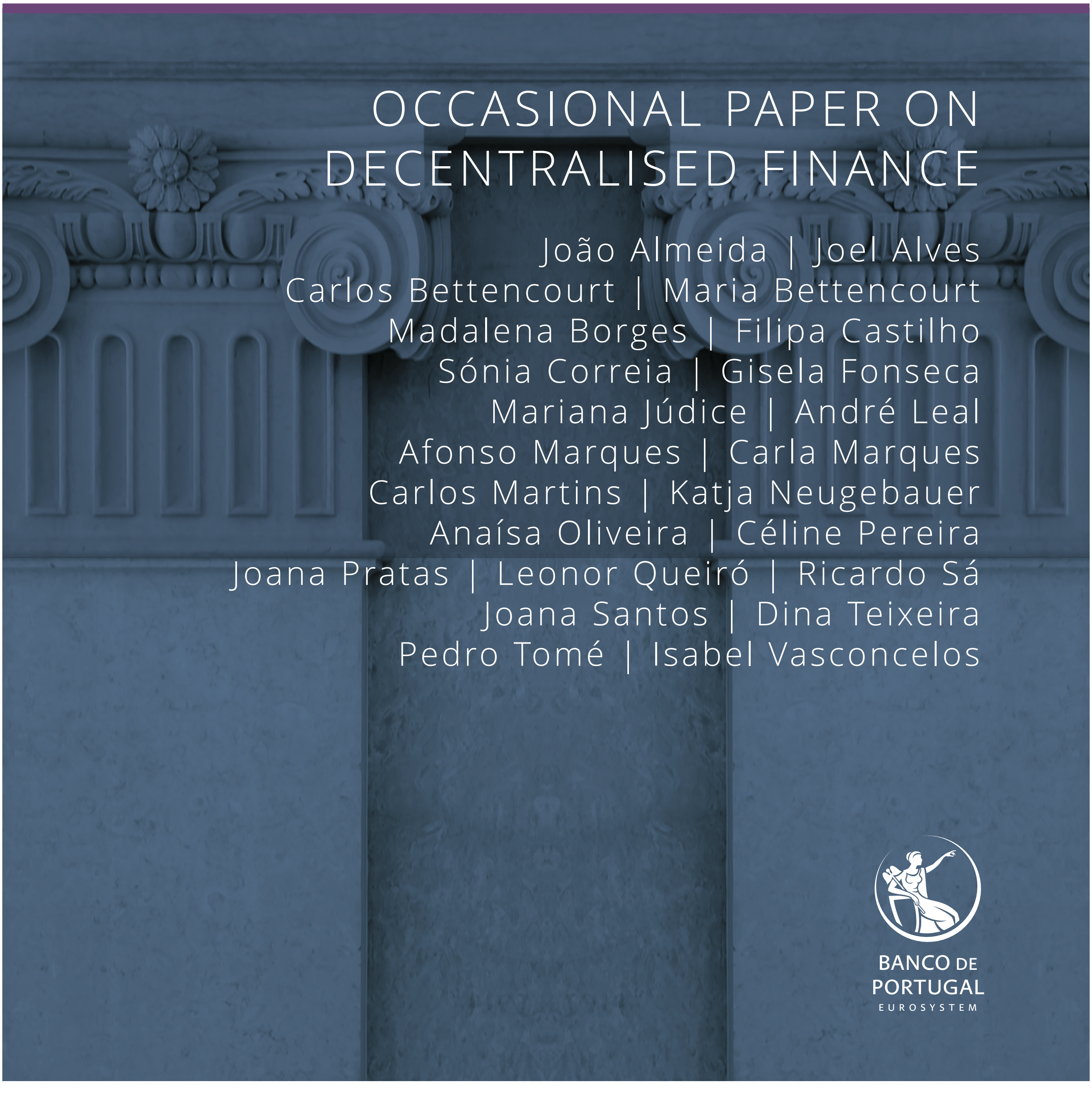
02

OCCASIONAL
PAPERS 2024



OCCASIONAL PAPER ON DECENTRALISED FINANCE

João Almeida | Joel Alves
Carlos Bettencourt | Maria Bettencourt
Madalena Borges | Filipa Castilho
Sónia Correia | Gisela Fonseca
Mariana Júdice | André Leal
Afonso Marques | Carla Marques
Carlos Martins | Katja Neugebauer
Anaísa Oliveira | Céline Pereira
Joana Pratas | Leonor Queiró | Ricardo Sá
Joana Santos | Dina Teixeira
Pedro Tomé | Isabel Vasconcelos

BANCO DE
PORTUGAL
EUROSYSTEM

02
OCCASIONAL
PAPERS 2024

OCCASIONAL PAPER ON DECENTRALISED FINANCE

João Almeida | Joel Alves
Carlos Bettencourt | Maria Bettencourt
Madalena Borges | Filipa Castilho
Sónia Correia | Gisela Fonseca
Mariana Júdice | André Leal
Afonso Marques | Carla Marques
Carlos Martins | Katja Neugebauer
Anaísa Oliveira | Céline Pereira
Joana Pratas | Leonor Queiró Ricardo Sá
Joana Santos | Dina Teixeira
Pedro Tomé | Isabel Vasconcelos

JULY 2024
The analyses, opinions and findings of this paper represent
the views of the authors, and not necessarily those of the
Banco de Portugal or the Eurosystem

Please address correspondence to
Banco de Portugal
Rua do Comércio 148, 1100-150 Lisboa, Portugal
Tel.: +351 213 130 000, email: info@bportugal.pt

BANCO DE PORTUGAL
EUROSYSTEM

Lisboa, 2024 • www.bportugal.pt

Occasional Papers | Lisboa 2024 • **Banco de Portugal** Rua do Comércio, 148 | 1100-150 Lisboa • www.bportugal.pt •
Edition Banco de Portugal • **ISBN (online)** 978-989-678-903-9 • **ISSN (online)** 2182-1798

Occasional paper on Decentralised Finance

João Almeida Joel Alves Carlos Bettencourt
Maria Bettencourt Madalena Borges Filipa Castilho
Sónia Correia Gisela Fonseca Mariana Júdice
André Leal Afonso Marques Carla Marques
Carlos Martins Katja Neugebauer Anaísa Oliveira
Céline Pereira Joana Pratas Leonor Queiró
Ricardo Sá Joana Santos Dina Teixeira
Pedro Tomé Isabel Vasconcelos

July 2024

Abstract
Decentralised Finance (DeFi) has gained significant attention in recent years. It aims to replicate the functions of the traditional financial system in a disintermediated way leveraging on the interplay between blockchain technology, smart contracts and stablecoins. This paper provides an overview of the underlying components of this relatively new ecosystem, as well as its associated risks from the perspective of a financial supervisory authority. While DeFi inherits the risks present in traditional finance, some of these risks could be amplified due to the lack of a clear regulatory framework and the intrinsic features of the DeFi space. Therefore, this paper also takes a closer look at the regulatory challenges involved, including the promise of self-regulation, and explores potential avenues for addressing these challenges without stifling the innovation that DeFi can foster.

JEL: E42, G18, G19, 033

Keywords: decentralised finance, DeFi, blockchain, DLT, stablecoins, crypto-assets, financial stability, DeFi risks.

Acknowledgements: This paper summarises the findings and reflections of a Banco de Portugal expert team. The authors would like to thank the valuable inputs and insights from the heads of Departments, Divisions and Units involved and from the participants at Banco de Portugal meetings in which the conclusions of the paper were presented. The analyses, opinions and findings of this paper represent the views of the authors, which are not necessarily those of Banco de Portugal or the Eurosystem.

1. Introduction

The last years have seen a vast increase in technological innovations in the field of finance. One example is Decentralised Finance (DeFi).

There is no clear-cut definition of DeFi. According to the Financial Stability Board (FSB 2023), DeFi is "an umbrella term commonly used to describe a variety of services in crypto-asset markets that aim to replicate some functions of the traditional financial system (TradFi) while seemingly disintermediating their provision and decentralising their governance". This apparent similarity with TradFi, together with the potential for fast growth and spill-over effects, make DeFi a relevant field for financial authorities to understand and monitor.

The first DeFi-code based protocols (also called smart contracts, detailed in section 2) were officially launched in 2017, but it was not before 2020 that DeFi really gained traction. This happened after the outbreak of the Covid-19 pandemic. During this time, crypto prices ballooned, driven by a search for yield and excess liquidity. These developments were further driven by the phenomenon known as "Fear of Missing Out" (FOMO).

DeFi aims to revolutionise the traditional provision of financial services and products through the utilisation of blockchain technology and smart contracts. DeFi waives the need for centralised intermediaries, operating through automated protocols for trading, lending and investing on blockchains. The DeFi ecosystem revolves around some key elements, including stablecoins, which facilitate fund transfers into and out of the crypto ecosystem as well as trading within the system.

While DeFi is largely separate from the traditional financial system at present, connections could increase in the future, raising the potential for externalities. One plausible scenario is that DeFi continues to grow and becomes more interconnected with the real economy and the broader financial system. As DeFi expands and takes up more space in the financial system, regulators are discussing about how to regulate it and safeguard traditional financial markets from potential negative spillover effects.

DeFi inherits and may amplify the vulnerabilities of the traditional financial system, including operational fragilities, liquidity and maturity mismatches, leverage and interconnectedness. The turmoil in crypto-asset markets and in DeFi in 2022 exposed a number of these vulnerabilities.

There are also concerns regarding the risk of money laundering in DeFi, as the lack of centralised control and the pseudonymous nature of transactions might facilitate illicit activities. Regulators are starting to look at the sector with some exchanges under investigation or banned in certain jurisdictions.

In response to these risks, regulatory bodies are actively exploring ways to address the challenges posed by DeFi, while fostering innovation and growth in the sector. The European Union (EU) has been at the forefront of regulatory developments. One example is the Markets in Crypto-Assets Regulation (MiCAR), which establishes a comprehensive framework for regulating crypto-assets, to ensure investor protection and financial stability. DeFi services, however, when provided in a fully decentralised manner, are not covered by MiCAR.

As DeFi continues to evolve rapidly and potentially becomes more interconnected with the traditional financial system, it will be crucial for regulators to monitor and understand it in order to strike a balance between fostering innovation and ensuring financial stability and integrity. As the sector matures, it will be imperative for regulators, industry participants and policymakers to collaborate effectively to mitigate risks and ensure compliance with regulatory standards.

This paper takes a closer look at DeFi from several perspectives and is structured as follows. Section 2 lays out the basic concepts of DeFi. Section 3 takes a deep dive into DeFi products and services. Section 4 takes a closer look at the current state of regulation and its possible application to DeFi. Section 5 is the backbone of this report and looks at the different risks and vulnerabilities associated with DeFi, both at the national and the European level, especially considering Banco de Portugal's responsibility for ensuring financial stability. Section 6 gives an outlook on what DeFi regulation might look like in the future and assesses the need for international collaboration. Section 7 concludes.

2. Basic concepts of DeFi

The interplay between blockchains, smart contracts and crypto-assets, including stablecoins, constitutes the core infrastructure of DeFi (Box 1). Blockchains aim to provide transparency and decentralised transaction recording, while smart contracts' purpose is to enable automation and eliminate the need for intermediaries. This re-quires the establishment of a dedicated crypto monetary system, ensuring the existence of a decentralized financial infrastructure.

Without aiming to be exhaustive, and in a non-technical way, this section introduces the core concepts that play a crucial role within the DeFi ecosystem.

2.1. DLT - Blockchains

At the core of DeFi lies the **blockchain technology**, a specific type of Distributed Ledger Technology (DLT). A blockchain records transactions in a chain of blocks, each containing a list of transactions validated cryptographically in a secure, transparent, and immutable manner across multiple nodes (computers), ensuring the information's integrity.

This technology aims to support financial systems within DeFi, independent from a central authority, by enabling real-time transaction recording and verification, which eliminates the need for reconciliation or reliance on a centralised third party. This technology also significantly reduces settlement times, enhancing efficiency in financial transactions, and promotes transparency by ensuring that the transaction history and account balances within the DeFi ecosystem can be verified by anyone.

Although blockchain may be used as a universal and generic concept, the way it is implemented on real world solutions affects its inherent characteristics as it is shaped by deliberate human design and implementation. It is crucial to emphasize that while decentralised blockchains serve as the backbone of DeFi, there are instances where a blockchain may exhibit centralised elements or features. In addition, the degree of decentralisation of a Defi protocol depends on more than just the inherent blockchain. It is also influenced by other factors such as governance structures, decision-making processes and interoperability (Wilkins 2022).

2.2. Smart contracts in DeFI

Smart Contracts serve as self-executing agreements, where contractual terms are encoded directly into the blockchain. This intrinsic component of blockchain technology facilitates automation and decentralization in contractual agreements. Upon meeting predefined conditions, smart contracts autonomously execute specified actions, eliminating the necessity for intermediaries.

Immutability and automation are the key features of smart contracts. Once deployed on a blockchain, they become immutable, making it impossible to alter the code or agreement. Automation ensures precise execution of contractual terms, while transparency is achieved through the public nature of the blockchain, allowing open auditing of code and transaction history.

Smart contracts have found significant applicability in the field of DeFi, empowering various financial services such as lending, borrowing and exchanges. DeFi platforms leverage smart contracts to operate transparently and automatically, removing reliance on traditional intermediaries. This programmability enables the creation of innovative financial applications accessible to anyone with an internet connection.

2.3. Stablecoins and other crypto-assets

Crypto-assets are "a digital representation of a value or of a right that is able to be transferred and stored electronically using distributed ledger technology or similar technology" (MiCAR[1]). It can be used for peer-to-peer transactions on decentralized networks, thus removing the need for intermediaries like banks or governments. Within the broader spectrum of crypto-assets, a particular category of asset-referenced token known as 'stablecoins' has gained prominence due to its aim of reducing price volatility.[2]

[1] Article 3 of MiCAR.

[2] Please also refer to the occasional papers on Crypto-assets and on Stablecoins elaborated by Banco de Portugal, where those concepts, features and risks are thoroughly detailed.

Stablecoins, designed to maintain a stable value often pegged to a fiat currency or an underlying asset, mitigate the volatility of crypto-assets and offer potential benefits for DeFi applications. Stablecoins serve as a bridge between the traditional financial world and the decentralised space, allowing users to easily move value between these segments. Users can deposit fiat currency into a custodian and receive an equivalent amount of stablecoins on a blockchain. Nonetheless, the lack of central control and potential risks of insufficient reserves backing stablecoins raise doubts about their stability and ability to withstand market stress.

Crypto-assets are expressions of the concept of **tokenization** – conversion of real-world assets or digital representations of value into tokens. All these digital assets can be traded, transferred, and used as collateral within the DeFi ecosystem.

2.4. Other key concepts

Notwithstanding the abovementioned core aspects shaping the DeFI ecosystem, there are other relevant concepts playing a crucial role within the ecosystem.

Oracles are mechanisms that provide external data to smart contracts. They act as bridges between the blockchain and real-world data sources, enabling smart contracts to interact with real-time information such as market prices or weather conditions which allows the creation of more sophisticated financial instruments within the DeFi ecosystem.

DeFi platforms often operate through **Decentralised Applications (dApps)**, which are software applications built on top of blockchains that are capable of interacting with smart contracts. These dApps provide various financial services, such as lending, borrowing, decentralised exchanges, and asset management, directly to users without intermediaries. Many of DeFi dApps interoperate and integrate with each other, creating a more interconnected and robust ecosystem.

Decentralised Autonomous Organizations (DAOs) are organizations that operate based on predefined rules and smart contracts, allowing participants to have a say in decision-making processes through voting mechanisms. DAOs enable decentralised governance and community-driven management of protocols and platforms. DAOs are used for various financial applications, including fund management, protocol upgrades, and governance of decentralised exchanges.

Box 1 DeFi architecture

The DeFi ecosystem is a multi-layered architecture. In early research, Schär (2021) introduced it as a DeFi Stack Model, structuring it into five distinct layers, each one with a distinct purpose (Figure 1). These layers are hierarchical, in the sense that each layer is as secure as the layers below.

The first layer is the settlement layer. This is the foundational layer and consists of the blockchain with its native protocol assets.

The second layer, the asset layer (which sits on top of the settlement layer), consists of the different types of tokens like stablecoins and other crypto-assets.

The third layer, the protocol layer, defines the different standards for applications running on the blockchain that usually take the form of smart contracts. These protocols are highly interoperable. Indeed, the DeFi community speaks of so-called DeFi legos, as different applications can be combined to create new ones (Aramonte *et al.* 2021).

The fourth layer, the application layer, is where the dApps are created. The fifth and final layer is the aggregation layer. It is similar to the application layer but more en-compassing. In essence, it creates platforms that are user-friendly and that can be used to compare the different services, access different protocols, etc.

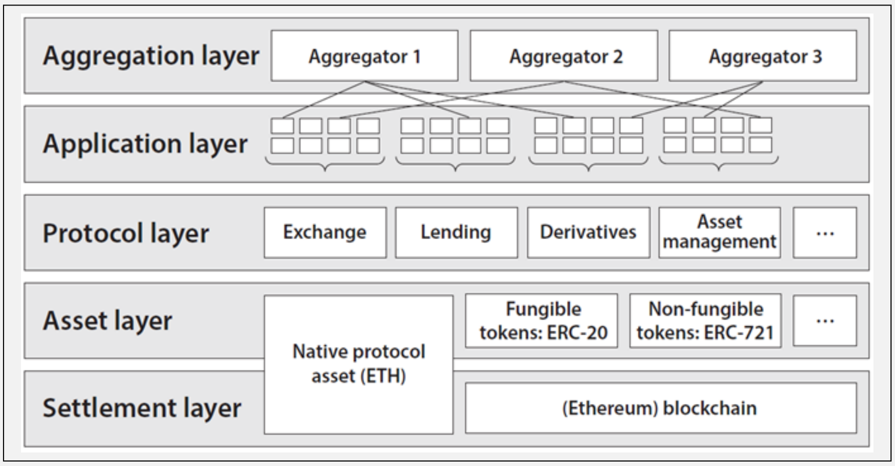


Figure 1: DeFi stack
Source: Auer *et al.* (2023).

Auer *et al.* (2023) builds on Schär's Defi Stack and other related DeFi stack approaches and introduces the DeFi Stack References (DSR) Model, a conceptual reference for DeFi services and products. This model is also structured into five distinct layers (Figure 2) where each layer is a specific block in which different functionalities of DeFi services are performed, and each layer is associated with real-world entities in a broader ecosystem.

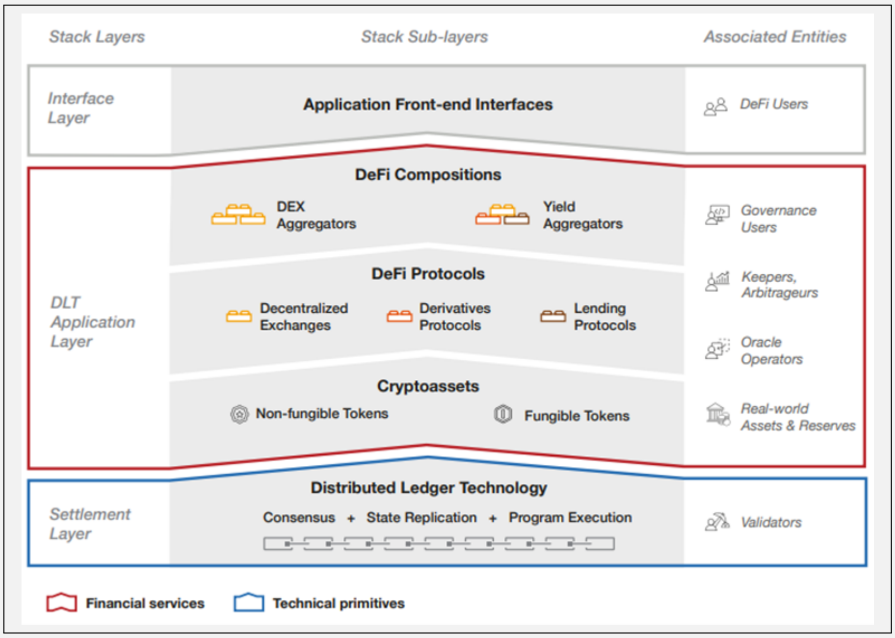


Figure 2: DeFi stack Reference (DSR) Model
Source: Auer *et al.* (2023).

3. DeFi products and services

Different types of DeFi protocols enable different financial services, depending on the financial functions written in the smart contracts. This section takes a closer look at the currently most prominent DeFi products and services.

3.1. Payments

All payment transactions associated to a certain DeFi service (e.g., the payment of a fee, or a yield from an investment, or even the payment executed in exchange for a specific product or service) are validated and performed in a decentralised way, and registered and stored in the blockchain, the first layer of the DeFi stack (the settlement layer). It is on top of this layer that all Defi services are built. Miners and validators compete in the DeFi space to settle and register transactions in the settlement layer, allowing payments to be executed and confirmed on the network through a consensus mechanism without the involvement of centralised intermediaries.

The traditional concept of “payment” includes the transfer of cash or other acceptable monetary claim (e.g. scriptural money or electronic money).[3] Similarly, payment transactions in DeFi are a transfer of value between two parties interacting in the DeFi space (the “payer” and the “payee”), whereby the value transferred is represented by crypto-assets acting as the accepted monetary claim or the mean of exchange.

For instance, in the Ethereum blockchain there is a native token - Ether (ETH) - that is transferred between parties, representing a mean of exchange, when smart contracts are executed. Both Ethereum blockchain and its native token ‘Ether’ represent the settlement layer of the Ethereum DeFi ecosystem. Besides native tokens and other fungible and non-fungible tokens, also stablecoins can be used as means of exchange in the DeFi space. Due to its objective to maintain a stable value, several types of stablecoins can be used as a replacement for fiat currency in the DeFi ecosystem.

In addition to traditional payment scenarios like fees, investment yields and peer to peer transactions, DeFi enables a wide range of unique payment use cases. For instance, decentralised lending platforms allow users to receive loan payments or make loan repayments without involving traditional banking intermediaries. Investment yields, staking (e.g., deposit like) rewards and automated yield farming[4] strategies can generate passive income for users, and the earned yields are automatically distributed as payments through smart contracts. Moreover, DeFi protocols offer decentralised insurance services (Cover protocol) where policy holders receive payments automatically when a claim is verified. These innovative payment scenarios demonstrate the versatility of DeFi. However, it should not be taken for granted that this whole set of payment services is effective in providing a decentralised and inclusive financial ecosystem.

The execution of payments in a decentralised way is attracting the attention of the financial industry and its players, which are curious to explore if DLT can allow for cheaper and more efficient payments in traditional finance. In fact, there are already some DLT projects being developed by traditional financial service providers.

One of the advantages of payments performed in DeFi is the possibility to perform automatic settlement, also referred to as “atomic settlement”, whereby a bundle of transactions can only be settled and executed, automatically and simultaneously, in case certain predefined conditions are verified. Otherwise, the transactions are reverted and the ‘value’ transferred back to the original user. This is possible due to the way smart contracts in DeFi can be constructed and programmed.

[3] Cf. Directive (EU) 2015/2366 (PSD2), or BIS’s Committee on Payments and Market Infrastructures Glossary.

[4] Yield farming in DeFi involves leveraging crytpo-assets holdings to earn returns through activities like providing liquidity or staking assets in decentralised finance protocols.

However, several challenges remain to be solved, such as overcoming scalability issues and the level of fees implied. In this respect, it is important to mention that the cost and efficiency of DeFi payments are extremely dependent on the technical capacity of the blockchain in which they are cleared and settled (for instance, the speed and cost of transactions in the Ethereum blockchain is becoming less attractive due to the high and increasing volume of transactions it processes).

3.2. Lending and Borrowing

Lending and borrowing of crypto-assets in DeFi is operated through **Protocols for Loanable Funds (PLFs)**. These protocols rely on smart contracts running on blockchains with which users interact directly, thus allowing for a decentralized intermediation of funds. Some protocols also have off-chain complementary platforms, but all transactions are conducted on-chain.

PLFs allow for collateralized and uncollateralized lending. In the former, users borrow crypto-assets by locking in the smart contract crypto-assets that serve as collateral. The existence of collateral allows smart contracts to enforce repayment, as they enable the liquidation of collateral in case the borrower fails to meet the conditions of the loan. If a loan is uncollateralized, the smart contract cannot enforce repayment.

PLFs also differ in the amount of information users have about each other. In **Peer-to-Pool PLFs**, lenders supply funds to lending pools and borrowers borrow funds from those pools without information about each other. In this case, terms and conditions are defined by the protocol and are embedded in the smart contracts. In **Peer-to-Peer (P2P)** PLFs, lenders supply funds to specific borrowers or borrowers borrow from specific lenders. Here, the loans' terms and conditions are firstly agreed off-chain and transactions on-chain start afterwards.

Another dimension in which PLFs differ is the type of asset being borrowed. In **Lending Protocols (also called Debt Markets)**, users borrow an already existing crypto-asset, while in **Collateralized Debt Positions (CDPs)**, users borrow a crypto-asset newly minted by a protocol, which is usually a stablecoin.

Although transactions in PLFs occur in a decentralized manner, smart contracts may be connected to centralized systems living outside of the blockchain. One example of how this is achieved is through Oracles, leading to more functionalities of the smart contracts.

Being unregulated and unguaranteed, lending protocols bear risks, the main ones being smart contract risk (technical security of the code), token risk (the price risk of crypto-assets) and debtor repayment risk. Protocols have mechanisms to mitigate these risks, such as audits to the smart contracts' code, emergency oracles and collateralization.

Decisions regarding smart contract design or protocol management are taken by the protocol's governance, which is operated through governance tokens that run in the blockchain. Any user can buy governance tokens.

In what follows, the main types of lending and borrowing in DeFi are described in further detail, according to the dimensions referred above. Appendix A contains a table with the features of specific PLFs.

- **Peer-to-Pool Lending (also called Pooled Collateralized Debt Markets)**

This is a type of collateralized lending and borrowing in DeFi, in which users lend and borrow existing crypto-assets through lending pools.

Users depositing funds in the pool receive pool tokens, which represent the supplied funds and the interest accrued on the funds. Users who want to borrow from the pool must lock some asset as collateral in the pool and are bound to pay interest on the borrowed funds.

The assets accepted as collateral can be fungible tokens, non-fungible tokens (NFTs) or real-world assets (RWAs), that is, tokens representing a real-world asset. When the collateral type is NFT or RWAs, the protocols are called NFT Lending or RWA Lending, respectively, but the most popular collateral type is fungible tokens and, in this case, protocols are just called Lending protocols.

The loan conditions and specificities are supported by parameters that are embedded in the smart contract.

The collateralization parameters are a Loan-to-value ratio (LTV) and a Liquidation Ratio. The LTV is computed as the ratio of outstanding debt (including accrued interest) to the value of the collateral and must be met at loan origination. The Liquidation Ratio is the value of the LTV ratio beyond which the loan can be liquidated. It can be attained after a loan starts due to variations in the market price of the collateral.

A loan's maturity can last for as long as the Liquidation Ratio is not met. However, lenders can withdraw the funds they deposit in a pool at any time as long as the pool's utilization rate is not too high. This is done by redeeming their lending tokens. These tokens can usually also be traded or transferred in the blockchain.

The interest rate on loans is usually determined by a formula depending on a pool's utilization rate, therefore reflecting supply and demand of the funds.

If the loan's Liquidation Ratio is achieved, it can be liquidated, which is done by activating a function in the smart contract. This can be done by anyone. In a liquidation, the collateral becomes the possession of the liquidator, who must repay the outstanding debt to the lender, keeping any value remaining from the sale of the collateral.

The Governance of the protocol is usually conducted on-chain by the holders of Governance tokens, who have proposal and voting powers regarding smart-contracts' parameters, such as the interest rate parameters and the LTV or the Liquidation Ratio.

Peer-to-Pool protocols are usually permissionless, which means that users do not need to be approved by the protocol to engage with it.

Examples of Peer-to-Pool protocols are Aave, in which the collateral asset is a fungible token, BendDAO and Drops, in which collateral is an NFT and Maple Finance, Fortunafi and Goldfinch Finance, where collateral is a RWA.

- **Peer-to-Peer Lending (or P2P)**

In P2P protocols users lend and borrow existing crypto-assets directly to each other. Usually, they agree on loans' terms and conditions off-chain before starting transactions on-chain. This can be done directly between the borrowers and the lenders or through protocol managers who act as middlemen.

When lenders and borrowers interact off-chain directly, this interaction usually consists of take-it-or-leave-it offers which are posted by the users (lenders or borrowers) in off-chain repositories and then picked by other users. Upon agreement, funds are transferred directly between the borrower and the lender. The lender may still be able to recover the loan on demand through the launch of an auction to find a new lender to the loan. Default may be triggered because an auction is launched by an existing lender and does not find a new lender willing to take the loan at any interest rate.

When there is a protocol manager, there is a risk-assessment procedure of the borrowers, followed by a negotiation of the loan terms between the borrower and the manager after which the manager launches a pool where interested lenders can deposit funds for that borrower. The borrower's risk profile is made public to potential lenders. There may be permissioned pools, i.e., private pools, where lenders are subject to AML tests or other approval mechanisms before starting transactions. After-wards, lenders deposit funds in exchange for pool tokens which can be transferred to other lenders who have also been approved by the protocol. Loans can be open- or fixed-term and can be collateralized or uncollateralized. Default may be declared either because the manager calls an open-term loan and the borrower does not pay or because the term of a fixed-term loan is attained without repayment. In case of de-fault, the pool loses the amount of outstanding debt and the manager assumes the first losses on the pool up to a threshold amount. If the loan is collateralized, the col-lateral is liquidated, and the value of its sale is added to the pool.

Governance is conducted by the protocol's native token holders. Examples of proto-cols that offer P2P lending and borrowing are Maple Finance and Lenfi (AADA), when the collateral asset is a fungible token, and NFTfi, Arcade and Blur (Blend), when it is an NFT.

- **Collateralized Debt Positions (CDP)**

This is a type of collateralized lending and borrowing in DeFi, in which users borrow a stablecoin minted by a protocol against collateral owned by the borrower.

A CDP is a smart contract that users can open. In order to borrow, users transfer col-lateral to the CDP and can borrow the stablecoin minted by the protocol. When bor-rowers get the stablecoin, a debt is created and their collateral is locked until debt repayment. There is a stability fee that accrues, which is an annual percentage computed on the outstanding debt. In order to unlock the collateral, the debt and the stability fee must be repaid. CDPs are non-custodial, which means that users interact directly with the CDP.

Similar to Peer-to-Pool Lending, if the Liquidation Threshold is reached, an auction is triggered to sell the collateral. If the auctioned collateral net of debt and a penalty fee is positive, it is given back to the CDP. In some protocols, if the value of the collateral is insufficient to repay the outstanding debt, the latter becomes protocol debt, which can be covered by the protocol's reserves or through the sale of the protocol's native token, which dilutes existing token holders.

There are mechanisms to maintain the peg of the stablecoin, which work by influencing the demand and supply of the stablecoin.

Protocol governance is operated through the protocol's native token, whose holders usually have proposal/polling and voting rights.

- **Uncollateralized lending**

This is a type of lending and borrowing in DeFi, in which users lend and borrow existing crypto-assets without the need to provide collateral.

There are protocols in which borrowers are risk-assessed and receive a risk score. Borrowers are then portrayed in a pool list, together with the respective risk score, and can be chosen by any user who decides to become a lender. In uncollateralized lending protocols, borrowers are usually institutions. Lending is permissionless.

The borrowable assets are just stablecoins. Borrowers can borrow up to a threshold on a pool's utilization rate. Beyond such a threshold, default is triggered by the protocol after a period of time.

Lenders receive Liquidity Provider tokens in exchange for the deposited funds which can be redeemed until the pool reaches a certain utilization rate.

Interest rates are determined by oracles and depend on the supply and demand for the liquidity of each pool (therefore on the utilization ratio of the pool).

In case of default, an auction is started for the tokens of the defaulting pool. To participate in this auction, users have to be approved by the protocol. To accommodate default, there is also pool-specific insurance. The winning bid of the auction can be accepted or rejected. In case of acceptance, the winner is entitled to the borrower debt, gets the rights to legally pursue the defaulting borrower and lenders receive the bid amount. Otherwise, lenders maintain the right to legally pursue the defaulting borrower and receive insurance from the pool's insurance account.

- **Flash Loans**

This is a form of uncollateralized borrowing in DeFi, in which users borrow existing crypto-assets without the need to provide collateral and in which the loan and the repayment happen within one unique transaction.

In a flash loan, if the repayment is not made, the whole transaction is reverted, which means that defaulting on a flash loan is not possible. Since the borrowing is condition-al on the repayment, these loans do not require collateral.

One use of this type of loan is to take advantage of arbitrage opportunities, for example during loan liquidation processes. Another use is within NFT lending, where a borrower buys an NFT from a market place, partly with a down payment and partly with funds borrowed in a Flash Loan. Simultaneously, the borrower uses the NFT as collateral in a protocol pool to obtain loans, which are used to repay the Flash Loan. This way, a borrower can make an NFT collateralized loan without entirely paying for the NFT in the first place.

- **Buy Now Pay Later (BNPL)**

This is a form of uncollateralized borrowing in DeFi, in which users buy assets with a downpayment and a series of future installments, without the need to provide collateral.

One use of this type of loan is to buy NFTs. In BNPL operations, the borrower receives crypto-assets from the platform's pool to buy the NFT and has an installment plan, which includes interest. If the NFT appreciates before the end of the installment payment horizon, the borrower can repay early and sell the NFT.

- **Comparison of lending and borrowing in TradFi and DeFi**

TradFi and DeFi operate in different technological infrastructures, which has implications across all products and services in terms of concentration of responsibilities, perceived transparency and immutability (ability to erase past transactions). Specifically for lending and borrowing services, there are implications across additional dimensions:

  - **Accessibility**. On the one hand TradFi can be perceived as more accessible to users than DeFi, given that the lack of a human intermediary in DeFi requires users to be able to manage the smart contract language and technology. On the other hand, TradFi needs credit operations to be approved by financial intermediaries (banks or Fintechs), which may result in the exclusion of some users from the credit market due to poor risk assessment or lack of information. In the DeFi world, and specifically in collateralised lending protocols, lending and borrowing can be permissionless, which means that users are able to borrow available funds in the market as long as they lock in tokens accepted as collateral by the protocol.
  - **Risks**. In terms of operational risk, DeFi may avoid the single point of failure risk presented by TradFi, but it is subject to smart contract risk, which is the risk of attacks to the smart contract code. Protocols usually have mechanisms to mitigate this risk. As for the market risk of collateral, crypto-assets are historically more volatile than fiat currency or physical assets, which are used in TradFi. Finally, regarding credit risk, collateralized lending in DeFi relies solely on collateral as a credit risk mitigator and lacks the monitoring pursued by financial intermediaries that mitigates default risk. Although DeFi collateralized lending protocols have mechanisms to prevent loans from being undercollateralized, the value of collateral is subject to

market conditions. There are protocols in DeFi, such as P2P protocols, in which the protocol provides diligence on the borrower and in which loans are subject to legal recourse, but the recovery efforts conducted in TradFi appear to be more unequivocal than in DeFi.

- **Pricing**. Pooled protocols in DeFi determine interest rates mainly based only on demand and supply of funds (although some protocols also take into account other market conditions). In TradFi, interest rates reflect not only supply and demand conditions but also the borrower's credit risk, creating a risk-return trade-off. Some P2P DeFi protocols, though, allow for interest rates to be customized to the borrower's risk since the borrower is known.
- **Governance**. DeFi protocols are maintained and developed through an on-chain mechanism which relies on tokenization. Holders of protocols' native token make decisions about the parameters of the smart contracts and can also call a freeze of the protocol. This compares with decision powers conveyed to TradFi financial institutions' shareholders or managers. The system in DeFi is effective in ensuring that there are no deviations from approved decisions, while the system in TradFi is more flexible, which might prove relevant in face of rapidly changing market conditions.
- **Stability**. Bank deposits can be partially covered by Deposit Insurance schemes. Such a protection scheme is absent for DeFi's deposited funds. This can convey a higher level of stability of loanable funds in TradFi than in DeFi.

3.3. Trading

The DeFi ecosystem comprises Decentralised Exchange (DEX) platforms, such as Uniswap, SushiSwap, and PancakeSwap. These platforms are built on top of blockchain technology and operate without intermediaries, enabling users to trade directly with each other using smart contracts.

Trading possibilities comprise a wide range of instruments with different underlying assets (such as crypto-assets or digital assets, among others) traded on DEX platforms instead of the "traditional" centralized exchange platforms.

DEX platforms mostly use Automated Market Makers (AMMs), which are algorithms that enable peer-to-peer trading by utilizing liquidity pools instead of order books. Hence, users can become liquidity providers by adding funds to these pools and earning trading fees in return. In addition, DeFi trading is typically permissionless, which means, for instance, that users can participate without requiring approval or enforcing anti-money laundering and counter terrorism financing (AML/CTF) rules, such as Know Your Customer (KYC) procedures.

DEX platforms can support the following possibilities:

- **Decentralized Exchanges**. A decentralized exchange is a type of crypto-asset exchange that enables users to execute trades directly with one another through peer-to-peer transactions. It is supported by a DEX platform, which is the broader ecosystem or infrastructure.

- **Decentralized Margin Trading**. DeFi platforms also offer decentralized margin trading, which allows users to trade leveraged, hence borrowing assets from liquidity pools and use them as collateral for leveraged trading positions, without the need for a centralized exchange or intermediary. Some DeFi protocols combine margin trading with yield farming, enabling users to borrow assets, use them for leveraged trading, and simultaneously participate in liquidity providing pools to earn additional rewards.
- **Flash Loans**. Flash loans, as stated on section 3.2, are uncollateralized loans that allow users to borrow funds for a single transaction within a single block. Flash loans enable arbitrage opportunities and potentially complex trading strategies that require significant liquidity positions for shorter periods.

There are various DeFi trading strategies, including the following: i) market making, which involves providing liquidity to a DeFi platform by depositing assets into a liquidity pool and in return earn fees based on the trading volume of the platform; ii) arbitrage operations, by taking advantage of price discrepancies between different DeFi platforms or between a DEX and a centralized exchange platform; iii) swapping, through exchanging one crypto-asset for another (typically) instantly, with fees generally lower than those from centralized exchanges; iv) margin trading, which involves borrowing assets (from a liquidity pool or from other traders) to increase trading capital, hence leveraging their positions to increase their potential profits; and v) yield farming, by depositing assets into a liquidity pool to earn several types of rewards which can be yields in the form of interest, governance tokens, or other incentives.

3.4. Derivatives and synthetics

DeFi has allowed new ways of trading financial instruments and products and, among the most popular and innovative ones, are derivatives and synthetics - financial instruments that allow users to gain exposure to various assets and price movements without owning the underlying assets.

- **DeFi derivatives**

DeFi derivatives are financial contracts that derive their value from an underlying asset, such as crypto-assets, traditional assets, or even other tokens.

The most common types of DeFi derivatives include futures contracts, options contracts, and perpetual swaps. They share some similarities with traditional derivatives, and the main differences rely on the following aspects:

- **Decentralization**: DeFi derivatives operate on decentralized platforms built on blockchain technology without the involvement of any intermediaries;
- **Ownership and Custody**: DeFi derivatives are tokenized on the blockchain, and users have full ownership of their digital assets. Traders interact with smart contracts directly from their crypto wallets, which means they retain custody of their assets throughout the trading process;

  - **Access and Inclusion**: DeFi derivatives are typically permissionless and accessible to everyone and users don't need to comply with various AML/CTF rules, such as KYC requirements, to access this market;
  - **Transparency**: it operates in public blockchains, which means all transactions and smart contract interactions are transparent and verifiable by the chain. This level of transparency ensures that users can audit the smart contracts and verify the platform's integrity;
  - **Programmable Smart Contracts**: DeFi derivatives use programmable smart contracts to execute trades and manage positions automatically;
  - **Interoperability and Composability**: DeFi protocols are designed to be interoperable, which means that they can interact with each other seamlessly. This composability allows users to combine different DeFi services and create trading and investment strategies across multiple platforms.

- **DeFi Synthetics**

DeFi Synthetic are tokenized assets created on top of blockchain technology, that mimic the value and price movements of real-world assets. These can include commodities, stocks, fiat currencies, and other crypto-assets. Synthetics are usually over-collateralised with other crypto-assets as collateral to maintain their peg to the underlying asset.

  - **Synthetic Assets**: For example, a synthetic USD (sUSD) would be designed to track the value of the US dollar. sUSD holders can gain exposure to the USD's price movements without holding the currency in a traditional bank account;
  - **Synthetic Indices**: Some DeFi protocols offer synthetic indices, which are baskets of assets designed to track the performance of a specific sector or market. Examples include decentralized stock indices that represent the overall performance of stocks listed on traditional stock exchanges.

Some DeFi derivatives and synthetics are traded over-the-counter (OTC), which means that they are traded directly between two parties without going through an exchange. However, OTC trading is less common in the DeFi space compared to the traditional finance.

4. DeFi regulation

4.1. Current state of regulation

In this section we present an overview of the current state of regulatory developments regarding DeFi with a focus on Europe. Appendix B provides additional insight on Europe and other selected jurisdictions.

Given the disruptive nature of DeFi and its potential impact on the traditional financial ecosystem, over the past few years, regulation of DeFi has been a matter of concern for several recognised institutional bodies, both European and International, who have published reports and studies on the matter addressing DeFi risks to financial stability, identified related vulnerabilities, and explored potential opportunities brought by DeFi.

However, the regulatory approach concerning DeFi is still undergoing a significant development, with a primary emphasis on establishing a more defined structure for crypto-assets and addressing concerns regarding AML/CTF.

There is a consensus that the decentralized nature of DeFi poses a challenge to the traditional regulatory framework, in particular given the absence of centralized decision-making entities (e.g. financial intermediaries) upon which regulators could enforce their rules (FSB (2019), OECD (2022) and European Commission, Roukny (2022)). In response:

- The FSB (2019) argues that "A more decentralised financial system may reinforce the importance of an activity-based approach to regulation, particularly where it delivers financial services that are difficult to link to specific entities and/or jurisdictions". It also identified three potential implications of DeFi for public policy, since its underlying technology could: (i) be used to avoid regulation or engage in misconduct; (ii) raise issues around enforcement; and (iii) increase jurisdictional uncertainty.
- The OECD (2022) notes that DeFi activities can be "(. . .) broken down into its components and, in concept, existing financial regulation and policies can be applied for the same activity/risks, irrespective of the technological means through which they are provided, given the technology-neutral approach adopted by regulators in most jurisdictions with active markets for compliant tokenised assets".
- The European Commission study (Roukny 2022) considers that regulating DeFi activities from a pre-identified set of legal entities is possible.
- A report from BIS (Makarov and Schoar 2022) argues that a potential area of intervention is at the level of developers and validators that control the network protocol. If this level of regulatory compliance is addressed, other regulatory provisions could be built on top of it to address other issues that lack a regulatory framework.

In this respect, the IMF (2022) - echoed by the OECD (2022), BIS (Makarov and Schoar 2022), and IOSCO (2022) – stated that: *"[a]s financial services move from regulated banks to less regulated — or even unregulated — entities and platforms, as in the case of DeFi, so do the associated risks. This poses challenges for financial authorities in the form of regulatory arbitrage, interconnectedness, and contagion that require supervisory and regulatory action, including better consumer and investor protection"*.

Recently, the FSB published another report where it noted that some vulnerabilities of DeFi infrastructures are amplified by its non-compliance with existing regulatory requirements and the lack of applicable regulatory framework (FSB 2023). The FSB also pointed out that the cross-border nature of DeFi platforms and their governance models may obscure the task to identify the applicable jurisdiction, since they make it difficult to identify the relevant legal entity subject to rights/obligations, and also the relevant competent authority (whether we are talking about supervision, resolution or even consumer protection rules).

Currently, at European level, there is not yet a regulatory framework specifically applicable to DeFi services, although, as part of the Digital Finance Package, the regulations on crypto-assets (MiCAR)[5] and digital operational resilience (DORA)[6] and the pilot regime on distributed ledger technology (DLT) infrastructures[7] are already in force. In any case, MiCAR does not apply to DeFi services when these are provided in a fully decentralised manner without any intermediary.[8] Additionally, in the absence of specific regulation on this matter, general laws will apply, for instance civil law or banking law.

In the same vein, the use of DeFi, when completely decentralised, is not currently covered by the national anti-money laundering and counter terrorism financing legal and regulatory framework. The present national AML/CTF regulatory response – as determined by international standards and European Union law – presupposes and focuses on activities that are undertaken by an intermediary, i.e., the virtual assets service provider ("VASP")[9] (detailed discussion in Appendix C).

Box 2 AML Package

On 20 July 2021, the European Commission presented a package of legislative proposals to strengthen the EU's AML/CFT rules, widely known as the "AML Package".[a]

[a] All legal acts and further information are available for consultation at AML/CFT legislative package (europa.eu).

[5] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets ("MiCAR").

[6] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector ("DORA Regulation").

[7] Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology.

[8] See also FSA (2024), where, in addition to clarifying MiCAR's scope, the Danish Financial Su-pervisory Authority proposes some principles for the evaluation of decentralization.

[9] Arguably, from an AML/CTF perspective, this reality makes the regulated virtual asset ecosystem, populated by VASPs, mutually exclusive from what the purest form of DeFi wishes to achieve, which is true decentralization.

It consists of four legislative proposals, through which the European Commission intends to: (i) establish a single set of EU rules on AML/CFT (the "EU Single Rulebook"), (ii) introduce an AML/CFT supervision authority at EU level, (iii) establish a support and cooperation mechanism for the Financial Intelligence Units of the Member States and (iv) strengthen the international dimension of the EU AML/CFT framework.

One of the proposed acts, as part of the EU Single Rulebook, is a new Regulation containing directly applicable rules for preventing AML/CFT (the "AMLR").

During the negotiations, the European Parliament position on the AMLR proposal put forward the inclusion of Decentralised Autonomous Organisations ("DAO") and other "DeFi arrangements" to comply with EU AML/CFT rules "to the extent they perform or provide, for or on behalf of another person, crypto-asset services which are controlled directly or indirectly, including through smart contracts, or voting protocols, by identifiable natural and legal persons".

The European Parliament considered that, in the aforementioned cases, "DAO or DeFi arrangements should be considered to be crypto-asset service providers falling within the scope of [MiCAR] and this Regulation, regardless of the commercial label or their self-identification as DAO or DeFi". This proposal was, however, not incorporated in the final version of the AMLR, and DeFi is not specifically targeted by the AML Package. The AML Package was adopted by the Council on May 30 and is currently awaiting its publication in the EU's Official Journal and entry into force.

4.2. How to regulate smart contracts

Broadly speaking, a contract can be defined as a bilateral legal agreement, which, by means of declarations of will and using the powers of freedom of stipulation and celebration, aims to produce legal effects. Considering this, a smart legal contract can truly be a contract when representing an implementation of a contractual agreement, characterized by legal provisions written in the form of a code in a register based on DLT (Dell'Erba 2018).

Following this definition, it is important to question if there is a need for a new (specific) regulatory framework for smart contracts, and if this kind of contracts are already regulated by contract law.

Currently, there is no specific framework for smart contracts (namely in Portugal) and the development of the right regulation in the backdrop of fast technological innovation is a considerable challenge. It is necessary to gather efforts from developers, computer scientists and legal experts to be able to properly regulate new technologies, to reduce legal uncertainty regarding these technologies, so that it does not deter potential users.

Regulation on technology can arise directly or indirectly. When the content of regulation is specifically and primarily focused on the concrete technology, we are dealing with direct regulation. By contrast, in indirect regulation, the technology is only secondary and regulated in an accessory way.

Although Portugal does not have a specific legal framework for smart contracts, some other Member States of the European Union have approved legislation regarding this matter, such as Italy with the Law Decree No 135/2018, better known as "*Decreto Semplificazioni*", which regulates smart contracts in a direct way. This law introduces a definition of DLT and of Smart Contracts and sets out the legal effects of adopting such technologies. It defines smart contracts as "*computer programs that operate on distributed registers-based technologies and whose execution automatically binds two or more parties according to the effects predefined by said parties*".

The idea underlying smart legal contracts is to facilitate the proof and the enforcement of contracts. Even the so-called normal contracts have some challenges, among which the risk of non-compliance and the risk of lack of proof are emphasised. Considering these risks, the idea of smart legal contracts becomes very useful, since it operates based on a code and a Blockchain registration technology making it possible for two people to write a contract along agreed terms and send it to the Blockchain, which saves the contract, verifies its validity, and executes it. Also, a smart legal contract will always be registered on the Blockchain, thus providing proof of its existence.

The main difference between contracts and smart legal contracts is the self-execution of the latter. On the one hand, this self-execution, plus the immutability associated with Blockchain, means that smart legal contracts are pointed to their rigidity, making it a possible disadvantage. In addition, these types of contracts are not sensitive to events such as termination or modification of the contract due to the change of circumstances (regulated by Article 437 of Portuguese Civil Code) and may even be self-executing going against a court decision (Freire 2021).

On the other hand, the immutability of Blockchain protects the authenticity and integrity of data and, applied to smart contracts, reduces the risk of non-compliance.

To fight the beforementioned rigidity and considering the values at stake, it may be possible to create a more flexible protocol, so that it is possible to change the information contained in the Blockchain on tight and very well-defined criteria. This change of information may involve the creation of hard forks in the network when justified, a situation in which users must all agree in advance and follow the new Blockchain. However, this possibility reduces the security of the Blockchain (*ibid*).

The concept of modification due to the change of circumstances can be considered in a smart legal contract through the inclusion of oracles. Within the DeFi ecosystem, in a context of private autonomy, it seems that there is nothing to prevent the parties from establishing that, for example, in the event of an abrupt rise in an interest rate resulting from an anomalous condition, the injured party has the right to terminate the contract.

This is an example of how to address an intrinsic problem of Blockchain, while keeping its characteristic of immutability.

In what concerns indirect regulation on smart contracts, a good example is the European proposal for a Data Act.[10] This constitutes an indirect regulation, since its primary objective is to regulate access to data and its use, but in doing so it also establishes the essential requirements regarding smart contracts for data sharing (Article 30). It establishes inter alia essential requirements regarding the cessation and interruption of data sharing (e.g. the need of a mechanism to stop the continued execution of operations).

In this regard, it is important to highlight an article by Marino and Juels (2016) that demonstrated the possibility of altering and extinguishing[11] smart contracts on the Ethereum platform. However, the programming must be done at the time of inception of the smart contract, since it is immutable once inserted in the Blockchain. In Ethereum, the extinction of smart contracts is possible by inserting a self-destruct function in the code.

To conclude, contract law should not, and cannot, be removed ab initio from smart legal contracts. The form, the object and the content of smart contracts is already regulated by the existing contract law, as well as the use of legal techniques of interpretation and integration to regulate them. As previously mentioned, there is already regulation that, directly or indirectly, give legal validity to smart contracts.

Yet, there are features that could be regulated about smart contracts, regarding its specific nature, and for which the existing contract law is not sufficient, or it does not give the necessary legal certainty, like the application of the law across jurisdictions of a specific smart contract (international competent law and international jurisdictional competence). Also, harmonising legislation and general principles by which the parties and smart contracts should be governed, would contribute to mitigate costs for the parties and not to block technological innovation (Freire 2021).

4.3. Discussing self-regulation

Self-regulation[12] may assume different forms. Black (1996) argues that, when discussing self-regulation, authors can set three dimensions. First, the term 'self' could be used as in individual. Therefore, self-regulation could be 'described as the

[10] Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (COM/2022/68 final) of 23.2.2022.

[11] In this context, extinction refers to the termination of legal effects and not to the disappearance of the smart contract, since its association with Blockchain means that it cannot be de-lete.

[12] Other concepts are also used with closer meanings to the one presented in this occasional paper, i.e. 'coregulation' or 'enforced self-regulation' (cf. Ayres and Braithwaite (1992) and Ogus (1995)).

disciplining of one's own conduct by oneself' - a frequent definition in financial services regulation. Second, 'self as in collective', where self-regulation could be pointed out as 'regulation tailored by the circumstances of particular firms', including 'that regulation by a collective group of the conduct of its members or others'. Finally, the third dimension of the term 'self' refers to the lack of relationship with the state or to describe a kind of collective government or arrangement.[13] In that sense, 'self-regulation describes the situation of a group of persons or bodies, acting together, performing a regulatory function in respect of themselves and others who accept their authority'.

As it enables the discussion and preparation of regulatory solutions by those that are affected by DeFi, but also by those that have a true understanding of its functioning, expertise is without a doubt one of the clearest advantages of applying a self-regulatory approach to DeFi.

However, the possible effectiveness of self-regulatory solutions, in comparison with more traditional regulatory regimes, may be also seen as a valuable recourse when it comes to the analysis of the acceptance by the regulated parties of self-regulatory rules and standards, namely in what regards very specialized and technological financial solutions, like DeFi.

In this regard, certain existing examples can be seen as initial attempts towards a self-regulatory approach. However, it is important to note that these initiatives currently lack a unified and standardized framework, and their compliance is purely voluntary.

- **Smart Contracts Audits**

  Smart contract audits play a crucial role in enhancing the security and reliability of DeFi protocols. Given the highly technical and decentralised nature of these projects, where the absence of intermediaries poses unique risks, independent third-party firms specializing in blockchain security conduct comprehensive smart contract audits.[14] These audits aim to identify vulnerabilities and potential exploits in the codebase of regulatees that may compromise the integrity and safety of user funds. By voluntarily subjecting their smart contracts to external evaluations, DeFi regulatees seek to proactively address security weaknesses, reduce systemic risks, and instill confidence in users and investors alike.

  Furthermore, it is widely acknowledged that market participants heavily rely on these assessments as a form of endorsement for a particular project, making

[13] Black (1996) identifies four types of self-regulatory approaches in terms of relationship with the state: 'mandated', in which a collective group is somewhat mandated by the government to formulate and enforce norms within a predefined and broad governmental framework; 'sanctioned', in which the norms are formulated by a collective and then submitted to the government approval; 'coerced', in which the industry is subject to some form of coercion by the government to act, namely through regulation; and 'voluntary', where there is no government involvement.

[14] Certik, ConsenSys Diligence and Trail of Bits are examples of established companies within the DeFi space providing this kind of services.

the credibility of such assessments a crucial feature. The potential perception of misconduct by these auditors could significantly undermine overall trust in the auditing segment of the DeFi ecosystem.

- **Community Governance**

  Community governance could be seen as empowering token holders to participate actively in decision-making. Using decentralised governance mechanisms (such as DAOs), users propose, debate, and vote on protocol upgrades, feature enhancements, and strategic directions. This approach can foster a sense of ownership and accountability, aligning project trajectories with the community´s collective interests.

  However, community governance introduces challenges, including the potential for governance gridlock and concentration of voting power among larger token holders. Despite this, involving users in governance decisions is crucial for maintaining a dynamic and adaptable ecosystem, provided mechanisms ensure inclusivity and responsiveness to diverse participant needs. Annex 4 presents the case of Uniswap to exemplify in detail how a DAO functions and what actions can be performed collectively.

- **DeFi Best Practices Standardisation**

  The DeFi space still needs to fully reconcile the recognition of the need for standardization with concrete and comprehensive actions. In fact, there are only a few projects establishing not industry-wide but segment-specific guidelines.[15] DeFi standardization organizations convene stakeholders, including developers, researchers, and experts, to collaborate on defining common security, transparency, and user protection principles. While adherence to these standards remains non-mandatory, it offers a reference point for industry participants to evaluate their practices and demonstrate their commitment to responsible self-regulation.

  Yet, challenges may arise concerning the adoption and enforcement of such standards, as the decentralized nature of DeFi leaves room for divergence in interpretations and practices. Also, at the moment, most of the work done in this field is more related to identity security and data protection. Other levels of a DeFi project remain widely heterogeneous with a lack of uniformization. As the DeFi ecosystem evolves, the role of standard setters' organizations may become pivotal in shaping a more cohesive and resilient regulatory landscape, conducive to the long-term sustainability of the sector.

To foster a self-regulatory approach within DeFi, it's crucial that the regulations are perceived as legitimate and binding by those being regulated, akin to traditional

[15] One well-known organisation within this space is the Decentralized Finance Security Standard (DFSS), whose primary purpose is to establish security best practices and guidelines for DeFi projects.

statutory regulations. Although upfront better prepared than more 'traditional regulators', self-regulators could be confronted with severe enforcement issues, namely because the market might tend to see the rules as not equivalent to governmental rules and, therefore, not valid. In what refers to enforceability of self-regulatory rules and standards, DeFi solutions will not be an exception to other solutions where self-regulation strives to succeed.

Critics of self-regulation tend to indicate its lack of legitimacy combined with lack of accountability and unfairness of procedures as shortcomings of this type of regulatory approach (Ogus 1995). Also, the potential creation of artificial market barriers to detain the entrance of new players, indicated by some authors as an emergent risk of self-regulation (Shared and Sutton (1981), Ogus (1995)), should not be disregarded in what refers to applying self-regulation to DeFi solutions.

To conclude, self-regulation will not be a silver bullet for DeFi solutions as it has not proved to be for any other financial solutions. Nevertheless, due to the complexity of DeFi it is a regulatory approach that could be interesting to explore. Particularly, the exponential evolution of DeFi could make traditional statutory regulations less well-suited for this constantly changing landscape, as rigid rules could risk a dogmatic-type approach delaying and disincentivizing financial and technological innovation.

5. DeFi risks and vulnerabilities

5.1. Cyber and other operational risks

Operational risks pertaining to DeFi activities can be broadly classified into two categories: the **Cyber Risk**, encompassing threats arising from malicious activities and attacks, and the **Technological & Operational Risks**, associated with the vulnerabilities and operational aspects of technology systems. This division allows for a more nuanced approach in developing comprehensive strategies to address the distinct challenges posed by cyber threats and technological vulnerabilities to DeFi.

5.1.1. Cyber risks

Cyber threats are fundamentally asymmetrical threats where highly skilled individuals with a wide variety of motivations can cause a disproportionate amount of damage (BIS, Project Polaris). Threat actors can range from state-sponsored adversaries, cyber criminals, hackers-for-hire, and hacktivists, all with different capabilities and goals.

Related cyber-attacks essentially focus on accessing and manipulating data, which is the main asset to protect. Information security, in its three aspects (confidentiality, integrity, availability) is a key topic for risk assessment and the identification of risk mitigation controls.

With the increasing interest in crypto-assets, threat actors have been quick to react.[16] This section touches upon the most common threats in the DeFi ecosystem and possible mitigants and counteracting measures.

- **Hacking and Exploits**

DeFi platforms face advanced persistent threats (APTs) from hackers aiming to exploit vulnerabilities in the network infrastructure. These malicious attacks can have severe consequences, including the theft of funds, manipulation of prices, and disruption of services.[17] To counteract these evolving risks, DeFi platforms must employ a comprehensive cybersecurity strategy. **Multi-layer security protocols** are essential, providing a layered defense against various attack vectors. **Regular security assessments**, conducted through code audits, help identify and address vulnerabilities before they can be exploited.

Robust encryption techniques play a crucial role in safeguarding data integrity and confidentiality. Measures such as the use of **multi-signature wallets** enhance the security of transactions, requiring multiple authorizations. **Hardware wallets**, which store user's key offline, offer secure key storage, mitigating the risk of unauthorized access to sensitive cryptographic keys.

Enhancements to agreement mechanisms serve as a proactive defense. By fortifying the consensus layer, DeFi platforms can resist manipulation and unauthorized transactions.

Compounding this challenge is the looming **quantum threat** that has the potential to compromise the cryptographic foundations that underpin the security of blockchain ecosystem, including DeFi platforms. Quantum computing uses the principles of quantum mechanics to perform complex calculations at speeds exponentially faster than classical computers. This breakthrough in computing power could potentially render current cryptographic algorithms obsolete, thereby threatening the integrity of smart contracts and the security of user wallets.

Futureproofing DeFi platforms requires a collaborative effort from researchers and developers. Actively working on quantum-resistant cryptographic solutions is crucial to mitigate the quantum threat and ensure the continued security of DeFi platforms in the ever-evolving technological landscape.

- **Phishing Attacks**

In phishing attackers trick users into unwillingly sharing their private keys or other sensitive information. These malicious actors often create fraudulent websites or deploy deceptive communications to mimic legitimate platforms, aiming to

[16] Recent data from "CoinGecko" support a surge in crypto-assets asset theft (CoinGecko, 2023).

[17] Examples of notorious cases are the hacking of the Poly Network (August 2021), the Qubit hack by North Korea-linked hackers (January 2022), the Mango Markets oracle manipulation (October 2022) and the heist of the lending protocol Euler (March 2023). Please refer to Chainalysis' annual Crypto Crime Report for further information.

deceive users and gain unauthorized access to their funds or personal data. The consequences can be severe, leading to financial losses, unauthorized transactions, and compromise of user accounts.

To address this risk, the implementation of robust security practices is primordial. This includes promoting the use of **hardware wallets** (previously mentioned as a possible safeguard against hacking). **Multi-factor authentication** (MFA) adds to security by requiring users to provide multiple forms of verification before accessing their accounts.

Also, **user's technological literacy and awareness** play a crucial role in combating phishing attacks, so DeFi platforms should invest in it.

- **Data Leakage**

Data leakage, particularly the **exposure of private keys**, presents a substantial threat to the security of crypto-assets within the DeFi ecosystem. It can jeopardize individual user accounts, potentially compromising sensitive information and resulting in the loss of funds, but also poses systemic risks to the overall integrity of DeFi platforms by undermining users' trust.

To mitigate this risk, a multifaceted approach is essential including: i) the implementation of **secure storage solutions**, like hardware wallets; ii) **encryption techniques** so as, even if unauthorized access occurs, the data remains unreadable and unusable without the proper decryption keys, and iii) **strict access policies** to ensure that only authorized entities have the necessary privileges to access sensitive data, thus mitigating inadvertent or malicious leakage of information.

5.1.2. Technological and Operational risk

These risks are related with the challenges and vulnerabilities that arise from the daily operational activities and processes within DeFi platforms and protocols or from the underlying technology used, that could cause operational disruptions, disturb normal activities, and cause financial losses.

Mindful of Schär' DeFi Stack Model (Box 1), the hierarchical connection between layers implies that to build a secure and reliable DeFi ecosystem, all layers must be secure and both operational and technology risks must be addressed. Smart contract vulnerabilities, oracle manipulation, coding errors, and blockchain-related issues, are examples of technology risks that must be address.

On the following paragraphs some of the most relevant operational and technology risks are highlighted.

- **Smart contract risk**

Smart contracts are responsible for the **top incidents in the DeFi ecosystem** often enabled by their intrinsic vulnerabilities that are exploited in the blockchain network, with malicious actors taking advantage of such vulnerabilities or flaws in the code. Smart contracts vulnerabilities and bugs are more difficult to fix than a traditional piece of code because its code can be totally or partially locked from its initial release, meaning that needed changes might not be allowed and that the smart contract conditions will execute automatically, even if with bugs or errors.

Smart contracts play a vital role in the DeFi ecosystem, but their integration introduces challenges that require strategic risk mitigation and a multifaceted approach. For instance, **conducting routine and meticulous code audits** (preemptive measures to identify and rectify vulnerabilities and bugs), **implementing upgradable smart contracts** (to allow for the seamless incorporation of fixes and improvements without compromising the immutability of the entire codebase) and **ensuring secure coding in smart contract development**. Consistent application of these practices significantly reduces the likelihood of introducing vulnerabilities during the development phase.

- **Oracle risk**

Oracles play a crucial role in the DeFi ecosystem by setting bridges with real world data (cf. subsection 2.3 and subsection 2.4). Since the data is generated off-chain, it is **susceptible to manipulation and inaccuracies**, e.g., security breaches have been exploited to manipulate prices. This highlights the importance of using trusted and secure oracles with robust security measures. It is essential that the data retrieved through oracles is accurate and untampered by malicious agents.

Ensuring the use of multiple oracles to retrieve and validate data, could reduce the impact of a single faulty oracle in a smart contract execution. Aggregating data from multiple oracles and using a consensus mechanism to determine the most accurate and reliable information could mitigate oracle risk.

- **Scalability risk and concerns**

The scalability of a system refers to how much it can grow without encountering performance degradation. Although potentially scalable, actual scalability is dependent on the network peers to validate transactions before permanently registered them on the blockchain. Since DeFi Applications are often deployed on the same network as other applications, heavy congestion could occur, leading to delays in the execution of transactions.

The DeFi network experienced a dramatic increase in transactions over the past years, making scalability a critical factor that profoundly influences the performance of the entire DeFi ecosystem. Even considering the technology limitations, there are some strategies that may be employed to improve the scalability, namely, but not limited to:

- **Layer 2 solutions**, like sidechains or state channels, that enable the processing of transactions off the main blockchain, reducing the burden.
- **Sharding** involves breaking the blockchain into smaller, more manageable parts, allowing for parallel processing.
- **Off-chain transactions** can alleviate congestion by processing certain transactions away from the main chain.

In addition to the scalability concerns, the way blockchains are built need a consensus protocol to ensure its immutability and continuity - the most renown being Proof of Work (PoW)[18] and Proof of Stake (PoS).[19]

5.2. Legal risks

Currently, the DeFi ecosystem stands in a legal and regulatory limbo. As discussed previously (subsection 4.1), DeFi is out of scope of the European MiCAR and most of the characteristics of DeFi are incompatible with existing legislation, for example, the registration, licensing and supervision of intermediaries involved in issuance, trading, custody and lending activities. Traditional bank regulatory frameworks, which were created for centralised financial systems (reserved only for licensed entities), are being truly challenged by the decentralised and borderless nature of DeFi, exposing participants and the market to significant risks.

Given the decentralised nature of the networks on the basis of which DeFi operate, and their community-driven governance, it is difficult to identify the decision-making entities/operators that can be held accountable for the operation of the network. In this context, the attribution of responsibility, and even the communication with supervisors, prove to be cumbersome, given that currently supervisory mandates are designed based on the existence of centralised decision-making bodies (OECD 2022).

As previously mentioned (subsection 4.2), there are some legal issues that can arise from smart contracts, conceived as the foundation of DeFi protocols, regarding its specific nature and for which the existing contract law does not give the necessary certainty. Considering that smart contracts are the foundation of DeFi protocols, risks that arise from smart contracts are also risks from DeFi, especially legal uncertainty, as well as challenges in respective enforcement. This further obstructs oversight and regulatory compliance of such protocols, given the speed and ease with which financial service providers can change locations in response to actions of authorities.

It is also extremely important to mention the principle of exclusivity laid down in Article 8 of the Legal Framework of Credit Institutions and Financial Companies.[20] The first paragraph of this Article states, *"[o]nly credit institutions may take deposits or other repayable funds from the public for their own account"* and the second paragraph states that *“[o]nly credit institutions and financial companies*

[18] Proof of Work (PoW) is a consensus algorithm foundational to the operation of several blockchain networks. It involves participants (miners) solving complex mathematical problems to validate transactions and create new blocks. This mechanism is energy-intensive but provides high security by making attacks economically impractical.

[19] Proof of Stake (PoS): An alternative consensus mechanism where the probability of validating transactions and creating new blocks is proportional to a participant's holdings (Stake) in the blockchain network. PoS aims to reduce energy consumption and the risk of centralization.

[20] Legal Framework of Credit Institutions and Financial Companies, approved by Decree-Law Nº. 298/92 of 31 December 1992, mostly known in Portuguese by the acronym RGICSF.

may carry out on a professional basis" credit activities.[21] This principle is based on the traditional function of financial intermediation assigned to credit institutions - receiving funds from the public and financing the economy on their own account by granting credit –, ensuring that these activities are carried out on a professional basis only by entities legally allowed for those purposes and that such entities are subject to prudential and conduct requirements.[22]

DeFi is characterized by a decentralised nature and may involve the performance of credit activities on a professional basis; in this sense, the pursuing of such activities by "entities" not subject to authorization and supervision appears to, at least, pose important challenges concerning this principle, and may be qualified as unauthorized activity, which may have legal consequences.

We can conclude that traditional bank regulatory frameworks, which were created for centralised financial systems, are not ready to address DeFi, due to its decentralised and borderless nature. Also, it is worth emphasising once again that DeFi is not currently subject to specific regulation, both at the EU and national level.

Two opposite options can be envisaged to address DeFi issues: regulate it or not, both with its own risks.

The option to not regulate DeFi may have the advantage of mitigating risk contamination to the TradFi, as it may discourage or even prevent clients with a conservative risk profile and institutional investors from taking part of DeFi activities. Still, it will leave significant risks related to the absence of clients' protection and does not address ML/TF concerns. Both these risks will be discussed further in the following sections, the common point being that the absence of regulation may be seen as favouring the malicious operators. Furthermore, the absence of regulation does not solve the issue regarding the fact that this kind of activities may be qualified as unauthorized activities when performed by non-regulated entities.

The option to regulate DeFi could bring legal certainty, legitimate this kind of activity, provide more security to the clients, and favour the activities that arise from DeFi. It may also help to define clearly the border between authorized and unauthorized activities. This option also includes some risks related to the DeFi distinct features as discussed previously, in particular its decentralized and borderless nature. The regulation approach faces the difficulty, as well as the risk, to define what to regulate (only the activity, only the entity, or both), at what

[21] In this respect, the above-mentioned provision also establishes some exceptions, allowing the performance of credit activities in certain cases, namely when it's performed on a non-professional way.

[22] It should also be noted that it is currently the responsibility of Banco de Portugal to investigate and sanction the exercise of unauthorised activity, namely the granting of credit by unauthorised entities, which constitutes a particularly serious offence, under the terms of Article 211(1)(a) of the Legal Framework of Credit Institutions and Financial Companies. It is also Banco de Portugal's mission to monitor whether this activity is carried out only by legally authorised entities according to said Legal Framework and to Law Nº. 78/2021, of 24 November.

level (national, European, or international), and who should be the responsible supervisory authority.

To minimize legal risks and regulatory problems of DeFi, all parties, including regulators, industry participants, and legal experts, should consider working together to mitigate the risks. It is critical to maintain open and continuing conversations to comprehend the characteristics of DeFi and its potential consequences. This collaboration has the possibility to result in the creation of practical and effective regulatory frameworks that strike the desired appropriate balance between innovation and consumer protection.

Furthermore, international cooperation at the legal level will be important to mitigate these risks. Since DeFi is borderless, one possibility to minimise regulatory arbitrage and maintain a level playing field for market participants is to harmonise regulations and standards across jurisdictions, while taking also into account national specificities regarding the way each jurisdiction regulates financial activity (for instance, there are countries that regulate more intensively the granting of credit and others that have less restrictions to credit origination by non-regulated entities). Regulators and policymakers at international level are starting to grasp the necessity of encouraging innovation and technological progress while simultaneously providing fair conditions for all market participants.

5.3. Governance risk

One of the mentioned advantages of blockchain technology in general, and DeFi in particular, is that there is no need for a trusted third party to verify transactions and execute contracts. However, despite this degree of automation, some human intervention is still necessary. First of all, the rules of the DeFi protocol need to be determined. Second, any upgrade to the smart contract needs to be agreed upon (Makarov and Schoar 2022). The blockchain community has therefore come up with a new form of governance arrangement, the so called DAOs.[23]

The idea behind a DAO in DeFi is straightforward: spread among the interested stakeholders the control over decisions concerning the respective DeFi protocol. To this end, governance tokens are issued and distributed to stakeholders. The rule is often very simple: one governance token equals one vote (Makarov and Schoar 2022). While this appears to be a very democratic setup at first glance, there are a number of potential drawbacks already touched upon in subsection 4.3 when discussing self-regulation. First of all, voting power could be dispersed among many small shareholders, who might not be interested or willing enough to engage in the decision-making process. This is exacerbated by the fact that voting in a DAO setup is done via on-chain transactions, which incurs in costs in the form of gas fees (transaction fees). During times of high network activity, gas fees tend to be higher.

[23] See subsection 2.4 for a definition and examples in Appendix A.

Dotan *et al.* (2023) find that this often leads to voting centrality, meaning that token holders do not vote against proposals. Any user with a certain number of governance tokens can submit a proposal that will be voted on. In essence, proposals are difficult to verify without a solid knowledge of the code. Indeed, attackers can leverage on this. Attackers can accumulate a certain amount of governance tokens and then launch an attack on a DeFi protocol during times of high network activity when gas fees are high. This increases the chances of the attack being successful, as the proposal will have a higher chance of being voted through. Furthermore, voting participation might be low because users are staking their governance tokens, thereby locking them up (FSB 2023). However, some DeFi protocols allow for escrowed governance tokens. This solution allows for locking up the original governance tokens and being issued voting rights in return. The longer the tokens are being locked into the contract, the more voting rights the user is being awarded (Dotan *et al.* 2023).

Another problem is that governance tokens are usually freely tradable. This means that users can amass a large share of the governance tokens of a certain DeFi protocol, thereby gaining influence. This could even go unnoticed due to the pseudonymous nature of DeFi, meaning that one individual could buy these tokens through different accounts without being spotted. In addition to that, voting rights can also be delegated.

While it might appear that governance tokens are democratically distributed, at least at the outset, this is not always necessarily the case. Aramonte *et al.* (2021) speak of '*decentralisation illusion*'. In essence, smart contracts can never be complete, meaning that not every eventuality can be coded. This is equivalent to standard written contracts and what the literature calls '*contract incompleteness*' (Coase 1993). However, while in TradFi this can be dealt with, for example, by parties resorting to lawyers to solve open issues, recourse to the legal system contradicts the fundamental principles of DeFi. In DeFi, this is often dealt with by a small number of people (often developers or initial investors), holding a large share of governance tokens. This is comparable to blockholders in TradFi but without the obligation to declare its position.[24] This concentration of voting power can be useful in the early phases of the protocol, when potential glitches need to be fixed quickly (Gorjón 2023). However, this concentration is not desirable in later stages of the protocol, as it goes against the principle of decentralisation. In practice, some DeFi protocols dilute the share of governance tokens of these blockholders over time.

While the idea behind DAOs is intriguing, it is unlikely that this form of governance will work smoothly and securely in the long run.

[24] In TradFi, blockholders own a large block of a firm's shares or bonds. This often translates into a large share of voting rights.

5.4. Investor and consumer protection risks

DeFi systems and products involve speculative trading, lending, and borrowing with highly leveraged strategies, as described in the previous sections. Therefore, DeFi can involve risks analogous to those in traditional markets, as the ones "*caused by trading and price misinformation or manipulation and conflicts of interest*" (IOSCO 2022).

DeFi environment can also be the stage of many criminal behavior. Consumers/investors can be victims of wash trading, pump and dump schemes and front-running.[25]

In addition, this environment is susceptible to market manipulation,[26] cyber-attacks (as presented in subsection 5.1) and fraudulent conduct. As reported by IOSCO (2022), there have been numerous reports of DeFi fraud schemes as rug pulls,[27] Ponzi schemes and other types of misconduct, such as theft of private keys. All this can not only result in the loss of funds but also in the leak of sensitive information.

Another risk to consumer/investor is identified by OECD (2022) as '*gamification of finance*'. Platforms providing a user-friendly experience to DeFi make trading an enjoyable and attractive process, similar to interacting on social media or playing online games. As stated by IOSCO (2022), retail investors in DeFi usually are part of an online community or are lured by influencers, social media or "*other forms of digital engagement and promotional activities*". Therefore, misrepresentation, misinformation, and inappropriate advertising – either through gamification or other "social" promotional channels - present risks to investors, especially if they are unexperienced and thus more likely to follow unsound financial advice.

Moreover, DeFi products and systems do not to provide important disclosures, as information about a service, a product, or the participants, and therefore, investors/consumers may not have the conditions to make informed decisions. In this line, there may exist misconduct, as situations of hidden information/lack of transparency or the promotion of situations of uneven playing field between participants, leading to an asymmetric concentration of risks.

However, the major risk is, in fact, that DeFi has no traditional regulatory safeguards for investor/consumer protection. As there are no recovery schemes or dispute resolution mechanisms, participants are exposed to risk of total loss

[25] Front-running can be defined as "*trading ahead of transactions in the queue of transactions to be validated in order to gain advantage*" (IOSCO 2022). This activity can result in "*users with transactions that have been re-ordered obtaining less favorable transaction terms*", which can ultimately undermine trust in the blockchain (*ibid*).

[26] See Gorjón (2023) for examples of market manipulation. OECD (2022) also notices that market manipulation cases observed are usually associated with manipulation of oracles. Market manipulation can happen, for instance, in flash loans (refer to subsection 3.2 of this paper).

[27] In rug pulls "*a project developer launches a token, attracts investors and defrauds them by taking all the liquidity, resulting in the near total loss of the token's value*" (Gorjón 2023).

in case of default.[28] Users have no recourse in the event of default or failure of a DeFi protocol. Additionally, due to DeFi decentralized nature, it is frequently difficult to identify a responsible party or centralized authority to turn in case of consumer/investor concerns, as highlighted by several organizations (cf. OECD (2022), BIS (Ocampo *et al.* 2023), and Banco de España (Gorjón 2023)).

Regardless of the discussion about the need for regulation of DeFi, it is widely understood that its absence erodes investor/consumer protection and, therefore, a regulatory framework to ensure at least consumer/investor protection is needed (WEF (2021), BIS (Aramonte *et al.* 2021), FSB (2022), Bank of England (2022), OECD[29]).

Moreover, the novelty of DeFi together with this lack of regulation creates the idea of uncertainty linked with DeFi, which can also pose a risk for its users.

These risks are heightened by the lack of financial literacy. IOSCO (2022) and OECD (2022) argue that the average investor/consumer may not have the required level of technological and financial literacy to duly understand the implicit risks of DeFi.

The overall setting highlights the relevance of the supervisors' role in taking the adequate measures to ensure investor/consumer protection. At its core is the rise of financial consumer awareness and literacy, e.g., by engaging and encouraging initiatives that promote consumer/investor protection updates, providing guidance and issuing of warnings.

5.5. ML/TF risk

As much as DeFi may introduce innovations in financial services and products, it also brings forth significant ML/TF risks. As mentioned in previous sections regarding illicit activities that may hinder consumers/investors in DeFi,[30] the same characteristics that make DeFi appealing for the common user are the ones that may be used by illicit actors to pursue criminal activities (US Treasury 2023).

In what concerns the current regulation discussed under subsection 4.1, AML/CTF legal framework is not applicable to software or technology, but rather to specific entities in the context of the services they provide. DeFi itself is not considered a VASP and is therefore not subject to these rules. However, and despite its apparent decentralisation, some entities who have control or influence over the DeFi system, depending on the services provided, may be classified as falling under AML/CTF regulation (FATF 2021).

The FATF (2023) identifies DeFi as an emerging risk associated to market development, concluding that "*DeFi markets had grown significantly*" throughout

[28] As discussed in subsection 4.1 regarding the current state of DeFi regulation, noting that DeFi is not directly covered by the current regulatory framework.

[29] In this matter, OECD defends that, when and if possible, existing financial regulation and policies should be applied, to promote investor/consumer protection.

[30] See subsection 5.1 regarding cyber-attacks and subsection 5.4 on clients' risks.

2022 and early 2023, although "*several jurisdictions noted that DeFi arrangements still account for a relatively low percentage of overall VA [virtual asset] activity*" (*ibid*).

In the following subtopics, we delve into a brief analysis of the key ML/TF risks associated with DeFi, focusing on the main vulnerabilities that warrant careful consideration in this dynamic landscape.

- **Anonymity**

Unlike TradFi, where the obligations to identify the customer and of due diligence are closely tied to transactions, DeFi platforms often operate on blockchain networks that allow users to operate with a certain degree of anonymity, without revealing their real-world identities.

As highlighted by the ESRB (2023), "*[t]he nature of the distributed ledger means that the owners of tokens may only be identified by a cryptographic signature. Any individual can easily generate more than one identity (address) to split their holdings of any token across multiple addresses. Beyond that, it is simple enough for anyone to mask their location when accessing any website providing services related to crypto-assets. Taken together, this makes the crypto-asset world pseudonymous, albeit law enforcement and anti-money laundering authorities have made significant progress in deploying technology solutions to help trace crypto-assets and make it more difficult to use anonymously "on-ramps" and "off-ramps", such as crypto-asset trading platforms, wallets and transfers of funds to bank accounts*".

This pseudonymity creates increased challenges for competent authorities, as it becomes difficult, complex, and costly to identify and monitor the source and destination of assets, for AML/CTF purposes, as users may potentially move assets without proper scrutiny (European Commission in Roukny (2022)).

- **Universal access, non-custodial services, and absence of customer due diligence**

The borderless and permissionless nature of DeFi offers the promise of universal access, allowing anyone with an internet connection to participate, aiming for financial inclusion for individuals who may be excluded from traditional banking systems.

However, this inclusivity and ease of onboarding presents unique challenges from an AML/CTF perspective, as, without an intermediary and traditional regulatory oversight, it becomes challenging to enforce user identity verification and due diligence.

True DeFi schemes, i.e., without intermediaries, where users maintain control of their private keys and assets without relying on an intermediary, present a distinctive challenge in the implementation of robust AML/CTF measures. It is anticipated that AML/CTF regulatory frameworks will need to address the nuanced difficulties stemming from the non-custodial nature inherent in these decentralised transactions in the foreseeable future.

In this regard, the FATF (2021) recommends, where it is not possible to "*identify a legal or natural person with control or sufficient influence over a DeFi arrangement*", that countries "*monitor for the emergence of risks posed by DeFi services and arrangements*", and "*consider, where appropriate, any mitigating actions, where DeFi services operating in this manner are known to them. Such actions may be taken before the launch of the service or during the course of the DeFi services being offered, as necessary*". It further adds that "*(a)s an example, where no VASP is identified, countries may consider the option of requiring that a regulated VASP be involved in activities related to the DeFi arrangement in line with the country's RBA [risk based approach] or other mitigants*".

Additionally, the composability and interoperability features of DeFi, allowing different protocols and applications within the ecosystem to seamlessly integrate with each other, via smart contracts, poses a challenge in tracking and monitoring the flow of assets. Illicit actors can take advantage of this interconnectedness for ML/TF purposes, across multiple decentralised applications, making it intricate and expensive for competent authorities to identify and prevent illicit activities effectively.

- **Fast evolving technology**

The rapid pace of innovation within the DeFi space can surpass regulatory responses, leaving potential gaps in addressing emerging ML/TF risks. This demands constant vigilance from competent authorities to adapt and implement effective measures against ML/TF having in mind that self-regulation presents caveats and is not an adequate response for AML/CTF purposes (as discussed in subsection 4.3). The FATF (2021) underlines that "*[d]ue to the global presence of the many open source projects and developmental contributors in this space, DeFi projects are rapidly expanding in their number and capabilities*".

This environment could also be exploited by wrongdoers to circumvent traditional AML/CTF measures and sanctions. As an example, protocols such as DEXs and Liquidity Pools are used solely or combined in order to prevent tracing of illicit proceeds (US Treasury 2023).

The dynamic nature of DeFi challenges authorities to establish and enforce standardized regulations. As technology evolves, addressing AML/CTF concerns will require adaptive regulatory approaches to handle DeFi's agility and complexity.

5.6. Payment systems' risks

The smooth and efficient operation of payment systems is a crucial element of any reliable and sound economy. Any disruption in a widely used payment system can have severe impacts in all economic agents (such as citizens, businesses, and payment service providers, such as banks), ultimately affecting financial stability.

Currently, most DeFi applications provide a wide range of decentralised financial services that do not include core payment and settlement services. In fact, there are some DeFi solutions in the realm of payments, such as stablecoins managed by

DAOs that act as substitutes of fiat currencies in the crypto-space ecosystem, but these decentralised solutions for payments and settlement are still at an early stage of development and far from creating a widely accepted means of payment.[31]

Still, given the payment systems' relevance, it is essential to consider the inherent risks that steam from a world where DeFi services and related decentralised infrastructure become widely used and highly interconnected with traditional finance payment systems.

Firstly, in a decentralised system, there are more entities and components involved to keep the system running. The system is highly interconnected, increasing the spill-over effects from a cyber-attack. However, the management of cyber risk in a decentralised infrastructure, especially in a crisis, can be much more complex and difficult than in a traditional payments' infrastructure. Without a central entity to intervene providing technical or financial support, the whole system can be compromised, and the consequences can be massively amplified.

Moreover, if a systemic decentralised payment system experiences a cyber-attack, this will most probably impact other financial infrastructures to which it is interconnected, eventually spreading the damages to the whole payment ecosystem and economy.

Furthermore, the inexistence of an applicable regulatory and supervisory framework covering DeFi applications can endanger the capacity of the system to perform efficiently, as it may create asymmetries between participants, lead to severe financial losses, and undermine the good management and evolution of the software and code supporting the system.

On top of this, the automatism that exist in DeFi systems can exacerbate the propagation of a crisis in a short period of time, which may also have a systemic impact in traditional financial markets.

At this stage, to consider a global DeFi payment system as a solution for the real economy is dependent on authorities and regulators solving the question "How to regulate DeFi?". Ideally, existent and future requirements applicable to either payment systems (such as Eurosystem frameworks and regulations) or crypto-assets (such as MiCAR) should somehow also apply to DeFi applications (ESRB 2023). This discussion is picked up on section 6.

5.7. Risks for monetary policy

While the current DeFi ecosystem does not pose an immediate concern for monetary policy, the dissemination of financial activities in a decentralised environment (like DeFi) could place risks for monetary policy if it experiences a relevant growth, if the interconnectedness with the TradFi environment rises substantially or if it facilitates the emergence of large reserve-backed stablecoins

[31] Please see the occasional paper on Stablecoins by Banco de Portugal for more information regarding stablecoins' risks for payment systems.

which may also gain prominence as a store of value or a medium of exchange. Additionally, a diminished role of commercial banks in lending and borrowing activities, and the lack of transparency and regulatory uncertainty that is inherent to DeFi may also impact monetary policy.

This section elaborates on risks for monetary policy should any of these scenarios occur.

- **Interconnectedness**

If interconnections between DeFi and TradFi rise markedly, financial instability in DeFi may propagate to TradeFi and the real economy, potentially challenging monetary policy. DeFi is subject to the same vulnerabilities as TradFi, like leverage, risk taking and liquidity mismatches. However, it has specific features that enhance those vulnerabilities, such as i) a greater interconnectedness within the ecosystem, ii) lack of regulation which can promote excessive risk-taking behaviour, iii) automatic procedures like smart contracts and iv) an absence of buffers or other shock absorbers, like banks or access to central bank facilities. A failure in a part of the DeFi ecosystem, like a collapse in trust or prices, may impact in other parts of the system and beyond. The financial instability associated with deleveraging and defaulting by relevant economic agents may affect the real economy and threaten price stability.

The extent and severity of spillover effects from Defi onto TradFi and, consequently, the real economy, are contingent upon the nature and scale of financial institutions' exposure. Financial institutions connections with the DeFi space may be direct or indirect and encompass both the asset and liability sides of their balance sheets. A direct connection on the asset side would exist when financial institutions act either as liquidity providers or as investors in the DeFi ecosystem or, in the liability side, when they accept deposits that serve as reserves for a specific stablecoin. Indirect relationships may involve the creation by financial entities of Exchange Traded Products (ETPs) focused on investing in financial products or companies operating within the DeFi space (asset side).

- **Stablecoins**

Stablecoins are an important element in the interconnection between DeFi and TradFi that may affect financial stability and monetary policy. subsection 2.3 already briefly presented their main features and roles within the DeFi ecosystem, with an emphasis on their role as a means of payment for which the nominal stability, typical through pegging to fiat currencies, is critical. Those that best serve the purpose of stabilizing their value are normally backed by a collateral reserve, which ideally should be fully composed by safe and liquid assets available in TradFi.[32]

[32] Contingent on the type of crypto-asset, MiCAR sets out requirements on the reserve assets.

The most relevant reserve-backed stablecoins today are mainly used in the DeFi environment and do not present a systemic risk. They are still largely unregulated and present many vulnerabilities and thus their use has remained circumscribed to the DeFi space. The eventual further development of the DeFi ecosystem and the inherent growth in the use of stablecoins, together with a possible use in transactions outside DeFi, instead of traditional means of payment, raise risks for the implementation and transmission of monetary policy, if not subjected to adequate regulation.

The risks for monetary policy related to stablecoins differ according to which currency the stablecoins are pegged to and the type of assets in the stablecoins' reserve.[33]

If stablecoins are pegged to the official currency of the jurisdiction, the most straightforward choice of assets for the stablecoins' reserve are safe and liquid securities or deposits. Opting for short-term public debt securities can impact its price and availability, which bear upon monetary policy given that these securities are used as collateral for monetary policy operations. Alternatively, if the stablecoins' reserve comprises banks' deposits, the subsequent shift in the bank's financing structure from retail deposits to custody deposits may reduce the bank's financing capacity, which can be significant for smaller banks, potentially impacting bank intermediation and monetary policy.

There have been incidents in the past where stablecoins have lost their peg, setting off runs similar to bank runs in the traditional financial system. This could occur if there was a loss in confidence in a certain stablecoin, triggered by doubts about its reserves. An eventual run on a large stablecoin could have spill-over effects to the financial sector, damaging the financial stability and subsequently the monetary policy transmission mechanism. A run may occur if a robust reserve asset management to instil confidence is not ensured. It may generate either forced selling of marketable debt, or withdrawals from banks while the stablecoins' peg could be at risk. Moreover, stablecoins' issuers may lack access to liquidity and lender-of-last-resort facilities of the central bank, or, even if they have access, the efficacy of such tools may be reduced in a decentralised setting.

On the other hand, if stablecoins' reserves are allowed to be deposited at the central bank, it could significantly impact commercial banks' financing capacity and the central bank's balance sheet. This substitution of commercial banks' deposits for stablecoins may negatively affect banks' financial intermediation if alternative financing sources are unfavourable or unavailable. Also, the central bank balance sheet may change significantly, initially shifting its composition from commercial banks reserves to deposits from stablecoins' reserve, and potentially increasing in dimension afterwards, if the central bank increases financing to commercial banks.

[33] Refer to the occasional paper on Stablecoins elaborated by Banco de Portugal, where these risks are thoroughly detailed.

Also, the extensive usage of a stablecoin pegged to one or more currencies of foreign jurisdictions may threaten monetary sovereignty. In this case, the scope of domestic monetary policy is reduced, and its transmission weakens. Monetary sovereignty can ultimately be significantly reduced. This case is more unlikely in economies with sound institutions and rules.

- **Decentralized nature, lack of transparency and regulatory uncertainty**

Another relevant concern lies in the ability of DeFi's inherently decentralised nature to compromise the effectiveness of monetary policy transmission channels. In a scenario where DeFi becomes more prominent in lending and borrowing activities, an eventual diminished role of commercial banks, may compromise the effectiveness of important policy transmission channels. Moreover, the lack of standardized risk management and transparency in DeFi introduces information asymmetry risks. Central banks may face difficulties in obtaining accurate and timely information, impeding effective monetary policy execution and the righteous assessment of transmission channels.

The legal and regulatory uncertainty about DeFi products and services (as discussed under subsection 4.1 and 5.2), together with the regulatory lag spurred by the fast evolving landscape of DeFi, pose a risk of regulatory arbitrage. Market participants can exploit this regulatory gap, potentially undermining the effectiveness of traditional prudential and monetary policy tools, which could warrant complex changes to the monetary policy frameworks.

5.8. Risks for financial stability

To date, DeFi is mainly self-referential and therefore does not pose a threat to overall financial stability (ESMA (2023), FSB (2023), ESRB (2023)). However, should DeFi undergo new cycles of substantial growth, as happened in 2020, risks to financial stability might start to materialise. This section therefore explores the channels through which a growing DeFi ecosystem might negatively impact financial stability.

- **Liquidity and maturity mismatches**

One of the most concerning risks in DeFi regards liquidity and maturity mismatches, analogous to what can be found in banks and non-bank financial institutions (FSB 2023). Liquidity mismatches in DeFi can arise because many DeFi protocols rely on so-called liquidity providers. These use smart contracts to lock up their assets to gain returns. By doing so, they provide funds for decentralised applications. These assets can be used for borrowing or trading by users. Risks can materialise if liquidity providers suddenly withdraw their funds, which can lead to liquidity shortages and potentially the collapse of the respective DeFi project.

Similarly, DeFi is prone to maturity risk because liquidity providers can lock up their assets for different time spans. Maturity mismatches can occur when users need to access their assets before their lock-up periods end, resulting in penalties or loss of interest.[34]

- **Stablecoins**

The DeFi system evolves heavily around stablecoins, comprising risks to financial stability similar to those presented for monetary policy (subsection 5.7).[35] Namely, a run on reserve-backed stablecoins could have negative contagion effects on the traditional financial system if the reserves' assets are also traded in traditional financial markets (e.g., the short-term government debt market) bringing about significant price volatility similar to "fire sales.". In addition, the potential impact on banks' deposits and, consequently, in banks' profitability, can hinder their financial intermediation role with negative consequences for the financing of the economy.

- **Leverage and volatility**

Another challenge concerns the high degree of leverage that DeFi allows all investors to achieve, regardless of their level of financial literacy. High leverage exacerbates volatility (Makarov and Schoar 2022) and can lead to procyclicality (Demertzis and Martins 2023), increasing the risks to financial stability.

DeFi allows for an easy built-up of leverage chains. This is achieved by borrowing on one DeFi protocol and then using the borrowed funds to pledge them as collateral in another DeFi protocol. This process can be repeated without any formal limit, potentially leading to very long chains of leverage. In the case of a sudden drop in the value of one or more of the underlying crypto-assets, this can lead to a sudden unravelling of the chain, as DeFi positions get automatically liquidated once the collateral falls under a pre-defined threshold (see subsection 3.2). Given the highly volatile nature of crypto-assets, automatic liquidation is a constant risk. This also links to the risk that oracles pose. As DeFi protocols need oracles to receive "real world" data, a malicious actor can use it to feed in incorrect data (see subsection 5.1). This could lead to the liquidation of DeFi positions, as the respective smart contract will simply execute based on the oracle data it receives and there are no circuit breakers.

- **Exposure of institutional investors**

The most obvious connection with the traditional financial system is the exposure of commercial banks to DeFi. However, according to the Basel III Monitoring Report (BCBS 2023), the exposure of Banks to the crypto sphere is still negligible, with the largest exposures of around 0.013% of their own total exposures found in the Americas (Adrian 2022). Furthermore, exposures are usually concentrated in highly specialised banks.

[34] The DeFi space has already witnessed the materialisation of this risk when the algorithmic stablecoin TerraUSD and the associated Anchor lending protocol collapsed (see Box 3).

[35] Refer to the occasional paper on Stablecoins elaborated by Banco de Portugal, where these risks are thoroughly detailed.

Looking more widely, there are now DeFi applications emerging that are aimed at institutional investors. Unlike regular DeFi protocols, these need to comply with AML/CTF regulations and therefore require participants to have verifiable identities (Gorjón 2023).

- **Interconnectedness**

The DeFi system is very interconnected. This is due to the high degree of composability, and interoperability, allowing different protocols to interact with and build upon each other, as laid out in Box 1.

While, from an innovation point of view, this feature allows for the seamless creation of new and innovative financial products, it also comes with certain risks attached. On the one hand, flaws in the code of one protocol, if going unnoticed, might perpetuate if the code is simply used to create a new product. Furthermore, the interconnectedness of DeFi protocols can have feedback effects with the wider crypto ecosystem, e.g., through the heavy use of stablecoins, and could ultimately also lead to contagion effects with the traditional financial system, as discussed earlier.

Box 3 Stablecoins and the crash of TerraUSD

Just before its collapse in May 2022, TerraUSD was the 4th largest stablecoin in terms of market capitalisation (see Figure 3). Its 1:1 peg to the US dollar was ensured by minting and burning units of TerraUSD according to an arbitrage relationship with LU-NA, its sister currency. Turmoil in the crypto market in the spring of 2022 had led to a loss in confidence in the crypto sphere. This also led to doubts about the stabilisation mechanism of TerraUSD. Ultimately, Terra USD and LUNA collapsed within a few days.

The collapse was closely linked to the DeFi lending protocol Anchor, which was based on the Terra blockchain network.

Anchor offered a 20% annual rate to liquidity providers (i.e., lenders) of TerraUSD. However, this business model was not sustainable and ultimately led to large withdrawals, which destabilised the demand for TerraUSD. Attempts to stabilise TerraUSD and LUNA failed.

The collapse had wide-spread ripple effects within the crypto ecosystem, which suffered a vast loss in confidence. The values of prominent crypto-assets like Bitcoin and Ether fell in the aftermath of the Terra-LUNA collapse. By mid-June 2022, the crypto market had lost $1.7trn compared to its all-time high. Consequently, several centralised intermediaries in the crypto-asset market failed, including Celsius Network, Voyager Digital Holdings, and BlockFi.

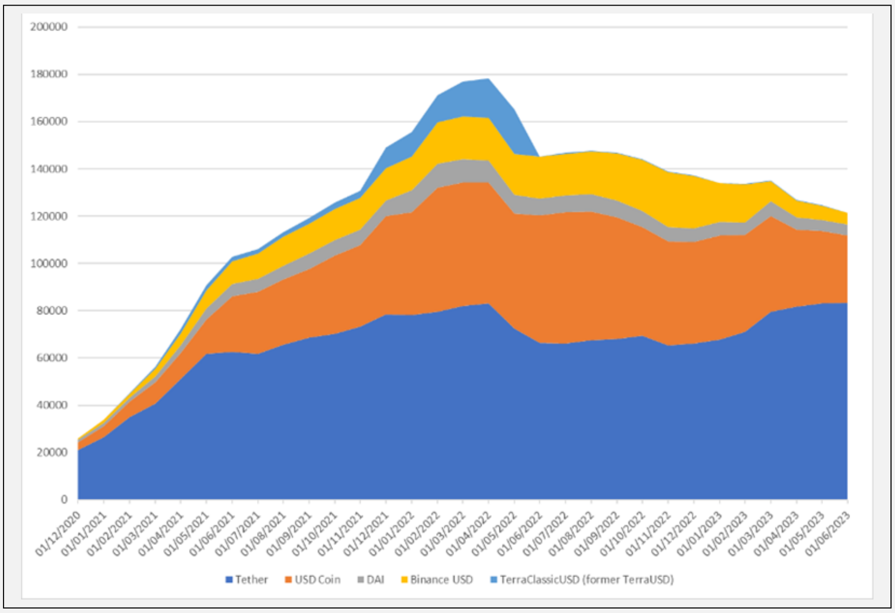


Figure 3: Market capitalisation of selected stablecoins | in USD Millions
Source: Defillama.

The most prominent failure to date occurred in November 2022, when FTX, one of the largest centralised crypto exchanges, filed for bankruptcy. US Secretary of Treasury Janet Yellen referred to it as crypto's "Lehman moment" during the 2022 DealBook Summit. After the failure of these centralised entities, DeFi proponents argued that collapses like the ones of FTX were the result of mismanagement inherent to centralised structures and that DeFi applications were the solution to these problems. However, as stated by FATF (2023), many DeFi protocols are Decentralised In Name Only (DINO). Furthermore, they are prone to hacking. In 2022, $3.1bn worth of crypto-assets were stolen by hackers from DeFi protocols. This accounts for 82% of the overall value of crypto-assets stolen through hacks in that year.

6. Outlook

6.1. Considerations for the future of DeFi regulation

Both the ESRB (2023) and the FSB (2023) have converging views on what needs to be done for the time being, while DeFi does not have (yet) a systemic relevance for the real economy. This comprises the following three top priorities: i) improve the capacity to monitor the interconnectedness of DeFi with the TradFi system; ii) keep a regular assessment of the DeFi ecosystem's risks and vulnerabilities to explore potential mitigating actions; and iii) continue to monitor market developments in DeFi to keep track of its implications in terms of regulation and supervision.

Overall, there is a general and consensual recognition across institutional bodies that a regulatory approach to DeFi should be considered to provide more clarity and security on decentralised solutions operating in the financial system. Undoubtably, it also presents challenges to regulators and supervisors and, thus, there are currently different lines of discussion in what concerns the future of DeFi regulation, which will be discussed in this section.

On the one hand, some argue that envisioning a decentralised financial system is unrealistic, since DeFi has evolved in a way where its users still must trust on something (e.g.: core software developers; wallets; stablecoins issuers). Under this perspective, the argument is that Defi is merely shifting the focus of trust from regulated and supervised financial actors to new intermediaries who are difficult to identify and are still unregulated (as discussed under section 4. Consequently, it is proposed that "*[p]olicymakers should take a precautionary approach to DeFi regulation, limiting the use of DeFi where financial regulators are able to exercise jurisdiction and then cordoning off whatever DeFi remains from the established financial system and real-world economy*" (Allen 2022). This approach also believes that the risks brought about by innovation in DeFi outweigh any possible benefits it might bring to the financial system and, therefore, a policy based on preventing their interconnectedness is considered a good policy (*ibidem*).

On the other hand, some point out that DeFi might be able to deliver significant benefits to the participants in the financial market, particularly in terms of faster execution of operations and reduced transaction costs. These advantages result from harnessing DLT innovations to disintermediate traditional financial services, for example by replacing third-party intermediaries with self-executing smart contracts. Other possible benefits are associated with the open-source nature of DeFi protocols, making it a platform for new financial solutions. Depending on the governance arrangements and associated transaction fees, DeFi could even facilitate a more equitable participation of users in financial markets, enhancing accessibility and reducing barriers. It could even facilitate supervisory and regulatory activities since, in a near future, and considering the rapid technological advances in this area, supervisors could "*(...) participate as nodes in the network and/or intervene at the smart contract level. Similarly, supervisors could have access to all data involved in DeFi protocol given the transparent nature of blockchain-based finance (albeit in a pseudonymous way at the moment), while the protocol could incorporate automated provisions for regulatory compliance directly in the code of the smart contracts*" (OECD 2022).

In line with this, it is argued that "*(...) policy makers should consider exploring lessons drawn from DeFi for the use of DLTs in traditional finance. While DeFi could end up being a short-lived phenomenon, deeper consideration of what value added*

DeFi services could bring to users, the financial system and the real economy could be beneficial" (*ibidem*).

Regardless of the avenues taken, the following regulatory/policy considerations, some of which already tackled in previous sections, should be taken into account.

Firstly, any financial regulation or policy should be technologically neutral. Regulators should focus on DeFi specific risks and analyse if they are already addressed by an existing framework. In fact, although we acknowledge DeFi's complexity, it can still be broken down into its core activities and related risks, some of which may already have comprehensive applicable frameworks. Regarding this point, the Crypto Council for Innovation (CCI 2023) makes note that although DeFi and TradFi activities have similarities, their intrinsic technological differences may result in different risks. Consequently, before transposing specific TradFi regulations to DeFi, regulators should first analyse if the risk being addressed is the same, rather than the activity. The framework on investor and consumer protection is an example that can illustrate this point. As previously noted (e.g. subsection 5.4), current regulatory frameworks fail at ensuring protection to investors and financial consumers in DeFi markets. Nonetheless, some of the core principles of the framework applicable to TradFi can be transposed to DeFi to ensure and incentivize DeFi market participants to educate their customers about potential risks and to provide regular information about the risks involved.

Secondly, specific characteristics of DeFi and, henceforth, potential different types of regulatory solutions from the ones already in place, should not be overlooked. TradFi largely relies on established financial intermediaries which bear the risk associated with the financial activities they carry out. As such, the regulatory framework should focus on those intermediaries and their activities' potential risks. Recognizing the challenges that may arise from the decentralized nature of DeFi, the OECD (2022) report suggests that "(. . .) *there may be a need to 'recentralise' DeFi in order to get some comfort from a regulatory and supervision standpoint, without necessarily completely undermining decentralisation*". In this report, the OECD argues that having a single accountable party, such as protocol developers, can help to strike a balance between having no central controlling authority and full supervision. While this approach may appear contrary to DeFi's ethos, the community should define regulatory and supervisory access points. In the same vein, BIS argues that "*[a] natural place for regulatory oversight in this new ecosystem is at the level of developers and validators, which in turn control the network protocol. Once this level of regulatory compliance is established, many other functions can be built*" (Makarov and Schoar 2022).

Nonetheless, restricting the focus of a future DeFi regulation on intermediaries may reveal itself inadequate, considering DeFi's characteristics. Therefore, the decentralised nature of DeFi should also be seen as an opportunity to explore other regulatory solutions. As suggested in a recent paper, these could be found in "(. . .) *non-financial regulations, such as those governing product safety in the European Union. In these particular regulations, a number of requirements are placed directly on products, thus building a chain of obligations for all players involved in their* *manufacture and distribution, which may notably lead to substitution mechanisms when one of these players is located outside the European Union*" (Banque de France, Fliche *et al.* (2023)).

Finally, policy makers must keep monitoring the evolution of this market. This is already expressly foreseen in European legislation – namely, in MiCAR -, where it is stated that the European Commission will need to monitor DeFi's development in order to produce reports assessing the development of decentralised finance in markets in crypto-assets and the necessity and feasibility of regulating decentralised finance.[36]

Also, it is important to engage actively with the DeFi market to better understand its' mechanics and find potential regulatory/supervisory solutions. In line with this approach, in September 2022 the European Commission proposed "*[a] pilot project to develop, deploy and test a technological solution for embedded supervision of decentralised finance (DeFi) activity. The project will seek to benefit from the open nature of transaction data on the Ethereum blockchain, which is the biggest settlement platform of DeFi protocols. Its main focus will be on automated supervisory data gathering directly from the blockchain to test the technological capabilities for supervisory monitoring of real-time DeFi activity*".[37] This is a promising supervisory solution and a good example of how supervisors can find solutions within the DeFi market. If nothing else, it may grant a deeper understanding of what added value DeFi technologies can bring to the supervision/regulation of the financial system.

6.2. National and international collaboration

As pointed out in this paper, the decentralised and borderless nature of DeFi makes regulating this market particularly challenging for policymakers and regulators. Current regulatory and supervisory frameworks, which were built around centralised intermediaries, will need to be adjusted to be fit for DeFi protocols which have no identifiable jurisdiction. Noting the uncertainty in many countries regarding the legal environment surrounding DeFi, the IMF (Adrian 2022) has advocated that "*regulators should prepare regulatory surveillance and globally consistent regulatory frameworks*". Policymakers, both at a national and international level, have been stepping up their work, calling for an increased international collaboration.

Given this context, international collaboration between regulators and supervisors should continue to be a major element to define a regulatory framework for DeFi as well as its subsequent enforcement. This need for collaboration has been highlighted by several institutions, including the ECB (Born *et al.* 2022) and the ESRB (2023).

[36] Cf. Article 140(2)(t) and 142(2)(a) of MiCAR, also reflected in EBA 2024 work programme and ESMA 2024 work programme.

[37] C.f. ted.europa.eu

A lot of the ongoing work on DeFi is, therefore, currently proceeding at international organisations. The FSB (2023) identifies as a future course of action exploring the need to enhance its proposed policy recommendations taking into account DeFi-specific risks, regarding international regulation of crypto-asset activities. Additionally, it has suggested that it could also be considered, in coordination with standard-setting bodies, assessing the regulatory perimeter across jurisdictions to determine which DeFi activities and entities fall or should fall within that perimeter. The IOSCO (2023) issued a set of nine policy recommendations that "*aim to address market integrity and investor protection concerns arising from DeFi by supporting greater consistency of regulatory frameworks and oversight in member jurisdictions*". Among others, these recommendations cover areas that include achieving common standards of regulatory outcomes and promoting cross-border cooperation and information sharing. IOSCO's future work will now focus on monitoring the implementation of the recommendations, capacity building and technical assistance to its members.

One of the main issues flagged by international organisations is related to the available data on DeFi, which makes it difficult to accurately estimate the size of the market and to fully assess its interlinkages with traditional finance and the real economy. As the FSB (2023) noted, "*the monitoring of [DeFi] vulnerabilities is hampered by the absence or low quality of available data, lack of or non-compliance with reporting requirements, and market practices oriented towards operating in opaque and nontransparent ways that create challenges for accurate data collection and analysis*". As such, one of the areas of future work for the FSB, again in collaboration with standard-setting bodies and regulatory authorities, will aim at addressing these data gaps, through the improvement of international and national collaboration. It will also proactively analyse the vulnerabilities of DeFi as part of its regular monitoring framework of crypto-asset markets, including through the development of DeFi-specific indicators of vulnerabilities to complement the current framework.

In a similar vein, the ESRB (2023) proposes as a main area of focus improving the EU's monitoring capacity through the introduction of regular reporting requirements for financial institutions and enhancing reporting requirements within the crypto-asset sector. It also proposes the promotion of EU-level knowledge exchange and the monitoring of market developments on DeFi, arguing in favour of pursuing further work to increase its understanding and implications for regulation and supervision.

Another collaborative effort aimed at improving the understanding and measurement of DeFi is Project Atlas, a platform developed by the Bank for International Settlements, the Deutsche Bundesbank and De Nederlandsche Bank. By providing central banks and regulators with data tailored to their needs, it "*sheds light on the macroeconomic relevance of cryptoasset markets and decentralised finance*". Also, regarding the development of DeFi in markets in crypto assets, the MiCAR claims a cooperation between the financial authorities and the

European regulators in order to determine an appropriate regulatory treatment of decentralised crypto-asset systems.[38]

7. Conclusions

The paper gives a comprehensive overview of the DeFi ecosystem, with a special emphasis on the discussion of current and future regulation, and on the inherent risks from the perspective of a supervisory authority of the financial system.

Monitoring developments in DeFi is of utmost importance. DeFi has brought, and is still bringing, a lot of technological innovation to the financial system, some of which is also making its way into traditional finance. One of the most important is blockchain technology, which builds on distributed ledgers, and aims to provide transparency and decentralised transaction recording. While this technology was invented before the use of crypto-assets, it only gained widespread use with this new space. This was followed by the use of smart contracts, which allow for putting a vast range of financial services, including lending, borrowing and decentralised exchanges, onto the blockchain. This allows for the automated execution of financial operations without the need for a financial intermediary and, in most cases, through permissionless processes.

The interplay between blockchains, smart contracts and crypto-assets, including stablecoins, composes the core infrastructure of DeFi, which, while bringing a lot of innovation, also carries many risks.

A first significant group encompasses cyber, technological and other operational risks. There are a wide variety of cyber threats - phishing and other malicious activities and attacks -, as well as vulnerabilities associated with the operational aspects of technology systems. Security breaches, including blockchain hacking and smart contract vulnerabilities, pose significant threats to DeFi protocols and the underlying blockchain network. Still, as presented in this paper, there are also possible strategies to address these cyber threats and technological vulnerabilities, many of which endogenous to the DeFi ecosystem. In what concerns cyber risk, users' technological literacy and awareness play a crucial role.

Another risk lies in the governance structure of DeFi protocols, often in the form of DAOs. While the idea of DAOs is to spread the control over decisions concerning the respective protocol over a large number of users, voting power can easily end up in the hands of a small group of actors, which defeats the basic idea of making decisions as democratic as possible and poses a risk of malicious attacks.

Investor and consumer protection is another vital concern. DeFi allows for highly leveraged trading, while not providing the same safeguards as the traditional financial system. Furthermore, the above-mentioned cyber-attacks can directly affect the end user and there have been numerous cases of market manipulation

[38] Article 140(2)(t) and 142(2)(a) of MiCAR.

and fraudulent conduct. Online platforms and dedicated apps are resorting to gamification of finance, which can spur misrepresentation, misinformation and inappropriate advertising, and thus inadequate financial advice, in a framework where regulatory safeguards for investors and consumers protection are still largely missing. Therefore, investing in financial literacy of citizens is of crucial importance.

DeFi also poses substantial challenges for the prevention of money laundering and terrorist financing. Since users can potentially move assets without proper oversight by using pseudonyms instead of real identities, it becomes very difficult, complex and expensive for competent authorities to identify the source and destination of funds. In addition, the composability and interoperability of DeFi also pose challenges for tracking and monitoring the movement of assets for AML/CTF purposes. The decentralised non-custodial nature of DeFi also triggers ML/TF risks, as it hampers the enforcement of user identity verification and other user-related due diligence.

While DeFi currently does not pose a risk for the traditional payment systems, this could change once it gains popularity and relevance. Given the high level of interconnectedness between different DeFi applications and the level of automatism in place, the impacts of a cyber-attack or of other crisis scenarios could quickly spread and compromise the well-functioning of the payment system or otherwise impact on TradFi markets. Furthermore, the lack of regulation and supervision could lead to information asymmetries, potentially causing substantial losses for consumers and undermining the management of the underlying software system.

At present, DeFi is largely self-referential, operating within its own ecosystem, and thus does not pose a significant threat to monetary policy or overall financial stability. Still, if DeFi experiences significant growth, becomes more interconnected with traditional finance or enables the emergence of sizable reserve-backed stablecoins, risks to monetary policy and financial stability could start to emerge. These include risks known from traditional finance – risk-taking behaviour, liquidity and maturity mismatches, excessive leverage and volatility - which are enhanced by DeFi-specific features. At the current juncture, the most likely risks emanate from stablecoins, which are heavily used in DeFi. In the case of reserve-backed stablecoins, the impact on the reserve assets' price and availability can affect banks' intermediation, monetary policy tools and traditional financial markets. Such would be the case of stablecoins backed by bank deposits and short-term public debt securities.

Finally, DeFi carries a number of legal risks, which are mainly due to the current lack of clear and comprehensive regulation. Traditional bank regulatory frameworks are not adequate to handle DeFi's decentralised and borderless nature, as DeFi operates in a fast-evolving landscape without traditional intermediaries and relies on automated protocols. Additionally, considering current Portuguese regulation on the granting of credit, the performance of credit activities on a professional basis may be considered as non-authorised.

Currently, DeFi is not covered by specific regulation at either the EU or national levels. The known regulatory initiatives have been focused on establishing a clearer structure for crypto-assets and on addressing ML/TF concerns, as is the example, respectively, of MiCAR and of the AML Package. The regulatory challenges posed by DeFi highlight the need for innovative regulatory approaches. Self-regulation could be an interesting possibility to explore, but may not be a silver bullet.

To mitigate legal risks and regulatory issues in DeFi, all parties need to collaborate to understand its characteristics and their potential consequences. This cooperation could lead to the development of practical and effective regulatory frameworks that balance innovation and consumer protection. In addition, international cooperation is crucial to articulate regulations across jurisdictions, ensuring a level playing field for market participants and minimising regulatory arbitrage, while considering national specificities, e.g. regarding the way each jurisdiction regulates financial activity.

The future is still unclear, although there is a consensual recognition of the need to consider a regulatory approach to DeFi. In this regard, a few principles should be kept in mind. Regulators should take a technology-neutral approach, focussing on the specific risks of DeFi and analysing whether existing frameworks can address them, or if there is a need to adjust traditional finance regulations. Authorities should consider that, while DeFi and TradFi activities may have similarities, their underlying technological differences can result in diverse risks and/or require other regulatory solutions. One way of overcoming the difficulties that arise from DeFi's decentralised nature would be to recentralise DeFi protocols in order to have regulatory and supervisory access points. This, however, goes against the original idea of DeFi, and it is not obvious how a careful balance can be struck.

Authorities not only need to monitor developments in the DeFi space but also actively engage with this new market. Monitoring requires appropriate data. Therefore, collecting and sharing data among supervisory authorities is key. National and international collaboration is essential, also considering the cross-sectoral and borderless nature of crypto and DeFi markets. The lack of international coordination could enable regulatory arbitrage.

To conclude, DeFi carries opportunities as well as risks. Regulators will need to strike a careful balance between containing these risks and not hampering innovation and the benefits it may entail.

References

Adrian, Tobias (2022). "Cryptocurrencies and Decentralized Finance." Speech by Tobias Adrian (IMF Financial Counsellor and Director of the Monetary and Capital Markets Department) at BIS 21st Annual Conference.

Allen, Hilary J (2022). "DeFi: Shadow Banking 2.0?" *William & Mary Law Review*, 64, 919.

Aramonte, Sirio, Wenqian Huang, and Andreas Schrimpf (2021). "DeFi risks and the decentralisation illusion." *BIS Quarterly Review*, 6.

Auer, Raphael, Bernhard Haslhofer, Stefan Kitzler, Pietro Saggese, and Friedhelm Victor (2023). "The technology of decentralized finance (DeFi)." *BIS Working Papers*, January 2023(No 1066).

Ayres, Ian and John Braithwaite (1992). *Responsive regulation: Transcending the deregulation debate*. Oxford University Press, USA.

BCBS, Basel Committee on Banking Supervision (2023). "Basel III Monitoring Report."

Black, Julia (1996). "Constitutionalising self-regulation." *The Modern Law Review*, 59, No.1, 24–55.

BoE, Bank of England (2022). "Financial Stability in Focus: Cryptoassets and decentralized finance." *Financial Policy Committee*, March 2022.

Born, Alexandra, Isabella Gschossmann, Alexander Hodbod, Claudia Lambert, and Antonella Pellicani (2022). "Decentralised FinanceâA New Unregulated Non-Bank System?" *ECB Macroprudential Bulletin*, 18.

CCI, Crypto Council for Innovation (2023). "Key elements of an Effective DeFi framework." Tech. rep., Crypto Council for Innovation.

Coase, Ronald H (1993). "The nature of the firm (1937)." *WILLIANSON, OE; WINTER, SG*.

Dell'Erba, M (2018). "Do Smart Contracts Require a New Legal Framework? Regulatory Fragmentation, Self-Regulation, Public Regulation." *SSRN Electronic Journal*.

Demertzis, Maria and Catarina Martins (2023). "Decentralised finance: good technology, bad finance." Tech. rep., Bruegel Policy Brief.

Dotan, Maya, Aviv Yaish, Hsin-Chu Yin, Eytan Tsytkin, and Aviv Zohar (2023). "The vulnerable nature of decentralized governance in defi." In *Proceedings of the 2023 Workshop on Decentralized Finance and Security*, pp. 25–31, arXiv preprint.

ESMA, TRV Risk Analysis (2023). *Decentralised finance in the EU: developments and risks*, vol. October 2023. ESMA, European Securities and Markets Authority.

ESRB, European Systemic Risk Board (2023). "Crypto-assets and decentralised finance." *ESRB Report*.

FATF, Financial Action Task Force (2021). "Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers." *FATF Guidance*, October 2021.

FATF, Financial Action Task Force (2023). "Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers." *FATF Guidance*, June 2023.

Fliche, Olivier, Julien Uri, Mathieu Vileyn, and Fintech-Innovation Hub (2023). "Decentralised or disintermediated finance: what regulatory response?" *Banque de France Discussion Paper*, April 2023.

Freire, João Pedro (2021). *Blockchain e Smart Contracts*. Almedina.

FSA, Danish Financial Supervisory Authority (2024). "Principles for the assessment of decentralisation in the markets for crypto-asset." *FSA Briefing*, June 2024.

FSB, Financial Stability Board (2019). "Decentralised financial technologies: Report on financial stability, regulatory and governance implications." *FSB Report*, June 2019.

FSB, Financial Stability Board (2022). "Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets." *FSB Consultative document*, October 2022.

FSB, Financial Stability Board (2023). "The financial stability risks of decentralised finance." *FSB Report*, February 2023.

Gorjón, Sergio (2023). "Decentralised finance: the latest generation of crypto-assets." *Banco de España Article*, 4.

IMF, International Monetary Fund (2022). "Shockwaves from the War in Ukraine Test the Financial Systemâs Resilience." *IMF Global Financial Stability Report*, April 2022.

IOSCO, International Organization of Securities Commissions (2022). *IOSCO Decentralized Finance Report*, vol. March 2022. International Organization of Securities Commissions.

IOSCO, International Organization of Securities Commissions (2023). *Final Report with Policy Recommendations for Decentralized Finance (DeFi)*. International Organization of Securities Commissions.

Maia, Guilherme and João Vieira dos Santos (2021). "MiCA and DeFi ('Proposal for a Regulation on Market in Crypto-Assets' and 'Decentralised Finance')." *Forthcoming article in "Blockchain and the law: dynamics and dogmatism, current and future"*. Eds: Francisco Pereira Coutinho, Martinho Lucas Pires and Bernardo Barradas.

Makarov, Igor and Antoinette Schoar (2022). "Cryptocurrencies and decentralized finance (DeFi)." *BIS Working paper*, December 2022(No 1061).

Marino, Bill and Ari Juels (2016). "Setting standards for altering and undoing smart contracts." In *Rule Technologies. Research, Tools, and Applications: 10th International Symposium, RuleML 2016, Stony Brook, NY, USA, July 6-9, 2016. Proceedings 10*, pp. 151–166, Springer.

Ocampo, Denise Garcia, Nicola Branzoli, and Luca Cusmano (2023). "Crypto, tokens and DeFi: navigating the regulatory landscape." *FSI Insights on policy implementation*, (49).

OECD, Organisation for Economic Co-operation Development (2022). *Why decentralised finance (DeFi) matters and the policy implications*. OECD.

Ogus, Anthony (1995). “Rethinking self-regulation.” *Oxford Journal of Legal Studies*, 15, 97.

Roukny, Tarik (2022). *Decentralized Finance: information frictions and public policies*. Commission européenne.

Schär, Fabian (2021). “Decentralized finance: On blockchain-and smart contract-based financial markets.” *FRB of St. Louis Review*, Second Quarter 2021.

Shared, Avner and John Sutton (1981). “The self-regulating profession.” *The Review of Economic Studies*, 48(2), 217–234.

US Treasury, U.S. (2023). *Illicit Finance Risk Assessment of Decentralized Finance*. U.S. Department of the Treasury.

WEF, World Economic Forum (2021). “Decentralized finance (DeFi) policy-maker toolkit.” *WEF White Paper*. In collaboration with the Wharton Blockchain and Digital Asset Project.

Wilkins, Carolyn (2022). “Governance of "Decentralised" Finance: Get up, Stand up!” Speech by Carolyn Wilkins (external member of the Bank of England’s Financial Policy Committee) at UCL Centre for Blockchain Technologies.

Appendix A: Protocols enabling lending and borrowing in DeFi

The information presented in the following tables are taken from the protocols' websites.

Table A.1. Characteristics of main protocols for loanable funds

	AAVE	**Maple Finance**	**MakerDAO**
Protocol type	Pooled Lending protocol	2P2 Lending protocol	CDP
Blockchain of deployment	Ethereum	Ethereum and Solana	Ethereum
Protocol's token	AAVE	MPL	MKR
Borrowed Asset	All assets accepted by Governance (mostly Dai and USDC are borrowed).	The pool assets must be accepted by Governance.	DAI (1:1 with USD)

	AAVE	**Maple Finance**	**MakerDAO**
How to borrow	Borrowers must supply assets to be used as collateral. They receive debtTokens (not transferable) representing debt owed to the pool and aTokens representing the funds supplied as collateral.	Borrowers must be companies; Submit Request for a Quote (RFQ) and are subject to due diligence by Pool Delegate. Negotiate interest rate and collateral ratio with Pool Delegate off-chain (legally signed); Submit loan request on-chain and the Pool Delegate creates pool to fund the loan and the repayment schedule starts (interest starts to accrue).	Users can create Dai by locking collateral assets in Maker Vaults.
How to lend (cont.)	Lenders deposit funds in the smart contract and export aTokens which represent supplied funds and accrued yield.	Lenders view listed pools and their features in the protocol's app; when a pool is picked, they deposit funds there in exchange for Pool LP (Liquidity Provider) Tokens representing their share of the lending pool and accruing value from borrower repayment; Each pool is managed by one Pool Delegate; LP Tokens can be sent to other addresses on the pool's allow list.	In this protocol, there are no lenders. The asset borrowed is newly minted by the protocol.

	AAVE	Maple Finance	MakerDAO
How to lend (cont.)		Lending to a permissioned pool (private pool): lenders must submit KYC information to Pool Delegate and be accepted; addresses of accepted lenders are in an on-chain pool-specific allow list.	
Collateral requirements	Collateral can be any asset accepted by AAVE; LTV depends on collateral asset (least volatile assets at 75% and most volatile ones at 40% or 35%).	Collateral ratio is negotiated between the Pool Delegate and the borrower; The collateral asset must be an ERC-20 token. Loans can be undercollateralised.	There is over-collateralization of each Dai created. Collateral can be any asset accepted by "Maker Governance" ("Multi-Collateral Dai (MCD)") The risk parameters of each collateral asset are voted by Governance (i.e. MKR holders).
Loan payments (cont.)	Loans are perpetual, as long as they are sufficiently collateralized; interest accrues with time, decreasing the collateralization of the position; The loan is paid in the same asset of the loan; repayment consists of principal and interest accrued.	- Open-term loans: no explicit maturity, but Pool Delegate can call a loan (by declaring an "Early Default") and borrower has limited time to repay before a default may be initiated; borrower can repay before a call without penalty;	Repayment includes payment of the Dai generated and a Stability Fee.

	AAVE	Maple Finance	MakerDAO
Loan payments (cont.)	Loans can be repaid with collateral or with aTokens.	- Fixed-term loans: have an agreed-upon due date; cannot be called by Pool Delegate; Interest payments are made on a recurring basis and the principal amount is paid at the end of the loan.	Repayment includes payment of the Dai generated and a Stability Fee.
Interest rate (cont.)	- On borrowed funds: interest rate is asset-specific and is fixed or variable; variable rate model: slope on pool's utilization rate is a positive function of the utilization rate; borrowers choose and can change between variable and fixed rate; - On supplied funds: average of fixed and variable rates on borrowed funds deducted by a reserve factor.	Interest rate negotiated between the borrower and the Pool Delegate.	Stability Fee paid in DAI (continually accrues on DAI outstanding).

	AAVE	Maple Finance	MakerDAO
Interest rate (cont.)	aToken holders also receive a share of the Flash Loan fees corresponding to 0.09% of the Flash Loan volume.		
Fees	Fee for Ethereum blockchain usage (paid in ETH); In a liquidation, liquidators buy the collateral asset; they must pay a liquidation penalty (fee).	Fees paid by the borrower: - Origination fees (share of loan amount): Delegation Origination Fee (paid to the Delegate, set on loan level) and Platform Origination Fee (paid to the Protocol's Treasury, set on pool level). - Borrower fees (added to gross interest): Admin Fee (paid to the Delegate, set on loan level) and Platform Fee (paid to the Treasury, set on pool level). - Management Fees (share of gross interest paid by the Borrower): Delegate Management Fee (set on pool level) and Protocol Management Fee (set on pool level).	

	AAVE	**Maple Finance**	**MakerDAO**
Collateral unlocking	Collateral is not locked; rather, collateral is used as liquidity is its pool.	Only fixed-term loans can be collateralized. The borrower can remove collateral if the collateralization ratio is maintained.	Total or part of the collateral can be unlocked back to the user's wallet when the generated Dai and the Stability Fee accrued on the debt are repaid.
Lent funds withdrawal	aTokens can be moved and traded as any other crypto-asset on Ethereum or redeemed subject to pool availability.	Lenders can submit fund withdrawals at any time; withdrawal requests are processed by the Pool Delegate in cycles; If there is not enough liquidity for all withdrawal requests in a cycle, available funds are distributed pro-rata and remaining funds requested move to the following withdrawal window.	
Default (cont.)	Loan Health factor $<$ 1 –$>$ loan liquidation can be initiated; Liquidator claims value of collateral net of up to 50% of outstanding debt, which is repaid, plus Liquidation penalty (bonus for the liquidator).	If borrower fails repayment and does not pay during a grace period, a Default can be triggered (during grace period, borrower must pay Late Fees); In default, the pool value is reduced by the defaulted outstanding debt and accrued interest; A Default triggers a legal recollection process (recourse).	If a Vault's LTV ratio surpasses its liquidation ratio, the vault is automatically liquidated through a collateral auction. In the collateral auction, the protocol sells the collateral in an internal market-based auction and the Dai received is used to pay outstanding debt plus a

	AAVE	Maple Finance	MakerDAO
Default (cont.)	Liquidation penalty is collateral asset-specific. Liquidation threshold is collateral asset-specific (80% for least volatile assets and 65% for most volatile).	- If there is collateral, it is sold and the pool's value is increased by amount recovered in liquidation; collateral liquidation can occur on-chain or OTC; Delegate's first-loss capital[39] is moved into the pool up to the "liquidation maximum"[40] per default; Collateral value and first-loss capital cover fees owed to the protocol before being added to the pool. Any user can be a collateral liquidator. - In uncollateralized loans, only first loss capital covers losses.	Liquidation Penalty[41] that goes into the protocol's buffer (the "Maker Buffer"). Leftover collateral from liquidation auction returned to original collateral owner. i) If auction does not raise enough Dai, deficit becomes protocol's debt, covered by the Maker Buffer. If Maker Buffer does not have enough Dai, a Debt auction is initiated, bidding MKR tokens for Dai (diluting existing MKR holders). ii) If Dai collected in auctions and in the Stability Fee exceed Maker Buffer limit, they are sold in a Surplus auction, bidding Dai for MKR tokens. Loan amount in the LTV ratio: amount of Dai outstanding valued at the Target Price.

[39] First-loss capital: provided solely by the Pool Delegate; it is pool-specific and negotiated between Delegate and protocol's team.

[40] Liquidation maximum: percentage of the Delegate's First-loss capital decided previously for that Delegate.

[41] Liquidation penalty fee is collateral asset-specific and set by MKR voters.

	AAVE	Maple Finance	MakerDAO
Other risk mitigants	- Reserve factor: share of the protocol's interests that goes into the protocol's treasury; applied on collateral assets (10% for least risky assets to 35% for riskiest). - Liquidation Factor: share of the liquidation penalty that goes into a collector contract of the protocol's treasury. - Safety Module: covers the protocol's solvency risk. AAVE holders can stake their AAVE in the protocol's "Safety Module" to give insurance to suppliers, in exchange for staking rewards and fees from the protocol. - Supply cap, Borrow cap, Isolation Mode, Siloed Mode, eMode (Efficient Mode) and custom price oracle. - Smart contract code is public, open-source and audited by third-party auditors.	- List of allowed Pool Delegates coded in smart contract allow list (only Delegates can create pools). - Impairment: Pool Delegate can declare a loan to be impaired; under impairment, lenders can withdraw funds with a penalty, new lenders can deposit into a pool but their lending balance is affected by the impairment; if impaired borrower is able to repay in full, balances of remaining pool depositors brought back to full amount. - Smart contract risk mitigated through internal and external protocol audits. - Undercollateralization compensated by underwriting system of borrowers. - The "Governor" - a special wallet - can pause functionality of the protocol.	Debt ceiling (collateral asset-specific).

	AAVE	**Maple Finance**	**MakerDAO**
Governance	AAVE token holders can vote and decide on Aave Improvement Proposals (AIPs).	MPL holders can participate in governance (voting rights).	MKR holders manage the protocol and the financial risks of Dai through Executive Voting and Governance Polling. MKR voting weight is proportional to amount of MKR staked in the voting contract (DSChief) by the MKR holder.
External players	Price oracles.	Keepers: have incentives to perform liquidations when necessary; Anyone can be a Keeper, but Keeper actions are constrained by Protocol rules.	Keepers (have incentives to buy and sell Dai in Surplus, Debt and Collateral auctions) Oracles (price Oracles and Global Settlers) Maker community members (independent individuals and organizations who provide services to the protocol).
Other	The protocol offers a Flash Loan feature.	Loans may be refinanced; refinancing terms are agreed between borrower and Pool Delegate off-chain. MPL holders can earn fees if they stake MPL into the xMPL protocol revenue contract.	Interest can be earned by locking Dai holdings in Dai Savings Rate (DSR) smart-contracts Interest rate in DSR voted by MKR holders; takes into account market price of Dai. Users can withdraw Dai from DSR at any time.

Table A.3. Characteristics of main protocols for loanable funds

	Clearpool	**Blur (Blend)**	**BendDAO**	**Centrifuge**
Protocol type	Uncollateralized lending	NFT Lending P2P	NFT Lending Peer2Pool	RWA Lending
Blockchain of deployment	Polygon and others	Ethereum	Ethereum	Centrifuge Chain
Protocol's token	CPOOL	BLUR	BEND	CFG
Borrowed Asset	In permissionless pools:USDC or USDT.	ETH	ETH	Stablecoins (eg: DAI)
How to borrow (cont.)	- In permissioned lending: borrowers have to undergo KYC and AML due diligence; borrowers can then launch pools with custom-made terms; After pool creation, the borrower invites	Borrowers look at off-chain offers and pick one; then, they create an on-chain transaction that matches the lender's offer, lock	Borrow positions are tokenized to debtTokens; debtTokens just partly follow the ERC-20 standard, since they are not transferable;	Each pool is connected to a special purpose vehicle (SPV). The owner of the real-world assets ("asset originator") pledges them to the SPV, which has the legal ownership

	Clearpool	Blur (Blend)	BendDAO	Centrifuge
How to borrow (cont.)	other whitelisted institutions to fund the pool. - In permissionless lending: borrowers (institutions) must request to be whitelisted. They will be assessed: KYC and AML conducted by a third-party service provider; borrowers must agree to the protocol's Terms and Conditions; borrowers receive a credit risk score and borrower capacity by the third-party service provider. After this, a liquidity pool is created by the protocol and become listed on a pool list where it can be seen and funded by lenders. If the utilization rate reaches 95% ("High Utilization" state), borrower no longer can take liquidity from the pool, interest continues to accrue and add up to the utilization rate.	their collateral on a vault and send the loan principal from the lender to themselves.	debtTokens accrue interest, accumulating that debt too.	of the assets when these are securitized (this is made off-chain). The SPV wallets convert the assets into NFTs, which are locked in a liquidity pool. Then the SPV takes liquidity from the pool and, in exchange, issues tranche tokens for lenders. The borrower tokenizes her Real World Asset, with enough information about the NFT on-chain, so that it can be priced. The same SPV have have several asset originators.

	Clearpool	Blur (Blend)	BendDAO	Centrifuge
How to lend	- In permissioned lending, lenders have to undergo KYC and AML due diligence; In order to lend, lenders must be whitelisted institutions who have received an invitation to fund a borrower pool and respective borrower and pool terms. Lenders send the loaned assets automatically and directly to the Borrower's wallet address, constrained by the pool terms and supply window. - In permissionless pools, anyone can be a lender. The lender just needs a compatible wallet and funds. The lender must find a pool of a borrower in which she is interested and choose amount of assets to lend in exchange for cpTokens which are pool-specific, represent liquidity supplied to the pool and accrued pool-specific interest. Pools have no limit of liquidity that lenders can deposit.	Lenders make offers of some ETH amount with a certain interest rate, against any NFT of a certain collection; Lenders post these offers on an off-chain offer repository.	Deposited funds in the pool are tokenized to bendTokens which bear interest; bendTokens follow most of ERC-20 standards, having slight modifications; bendTokens are pegged 1:1 to the value of assets deposited in the pool with interest; bendTokens can be stored, transferred or traded; Interest collected by bendTokens reserves is distributed to bendToken holders by continuously increasing their wallet balances.	Lenders have to meet KYC and AML regulations, accredited investor verification and tax procedures. The protocol uses a third party to provide this service to issuers. Lenders deposit funds (stablecoin) in pools by tranches, in exchange for which they receive tranche-specific tokens, which are considered securities. The borrower can specify which accounts are allowed to hold each tranche token of her pool.

	Clearpool	Blur (Blend)	BendDAO	Centrifuge
Collateral requirements	No collateral requirements.	LTV ratio determined by lenders' offers. The collateral asset is an NFT.	Deposited NFTs go into an NFT pool and are converted into boundNFTs. [Collateral is tokenized into boundNFTs (pegged 1:1 to the token of the NFT collateral)]; boundNFTs are non-transferable; Predefined List of accepted collateral assets. Collateral ratio varies with collateral asset (goes from 30% to 60%).	Real world assets are tokenized as NFTs by the legal issuer of the pool (SPV) after being pledged to the latter by the asset originator (the borrower and owner of the asset) and locked in a pool as collateral. The issuer can take financing from the pool up to the value of the NFT.
Loan payments (cont.)	- In permissioned pools, single-lender pools can be rolled over.	Borrowers can repay at any time as long as there is some lender	Overcollateralized loans are perpetual; Loans can only be totally repaid.	The borrower repays principal and interest over time. Each tranche above the junior

	Clearpool	Blur (Blend)	BendDAO	Centrifuge
Loan payments (cont.)	The borrower calls the Roll function and the lender may accept to extend the maturity of the pool or not. - In permissionless pools, the amount and frequency of repayments is chosen by the borrower, conditional on the utilization rate remaining below a Governance-set threshold of 95% ("High Utilization" state).	willing to lend the loan amount against the collateral at some interest rate; Repayment consists of the borrower paying the lender the loan's principal and interest accumulated since the beginning of the loan.	Overcollateralized loans are perpetual; Loans can only be totally repaid.	one has a fixed APR, a position in the waterfall and a subordiantion ratio. The junior tranche is last in the waterfall, does not have a subordination ratio or fixed returns.
Interest rate (cont.)	- In permissioned pools, interest rates are fixed and determined when the pool is created; interest starts to accrue when the funds are transferred from the lender to the borrower. - In permissionless pools, interest starts to accrue when borrower takes funds from pool;	Interest rate is determined by what the lender is willing to offer; The interest rate is fixed until there is a loan auction and the loan passes over to another lender, who may have offered a different interest rate.	Mathematical function specific for each asset pool, which is a function of the utilization rate of the pool.	Every loan accrues interest at the financing fee, which is represented as an Annual Percentage Rate (APR) and compounds interest every second; Different token tranches receive different returns: - Senior token return: the senior token rate (APR); fixed rate.

	Clearpool	Blur (Blend)	BendDAO	Centrifuge
Interest rate (cont.)	In permissionless pools, interest rate is a function of the pool's utilization rate; parameters of interest rate curve provided by Oracles.	Interest rate is determined by what the lender is willing to offer; The interest rate is fixed until there is a loan auction and the loan passes over to another lender, who may have offered a different interest rate. Interest accumulates continuously.	Mathematical function specific for each asset pool, which is a function of the utilization rate of the pool.	- Mezzanine token return: fixed return, expressed as an APR. - Junior token return: usually higher than the Senior token return; it is the spread between the average financing fee on originated assets and the fixed Senior APY rate; Senior APY = APR compounded over one year. - Each tranche above the junior one has a fixed return, expressed as an APR. Different assets can have different financing fees as a function of their risk. The protocol's Financing Fees and the Senior APR are applied only on funds that have been borrowed and not on excess liquidity in the pool.

	Clearpool	Blur (Blend)	BendDAO	Centrifuge
Fees	- In permissioned lending: Origination Fee: sent to Clearpool Treasury and paid by the borrower when she makes the repayment of the loan. Protocol Fee: a percentage of pool interest (set by Governance) goes into the protocol treasury when loan is repaid.	Zero fees for borrowers or lenders.		CFG is used to pay transaction fees.
Collateral unlocking	There is no collateral.	After loan repayment by the borrower, the lender closes the position and releases collateral to be withdrawn by the borrower.	The borrower repays the loan amount, the owed loan is burnt and the collateral is returned to the borrower.	The issuer can unlock the collateral NFT after full repayment; full repayment consists of outstanding amount, which includes accrued interest.

	Clearpool	Blur (Blend)	BendDAO	Centrifuge
Lent funds withdrawal	- In permissioned pools, lenders may request an early withdrawal, but the borrower is not obliged to repay. If the borrower chooses to repay, interest due only accounts from time passes up until then. - In permissionless pools, lenders can redeem cpTokens (principal amount plus accrued interest), subject to funds availability (depends on pool's utilization rate); accrued interest adds to pool's utilization rate; If utilization rate is above 99% ("Warning State"), lenders can no longer withdraw funds from a pool.	Lenders can exit their positions by triggering a Dutch auction to find a new lender at a new rate. If a new lender is found, he pays the old lender the loan and keeps the loan at the new rate. If not, the borrower is liquidated. Instead of an auction, if there is a compatible offer from another lender, the current lender can submit the new lender's offer to the vault and exit the loan.	Depositers can withdraw funds from the pool, burning the equivalent bTokens owned.	Lenders can withdraw funds from pool at any time, following an "Epoch" (decentralized) system, which prioritizes withdrawal requests according to seniority and available liquidity. Lenders lock their tokens in the smart contract and collect the stablecoin back at the current token price. The protocol has a smart contract that computes the present value of outstanding loans in a given pool, which, together with the liquidity of the pool, determines the value of the tranches and therefore the token price at which investors invest and redeem funds.

	Clearpool	**Blur (Blend)**	**BendDAO**	**Centrifuge**
Default	- In permissioned pools, borrowers who cannot repay at the due date will have a penalty interest starting to accrue immediately. - In permissionless pools, if the utilization rate reaches 99% ("Warning state"), neither borrowers nor lenders can remove funds from a pool and the borrower has 120 hours (Grace period) to bring the utilization rate below the "High Utilization" state (95%). Otherwise, the borrower and the pool enter Default. In Default, an auction in the pool's cpTokens is initiated. Bidders must be whitelisted; the borrower cannot participate in the auction.	If a lender triggers an auction in interest rates to find a new lender to the loan and the auction fails, the borrower is liquidated and the lender takes possession of the collateral.	Liquidation occurs through English auctions (highest bidder wins) for the collateral; Liquidation can be triggered when loan's health factor reaches 1. A user can trigger a liquidation through an NFT auction; the borrower has a 24h period to repay the loan. The liquidation threshold is collateral-specific and expressed in percentage points.	Upon default, tranche token holders can only receive any proceeds from a recovery process that is conducted by the borrower. Token value is affected by defaults in a tranched manner: if a loan is not paid and is written off from the pool, this reduces the "net asset value" of the pool and hence the junior token value. Senior token's principal and returns are unaffected by a default as long as the loss of the pool is less than the total junior tranche of the pool. Upon default and after loss absorption by the junior tranche, as long as all subordinated ratios remain intact, the pool continues to work normally, despite the lower junior returns. Token holders have legal recourse over the real-world assets that have been tokenized as NFT collateral.

	Clearpool	Blur (Blend)	BendDAO	Centrifuge
Other risk mitigators	- Protocol's revenue pool: built up with share of each pool's interest; protocol's revenue used for protocol development and CPOOL buybacks on the open market. - Pool's insurance: each pool has an insurance account; insurance account built up with share of interest paid to the pool. When a pool is closed, insurance account converts to protocol revenue, which is then used for CPOOL buybacks.	Among other protocol parameters, governance decided the new lender auction formula.		- Lenders require off-chain information about the collateral. - Minimum subordination ratio: the degree to which more senior tranches are protected from default risk is given by the "subordination ratio", which is the ratio between the sum of the values of subordinated tranches to the value of the pool. If the current subordination ratio falls below the set minimum ratio, certain transactions are not possible (eg. junior tranche redemption or asset origination). The subordination ratio can be restored through, for example, more investments in more junior tranches and the sale of assets.

	Clearpool	Blur (Blend)	BendDAO	Centrifuge
Governance		Governance is pursued by BLUR token holders; They decide on protocol parameters, such as the fees paid by borrowers and lenders to the protocol, the auction maximum accepted interest rate and the auction formula.	BEND holders have governance powers.	CFG holders manage the development of the protocol (voting rights).
External players	Oracles vote on the parameters of the interest rate curves of permissionless pools.	There are no oracles.	Price oracles (Reserves price oracle and NFT price oracle).	

	Clearpool	Blur (Blend)	BendDAO	Centrifuge

Other	CPOOL tokens can be staked in an Oracle pool in exchange for yield.
	Lenders can earn rewards paid in CPOOL.
	In CPOOL buybacks, a percentage of CPOOL acquired is transferred to the rewards pool and the remaining CPOOL is burnt.
	Within permissionless lending, there is the addition of Term pools, which are subpools created by borrowers with fixed maturities and better yields. Lenders to these pools lock their cpTokens in these pools and receive in exchange tpTokens.
		Blend is permissionless;
		There may be a loan refinancing on the borrower's initiative;
		Blend has a BNPL feature;
			It is also possible to borrow NFT-backed loans in the protocol as part of Flash Loans with AAVE, for example. NFT-backed loans taken in this protocol can occur in the context of "Buy with Down Payment", which consists of users making a down payment to buy an NFT, borrowing the remaining from the protocol and in this loan they use the bought NFT as collateral (it works as a mortgage).
			This is different from BNPL, as it does not have the installments.
				The Centrifuge Chain is custom-built for this protocol. Interacting with this protocol is possible from other blockchains. Lenders also receive daily rewards in the protocol's native token CFG. These rewards are independent of the pool's issuer.

Appendix B: State of regulation on selected jurisdictions

The regulatory landscape on DeFi is still very much in development around the globe and the focus has been primarily to provide a clearer framework on specific matters such as crypto-assets or tackle issues related to specific regulatory topics such as AML/CTF.

- **Europe**

In line with this, at European level, there is not yet a regulatory framework specifically applicable to DeFi services, although the European Commission already approved, as part of the Digital Finance Package, regulations on crypto-assets,[42] digital operational resilience[43] and a pilot regime on distributed ledger technology (DLT) infrastructures.[44]

DeFi is not expressly covered by any of the above regulatory instruments, largely due to its technological and operational specificities. As expressed by the ECB (Born *et al.* 2022): "*[t]he lack of traditional centralized entry points for regulation and its opaque and anonymous nature pose challenges for policymakers in terms of enforcement and effective regulation and supervision*".

The legislator's unwillingness (for the moment) to regulate DeFi is understandable, given that attempting to regulate a volatile subject matter such as DeFi may render to be premature and lead to an unsuitable legal framework that ultimately hinders the development of DeFi projects in the market.

Even if the European Regulation on Markets in Crypto-Assets ("MiCAR") may be perceived by some as the natural framework for DeFi matters, the reality is that fully decentralised provision of services, such as DeFi, is out of the scope of MiCAR. Pursuant to Recital 22 of MiCAR, "*[t]his Regulation should apply to natural and legal persons and certain other undertakings and to the crypto-asset services and activities performed, provided or controlled, directly or indirectly, by them, including when part of such activities or services is performed in a decentralised manner. Where crypto-asset services are provided in a fully decentralised manner without any intermediary, they should not fall within the scope of this Regulation*" (emphasis added).

MiCAR is, in fact, applicable to "(...) *natural and legal persons and certain other undertakings that are engaged in the issuance, offer to the public and admission to trading of crypto-assets or that provide services related to crypto-assets in the Union*" (cf. Article 2(1) of MiCAR).

[42] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets.

[43] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector ("DORA Regulation").

[44] Regulation of the European Parliament and of the Council of 30 May 2022on a pilot regime for market infrastructures based on distributed ledger technology.

In line with the above, and as referred by Maia and Vieira dos Santos (2021), "(. . .) *a problem arises with the relation between DeFi and MiCA, which is the fact that, in DeFi, the operation of services is supposed to be decentralised and not controlled by one entity or a small group of entities and the obligation of always having an issuer or service providers that are legal entities responsible for complying with MiCA provisions. MiCA only applies to natural and legal persons and the activities, issuances, and services performed and provided by them. In some DeFi projects, it seems a stretch to consider that exists a natural or legal person who performs or provides those activities*".

The same Authors note, nonetheless, that some DeFi platforms exhibit some degree of centralization – e.g., concentration of voting rights, golden tokens, and control by developer teams -, which theoretically implies the presence of an identifiable intermediary that could be the liable legal entity for the purpose of MiCAR.

In any case, regulatory gaps related to DeFi should keep being monitored to bring those situations into the regulatory perimeter. In fact, MiCAR expressly foresees that the European Commission, after having consulted EBA and ESMA, presents a report to the European Parliament and the Council on the effective application of said Regulation, by 30 June 2027, and an interim report, by 30 June 2025, and if appropriate, they should be accompanied by legislative proposals. Among other subjects, these reports shall encompass a thorough "*assessment of the development of decentralised finance in markets in crypto-assets and of the appropriate regulatory treatment of decentralised crypto-asset systems*".[45]

Additionally, by 30 December 2024, and after consulting EBA and ESMA, the European Commission shall present a comprehensive report to the European Parliament and the Council, containing, among other matters, "*an assessment of the development of decentralised-finance 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 decentralised finance*".[46]

- **United States**

The Securities and Exchange Commission ("SEC") has proposed in 2023 to amend Rule 3b-16 under the Securities Exchange Act of 1934 ("Exchange Act"), which defines certain terms used in the statutory definition of "*exchange*" under Section 3(a)(1) of the Exchange Act. The Commission had initially proposed the amendments in January 2022, aiming to expand the definition of the word "*exchange*" to capture a broader swath of trading activity in the U.S. However, in

[45] Cf. Article 140(2)(t) of MiCAR.

[46] Cf. Article 142(2)(a) of MiCAR.

April 2023 the Commission reopened the proposal to explicitly include platforms for crypto transactions in the regulated perimeter.[47]

This re-write of the Commission's exchange proposal intends to explicitly absorb DeFi into the world of exchanges subject to SEC rules and oversight. The Commission believes that an updated rule would help modernize the securities regulator's approach to the changing markets.

In May 2024, the U.S. House of Representatives passed the "*Financial Innovation and Technology for the 21st Century Act*", as an important first step towards achieving regulatory clarity for digital assets. According to Chairman Patrick McHenry, it "*provides the regulatory clarity and robust consumer protections necessary for the digital asset ecosystem to thrive in the United States.*", by establishing clear and functional federal requirements over digital asset markets.[48]

- **United Kingdom**

In March 2022 the Bank of England's Financial Policy Committee (FPC) issued a report on crypto-assets and DeFi setting out the FPC's view on the financial stability implications from crypto and DeFi and the appropriate regulatory response.[49] Even though the FPC considers the risks associated with crypto and DeFi to the financial stability to be currently limited, it recognizes their potential to increase, while identifying several potential challenges around systemic institutions, operational risks, growth of activity outside the regulatory perimeter and difficulties associated with regulating new forms of firms and business models.

It also states that "*The FPC is of the view that as cryptoassets and DeFi grow and develop, enhanced regulatory and law enforcement frameworks are needed, both domestically and at a global level. These frameworks should address developments in cryptoasset markets and activities, to encourage sustainable innovation, and maintain broader trust and integrity in the financial system*".

[47] SEC Press Release, April 14, 2023.

[48] Financial Services Committee Press Release, May 22, 2024.

[49] Financial Policy Committee, "*Financial Stability in focus: Cryptoassets and decentralised finance*", March 2022.

Appendix C: Regulating virtual assets service providers

- **Financial Action Task Force**

Facing the threat of criminal and terrorist misuse of virtual assets, in October 2018, the Financial Action Task Force ("FATF")[50] amended Recommendation 15, extending the application of its international Recommendations[51] to virtual assets and VASPs, whose definitions were added to the FATF Glossary.

Consequently, in June 2019, the FATF adopted and issued an "*Interpretive Note to Recommendation 15 on New Technologies (INR. 15)*", describing and clarifying how countries and obliged entities must comply with the relevant FATF Recommendations to prevent the misuse of virtual assets for ML/TF purposes, as well as the financing of proliferation of weapons of mass destruction.

The new FATF Recommendations (FATF 2012, updated February 2023) aimed for an active and effective regulation of virtual exchanges, defining virtual assets as "*a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes*" and VASPs as "*any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:*

i. exchange between virtual assets and fiat currencies;

ii. exchange between one or more forms of virtual assets;

iii. transfer of virtual assets;

iv. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and

v. participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset."

In short, countries are required to "*assess and mitigate their risks associated with virtual asset activities and service providers; license or register service providers and subject them to supervision or monitoring by competent national authorities—(notably, countries will not be permitted to rely on a self-regulatory body for supervision or monitoring)—and implement sanctions and other enforcement measures when service providers fail to comply with their AML/CFT obligations; and underscore the importance of international cooperation*".[52]

[50] FATF is an inter-governmental body that, among other pursuits, sets international standards directed at ML/TF prevention and works as a policy-making body, aiming to generate the necessary political will to bring about national legislative and regulatory reforms in these areas. Portugal has been a member of FATF since 1991.

[51] Also often referred to as Standards, they set out a framework of measures which countries should implement to combat ML/TF, as well as the financing of proliferation of weapons of mass destruction. The FATF Standards comprise the Recommendations themselves and their Interpretive Notes, together with the applicable definitions in the Glossary.

[52] Countries could decide to prohibit altogether some virtual asset activities, based on their own assessment of the risks and regulatory context, or in order to support other policy goals, as per the *"Public Statement on Virtual Assets and Related Providers"*, FATF, 21 June 2019.

Furthermore, FATF required countries to ensure that VASPs also assessed and mitigated their ML/TF risks and implemented all applicable AML/CFT preventive measures under the FATF Recommendations, including customer due diligence, record-keeping, suspicious transaction reporting, and screening all transactions for compliance with targeted financial sanctions, among other measures.

Building upon this, FATF also published, in 2019, the *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, updated on October 2021, to support providers of virtual asset products and services in understanding and complying with their AML/CTF obligations.

In the Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, FATF directly addresses DeFi, stating that a "*DeFi application (i.e. the software program) is not a VASP under the FATF standards, as the Standards do not apply to underlying software or technology", but safeguards, however, that "creators, owners and operators or some other persons who maintain control or sufficient influence in the DeFi arrangements, even if those arrangements seem decentralized, may fall under the FATF definition of a VASP where they are providing or actively facilitating VASP services*".

Most importantly, FATF stresses the importance of the services and activities with virtual assets that are truly carried out and the profile of the entity, rather than the "DeFi" label, clarifying that "*countries will need to evaluate the facts and circumstances of each individual situation to determine whether there is an identifiable person(s), whether legal or natural, providing a covered service. Marketing terms or self-identification as a DeFi is not determinative, nor is the specific technology involved in determining if its owner or operator is a VASP. [. . .] It seems quite common for DeFi arrangements to call themselves decentralized when they actually include a person with control or sufficient influence, and jurisdictions should apply the VASP definition without respect to self-description.*".[53]

- **Europe**

Aiming to monitor the widespread use of virtual assets, the EU published Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 (the "5AMLD"), amending Directive (EU) 2015/849 of the European Parliament and of the Council, of 20 May 2015 on the prevention of the use of the financial system for the purpose of prevention of ML/TF ("4AMLD"), introducing the "*providers engaged in exchange services between virtual currencies and fiat currencies*" and "*custodian wallet providers*" in the list of entities obliged to comply with the provisions of the 4AMLD and subjecting such providers to prior registration and fit and proper checks of the members of the management body and beneficial owners with the respective competent authority.

[53] See paragraphs 67 and 68 of the *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, FATF, 2021.

Although 5AMLD "*virtual currencies*" definition is broad[54] and, as highlighted by Recital 10, aims to "*cover all the potential uses of virtual currencies*", the range of activities is less comprehensive when compared to the FATF definition, and does not cover, namely, direct exchanges between virtual assets.[55]

DeFi platforms are not specifically addressed in AMLD5, since the application of its rules depends on whether the virtual currencies activities are undertaken by an intermediary ("*an obliged entity*").

The 5AMLD acknowledges, in Recital 10, that "*The inclusion of providers engaged in exchange services between virtual currencies and fiat currencies and custodian wallet providers will not entirely address the issue of anonymity attached to virtual currency transactions, as a large part of the virtual currency environment will remain anonymous because users can also transact without such providers*".

- **Portugal**

The 5AMLD was internally transposed by Law nº. 58/2020 of August 31 ("Law nº. 58/2020"), namely amending Law nº. 83/2017 of August 18 ("Law nº. 83/2017"), which sets forth AML/CTF measures and partially transposed, among other legal acts, the 4AMLD. As of September 1, 2020, VASPs are obliged entities subject to AML/CFT rules and the supervision of Banco de Portugal.[56]

It should be noted that 4AMLD establishes a "*minimum harmonization*" regime,[57] expressly allowing Member States to adopt a more rigorous national regime than the one provided for in that Directive. The option taken by Portugal with Law nº. 58/2020 was to go beyond what was foreseen in AMLD5 and expand the scope of activities with virtual assets subject to AML/CFT rules, making it

[54] As previously addressed on the Occasional paper on crypto-assets (Banco de Portugal, 2020) "*This definition has the merit of encompassing the different "virtual currencies", the current and future ones. This is the case not only because it presents itself as a technologically neutral definition – and, therefore, capable of accompanying pari passu the technological progress in this field – but, above all, because it is potentially applicable to the various possible uses of "virtual currencies"*".

[55] "*However, as has been said – and without prejudice to the essentiality of the contribution made by the 5AMLD – the question of the anonymity (total or partial) for certain crypto-assets, which are particularly suited to use for illicit purposes, has not been fully resolved. First, the 5AMLD does not cover certain operations involving crypto-assets, such as direct exchange between crypto-assets, the acquisition of goods and services with crypto-assets without involving the exchange with fiat money or the use of custodian wallet providers. Second, certain relevant players in the crypto-assets market have not been included in the list of obligated entities, such as, for example, mining and trading platforms*", Occasional paper on crypto-assets (Banco de Portugal, 2020).

[56] As per Articles 2(1)(ll) and (mm), 4(1)(o), 112-A, 112-B, 89(1)(j) and 169-A(1)(ccc) of Law nº. 83/2017.

[57] See Article 5 of 4AMLD. This means that, when transposing the 4AMLD (and its subsequent amendments) into their internal legal order, the Member States are able, namely, to expand the range of activities with virtual assets subject to AML/CTF rules (and, consequently, of VASPs), as well as to expand the concept of relevant virtual assets for this purpose, in view of what is provided for in AMLD4, as amended by AMLD5.

aligned with what is provided for in the FATF Recommendations, as mentioned above.[58]

Consequently, Law nº. 58/2020 determines that all VASPs engaged in the exchange services between virtual assets and fiat currencies or between one or more forms of virtual assets, transfer services of virtual assets and safekeeping and/or administration of virtual assets or instruments that enable the control, ownership, storage or transfer of such assets, including private encrypted keys, when these activities are carried out within Portuguese territory and on behalf of a customer, are subject to prior registration with Banco de Portugal and to its supervision (including where the applicant exercises another profession or activity covered by Law nº. 83/2017).[59] This supervision from Banco de Portugal is limited solely to AML/CFT purposes, and does not extend to other areas (prudential, market conduct or other nature).

It should be noted that VASPs are currently considered by Law nº. 58/2020 as non-financial obliged entities.

Since September 2020, Banco de Portugal has issued two regulations regarding VASPs, both complementing Law nº. 83/2017 at a regulatory level: Notice nº. 3/2021 of 23 of April, regulating VASPs initial registration requests and any subsequent amendment requests to the registration (in force since April 24, 2021), and Notice nº. 1/2023 of January 24, regulating compliance by VASPs with the preventive AML/CFT duties (in force since July 15, 2023).

[58] The option taken was to subject to the national AML/CFT rules not only those providers engaged in exchange services between virtual assets and fiat money and custodian wallet providers, but also those providing exchange services between one or more forms of virtual as-sets and transfer of virtual assets.

[59] As per Articles 2(1)(ll) and (mm), 4(1)(o) 112-A and 112-B of Law nº. 83/2017.
Also, beneficial owners, members of the management and supervisory bodies and other per-sons occupying top management positions in the VASP are subject to a fit and proper assessment by Banco de Portugal (Article 112-A(3) and 111 of Law nº. 83/2017).

Appendix D: Uniswap Governance

Uniswap, a decentralised exchange (DEX) protocol, has played a prominent role in the DeFi ecosystem's growth and development since its inception in 2018. In 2020, it has launched UNI token giving users, liquidity providers and community members with ownership and governance rights over the Uniswap protocol. While functioning as a Decentralised Autonomous Organisation (DAO), Uniswap aims to embody the principles of self-governance, where token holders actively participate in decision-making processes. As a major player in the decentralised finance space, Uniswap is an example of how to use a DAO to propose and adopt self-regulatory measures that aim to enhance security and user confidence. This section explores how Uniswap, as a DAO, integrates code upgrades and bug bounty programs as integral components of its governance framework, aiming to promote a secure and user-empowered DeFi environment.

- **Code Upgrades for Enhanced Security**

Uniswap has a proven track record of implementing code upgrades to enhance the security and functionality of its platform. For instance, in May 2021, Uniswap conducted a governance vote to add a new fee tier to its fee structure. The proposal was to introduce an additional fee tier of 1 basis point (0.01%) on Uniswap trades. The purpose of this fee tier was to generate revenue for the Uniswap treasury, which could be used to fund future development and community initiatives.

Ultimately, the proposal was approved through the governance voting process, and the 'Add 1 Basis Point Fee Tier' was implemented as part of Uniswap's fee structure. This example showcases the decentralised governance model of Uniswap as a DAO and how the community's participation influences decisions on protocol upgrades and changes in the platform's fee structure.[60]

- **Incentivising Ethical Hacking through Bug Bounties**

As a DAO, Uniswap actively encourages ethical hackers and security researchers to participate in its bug bounty program,[61] a crucial element of its self-regulatory initiatives. In one instance, a white-hat hacker[62] identified and disclosed a vulnerability in Uniswap's codebase. The vulnerability, if exploited, could have led to significant potential financial losses for users. By reporting the issue through the bug bounty program, the hacker received a reward and contributed to Uniswap's commitment to proactive security measures. Such programs promote a

[60] Please refer to Uniswap Interface – Add 1 Basis Point Fee Tier governance proposal for a more comprehensive read.

[61] As exemplified in this governance proposal by Uniswap community to increase UNI grants program budget - UGP v3 Bug Bounty contribution - Temperature Check - Uniswap Governance.

[62] A white-hat hacker is someone who uses their cybersecurity expertise for ethical purposes, often working to protect individuals and organizations from cyber threats and promote online safety.

collaborative approach to threat identification, fortifying Uniswap's security posture and safeguarding user assets.

However, it is imperative not to overlook the possibility that a hacker may exploit these weaknesses and act unethically, showing no collaboration towards the DAO. The actions of such a hacker will largely depend on their ethical disposition and the incentives at play, such as the rewards offered through the bug bounty program versus the potential gains from a genuine hack. As a precaution, bug bounty programs often operate on a test environment,[63] where no real funds are at risk, providing a platform for "proof-of-concept" quasi-real technical experiences while eliminating the possibility of malicious attacks on actual funds.

- **A Collective Endeavor for a Secure and User-Empowered Ecosystem**

The integration of community governance, code upgrades, and bug bounties showcases Uniswap's dedication to self-regulation and user protection as a DAO. By empowering its community members to participate in governance decisions, Uniswap intends to align its trajectory with the collective interests of its users. Through these collective efforts, Uniswap, as a DAO, fosters a secure and robust DeFi ecosystem, upholding the core tenets of decentralisation and user empowerment.

This collective participation, however, deserves a closer look as it is obvious that its democratisation process differs from a standard political one. The reality is that the more Uniswap tokens a given investor has, the more votes it can use for any given decision-making process. Also, any initiative to employ a change of whatever levels of the platform are also only possible for big holders of the governance token of Uniswap.

- **In short**

Uniswap, functioning as a DAO with its governance protocol, embodies a community-led self-regulatory approach within the DeFi ecosystem. By allowing token holders to actively participate in decision-making processes, Uniswap promotes democratisation and inclusivity in shaping the platform's trajectory. However, it is crucial to acknowledge that this governance model, where voting power correlates with token ownership, may introduce challenges concerning true decentralisation and potential concentration of power.

[63] GitHub - Uniswap/v2-core: Core smart contracts of Uniswap V2. Platform in which UniSwap deploys the code it wants to be exploited, ensuring no chance for malicious action on such a test environment.

Occasional Papers

2021

1|21 Assessment of the exposure of the portuguese banking system to non-financial corporations sensitive to climate transition risks
Ricardo Marques | Ana Margarida Carvalho

2022

1|22 Climate change and the economy: an introduction
Bernardino Adão | António Antunes | Miguel Gouveia | Nuno Lourenço | João Valle e Azevedo

2|22 Um Indicador Compósito de Competitividade das Empresas
Mário Lourenço | Cloé Magalhães | Ana Martins | Fernando Martins | Eva Pereira Manuel Pereira | Rita Ponte | Hugo Reis

3|22 Modelling the financial situation of Portuguese firms using micro-data: a simulation for the COVID-19 pandemic
Carla Marques | Francisco Augusto | Ricardo Martinho

4|22 An economic estimate of capital stock at the firm level for Portugal
Ana Fontoura Gouveia | Manuel Coutinho Pereira

5|22 The Banco de Portugal balance sheet expansion during the last two decades: a monetary policy perspective
Joana Sousa-Leite | Diana Correia | Cristina Coutinho | Carmen Camacho

2023

1|23 Occasional paper on Stablecoins
Banco de Portugal working group on crypto-assets

2024

1|24 Policies to tackle energy poverty: the case of Portugal
Ana Fontoura Gouveia | Sónia Félix

2|24 Occasional paper on Decentralised Finance
João Almeida | Joel Alves | Carlos Bettencourt | Maria Bettencourt |Madalena Borges | Filipa Castilho | Sónia Correia | Gisela Fonseca | Mariana Júdice | André Leal | Afonso Marques | Carla Marques | Carlos Martins | Katja Neugebauer | Anaísa Oliveira | Céline Pereira | Joana Pratas | Leonor Queiró | Ricardo Sá | Joana Santos | Dina Teixeira | Pedro Tomé | Isabel Vasconcelos