023, p. 39).
9	Understand and Assess Interconnections Among the DeFi Market, the Broader Crypto-Asset Market, and Traditional Financial Markets When analyzing DeFi products, services, activities, and arrangements, a regulator should seek to understand the interconnections among DeFi arrangements, the broader crypto-asset market, and also the traditional financial markets. In so doing, a regulator should consider how those interconnections impact risks to investor protection and market integrity, and how they might identify further regulatory touchpoints, including potential Responsible Persons. A regulator should, as appropriate, seek to employ, maintain and develop suitable methods for monitoring and assessing DeFi products, services, activities, and arrangements (IOSCO 2023, p. 42).

Table 21: IOSCO policy recommendations for Decentralized Finance. Source: Own representation adapted from IOSCO (2023), p. 18-42.

VII.6 Miscellaneous Approaches on Regulating Decentralised Finance

A number of approaches on regulating DeFi has been floated recently.

Roukny (2022) discusses the following four specific points of entry for public policy in his DeFi policy paper ordered by the European Commission (ROUKNY 2022, p. 36):

- Regulating DeFi activity of legal entities falling under current supervisory and regulatory mandates (policing the policed);
- Offering voluntary compliance opportunities for both entities and protocols;
- Producing public supervision and issuing public opinions on DeFi activity and protocols;
- Supervising, regulating and monitoring approaches to oracle markets.

Table 22 shows the four policies by Roukny (2022) with corresponding targets and risk/welfare.

Policy	Target	Risk/Welfare
Policing the policed	Entity	• Key management • Liquidation risk and cascades • Collateralisation costs
Voluntary compliance	Entity	• Commitment problem • Key management • Liquidation risk and cascades • Collateralisation costs
	Protocol	• Rug pull • Maintenance & upgrade • Governance risk • Wash trading • Layering dependencies • Complexity • Liquidation risk and cascades
Public observatory	Protocol	• Complexity • Wash trading • Layering dependencies • Liquidation risk and cascades
Oracle policies	Entity	• Collateralisation costs
	Protocol	• Collateralisation costs • Layering with unverifiable information
	Oracle	• Operational risk • Price risk • Manipulation and centralisation • Cost of service • Dispute resolution

Table 22: Policies for DeFi by Roukny. Source: Adapted from Roukny (2022), p. 45, Table 7.

“Policing the policed” means imposing new requirements on already regulated entities. Disclosure requirements would allow regulators to observe the DeFi activity, monitor exposures and adjust regulatory requirements (GARCIA OCAMPO ET AL. 2023, p. 36). This approach is closely related to the “gatekeeper approach” in the paper by OECD (2022), which involves regulating entry and exit points to DeFi (on-and-off ramps). Relevant points would be exchanges and/or other financial and non-financial service providers at the edges of DeFi the regulatory access point to the decentralised system, when fiat money is converted to crypto-assets and vice-versa. By definition, the gatekeeper approach would only cover the first and last transactions at the entry and exit points of DeFi while all internal DeFi activity would remain unsupervised (OECD 2022, p. 59).

A similar approach is the introduction of a regulated DeFi “trust layer”. A trusted environment for the execution of DeFi protocols is established through a common trust layer of independent “trust anchors”. These are regulated financial institutions that screen, verify and issue verifiable credentials to entities that wish to participate in DeFi protocols (GARCIA OCAMPO ET AL. 2023, p. 36).

Another approach consists in establishing a legal framework that recognises the different actors who manage or enable the operation of DeFi protocols. Introducing a legal framework that recognises technology-mediated organisational structures (e.g., DAOs) as legal entities would make it possible to define the liabilities of entities and actors for their activities. Similarly, introducing a legal framework for the operation of oracles would make it possible to define oracles’ liabilities. This would allow to integrate some of the safeguards in TradFi into services provided through DeFi protocols. (GARCIA OCAMPO ET AL. 2023, p. 36).

Another approach looks at miners and validators as intermediaries that would be subject to registration and oversight. They would be accountable for extractable value and market manipulation in crypto-asset activities built on public permissionless DLTs (GARCIA OCAMPO ET AL. 2023, p. 36).

Another idea revolves around introducing an approval process for DeFi protocols by supervisory authorities. Various factors would be considered in the assessment, such as the ability to identify participants, the level of transparency regarding the protocol’s functionality and governance decisions, and the technology supporting the protocol (GARCIA OCAMPO 2023, p. 36).

VII.7 Hypothetical Approach of Embedded Supervision

According to OECD (2022), in a hypothetical future scenario, there could be technological means for supervisors to participate as nodes in the network and/or intervene at the smart contract level. Similarly, supervisors could have access to all the data involved in the DeFi protocol while the protocol could incorporate automated provisions for regulatory compliance directly in the code of the smart contracts. DAOs or similar governance arrangements could produce reporting for regulatory compliance purposes (OECD 2022, p. 58). Technology-based regulatory systems, so-called embedded regulation or supervision, could be built into the design of DeFi protocols i.e., embedding the regulatory requirements technically, thus potentially decentralising both finance and its regulation (BORN ET AL. 2022, section “Regulation”; ZETZSCHE ET AL. 2020, p. 1).

Auer (2019-2022) makes the case for embedded supervision, i.e., a regulatory framework that provides for compliance in decentralised markets to be automatically monitored by reading the market's ledger. This reduces the need for firms to actively collect, verify and deliver data (AUER 2019-2022, p. 1). Four principles would guide the use of embedded supervision (Table 23).

1	Embedded supervision can only function as part of an overall regulatory framework that is backed up by an effective legal system and supporting institutions DLT-based exchange can evidence the transfer of ownership of asset-backed tokens from one known entity to another, but the connection between the underlying asset and the digital token must be guaranteed by the legal system. Additional institutions may also be required, for example, to guarantee the accuracy of external reference points that are relevant to payoffs of smart contracts.
2	Embedded supervision can be applied to decentralised markets that achieve economic finality. If there is no central intermediary to guarantee that a transfer of funds or securities has become irrevocable, an economic one must be applied. Economic finality means that a transaction can be considered as final once it is certain that, from a specific moment, it will never be profitable to undo.
3	Embedded supervision needs to be designed within the context of economic market consensus, taking into account how the market will react to being automatically supervised. Embedded supervision creates incentives for a regulated firm to cheat the supervisor by altering the transaction history in the blockchain. Supervisors thus need to ensure that the market's economic consensus is so strong that any attempt to deceive the supervisor will be unprofitable.
4	Embedded supervision should promote low-cost compliance and a level playing field for small and large firms. Embedded supervision should be designed to keep the fixed costs of compliance low. The supervisor may need to monitor aspects of decentralised markets – such as the verification market and the governance of decentralised systems) to ensure a level playing field for entrants.

Table 23: Principles of embedded supervision. Source: Own representation adapted from Auer (2019-2022), p. 4.

The research paper by Auer (2019-2022) explores the conditions under which distributed ledger data may be used to monitor compliance. A decentralised market is modelled that replaces intermediary based verification of legal data with blockchain-enabled credibility based on economic consensus. The key results set out the conditions under which the market's economic consensus would be strong enough to guarantee that transactions are economically final, so that supervisors can trust the distributed ledger's data (AUER 2019-2022, p. 1).

VII.8 Takeaways for Regulators Worldwide

Another Crypto Winter unfolding could be seen as a major failure by the authorities themselves. Based on the publications selected in this working paper, the emerging consensus among regulators and academics is that the DeFi sector needs to be monitored or supervised somehow. So far, regulators worldwide are mostly acting within the existing legal framework. Trying to regulate the DeFi market with new legislation will be a very difficult task. The

traditional approach of targeting a few centralised entities and financial intermediaries and imposing restrictions on them, does not work in this case.

It seems unlikely, that a hypothetical approach like embedded supervision will be pursued on a large scale in the short term. What seems likely is that regulators worldwide will take some incremental steps to regulate the DeFi sector embedded in the legal frameworks applicable for the crypto-asset market. Where possible, already existing tools might be applied. Where sensible, incremental upgrades to legislation might be sought.

An important international regulatory benchmark on DeFi has been set in 2023 with the nine IOSCO policy recommendations which, on a high-level, aim at consistent treatment of the DeFi sector across the IOSCO member jurisdictions. The European Securities and Markets Authority (ESMA), one of the key players in crypto-asset market regulation at EU level, is a member of IOSCO. This will be a favourable factor for a regulatory convergence on DeFi between the EU and IOSCO member jurisdictions worldwide. Regulatory responses to DeFi established at EU level may even deliver a blueprint for IOSCO and other international standard-setting bodies. The particular regulatory landscape for DeFi at EU level is addressed in the following section.

VIII. Regulating DeFi in the EU

VIII.1 Decentralised Finance and MiCA Regulation

The legal framework for crypto-assets at EU level is mainly built upon:

- the Markets in Crypto-assets Regulation (MiCA) from June 2023 (and fully applicable by December 2024),
- the Transfer of Funds Regulation (TFR) from June 2023,
- the Anti-Money Laundering Directive (AMLD5) from 2018 (superseded by AMLD6 in 2024), and
- the Markets in Financial Instruments Directive (MiFID II) from 2014.

The goal of the MiCA regime was to plug a regulatory gap on crypto-assets (in particular stablecoins), crypto-asset issuers, offerors and crypto-asset service providers not already covered under MiFID II (READ/DIEFENBACH 2023, p. 1). During the legislative process for MiCA in 2020–2023, risks arising from new developments in the crypto-assets market like DeFi became apparent. The events from the Crypto Winter 2022–2023 gave many reasons why a tighter crypto regulation was required. Nonetheless, making amendments in the MiCA draft

legislation to bring DeFi and other areas of action under regulatory scope would have delayed the lengthy EU legislation process even more or lead to unintended consequences.

So, the EU legislators who worked on the MiCA legislative process went for a compromise on DeFi and other new developments on the crypto-asset market. On one hand, the final MiCA text acknowledges in its Recital 22 (Table 24) that crypto-asset services provided in a “fully decentralised manner without any intermediary” should not fall within the scope of the MiCA Regulation. On the other hand, articles under Title IX “Transitional and final provisions” put monitoring new developments on the crypto-asset market, including the DeFi market, and working out an “appropriate regulatory treatment” via mandatory reports on a to-do list. Similarly, lending and borrowing of crypto-assets (regardless of centralised or decentralised) was excluded from scope in Recital 94 (Table 24), but was specifically listed for mandatory reporting.

MiCA Recital or Article	MiCA Text Extracts Concerning Decentralised Finance
Recital 22	This Regulation should apply to natural and legal persons and certain other undertakings and to the crypto-asset services and activities performed, provided or controlled, directly or indirectly, by them, including when part of such activities or services is performed in a decentralised manner. Where crypto-asset services are provided in a <u>fully decentralised manner without any intermediary</u> , they should not fall within the scope of this Regulation. This Regulation covers the rights and obligations of issuers of crypto-assets, offerors, persons seeking admission to trading of crypto-assets and crypto-asset service providers. Where crypto-assets have no identifiable issuer, they should not fall within the scope of Title II, III or IV of this Regulation. Crypto-asset service providers providing services in respect of such crypto-assets should, however, be covered by this Regulation.
Recital 94	This Regulation should not address the <u>lending and borrowing of crypto-assets</u> , including e-money tokens, and therefore should not prejudice applicable national law. The feasibility and necessity of regulating such activities should be further assessed.
Art. 140	... 2.(t) an assessment of the development of <u>decentralised finance</u> in markets in crypto-assets and of the appropriate regulatory treatment of <u>decentralised crypto-asset systems</u> ; ...
Art. 142	... 2.(a) an assessment of the development of <u>decentralised-finance</u> in markets in crypto-assets and of the appropriate regulatory treatment of <u>decentralised crypto-asset systems without an issuer or crypto-asset service provider</u> , including an assessment of the necessity and feasibility of regulating <u>decentralised finance</u> ; (b) an assessment of the necessity and feasibility of regulating <u>lending and borrowing of crypto-assets</u> ; ...

Table 24: Text extracts concerning Decentralised Finance in the MiCA Regulation. Source: Own representation adapted from MiCA Regulation.

The path to a regulatory response to developments in the DeFi market has been partly laid in the MiCA Regulation text. Art. 140, 141 and 142 trigger the production of a series of mandated

reports and legislative proposals (Table 25) to deal with new developments on the crypto-asset market including DeFi (HUERTAS 2024).

- Pursuant to Art. 142, the European Commission would have to present by 30 December 2024 a report (and where appropriate with a legislative proposal) to the European Parliament and the Council on the application of the MiCA Regulation including an assessment on DeFi and appropriate regulatory treatment of decentralised crypto-asset systems without an issuer or crypto-asset service provider, including an assessment of the necessity and feasibility of regulating DeFi.
- Pursuant to Art. 140, the European Commission would have to present by 30 June 2025 an interim report and by 30 June 2027 a final report (and where appropriate with a legislative proposal) to the European Parliament and the Council on the application of the MiCA Regulation, including an assessment of the development of DeFi in markets in crypto-assets and of the appropriate regulatory treatment of decentralised crypto-asset systems.

The mandated reports, accompanied by legislative proposals by the European Commission, may lead to full-scope regulation of DeFi in the future (HUERTAS 2024). So far, the European Commission has missed both deadlines, 30 December 2024 for the Art. 142 report and 30 June 2025 for the Art. 140 interim report.

MiCA Article	Institutions	Deadlines	Text Extract
Art. 140 Reports on the application of this Regulation	Commission, EBA, ESMA	30.06.2025 30.06.2027	1. By 30 June 2027, having consulted EBA and ESMA, the Commission shall present a report to the European Parliament and the Council on the application of this Regulation accompanied, where appropriate, by a legislative proposal. An interim report shall be presented by 30 June 2025, accompanied, where appropriate, by a legislative proposal. 2. The reports referred to in paragraph 1 shall contain the following ... (t) an assessment of the development of <u>decentralised finance</u> in markets in crypto-assets and of the appropriate regulatory treatment of <u>decentralised crypto-asset systems</u> ; ...
Art. 141 ESMA annual report on market developments	ESMA, EBA	31.12.2025	By 31 December 2025 and every year thereafter, ESMA, in close cooperation with EBA, shall submit a report to the European Parliament and to the Council on the application of this Regulation and <u>developments in markets in crypto-assets</u> . The report shall be made publicly available. The report shall contain the following: ...
Art. 142 Report on latest developments in crypto-assets	Commission, EBA, ESMA	30.12.2024	1. By 30 December 2024 and after consulting EBA and ESMA, the Commission shall present a report to the European Parliament and the Council on the latest developments with respect to crypto-assets, in particular on matters that are not addressed in this Regulation, accompanied, where appropriate, by a legislative proposal. 2. The report referred to in paragraph 1 shall contain at least the following: (a) an assessment of the development of <u>decentralised-finance</u> in markets in crypto-assets and of the appropriate regulatory treatment of decentralised crypto-asset systems without an issuer or crypto-asset service provider, including an assessment of the necessity and feasibility of regulating <u>decentralised finance</u> ; (b) an assessment of the necessity and feasibility of regulating <u>lending and borrowing of crypto-assets</u> ; ...

Table 25: Mandated reports on Decentralised Finance by MiCA Regulation. Source: Own representation adapted from MiCA Regulation Art. 140-142.

VIII.2 2025 ESMA/EBA Joint Report on Market for Decentralised Finance, Crypto Lending, Crypto Borrowing and Crypto Staking

On 9 February 2024, the European Commission 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. Later a postponement was agreed. ESMA and EBA submitted a Joint Report to the Commission on 16 January 2025 as the contribution of these institutions to the mandated Art. 142 report (ESMA/EBA 2025, p. 3).

The Joint Report by ESMA/EBA (2025) is analytical and does not make any specific policy recommendations (ESMA/EBA 2025, p. 3). Two short factsheets, aimed at consumers, were

published on 24 January 2025, one on “Decentralised Finance” (EBA/ESMA 2025a) and the other one on “Crypto lending, borrowing and staking” (EBA/ESMA 2025b). The Joint Report establishes definitions for these four terms (Table 26), which may be used for a legislative proposal.

Term	Definition by ESMA/EBA
Decentralised Finance (DeFi)	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 centralised institutions.
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
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).
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.

Table 26: Definition of terms by ESMA/EBA. Source: Own representation adapted from ESMA/EBA (2025), p. 7, 37, 41, 42; EBA/ESMA (2025a), p. 1; EBA/ESMA (2025b), p. 1.

The Joint Reports finds that DeFi remains a “niche phenomenon”. TVL in DeFi protocols represents 4% of all crypto-asset market value at the global level. Also, EU adoption of DeFi is behind other developed economies like the US (ESMA/EBA 2025, p. 2).

The Joint Report points out that crypto lending, borrowing and staking services are offered by a number of crypto-asset service providers in EU jurisdictions, which in some cases also offer regulated crypto-asset services. The report complains that users may receive insufficient information on conditions in relevant areas (ESMA/EBA 2025, p. 2).

Now it is up to the European Commission to take into account the analysis and findings of the Joint Report for drafting its own Art. 142 report, perhaps accompanied by a legislative proposal where appropriate, to the European Parliament and the Council.

VIII.3 2023 European Systemic Risk Board Report

In May 2023, shortly before the publication of the final text of the MiCA Regulation in the Official Journal of the EU, the European Systemic Risk Board (ESRB) published a report titled “Crypto-assets and decentralised finance: Systemic implications and policy options”.

Members of the ESRB are the European Central Bank (ECB), the European Securities and Markets Authority (ESMA), the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA), the European Commission, the Economic and Financial Committee, as well as national macroprudential authorities.

The ESRB report sees DeFi as currently small and with no discernible connection to TradFi (ESRB 2023, p. 19). The report also sets out considerations to mitigate potential financial stability and macroprudential risks from crypto-assets and DeFi. Three policy priorities (Table 27) are identified which revolve around monitoring and understanding developments, not legislating (ESRB 2023, p. 30).

Priorities	Policy Options
Priority 1	Strengthen monitoring capacity 1.1: Introduce reporting requirements for financial institutions with exposure to crypto-assets 1.2: Monitor interconnectedness between the fund sector and the crypto-asset sector 1.3: Enhance reporting requirements within the crypto-asset sector 1.4: Introduce reporting requirements to map exposures between crypto-asset trading platforms and other relevant entities
Priority 2	Identify and assess risks from crypto-asset conglomerates and leverage using crypto-assets, and suggest policy options to mitigate identified risks 2.1: Identify and assess risks arising from crypto-asset conglomerates, taking account of market developments following the application of MiCA 2.2: Identify and assess risks from leverage using crypto-assets
Priority 3	Monitor market developments to ensure potential risks to financial stability and the effectiveness of macroprudential policy can be identified, assessed and mitigated 3.1: Understand market developments and implications for operational resilience 3.2: Understand DeFi developments and implications for regulation and supervision 3.3: Understand crypto-asset staking and lending and implications for regulation and supervision

Table 27: Priorities and policy options. Source: Own representation adapted from ESRB (2023), p. 31-47.

Concerning policy “3.2: Understand DeFi developments and implications for regulation and supervision” the ESRB report first spells out the following six reasons for monitoring DeFi (ESRB 2023, p. 45-46):

- There may be an indirect effect from forthcoming regulation on DeFi;
- DeFi services play an important role in crypto-asset lending and borrowing;
- DeFi services increase the complexity and interconnectedness of crypto-asset markets;
- Automated procedures within DeFi can cause volatility;
- The automation of DeFi services gives rise to new types of operational risk related to the robustness of code used to deliver these services;
- A key challenge for regulating and supervising DeFi services is linked to their governance.

The ESRB recommends to target on DeFi developers as relevant entry point for regulation (ESRB 2023, p. 47):

- DeFi developers could be required to abide by specific regulations covering the design and creation of smart contracts;
- DeFi developers' intellectual property rights relating to smart contracts could be regulated;
- DeFi could contain an upgrade/modification functionality to allow for the rectification of errors in code as well as the introduction of regulatory limits;
- The regulation of DeFi deployers could be built on tort liability or regulation in order to incentivise them to thoroughly audit smart contract code prior to deployment and thus reduce the likelihood that faulty code is deployed.
- Requirements for oracles that interact with DeFi smart contracts may be necessary.

VIII.4 2023 ECON Committee Study on How to Bring Decentralised Finance under EU Regulation

Zetzsche et al. (2023), in their study prepared for the European Parliament's Committee on Economic and Monetary Affairs (ECON), focus on regulatory action at EU level in order to bring DeFi activities under the EU regulation umbrella. Some of their specific suggestions may be regarded as likely to be included in a future legislative proposal by the European Commission.

The authors see decentralisation as a basis of regulatory arbitrage. Decentralisation has become the main argument for the non-application of many financial regulations, ranging from AML/CFT to disclosure, licensing and fit and proper rules and the sustainability-oriented disclosures. The same discussion implicitly concerns the non-application of certain rules in case of “non-custodial wallets”, “mixing services” and many other innovations crypto that fall out of scope due to their (apparent) decentralisation. The authors do not share the view that decentralisation justifies exemptions from all financial laws. At the heart of fully decentralised platforms thus lies human cooperation, exercised through the steering of computers and servers. Human cooperation already results in the entity status of a “cooperation” under the private laws of some EU countries. In particular, the mere cooperation of a team of developers or community members that either founded a crypto project or volunteered to keep it afloat suffices in some jurisdictions for entity status (ZETZSCHE ET AL. 2023, p. 115-116). Given that the smart contracts that underlie the functioning of DeFi protocols are coded, put into operation and modified by humans, and humans decide to let them operate on their information technology, the argument

that the use of smart contracts results in a product that is something different from the result of human cooperation, is inconclusive (ZETZSCHE ET AL. 2023, p. 116).

Zetzsche et al. (2023) propose to acknowledge the legal qualification assigned to human cooperation in EU financial regulation. In their view, a cross-sectoral EU legislation should be established such that DAOs are treated as entities for licensing purposes under EU financial regulation. This should be irrespective of:

- whether the DAO is incorporated, formally or informally established, capitalized or not,
- where the DAO is established,
- whether it is merely set up by way of protocols that apply in a decentralized manner, or by other means, and
- where and in which way the multiple token holders take collective decisions.

The DAO as a whole should be deemed an issuer or a crypto-asset service provider that would be subject to any relevant EU financial regulation and AML/CFT rules (ZETZSCHE ET AL. 2023, p. 115-116). Not all DAOs would be automatically subject to licensing. For that, a DAO collectively must: (ZETZSCHE ET AL. 2023, p. 116)

- provide a service that comes with licensing (which is not the case if it merely issues utility tokens, for instance, and has received the exemption from the default rule proposed herein),
- serve users,
- who reside in the Single Market,
- the exemption for reverse solicitation does not apply, and
- proportionate size thresholds are exceeded.

If, however, the DAO is acknowledged as an entity for regulatory purposes and if it is a crypto-asset service provider it will have to: (ZETZSCHE ET AL. 2023, p. 116-117)

- lay out the details of its operations, risk management, compliance functions and so on, in a programme of operations,
- provide a business continuity policy that allows for the proper winding-up of the DAO's operations in the case of insolvency, and

- meet all other requirements set for crypto-asset service providers under the Markets in Crypto-assets Regulation (MICA or MiCAR) and the respective other EU financial regulation.

Zetzsche et al. (2023) touch upon the argument that is used to evade EU financial regulation that DAOs do not serve clients, but only serve their members. The argument is similar to the case where investment clubs are exempted from the Alternative Investment Fund Managers Directive (AIFMD) and all members collectively participate in the investment decision at all times: these investment clubs are exempted from the AIFMD for lack of “external management”. However, in the context of alternative investment funds ESMA applies the “self-management exemption” quite strictly as it facilitates circumvention of EU financial regulation. The authors propose to clarify that only where all or an overwhelming (90%) majority of token holders are personally involved in all financial decisions at all times, the argument is accepted that there are no external clients, but members only, running the financial service. The “same risks, same rules” rationale should support a narrow construction of (potential) exemptions (ZETZSCHE ET AL. 2023, p. 117).

IX. Conclusion and Outlook

The size of the DeFi market has quickly grown to several hundred billion USD in TVL. Regulators and policymakers around the globe have issued warnings on consumer risks and financial stability risks. Following the events of the Crypto Winter 2022–2023 the emerging consensus is that the DeFi sector needs to be monitored or supervised somehow. A range of regulatory responses and approaches is being discussed by standard-setting bodies, regulators and academics. Currently, the first efforts are aimed at monitoring the DeFi market, issuing further warnings and observing any impact on the regulated entities from the TradFi system.

There is a likelihood that the DeFi market will continue growing into a larger shadow financial system with crypto-assets and connecting more to the traditional financial system. If regulators and policymakers worldwide perceive an increased contagion risk to the TradFi system, then a tightening of regulation will follow, also through legislation.

At the EU level, the mandatory reports by the EU institutions, built into the MiCA Regulation, will keep pressure on the European Commission to act before another Crypto Winter unfolds. A potential EU legislative proposal might be part of a “MiCA 2.0” or “MiCA II” package looking to extend EU law to DeFi, crypto lending, borrowing and staking, non-fungible token, and other crypto innovations. It is normal for EU regulations and directives on the financial

system to undergo upgrades from time to time. The suggestions contained in the ECON study by Zetzsche et al. (2023) featuring a cross-sectoral EU legislation on DAOs are likely to be considered.

Finally, Artificial Intelligence (AI) is increasingly influencing financial markets and business processes. It is likely to affect the development of crypto-assets and DeFi as well, an area that warrants further exploration.

References

- ARAMONTE, S. / DOERR, S. / HUANG, W. / SCHRIMPF, A. (2022): DeFi lending: intermediation without information? in: BIS Bulletin, 14 June 2022, <https://www.bis.org/publ/bisbull57.htm> (access: 03.10.2024).
- ARAMONTE, S. / HUANG, W. / SCHRIMPF, A. (2021): DeFi risks and the decentralisation illusion, in: BIS Quarterly Review, December 2021, p. 21–36, https://www.bis.org/publ/qtrpdf/r_qt2112b.pdf (access: 29.07.2025).
- ARNER, D.W. / RATNA, T. / ANIMASHAU, S. / BEDI, J. / MISHRA, N. (2025): Centralization in Decentralized Finance: Systematic Risk in the Crypto Ecosystem and Crypto's Future as a Regulated Industry, in: Law and Contemporary Problems, Vol. 87, pp. 185-210, <https://scholarship.law.duke.edu/lcp/vol87/iss2/8/> (access: 29.07.2025).
- ARNER, D.W. / ZETZSCHE, D.A. / BUCKLEY, R.P. / KIRKWOOD, J. (2023): The Financialization of Crypto: Lessons from FTX and the Crypto Winter of 2022–2023, University of Hong Kong Faculty of Law Research Paper No. 2023/19, UNSW Law Research Paper No. 23-31, March 2023, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4372516 (access: 21.08.2025).
- AUER, R. (2019-2022): Embedded supervision: how to build regulation into decentralised finance, BIS Working Papers No 811, September 2019 (revised May 2022), <https://www.bis.org/publ/work811.pdf> (access: 03.06.2025).
- BAFIN (2022): Decentralised Finance („DeFi“) and DAOs, undated English translation of web page, German version last revised 1 September 2022, https://www.bafin.de/EN/Aufsicht/FinTech/Geschaeftsmodelle/DLT_Blockchain_Krypto/DAOS/DAOS_node_en.html (access: 26.09.2024).
- BENEDETTI, Z. / PIAZZA, F. (2021): Decentralised Finance: A categorisation of smart contracts, ESMA Working Paper No. 3, 2024, 1 August 2024, https://www.esma.europa.eu/sites/default/files/2024-08/ESMA50-43599798-9913_Working_Paper_Decentralised_Finance_-_A_Categorisation_of_smart_contracts.pdf (access: 04.08.2025).
- BITKOM (2020): Decentralized Finance (DeFi) – A new Fintech Revolution?, <https://www.bitkom.org/Bitkom/Publikationen/Decentralized-Finance-A-new-Fintech-Revolution> (access: 03.10.2024).

- BORN, A. / GSCHOSSMAN, I. / HODBOD, A. / LAMBERT, C. / PELLICANI, A. (2022): Decentralised Finance - a new unregulated non-bank system?, in: ECB Macroprudential Bulletin, Number 18, July 2022, https://www.ecb.europa.eu/press/financial-stability-publications/macprudential-bulletin/focus/2022/html/ecb.mpbu202207_focus1.en.html (access: 26.09.2024).
- CORNELLI, G. / GAMBACORTA, L. / GARRATT, R. / REGHEZZA, A. (2025): Why DeFi lending? Evidence from Aave V2, Working Paper, April 2025, <https://www.bis.org/publ/work1183.pdf> (access: 24.9.2025)
- BRÜHL, V. (2021): Decentralised Finance (DeFi) – wie die Tokenisierung die Finanzindustrie verändert, in: Wirtschaftsdienst, Vol. 101, Number 8, p. 629-637, <https://www.wirtschaftsdienst.eu/inhalt/jahr/2021/heft/8/beitrag/decentralised-finance-wie-die-tokenisierung-die-finanzindustrie-veraendert.html>, <https://doi.org/10.1007/s10273-021-2981-7> (access: 03.10.2024).
- DEUTSCHE BUNDESBANK (2021): Crypto tokens and decentralised financial applications, in: Deutsche Bundesbank Monthly Report, July 2021, p. 31-48, <https://www.bundesbank.de/resource/blob/873132/74fc658db07569219ff74f4e4e55c36f/mL/2021-07-kryptotoken-data.pdf> (access: 29.07.2025).
- EUROPEAN BANKING AUTHORITY / EUROPEAN SECURITIES AND MARKETS AUTHORITY (2025a): Recent developments in crypto-assets: Decentralised Finance, Factsheet, 24 January 2025, <https://www.esma.europa.eu/document/factsheet-recent-developments-crypto-assets-decentralised-finance-defi> (access: 23.09.2025).
- EUROPEAN BANKING AUTHORITY / EUROPEAN SECURITIES AND MARKETS AUTHORITY (2025b): Recent developments in crypto-assets: Crypto lending, borrowing and staking, Factsheet, 24 January 2025, <https://www.esma.europa.eu/document/factsheet-recent-developments-crypto-assets-crypto-lending-and-staking> (access: 23.09.2025).
- EUROPEAN SECURITIES AND MARKETS AUTHORITY (2023): Decentralised Finance in the EU: Developments and risks, in: ESMA TRV Risk Analysis, 11 October 2023, https://www.esma.europa.eu/sites/default/files/2023-10/ESMA50-2085271018-3349_TRV_Article_Decentralised_Finance_in_the_EU_Developments_and_Risks.pdf (access: 04.08.2025).
- EUROPEAN SECURITIES AND MARKETS AUTHORITY / EUROPEAN BANKING AUTHORITY (2025): Recent developments in crypto-assets (Article 142 MiCAR), Joint Report, 16 January

2025, <https://www.esma.europa.eu/document/joint-eba-esma-report-recent-developments-crypto-assets-article-142-mica> (access: 23.09.2025).

EUROPEAN SYSTEMIC RISK BOARD (2023): Crypto-assets and decentralised finance: Systemic implications and policy options, ESRB Task Force on Crypto-Assets and Decentralised Finance, report, May 2023, <https://www.esrb.europa.eu/pub/pdf/reports/esrb.cryptoassetsanddecentralisedfinance202305%7E9792140acd.en.pdf?853d899dcdf41541010cd3543aa42d37> (access: 24.09.2025).

FINANCIAL STABILITY BOARD (2022a): Assessment of Risks to Financial Stability from Crypto-assets, report, 16 February 2022, <https://www.fsb.org/2022/02/assessment-of-risks-to-financial-stability-from-crypto-assets/>, <https://www.fsb.org/uploads/P160222.pdf> (access: 19.08.2025).

FINANCIAL STABILITY BOARD (2022b): FSB warns of emerging risks from crypto-assets to global financial stability, press release, 16 February 2022, <https://www.fsb.org/2022/02/fsb-warns-of-emerging-risks-from-crypto-assets-to-global-financial-stability/> (access: 19.08.2025).

FINANCIAL STABILITY BOARD (2023): The Financial Stability Risks of Decentralised Finance, report, 16 February 2023, <https://www.fsb.org/2023/02/the-financial-stability-risks-of-decentralised-finance/> (access: 03.10.2024).

GARCIA OCAMPO, D. / BRANZOLI, N. / CUSMANO, L. (2023): Crypto, tokens and DeFi: navigating the regulatory landscape, Financial Stability Institute, FSI Insights on policy implementation No 49, May 2023, <https://www.bis.org/fsi/publ/insights49.pdf> (access: 02.06.2025).

GOGEL, D. / BAKER-TAYLOR, T. / CLOOTS, A.S. / FORSTER, B. / GUSTAVE, J.L. / SCHÄR, F. / SOKOLIN, L. (2021): DeFi Beyond the Hype: The Emerging World of Decentralized Finance, Wharton Blockchain and Digital Asset Project / World Economic Forum, The Wharton School, University of Pennsylvania, May 2021, <https://wifpr.wharton.upenn.edu/wp-content/uploads/2021/05/DeFi-Beyond-the-Hype.pdf> (access: 03.10.2024).

GRAMLICH, V. / PRINCIPATO, M. / SCHELLINGER, B. / SEDLMEIR, J. / AMEND, J. / STRAMM, J. / ZWEDE, T. / STRÜKER, J. / URBACH, N. (2022): Decentralized Finance (DeFi) – Foundations, Applications, Potentials, and Challenges. Branch Business & Information

Systems Engineering of Fraunhofer FIT,
https://www.fit.fraunhofer.de/content/dam/fit/de/documents/Whitepaper_DeFi_English_Version_2022_07_15.pdf (access: 03.10.2024).

GUDGEON, L. / WERNER, S.M. / PEREZ, D. / KNOTTENBELT, W.J. (2020): DeFi Protocols for Loanable Funds: Interest Rates, Liquidity and Market Efficiency, Cornell University, working paper, submitted 11 June 2020, revised 15 October 2020, <https://arxiv.org/abs/2006.13922> (access: 03.10.2024).

HEIMBACH, L. / HUANG, W. (2024): DeFi Leverage, BIS Working Papers No 1171, Monetary and Economic Department, March 2024, <https://www.bis.org/publ/work1171.pdf> (access: 19.08.2025).

HUERTAS, M. (2024): Demystifying DeFi in MiCAR, PWC Legal Germany, 8 October 2024, <https://legal.pwc.de/en/news/articles/demystifying-defi-in-micar> (access: 23.09.2025).

INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS (2022a): IOSCO explains how Decentralised Financing is cloning Financial Markets, press release, 24 March 2022, <https://www.iosco.org/news/pdf/IOSCONEWS637.pdf> (access: 20.02.2023).

INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS (2022b): IOSCO Decentralized Finance Report, March 2022, <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD699.pdf> (access: 29.04.2022).

INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS (2023): Final Report with Policy Recommendations for Decentralized Finance (DeFi), December 2023, <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD754.pdf> (access: 27.09.2024).

KOKORIN, I. (2025): The decentralisation defence, in: Computer Law & Security Review, Vol. 57, July 2025, 106148, <https://doi.org/10.1016/j.clsr.2025.106148> (access: 23.09.2025).

MEYER, E.A. / WELPE, I.M. / SANDNER, P. (2021): Decentralized Finance - A Systematic Literature Review and Research Directions, working paper, 17 November 2021, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4016497 (access: 20.02.2023).

MEYER, E.A. / WELPE, I.M. / SANDNER, P. (2022): Decentralized Finance - A Systematic Literature Review and Research Directions, ECIS 2022 Research Papers 25, https://aisel.aisnet.org/ecis2022_rp (access: 27.09.2024).

OECD (2022): Why Decentralised Finance (DeFi) Matters and the Policy Implications, 19 January 2022, OECD Publishing, Paris, <https://doi.org/10.1787/109084ae-en>,

https://www.oecd.org/en/publications/why-decentralised-finance-defi-matters-and-the-policy-implications_109084ae-en.html (access: 05.08.2025).

QIN, K. / ZHOU, L. / GAMITO, P. / JOVANOVIĆ, P. / GERVAIS, A. (2021): An Empirical Study of DeFi Liquidations: Incentives, Risks, and Instabilities. In ACM Internet Measurement Conference (IMC '21), November 2-4, 2021, Virtual Event, USA, p. 336-360, <https://doi.org/10.1145/3487552.3487811>, <https://arxiv.org/pdf/2106.06389.pdf> (access: 03.10.2024).

READ, O. / DIEFENBACH, C. (2022): The Path to the EU Regulation Markets in Crypto-assets (MiCA), wifin Working Paper 13/2022, 03.11.2022, <https://econpapers.repec.org/paper/zbwwifinw/132022.htm> (access: 03.11.2022).

ROUKNY, T. (2022): Decentralized Finance: Information frictions and public policies, June 2022, prepared for the European Commission, Directorate-General for Financial Stability, Financial Services and Capital Markets, https://finance.ec.europa.eu/system/files/2022-10/finance-events-221021-report_en.pdf (access: 10.11.2022).

SCHÄR, F. (2021): Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets, in: Federal Reserve Bank of St. Louis Review, Second Quarter 2021, 103(2), p. 153-174, <https://research.stlouisfed.org/publications/review/2021/02/05/decentralized-finance-on-blockchain-and-smart-contract-based-financial-markets> (access: 03.10.2024).

SCHULER, K. / CLOOTS, A.S. / SCHÄR, F. (2024): On DeFi and On-Chain CeFi: How (Not) to Regulate Decentralized Finance, in: Journal of Financial Regulation, Vol. 10, Issue 2, September 2024, p. 213-242, <https://doi.org/10.1093/jfr/fjad014> (access: 19.08.2025).

SHAH, K. / LATHIYA, D. / LUKHI, N. / PARMAR, K. / SANGHVI, H. (2023): A systematic review of decentralized finance protocols, in: International Journal of Intelligent Networks, Vol. 4, p. 171-181, <https://www.sciencedirect.com/science/article/pii/S2666603023000179>, <https://doi.org/10.1016/j.ijin.2023.07.002> (access: 03.10.2024).

WORLD ECONOMIC FORUM (2021): Decentralized Finance (DeFi) Policy-Maker Toolkit, White Paper, June 2021, https://www3.weforum.org/docs/WEF_DeFi_Policy_Maker_Toolkit_2021.pdf (access: 30.07.2025).

ZETZSCHE, D.A. / ARNER, D.W. / BUCKLEY, R.P. (2020): Decentralized Finance, in: Journal of Financial Regulation, 2020, Issue 6, p. 172-203, <https://academic.oup.com/jfr/article/6/2/172/5913239>, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3539194 (access: 03.10.2024).

ZETZSCHE, D.A. / BUCKLEY, R.P. / ARNER, D.W. / VAN EK, M.C. (2023): Remaining regulatory challenges in digital finance and crypto-assets after MiCA, May 2023, study prepared for the European Parliament's Committee on Economic and Monetary Affairs (ECON), [https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU\(2023\)740083](https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2023)740083) (access: 09.06.2023).

Legal Sources

AIFMD: Directive 2011/61/EU of the European Parliament and of the Council of 8 June 2011 on Alternative Investment Fund Managers and amending Directives 2003/41/EC and 2009/65/EC and Regulations (EC) No 1060/2009 and (EU) No 1095/2010, <https://eur-lex.europa.eu/eli/dir/2011/61/oj/eng> (access: 10.05.2020).

AMLD5: Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, <https://eur-lex.europa.eu/eli/dir/2018/843/oj/eng> (access: 02.10.2022).

AMLD6: Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 on the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Directive (EU) 2019/1937, and amending and repealing Directive (EU) 2015/849, <https://eur-lex.europa.eu/eli/dir/2024/1640/oj/eng> (access: 26.09.2025).

MiCA: Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937, <https://eur-lex.europa.eu/eli/reg/2023/1114/oj/eng> (access: 09.06.2023).

MiFID II: Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (recast), <https://eur-lex.europa.eu/eli/dir/2014/65/oj/eng> (access: 22.10.2016).

TFR: Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849, <https://eur-lex.europa.eu/eli/reg/2023/1113/oj/eng> (access: 09.06.2023).