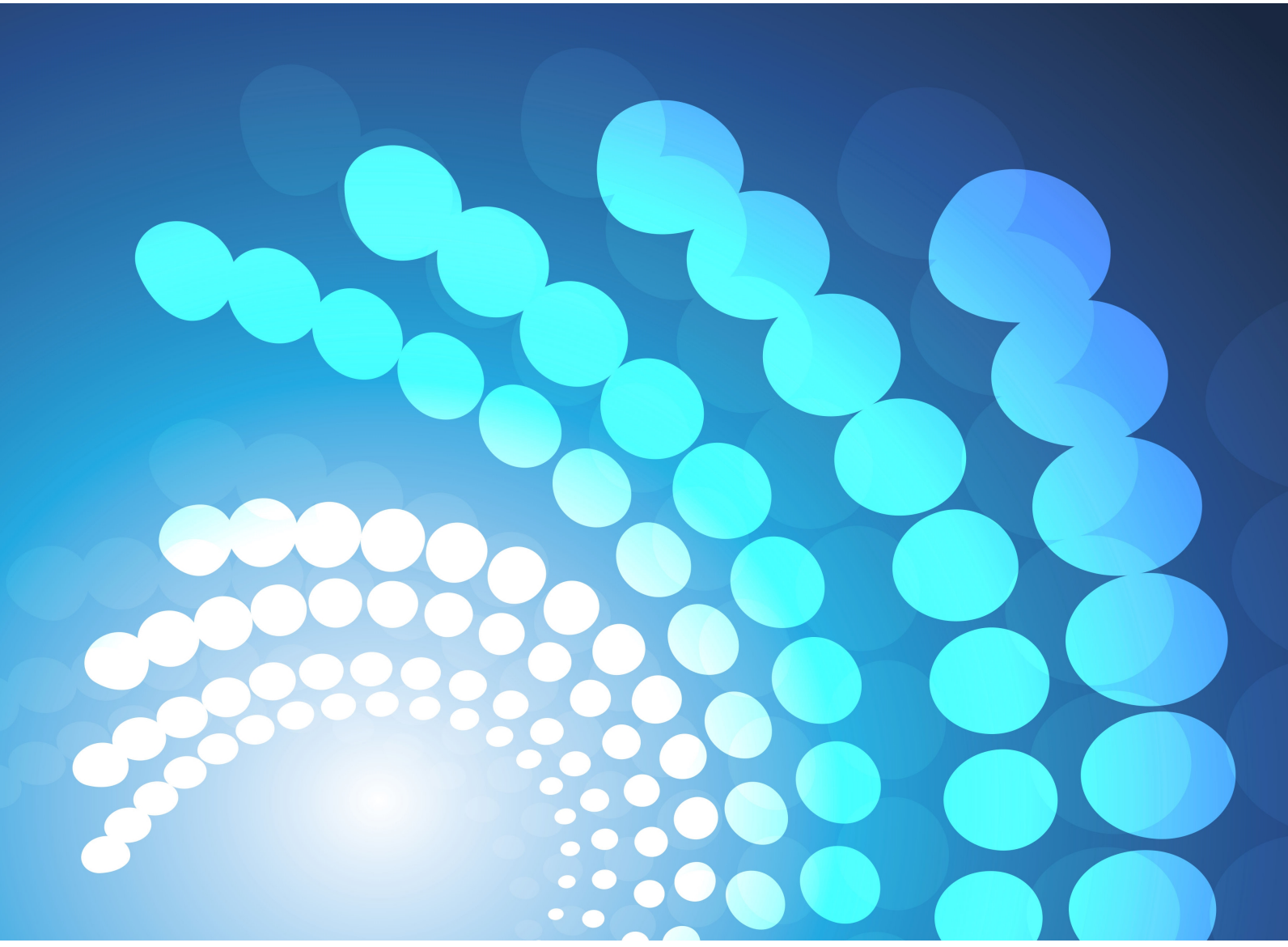
Why Decentralised Finance (DeFi) Matters and the Policy Implications



OECD

Why Decentralised Finance (DeFi) Matters and the Policy Implications

OECD (2022), Why Decentralised Finance (DeFi) Matters and the Policy Implications, OECD Paris, Why-Decentralised-Finance-DeFi-Matters-and-the-Policy-Implications.htm.

Preface

Decentralised Finance or 'DeFi' is an effort to replicate certain functions of the traditional financial system in an open, decentralised, permissionless and autonomous way, based on blockchains. As with any distributed ledger technology (DLT)-based application, DeFi could potentially offer efficiencies driven by automation and disintermediation powered by blockchains and smart contracts.

At the same time, DeFi gives rise to a number of risks for markets and their participants. The provision of financial services by DeFi applications in ways that do not comply with financial regulations expose retail and institutional participants to risks. These risks are related to excess volatility, unregulated leverage and other forms of regulatory arbitrage, governance-related risks, market manipulation, risk of illicit finance or outright fraud. Collectively, these activities could undermine investor confidence and market integrity.

The growing application of DeFi and its increasing interconnectedness with traditional markets presents an urgent challenge for policy makers seeking to maximise DeFi's potential efficiencies for financial markets, while managing risks. The institutionalisation of crypto-assets is growing. The market cap of stablecoins issued by the largest issuers exceeded USD 150 billion at the end of 2021, reflecting a nearly 500 percent increase over the last year, with DeFi recording a 50-fold increase over the same period, albeit from a very low level.

This trend reflects the increase in asset owners searching for yield in an ultra-low rate environment, or joining these markets for fear of missing out. The increasing institutional investor interest in crypto-assets, coupled with the heavy use of stablecoins in DeFi protocols, is also sharply increasing interconnectedness between traditional and decentralised financial markets. The increase in the use of stablecoins as collateral or as the bridge between DeFi and traditional finance could arguably increase adoption of DeFi, while at the same time constitutes one of the greatest points of vulnerability of the DeFi market and a potential channel of risk transmission to the traditional financial markets.

These trends are requiring policy makers to reconsider the conventional oversight framework that was built with intermediaries at its core, given the absence of single regulatory and supervisory access points in decentralised systems. Regulatory compliance of DeFi protocols may be further obstructed by their global reach and operation. These protocols have no defined jurisdiction and geographical location for their operations, making it difficult for supervisory authorities to establish jurisdiction. This jurisdictional uncertainty challenges enforcement, particularly given the speed and ease with which financial service providers are able to change locations in response to actions of authorities.

Nevertheless, supervisory authorities and international standard-setters have a role in assessing risks involved in DeFi, exploring ways to enforce existing rules in decentralised structures, and addressing any regulatory gaps where these may exist.

These efforts should be supported by the promotion of soft-law instruments, such as recommendations, to raise awareness and good practices. It is crucial that we promote greater international policy collaboration and discussion to overcome these challenges, particularly at the cross-border level, and to avoid regulatory arbitrage. A multi-stakeholder dialogue and collaboration is warranted between all parties involved in decentralised finance, including the engineering and software development communities.

The OECD and its Committee on Financial Markets have assessed, for the past few years, the impact of digitalisation in finance, with the foresight to understand and assess DLT-based applications in finance well before they become a pressing concern for policy makers. The OECD remains committed to exploring how to foster the benefits of digitalisation for financial markets and their participants, while proactively addressing the prudential and potentially systemic risks emerging from applications such as DeFi.

Yoshiki Takeuchi

OECD Deputy Secretary-General

Table of contents

FIGURES

Acknowledgements

This publication provides an explanation of DeFi and its applications and then describes the evolution of DeFi markets to date. It explores the benefits and risks of DeFi and the DeFi/CeFi intersection and puts forward policy considerations.

The report has been drafted by *Iota Kaousar Nassr* under the supervision of *Robert Patalano* from the Division of Financial Markets of the OECD Directorate for Financial and Enterprise Affairs. *Christophe Debonneuil* provided market data analytics and *Pamela Duffin* provided editorial and communication support.

The report supports the work of the OECD Committee on Financial Markets and is a product of its Expert Group on Finance and Digitalisation, both chaired by *Aerdt Houben*. It was first discussed by the Expert Group in April 2021 and then approved by the Committee in October 2022.

The author gratefully acknowledges valuable input and constructive feedback provided by the following individuals and organisations: *Béranger Butruille*, Banque de France; *Anne Chone* and *Claudia Guagliano*, European Securities and Markets Authority (ESMA); *Nancy Doyle*, US Commodity Futures Trading Commission; *Inês Drumond*, Banco de Portugal; *Adam Głogowski* and *Paweł Pisany*, National Bank of Poland; *Peter Grills*, US Treasury; *Oliver Hossfeld* and *Bernd Auras*, Deutsche Bundesbank; *Eleftheria Kostika*, Bank of Greece; *Antonina Levashenko* and *Ivan Ermokhin*, Russia - OECD Centre RANEPA; *Alex Ivančo*, Ministry of Finance of the Czech Republic; *Irina Mnohoghitnei* and *Teresa Cascino*, Bank of England; *Benjamin Müller*, Swiss National Bank; *Borut Poljšak*, Bank of Slovenia; *Mai Santamaria*, Department of Finance, Ireland; *Akiko Shintani*, Permanent Delegation of Japan to the OECD and *Ryosuke Ushida*, Financial Services Agency, Japan; *Giuseppe Grande*, *Ilaria Supino*, *Giuseppe Ferrero*, *Paola Masi*, *Silvia Vori*, *Marco Bevilacqua*, *Concetta Galasso* and *Vittorio Tortorici*, Banca d'Italia; *Nadia Linciano*, Commissione Nazionale per le Società e la Borsa (CONSOB) Italy, *Gian Paolo Ruggiero*, Ministry of Finance, Italy; *Giuseppa Bentivegna*, Istituto per la Vigilanza sulle Assicurazioni (IVASS), Italy. The report has also benefited from views and input provided by academia and the industry.

The report contributes to the horizontal OECD Going Digital project which provides policy makers with tools to help economies and societies prosper in an increasingly digital and data-driven world. For more information, visit www.oecd.org/going-digital.

Executive Summary

Decentralised Finance or 'DeFi' is the latest development in the crypto-asset space, and claims to replicate the traditional financial system in an open, decentralised, permissionless and autonomous way, through applications built mainly on the Ethereum blockchain network. Collateralised lending is the fastest growing DeFi product accounting for more than half of the value of crypto-assets locked in DeFi applications[1] at the time of writing of this report.[2] The second largest activity involves decentralised exchanges (DEX), while other applications offer derivatives and synthetics; asset management; insurance; payments; and prediction markets.

DeFi lending activities try to mirror market-based lending (securities lending, repos) rather than traditional consumer/retail bank lending, as most activity involves collateralised lending.[3] In particular, yield farming or liquidity mining is a process allowing DeFi users[4] to lock up their crypto-asset holdings in applications and generate rewards in exchange for the provision of liquidity to the system (interest or new tokens issued by the protocol). This is a key difference to traditional lending activity, as DeFi users essentially use such protocols to leverage their crypto-assets or lock them in DeFi protocols allowing others to borrow them for leverage, in exchange for some remuneration.

While DeFi is built upon distributed ledger technology (DLT) applications, DLT-based financial applications are not by default part of DeFi. The degree of decentralisation varies from one DeFi project to another and in many cases depends on the stage of development of the application. The key defining features used in this note to describe DeFi projects include its non-custodial nature (i.e. no central authority or other intermediary gets access or control over participants' digital assets), community-driven governance (relying on participants for decision-making) and composability (i.e. components of DeFi are pieced together to create new products).[5] Given the recent exuberance around DeFi, a lot of start-ups and projects arbitrarily market themselves as DeFi without being truly decentralised.

The DeFi market started making headlines in the summer of 2020, when a number of DeFi applications appeared to gain traction with users, and has since grown to a multiple of its initial size. The total value of crypto-assets locked in DeFi applications built on Ethereum blockchains as of November 2021 reached

[1] DeFi applications are otherwise called 'Dapps'.

[2] 53% of total value locked (TVL) in DeFi as of 14.06.2021, based on data from Defipulse.com. It should be noted that DeFi market data are provided by industry data sources that are unverified and could be unreliable.

[3] Uncollateralised lending is possible in DeFi through flash loans, which enable users to borrow and repay the loan to the pool in the same single transaction, but these are instantaneous transactions not comparable to traditional lending.

[4] DeFi users and DeFi participants are terms used interchangeably in this report.

[5] That said, this note does not exclude various DeFi protocols that are not truly decentralised/self-governed (e.g. where developers still have key access/some level of control).

USD 100bn from less than USD 2bn in July 2020a 50-fold increase[6]). There do not appear to be fundamental drivers of the surge in the price of DeFi tokens in what is clearly a market driven by speculation given the very high returns offered, fear of missing out and recycling of profits from other crypto-asset activity. Feedback loops exist between the prices of main crypto-assets (Bitcoin, ETH), with some investors joining this market in a search for yield or for what they perceive as an alternative inflation hedge, despite any evidence of crypto-asset performance during inflationary periods. For these reasons, the high volatility of major crypto-asset prices has contributed to the fragility of the DeFi market. The incidence and magnitude of exploits in DeFi applications add to such fragility; it is estimated that c. USD 1.4 billion was taken from DeFi protocols through exploits[7] and bugs in the period January – November 2021 (The Block, 2021[1]).

Although the size of the DeFi market itself is small relative to the wider market for crypto-assets at this stage, the DeFi space is still worth scrutinising due to its rapid growth within the volatile crypto-asset markets, attraction of an increasing number of retail and institutional investors and associated risks such as the use of leverage. As crypto-asset activity is increasingly becoming mainstream, the boundaries of the two systems become more porous, and the increased interconnectedness of DeFi with traditional financial markets may give rise to potential risks of spillovers to major financial markets and the real economy. Such risks are exacerbated by the extreme price volatility of main crypto-assets (Bitcoin, Ether); the recycling or reinvestment of profits in the DeFi space and the re-hypothecation of participants' assets in multiple DeFi applications at the same time.

DeFi applications have the potential to provide benefits to financial market participants in terms of speed of execution and transaction costs, driven by the efficiencies produced by DLT-technological innovation and disintermediation of third parties replaced by software code of smart contracts.[8] DeFi could possibly allow for a more equitable participation of users in markets depending on the design of governance arrangements. Given the open source nature of protocols, DeFi may promote innovation in financial services and could have some potential to promote financial inclusion depending on the design and transaction arrangements (e.g. fees charged)[9].

At the same time, DeFi applications give rise to important risks and challenges for participants and the markets, which call for policy consideration and possible action. These include the risk of money laundering, terrorist financing or other illicit use due to the lack of AML/CFT checks in most DeFi applications; the possibility to engage in almost unlimited leveraged trading; potential greater procyclicality and new forms of concentration risks that could give rise to financial stability vulnerabilities; the provision of financial services in a non-compliant manner exposing participants and the markets to risks related to market integrity and consumer protection and providing room for regulatory arbitrage by DeFi players; potential gaps in the regulatory/supervisory framework which may stem from the novel characteristics of financial service provision in decentralised systems; and the lack of traditional regulatory safeguards for

[6] Source: defipulse.com for DeFi applications built only on the Ethereum blockchain. DeFi applications are increasingly being built on alternative blockchains (e.g. Solana, Avalanche). It should be noted that sources vary widely and metrics on the same metrics depending on the source. It should also be noted that the price of most of the crypto-assets underlying DeFi applications have massively appreciated in the same period.

[7] Exploits are bad actor attempts to manipulate DeFi protocols by exploiting loopholes and logical errors in the smart contracts on which they're run, resulting in the theft of user assets (rugdoc.io).

[8] It should be noted, however, that these potential benefits have yet to materialise, given the relatively slow transaction speed/throughput of the Ethereum blockchain, as well as the related transaction costs in the form of 'gas' and other fees charged.

[9] For example, increased transaction fees linked to network congestion or complexity of smart contracts inhibit small transactions as users are dis-incentivised to execute small-valued transaction with disproportionately high fees, effectively being priced out.

investor protection and market integrity existing across the board of financial services regulation, which gives rise to risks requiring the attention and, possible action, by policy makers.

Anonymity (or pseudonymity) and lack of customer due diligence (CDD) and completion of other AML/CFT processes by most DeFi applications gives rise to risks of money laundering, terrorism financing, and other illicit use, facilitating misconduct. Participation in DeFi platforms only requires connection to a wallet, and some wallets do not require CDD or other AML/CFT controls for their opening. As such, participants can remain fully anonymous or pseudonymous without any link to the identity of the user, and with no controls as to the source of funds. In other words, although DeFi transactions are traceable and verifiable on the chain, they are so on an anonymous or pseudonymous way, without recourse to the identity of the participant.

The possibility to engage in almost unlimited leveraged trading of crypto-assets is one of the main risks involved in DeFi. Although currently DeFi applications have high levels of over-collateralisation, it could be expected that further growth of the DeFi market would bring down collateralisation levels to allow for better capital efficiency, as competition would put pressure on the tokenomics involved in DeFi protocols. This would translate into thinner protection threshold for automatic liquidations of users (the equivalent of margin calls for DeFi protocols). The volatility of crypto-asset prices intensifies the fragility of the DeFi market, and volatility spikes in the price of main crypto-assets (Bitcoin, Ether) pledged as collateral for borrowing and leverage or provided as liquidity for yield farming can induce massive automatic liquidations in DeFi protocols. Such liquidations can have a domino effect on investor holdings across the board, and may even have spill over effects in traditional markets.

The sizeable growth of DeFi for financial services such as lending could lead to greater procyclicality and to new forms of concentration risks, giving rise to financial stability vulnerabilities. The supply of credit on a peer-to-peer basis may lead to larger and sharper swings in credit provision compared to traditional lenders, especially given the volatility of the underlying collateral, and the use of automation and innovative technological processes. Risks of concentration relate to the technology used (e.g. Ethereum blockchain) and to the fact that key operations (e.g. code development, crypto-asset mining) are held in the hands of a relatively small set of persons or entities (e.g. software developers, owners of mining hardware) whose true identities may be unknown. At the current stage of development of the DeFi market, the activity is concentrated in a very small number of protocols, despite the existence of numerous smaller applications (e.g. the aggregated TVL of the top four DeFi applications accounts for almost half the TVL of the DeFi space as of May 2021).

The provision of regulated financial services by DeFi applications in a non-compliant way exposes participants and the markets to risks related to market integrity and consumer protection and provide room for regulatory arbitrage by DeFi players. Numerous DeFi applications (or part of their activities) are involved, at least for some part of their activity, in non-compliant provision of regulated financial services and products, often reserved only for registered or licensed entities. Despite its complexity, DeFi activity 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. Some DeFi applications, or part of their activities, may constitute regulated activities for which comprehensive frameworks are already in place aiming at preserving financial stability, protecting financial consumers, promoting investor protection and market integrity, and mitigating illicit finance risks. For example, the issuance of governance tokens has some characteristics of securities/investment contracts and their issuance, promotion or trading in DeFi platforms could be considered non-compliant in many jurisdictions. Equally, when DeFi applications or activities currently fall outside of the regulated space in some jurisdictions, they raise risks that may be left unaddressed by existing rules.

Challenges may also arise from the decentralised nature of DeFi systems and the sophistication of the technological innovation involved, and, depending on the jurisdiction, some regulatory or supervisory gaps may exist. Some of the characteristics of DeFi may be incompatible with existing regulatory frameworks, particularly given that the current framework is designed for a system that has financial intermediaries at its core. As the existence of intermediaries is contrary to the very essence of decentralised finance, it is difficult to identify parties involved that can be assessed or regulated, making it challenging to supervise DeFi constructs with the existing oversight architecture. Enforcement of existing regulation is also difficult to apply if there is the absence of an identified accountable entity. There may be a need to 'recentralise' DeFi in order to get some comfort from a regulatory and supervisory standpoint, without necessarily completely undermining decentralisation, by identifying forms of centralisation that may exist in such networks. Examples of such could include organised governance structures (e.g. Decentralised Autonomous Organisation (DAO)); holders of controlling shares of governance tokens; identified parties benefiting from the operation of DeFi services through profit sharing mechanisms or fees; or holders of admin keys, all of which could be considered as potential regulatory access points.

Potential regulatory gaps may also appear for new types of risks that arise in DeFi systems and which may stem from the novel characteristics of financial service provision in decentralised systems, and which may give rise to regulatory arbitrage opportunities. For example, it could be argued that in the absence of prudential and investor protection rules, DeFi is vulnerable to over-leveraging and other related financial risks. While certain aspects of current regulation may be applicable to DeFi operations, some of the regulatory tools applicable in centralised settings may need to be redesigned in order to be made interoperable and compatible with decentralised structures. Additional rules may need to be introduced to cover for the technological novelty of decentralised systems. For example, auditing of the code underlying the smart contracts by neutral external parties in specific intervals could help address the challenge that non-technical expert users are facing when required to trust software developers or programmers.

The lack of traditional regulatory safeguards for investor protection and market integrity, existing across the board of financial services regulation, gives rise to risks that call for policy consideration and potential action. There is a risk of moral hazard and absence of skin in the game for participants who launch an open protocol for a DeFi project and the economic incentives of developers and funding entities of protocols are not clearly understood or disclosed. A number of important risks relate to governance tokens, often issued and distributed for free to users as an incentive for participation in the network, and which could constitute securities or investment contracts in some jurisdictions. As governance tokens are freely traded in decentralised exchanges, a (group of) bad actor(s) can purchase enough governance tokens to manipulate the outcome of a vote to the detriment of minority tokenholders. Such risk is exacerbated given the possibility of using uncollateralised flash loans to borrow such governance tokens for the purpose of voting.

Due to the lack of implementation of traditional investor protection safeguards in the DeFi market, investors and financial consumers are exposed to numerous forms of loss or erosion of value (e.g. absence of recourse in case of default or failure, lack of recovery or resolution mechanisms). The risk of market manipulation by malicious actors, whether through concentrated holdings of governance tokens or through the existence of admin keys, or through other mechanisms, remains high. Technology-related risks present in projects that lack appropriate due diligence mechanisms give rise to additional consumer risks and are mostly associated with protocol flaws, errors in the code of smart contract or network risks (e.g. network congestion and high level of fees), cyber risks, risk of hacking and market manipulation. At the base layer level, community splits on contentious decisions can also occur, leading to forks and network splits with negative outcomes for participants without the technical skills to understand such mechanisms. The risks of cyber attacks and exploits is more pronounced in DeFi settings given pseudonymity and numerous examples of market manipulation of voting and token prices have been observed.

As the list of risks for investors and financial consumers in DeFi is very long, users should be made aware of the risks involved in such markets. The average consumer of DeFi-based financial products is, however,

unlikely to fully grasp the technical complexity of the market, exposing him/her to substantial financial risks. Financial education efforts and policies could be key in helping users understand the risks involved in decentralised finance products and protect themselves accordingly. A generalised trend of gamification of finance experienced in the markets may further increase the attraction of financial consumers to DeFi as an alternative to traditional finance. Therefore, regulatory bodies may want to consider encouraging or engaging in investor protection updates to raise financial consumer awareness of potential risks, thereby giving guidance to market participants to better articulate such risks to market participants. Supervisory authorities and international standard setters could contribute to such efforts by raising awareness of risks involved in DeFi and consider soft-law instruments, such as recommendations, to be proposed.

Improved disclosure in DeFi applications could be a first step towards greater protection of participants. Such disclosure can include, for example, governance tokenholding data and changes, similar to listed equity holdings. Disclosure around the existence of admin keys, their scope and the arrangements around them would also need to be encouraged so that users are aware of the potential risks involved. Details around the signers of those keys and the powers of the admin keys should be documented.

Growing interconnections between traditional, centralised finance (CeFi)[10] and DeFi and growing transmission channels of risk from decentralised finance to traditional financial markets increases the importance of user and market safeguards in DeFi. Growing interest in and adoption of crypto-assets by institutional investors and other traditional financial service providers (e.g. payments providers) has led to the creation of permissioned versions of DeFi applications with whitelisting of participants in a compliant manner. Such interconnectedness is expected to grow through the introduction of tokenised assets as collateral in DeFi protocols, in the place of mainstream crypto-assets or stablecoins, allowing traditional financial institutions to unlock liquidity and obtain leverage on pre-existing assets though DeFi.

The widespread use of stablecoins within DeFi protocols further increases interconnectedness between the market for such protocols and the traditional financial markets. Centralised stablecoins pegged to fiat currency with reserve assets managed with only limited transparency expose users and the system to risks related to their trustworthiness associated with the auditability and reporting around their reserves, as well as with the composition of such reserves and stability of the custodian of such reserves. The increase in the use of stablecoins could arguably increase adoption of DeFi, while at the same time constitutes one of the greatest points of vulnerability of the DeFi market and a potential channel of risk transmission to the traditional financial markets. In a scenario where USDT or USDC loses its peg due to solvency issues related to the reserves backing the stablecoin or its undercollateralisation, decentralised exchanges would go under severe stress and liquidity pools would be forced to mass liquidations. Investors exposed to losses in DeFi may have to close positions on traditional markets, too, propagating the shock. The ensuing risks of the wider use of stablecoins within and outside the crypto-asset space and their role as linkages between the DeFi and CeFi systems warrant compliance with a regulatory and supervisory framework and standards that will ensure appropriate protection levels for investors and financial consumers while supporting financial stability overall. It should be noted, however, that stablecoins are not the only source of financial stability risks: leverage, concentration risks, the potential for regulatory arbitrage and risk of contagion are additional dimensions that require the attention and possible action by macroprudential authorities.

Given the rapid growth of DeFi and high use of leverage, there is a need for policy makers to closely monitor this market to better understand its mechanics, potential benefits and underlying risks. As DeFi becomes more interconnected with CeFi, regulators are strengthening their knowledge of DeFi markets and products in order to evaluate emerging benefits and risks and how to mitigate such risks in order to

[10] For the purposes of this report, CeFi refers to traditional finance, sometimes referred to as TradFi. In the narrow sense, CeFi describes hosted crypto-asset products and services (i.e., exchanges, lending platforms) by centralised parties.

support a safe market for decentralised finance. A better understanding of the mechanics of the DeFi market will allow policy makers to assess whether potential policy gaps may exist; whether new regulatory approaches may be required or existing frameworks may need updating in order to ensure that similar activities are subject to similar regulation, and whether risk management practices are in place to encourage the safe functioning of these markets. More and better quality of data is also necessary for DeFi and crypto-asset markets in order to better analyse these markets and their possible impact and in preparation for any possible future policy intervention.

In addition to exploring ways to enforce existing rules in decentralised structures, policy makers could 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 DeFi services could bring to users, the financial system and the real economy could be beneficial. DeFi is fuelling innovation (conventional and disruptive) and leading established market infrastructures and players to review existing processes to make them more efficient (e.g. rethinking of post-trade processes and financial intermediation).

Oversight and regulatory compliance of DeFi networks may be further obstructed by their global in reach and operation, with no defined jurisdiction and geographical location for their operations. This jurisdictional uncertainty challenges enforcement, particularly given the speed and ease with which financial service providers are able to change locations in response to actions of authorities. Therefore, greater international policy collaboration and discussion can help overcome such challenges at the cross-border level and avoid regulatory arbitrage. Further collaboration is warranted between all stakeholders involved in decentralised finance and policy makers could benefit from actively playing a role towards establishing a cooperative environment among stakeholders. The engineering and software developing communities should be involved in such dialogue, given that the code embedded in DLT systems could factor into a discussion of the appropriate oversight on the activities of a blockchain-based financial ecosystem, and despite often disparate incentives and mind-sets of such communities.

1 Introduction

Decentralised Finance or 'DeFi' seeks to provide traditional financial services involving crypto-assets (i.e. mimicking the 'CeFi' or centralised finance market) in an open, decentralised, permissionless way. Decentralised finance as a high-level concept has been discussed at national and international levels following the introduction of Bitcoin. Indicatively, decentralised finance was discussed at the G20 Finance Ministers and Central Bank Governors in their meeting in Fukuoka on 8-9 June 2019 under the Japanese presidency of the G20 (FSB, 2019[2]).

The DeFi market is the practical application of decentralised finance and embodies this high-level concept by providing financial products and services built as decentralised applications (mainly) on the Ethereum blockchain network. The DeFi market started making headlines in the summer of 2020 (referred to as 'the DeFi summer'), when a number of DeFi applications appeared to gain traction with users, and has grown to a multiple of its initial size ever since. The total value of crypto-assets locked in DeFi applications built on the Ethereum blockchain as of November 2021 reached USD 100bn up from USD1.9bn on 2 July 2020 (c.2,150% increase in less than a year, albeit from a very low base).

Although the size of the DeFi market itself is still small, DeFi is rapidly growing from low levels and worth delving into for a number of reasons:

- The DeFi market is growing rapidly and attracts an increasing number of retail investors, exposing them to high risks;
- Increased interest and adoption of crypto-assets by institutional investors[11] and other traditional financial service providers is leading to increased interconnections between centralised finance ('CeFi' or 'CeFi') and the parallel DeFi system through intersection or convergence points;
- The increasing use of stablecoins, tokenised and digital assets makes the boundaries of the two systems more porous and increases risks of spillovers to the traditional financial system and the real economy. Such risks are exacerbated by the recent price volatility of main crypto-assets (Bitcoin, Ether) and the recycling of profits in the DeFi space.

While it remains questionable whether DeFi will continue to grow, further examination of the current state of the DeFi market by financial authorities may be warranted, with a view to better understand its activities, structures, potential benefits and underlying risks.

The Committee on Financial Markets has included analysis of the decentralisation of finance in the 2021-22 biennium's programme of work and budget and the corresponding workplan.

This report was discussed at the Experts Group on Finance and Digitalisation in April 2021 and was approved by the Committee in October 2021. The report was declassified by the Committee on Financial Markets on 7 January 2022.

[11] This includes investment by institutional investors and public companies in the DeFi space. See Section 4.3 for examples.

2 Definition and applications of DeFi

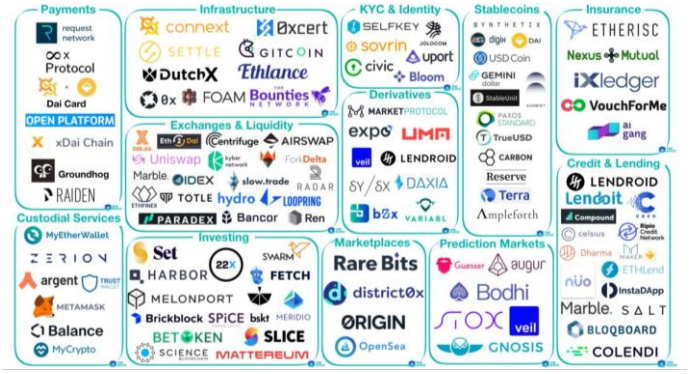
Given its novelty and complex characteristics, DeFi is not widely understood by many market participants and policy makers. This section provides an overview of DeFi activities and proposes characteristics that could help better define truly decentralised protocols. It then discusses the drivers of the growing participation of investors in DeFi markets and takes a deep dive into the activity of lending and yield farming protocols, which are the main application of DeFi at the time of writing of this report.

2.1. Defining DeFi

DeFi is the latest trend in the crypto-asset space, and promises to replicate various activities in the traditional financial system in an open, decentralised, permissionless and autonomous way. DeFi applications allow for the provision of financial products and services built as decentralised applications on the blockchain.[12] Such applications are mostly based on the Ethereum protocol, which was launched in 2015 and allows for the creation of smart contracts.[13]

The DeFi market brings to life the concept of 'decentralised finance' that has been in the agenda of certain policy makers following the advent of applications enabled by distributed ledger technologies ('DLT') and offering financial services without the need for intermediaries or centralised processes (FSB, 2019[2]). Rather than relying on centralised parties for trust, DeFi markets are community-based networks seeking ways to automate the factors that contribute to trust in centralised institutions, and operating in a global, borderless way.

Figure 2.1. The DeFi universe: select applications by activity



Note: This figure includes self-proclaimed DeFi projects, however, not all of these projects have a fully decentralised nature (as per main characteristics described in Section 2.1.1). Also, many of the DeFi applications depicted in the chart are still in a very early stage of implementation.

[12] Blockchain and Distributed ledger technologies (DLTs) are used interchangeably in this note.

[13] The development of the DeFi market relies heavily on smart contracts, which consist of self-executing contracts written as code on blockchain ledgers, and are automatically executed upon reaching pre-defined trigger events written in the code (OECD, 2019[9]).

Source: theblockcrypto.com.

Currently, DeFi applications aim to replicate most of the main traditional financial products and services in a decentralised manner relying on smart contracts (Figure 2.1). Lending is the fastest growing DeFi product, driven by yield farming, and at the time of writing of this report accounted for more than half of the TVL in DeFi applications (53% of total TVL in DeFi as of 14.06.2021)[14]. As of the writing of this paper, other products offered include decentralised exchanges (DEX) (33% of TVL); derivatives and synthetics; asset management; insurance; payments; and prediction markets account for the rest of the activity as of 14 June 2021.

DeFi lending activities try to mirror market-based lending (securities lending, repos) rather than traditional consumer/retail bank lending, as most activity involves collateralised lending. Importantly, these traditionally institutional activities are being promoted to retail actors in the DeFi space. It should be noted, however, that uncollateralised lending is also possible through flash loans (see Box 2.3). In particular, yield farming or liquidity mining is a process allowing DeFi market participants to lock up their crypto-asset holdings in applications and generate rewards in exchange for the provision of liquidity to the system (either interest on their locked up crypto-assets or new tokens of the platform, issued as rewards). In other words, DeFi users use such protocols to leverage their crypto-assets or lock their crypto-holdings in DeFi protocols allowing others to borrow them for leverage, in exchange for some remuneration.

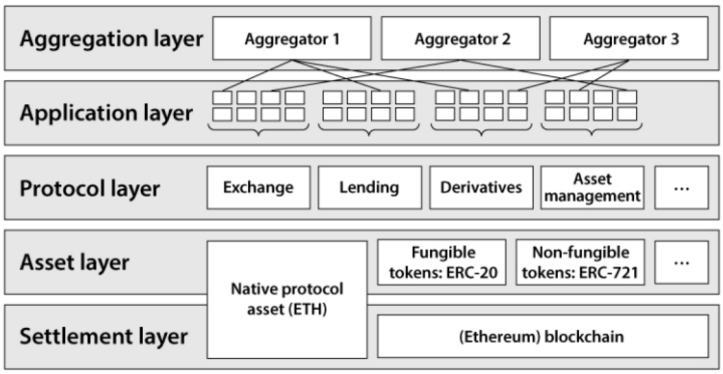
In terms of architecture, the DeFi market is composed of different layers, where each layer has a distinct purpose (Figure 2.2). The layers build on each other and create an open, highly composable and interoperable infrastructure that allows everyone to build on, propose amendments, or use other parts of the stack. The basis of the structure is a highly interoperable protocol stack, which allows smart contract functionalities, such as the Ethereum blockchain (Schär, 2021[3]). DeFi protocols consist of software built on top of the settlement layer, at the protocol layer, where specific use cases are being built and implemented as a set of smart contracts, executed upon the triggering of specific conditions. The protocols provide standards for specific use cases that can be accessed by any user or DeFi application, making these protocols highly interoperable (Schär, 2021[3]). Aggregators at the top layer create user-centric platforms that connect to several applications and protocols, allowing users to perform otherwise complex tasks by connecting to several protocols simultaneously (Schär, 2021[3]).

DeFi has brought the evolution of the P2P (peer-to-peer) model of DLT-based systems to a user-to-smart-contract model (or user-to-pool). Agreements between parties involved in DeFi are executed automatically based on smart contracts and certain processes involved in DeFi transactions are based on a smart-contract-to-smart-contract basis without any human intervention (e.g. automated liquidation). In such cases, smart contracts are triggered by price or other information feeds provided by nodes external to the chain, called Oracles (e.g. provision of spot price of a crypto-asset) (OECD, 2020[4]).

In terms of transaction recording, transactions are traceable and verifiable on the chain, although in a pseudonymous way. Similar to any DLT-based system, current and past balances and transactions are timestamped and recorded in a tamper-evident manner, and are accessible to all participants in the chain, promoting trust in the network. Nevertheless, participants of permissionless DeFi applications are generally not subject to CDD checks in the vast majority of DeFi applications, and as such, transactions can be traced back to wallets and accounts in a pseudonymous way, without recourse to the identity of the participating node.

[14] Source: DeFi Pulse.

Figure 2.2. The architecture of DeFi



Source: DeFi Stack (Schär, 2021[3]).

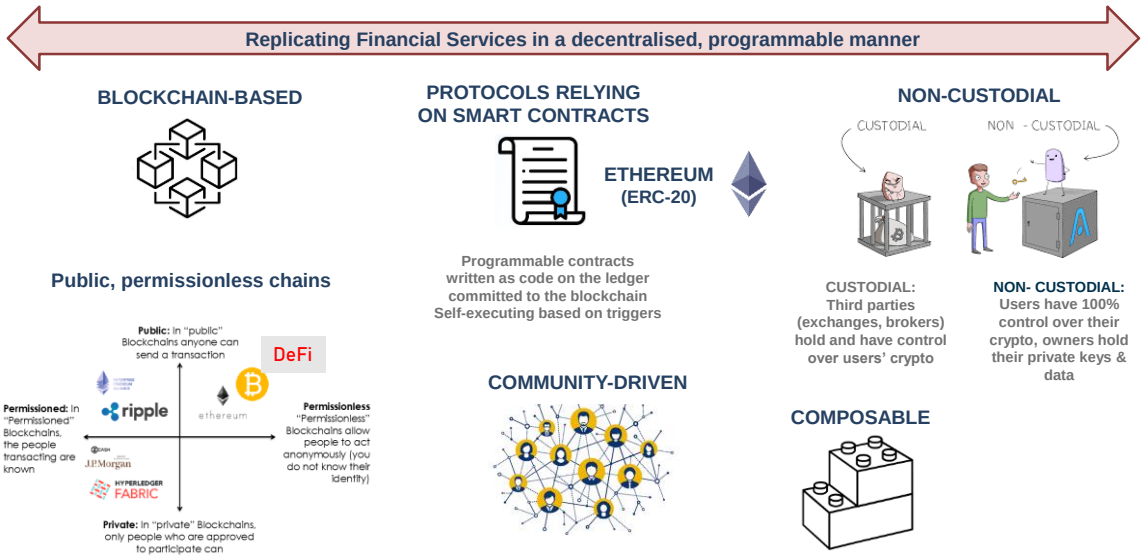
2.1.1. What is DeFi? Main characteristics

Although there is no widely accepted definition of DeFi, this report defines the key features differentiating DeFi from traditional financial markets as follows:

- Non-custodial: The non-custodial nature of DeFi is one of its main defining characteristics. In DeFi applications, no central authority or other intermediary gains access to or control over participants' digital assets; instead, participants manage their private keys, and therefore their digital assets, directly.
- Self-governed and community-driven: Most DeFi protocols are open-source and allow the community to review and further develop the code underlying the protocols. In terms of governance, the distribution of governance tokens in many DeFi applications allows users to participate in some decision-making related to the application, depending on the specific arrangements of each application.[15] The importance of the community of participants is fundamental for the materialisation of network effects, creating value as the number of participant in the network grows.
- Composable: This is one of the most important innovations brought by DeFi. Existing components of DeFi networks (i.e. digital assets, smart contracts, protocols and applications built on top of the protocol layer) can be combined to create new applications (see Box 2.1). Composability gives ample room for the creation of innovative products and structures, and has the potential to further amplify network effects, increasing the value of DeFi products and services as participation in the network grows. The open source nature of DeFi applications is a critical enabler of this attribute, as it allows everyone to look at the code and use it to create new applications. At the same time, the recycling of assets on different applications adds to the complexity of an already complicated market, and to the risks underlying its applications.

[15] It should be noted, however, that many DeFi protocols today are not community-governed, and it is questionable if many DeFi protocols to date are truly decentralised. In reality, not all participants get to vote and in many cases voting is disconnected from the governance token itself (e.g. through delegation to University clubs). Further, not all protocol or smart contract changes occur due to votes of governance tokens – and some entities retain veto rights over the vote or control over discussion boards discussing protocol and smart contract changes (see Section 4.2.2. for more).

Figure 2.3. Main characteristics of DeFi applications



Source: Author's illustration.

Box 2.1. Practical example of composability

The following example illustrates the composability enabled by DeFi applications:

A DeFi user can lock-up his crypto-assets in a lending or market-making protocol in order to earn rewards. For example, a user locks-up his ETH on the MakerDAO application, in exchange for DAI stablecoins and new units of the application's governance token, MKR, as a participation reward. The user can then pledge the DAI as collateral in other DeFi application, such as Compound, in exchange for the cDAI tokens and units of COMP, Compound's governance token, either of which he can then trade in a decentralised exchange (DEX) for another crypto-asset.

This example illustrates also that the TVL metric currently used to measure DeFi activity can lead to inaccurate estimates of the market: the cDAI tokens pledged as collateral at the second step of the above example will be counted by Compound as value locked in DeFi applications, while in reality it is just the product of the leveraged initial ETH locked in the MakerDAO application.

2.1.2. Is it truly DeFi? Defining by elimination

Given the recent exuberance around DeFi, a lot of start-ups and projects arbitrarily market themselves as DeFi without necessarily being true DeFi projects, for marketing and other purposes. For example, certain firms are self-proclaimed DeFi on the basis of them being open source code-based financial applications. Also, not all self-proclaimed DeFi projects have a decentralised organisational structure. It should be noted that Figure 2.1 includes some self-proclaimed DeFi projects that do not meet the criteria outlined in this section.

Having DLT-based financial services or product does not necessary place a firm under the DeFi category. For example, a system based on a permissioned DLT network cannot, by definition, be considered DeFi, as there is some authority deciding upon participation or other rights. For applications to be DeFi, governance needs to be community based (in general based on the distribution/holding of governance tokens), without any central authority or intermediary party holding an admin key or persons who maintain

control or sufficient influence in the DeFi arrangement. However, in reality, many DeFi projects end up being highly centralised. The existence of an admin key to the protocol raises important risks for users as it can allow malicious third parties to hack the protocol and/or compromise smart contracts (see Section 3.2).

At this stage of development of the market for DeFi, the degree of decentralisation varies from one DeFi project to another, while many such projects are centralised at the bootstrapping early creation stage (Ushida and Angel, 2021[5]). Decentralisation is by its nature on a spectrum and not a binary issue, and its measurement is difficult and may rely on human judgement (see Box 2.2).

Applications also need to be truly non-custodial.[16] When the management and safekeeping of users' private key, funds or information is performed by third party nodes/intermediaries, the design is clearly not in line with the non-custodial approach of DeFi networks, where users hold exclusive control of their private keys, and thus, their own assets (until they transact). The non-custodian nature of DeFi provides safety against expropriation of crypto-assets by parties other than the owner, and allows for a pseudonymous participation of users in DeFi, as they do not need to go through a regulated or custodial service provider. At the same time, users are responsible for their risk, as the loss of private keys translates into loss of access to their investment. Non-custodian wallets are largely being used as the means to access the DeFi ecosystem at this stage of development of the market.

A number of self-proclaimed DeFi projects are hybrid in nature. Such projects consist of a combination of a centralised front-end business set-up with a DeFi architecture at the back end of the application. This may take away some of the decentralisation potential of the application, but at the same time, it can allow for identification of an accountable entity and a regulatory and supervisory access point for regulatory compliance, oversight and enforcement purposes. Such an approach would eliminate the current possibility of DeFi markets to function in a pseudonymous way. It remains to be analysed how such structures would compare on a risk/return basis to fully decentralised applications.

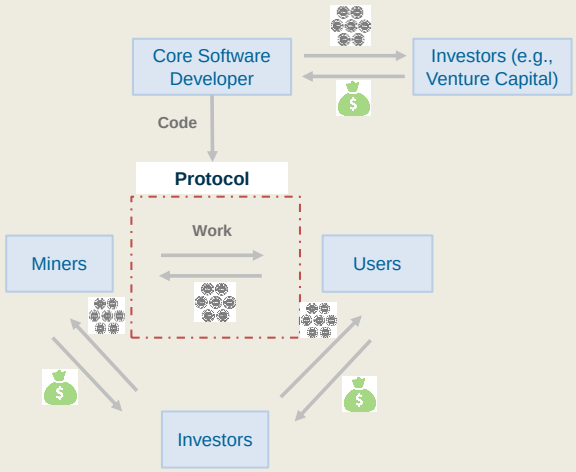
[16] It should be noted that shared custody arrangements could make this distinction blurry.

Box 2.2. The spectrum of decentralisation and the DeFi protocol lifecycle

The level of decentralisation of DeFi applications can follow the path of the protocol development cycle, starting from a very centralised project at inception and software development phase and becoming increasingly decentralised as it is deployed and shared with users.

Core software development teams, generally funded by VCs in exchange for tokens issued by the protocol, start off holding the admin keys to the protocol and the power to make the most important decisions around the design of the protocol. Such decisions reflect not only technical choices about the operation of the system but also policy choices about the level of fees, the voting thresholds and other decisive starting points, all written in code. The protocol is then deployed in the market and shared with market participants and users and, depending on the project, starts operating independently based on the rules incorporated into the protocol's code. Users maintain custody of their keys and make decisions on the project's development and evolution by exercising the voting rights attached to their governance tokens, depending on the protocol design. In some cases, core developers keep the admin keys for the initial stages of operation of the protocol as a testing phase to ensure the safe operation of the protocol in a controlled manner (e.g. ability to pause or stop the system if a bug occurs). The holding of the admin key[17] by an individual or a group of individuals, however, compromises the project and exposes users to risks of manipulation, especially when this is not disclosed or the admin key holders are not identified.

Figure 2.4. Funding crypto networks



Source: Adapted from placeholder.vc

At the initial stage of the project, a lot of prominent DeFi projects had total concentration of power in the hands of a few individuals. These individuals were incorporated or formed a Foundation/non-profit organisation, overseeing the development of the protocol and its implementation. Foundations are then often dissolved to give place to decentralised autonomous organisations (DAOs) which take over the governance of the protocol in a decentralised manner.[18] At the time of writing of this report, more than USD 6 bn worth of digital assets are held by the top 20 DAOs, while there are more than 190,000 DAO members across the crypto-space (DeepDAO, 2021[6]). Prominent DeFi projects that have set up DAOs include MakerDAO, Compound and Uniswap, although even in such cases, projects could still be influenced by concentrated groups of active participants.

The constantly changing nature of a blockchain system's level of decentralisation makes it difficult to determine what decentralised means and use decentralised as a basis for legal decisions (Walch, 2019[7]). The level of decentralisation could be described as a fluid characteristic along a spectrum, as the number of nodes in a blockchain system fluctuates, people enter and exit the system at will, and the hashing power and its distribution change frequently. Miner participation (in proof-of-work systems) fluctuates depending on whether the price of the crypto-asset makes it financially attractive to continue to provide transaction processing, or may depend on regulatory action (e.g. China crackdown on mining in June 2021 (FT, 2021[8]). Miner concentration and the level of distribution of nodes across the globe also fluctuates according to market conditions, policy action and crypto-asset valuations. Like this settlement layer, core software developers' participation and power are also in flux, depending on compensation prospects or perceived risk of liability, and the level of power concentration by initial developers also fluctuates as mentioned above, depending on the stage of the protocol's lifecycle.

It should be noted that the concept of decentralisation, linked to the power distribution and diffusion across the network, has more political and ideological undertones to it, tied to the cypher-punk and crypro-anarchist roots of the first blockchains and the Bitcoin (Walch, 2019[7]).

Shifting financial payoffs and important risks related to misconduct and conflicts of interests in DeFi applications can give rise to vulnerabilities for these markets and their participants. Financial authorities could consider how the shaping of the power distribution in DeFi markets, whether this involves the holding of admin keys, governance tokens or other, affects market participants and the markets for these products.

2.2. Drivers and users of DeFi activity

There are no fundamental drivers of the surge in crypto-asset prices in what is clearly a market driven by speculation given the very high returns offered by some of the products, fear of missed returns (so-called fear of missing out or 'FOMO') and recycling of profits from other crypto-asset activity. Feedback loops exist between the Bitcoin, the price of which has driven much of the activity in the entire crypto-asset market, and the evolution of DeFi measured by TVL in such crypto-assets. Some spillovers from accommodative monetary policy and a search for yield by retail and institutional investors may also have contributed to the DeFi trend. For some retail investors, crypto-assets such as Bitcoin are perceived as inflation hedges, although the direction of their price has thus far been highly correlated with traditional financial markets. The exponential growth of the DeFi market has a lot of the characteristics of the 2017-18 crypto-asset bull market associated with the Initial Coin Offering (ICO) boom in terms of its drivers (OECD, 2019[9]). Similarities exist also in terms of associated complexities and risks for participants.

The recent price increase of Ethereum's native asset, ether (ETH), can in part be attributed to the intensity of the use of ETH for DeFi applications, as well as to the increased investor interest in NFTs, also primarily issued on the Ethereum blockchain (see Section 4.3.3).[19] It is estimated that 90% of all listed tokens are issued on the Ethereum blockchain (Schär, 2021[3]). The Ethereum blockchain enables smart contract functionalities, which constitute the basis of most DeFi applications. Daily transactions of ETH have

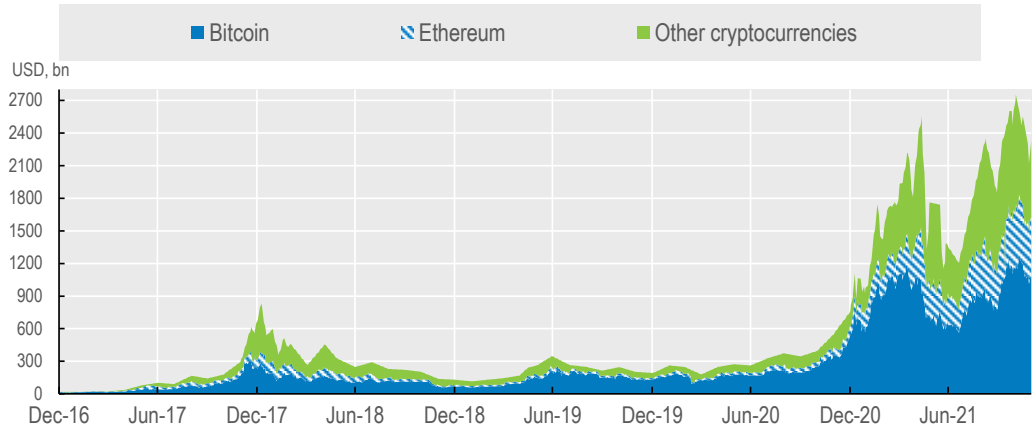
[17] Even in case of multi-sig admin keys, in the absence of disclosure of the holders of those keys, there is a risk that all keys are held by the same person.

[18] A list of DAOs is available under https://snapshot.org/#/ .

[19] The Ethereum London hard fork EIP-1559 is another reason behind the most recent ETH price increase, as this upgrade causes transaction fees to be destroyed ('burnt') rather than paid to miners and has decreased the overall supply of ETH.

reached new highs, while the activity of Ethereum-based decentralised exchanges activity (DEX)[20] has surpassed that of CeFi exchanges in terms of daily volume (e.g. decentralised exchange Uniswap surpassed daily activity of centralised exchange Coinbase on 30 August 2020)[21].

Figure 2.5. Crypto-asset valuations are one of the drivers of DeFi activity



Note: As of 1 December 2021.
Source: Thompson Reuters Eikon.

The volatility of crypto-asset prices intensifies the fragility of the DeFi market. The 'Black Thursday' event of the 12 March 2020 was the first noteworthy stress-test event in DeFi's short history, when Ethereum dropped by more than 20% in a day. Following such drop, users tried to shift their crypto from one application to another, raising ETH gas fees to 200 Gwei (a denomination of Ether, see Box 2.3). The value of collateral also dropped, causing waves of automated liquidations. Liquidated collateral is auctioned, and external players responsible for liquidations (known as keeper bots) were able to make zero bids for auctioned ETH collateral, due to a weakness in the protocol which allowed for the manipulation of such keepers, and it is estimated that c. USD 8.32m was withdrawn through zero bids auctions in total (Medium, 2021[10]). A total of USD 16m was liquidated in lending protocols on 11 March 2020, with another USD 5.7m the next day.

[20] Fully decentralised exchanges that rely on an automated market-making model and are part of the DeFi market. It is questionable whether fully decentralised exchanges exist at the day of the writing of this report.

[21] Based on data by Dune analytics.

Box 2.3. Gas fees in Ethereum-based applications

Transaction costs are paid in so-called gas fees, which in turn are paid in Ethereum's native currency, Ether. Gas prices are denoted in Gwei, which itself is a denomination of Ether: each Gwei is equal to 0.000000001 ETH (10-9 ETH). For reference and by way of an example of such changes in gas fees, these stood at 75 Gwei on 23 October 2021 vs. 211 Gwei on 3 November 2021.

In essence, gas refers to the fee required to successfully conduct a transaction on Ethereum, and gas fees are paid in Ethereum's native currency, ether (ETH). Gas fees are market-driven determined by the demand for resources on the network and are based on the demand to execute transactions vs. the supply of computing power to confirm them. Transaction fees depend on the complexity of the transaction (e.g. how large is the contract the user is trying to execute, nature of computations, need to retrieve data from an oracle, etc.). Since DeFi transactions often require multiple smart contract calls, they can become extraordinarily expensive even for a small transaction. Transaction fees are also determined by the desirable speed of execution, i.e. the faster the user wants the transaction executed, the higher the gas fee.

Recent developments around the Ethereum blockchain, including a surge in DeFi activity built mostly on the Ethereum network, a growing trend in NFT issuance on the same blockchain and the London hard fork designed to upgrade the network have led to a sharp increase in the price of Ethereum gas fees over the past year as the network was under heavy utilisation (see Figure 2.6). Such increase sometimes leads to situations whereby transaction costs surpass the value that is actually being transacted, rendering small transactions uneconomical.

The London Upgrade (EIP 1559) implemented on 5 August 2021 overhauled the Ethereum's transaction fee mechanism making transacting on Ethereum more predictable (although more complex, too) for users and offsetting the ETH issuance by burning a percentage of transaction fees. Starting with the London network upgrade, every block has a base fee, the minimum price per unit of gas for inclusion in this block, calculated by the network based on demand for block space. As the base fee of the transaction fee is burnt, users are also expected to set a tip (priority fee) in their transactions. The tip compensates miners for executing and propagating user transactions in blocks and is expected to be set automatically by most wallets. Users can submit transactions with a maximum fee per gas corresponding to how much they are willing to pay for the transaction to be executing, knowing that they will not pay more than the market price for gas (base fee per gas), and get any extra, minus their tip, refunded.

Source: ethereum.org

Volatility spikes in the price of the Bitcoin and Ether in H1 2021 have induced further massive liquidations in DeFi protocols. In May alone, the price of the Bitcoin fell by c.30% resulting in USD 8 billion of crypto-asset liquidations happening on 18 May, on top of another USD 3.4 billion having been liquidated on 12 May, unwinding leveraged traders with long positions.[22] In terms of DeFi lending protocols, USD 662m in loans unwound over 24 hours on 18 May, on top of another USD 39m on May 12.[23] The second-worst day for liquidations came on 22 February, when USD 129.6m was liquidated. In order to understand the scale

[22] Includes liquidations of leveraged positions on centralised exchanges. Liquidation data available at https://www.bybt.com/LiquidationData and https://defiexplore.com/liquidations.

[23] According to DeBank, (Dale, 2021[53]).

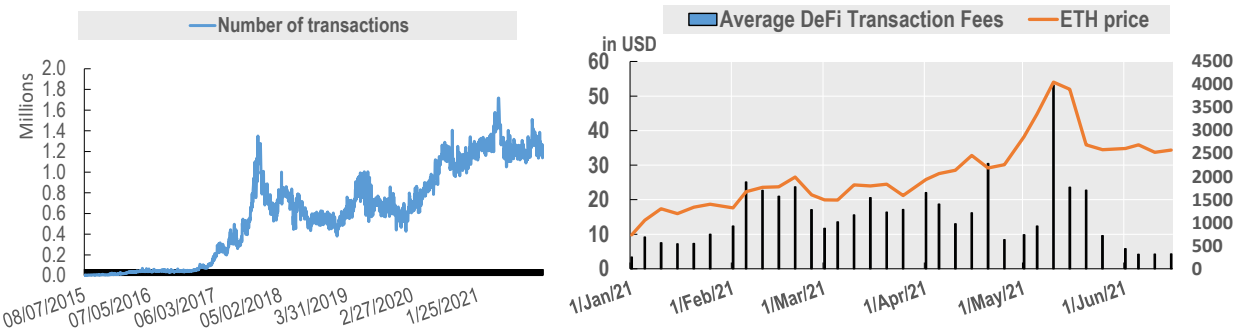
of these liquidations, these can be compared to a normal day of liquidations across DeFi products of USD 1m - 5 m (based on Debank statistics).

The rapid unwinding of leveraged positions and the massive liquidations in DeFi protocols in reaction to sharp drops in the value of major crypto-assets (Bitcoin, Ether) intensifies the pressure on the valuation of such crypto-assets, given the feedback loops that exist between the two markets. This can prolong sell-offs and drive valuations to even lower levels, creating downward spirals, as collateral is automatically liquidated by DeFi applications putting extra pressure to the valuation of the crypto-assets used as collateral. Interestingly, this has had the opposite effect on stablecoins used to close up positions in DeFi, with stablecoins trading at more than USD 1 per coin, as stablecoins are being used as a means to exit positions in DeFi tokens.

The sharp volatility of Ether also has implications to the fees paid by users as transaction costs, as these may sometimes be correlated with the price of the crypto-asset (Figure 2.6). As most of the DeFi activity sits on the Ethereum network, and given other recent developments around Ethereum (NFT issuance, EIP 1559), the Ethereum gas fees have reached new highs in the past year (see Figure 2.6, Box 2.3) and in some cases transaction costs exceed the value being transacted, effectively blocking users wishing to execute small trades.

Increased fees inhibit small transactions as users are dis-incentivised to execute small-valued transaction with disproportionately high fees, effectively being priced out. This results in an increase in the size of transactions executed in response to a surge in fees, and with the consequent blocking of users' assets as users are unwilling to transact at such fee levels. This has disruptive effects to smaller retail investors, weakening the purported benefits for financial inclusion and democratisation of finance proposed by DeFi. This, in turn, affects liquidity conditions in DEXs or centralised exchanges for crypto-assets. Transactions related to stablecoins like USDT also exhibit similar behaviour in response to high and volatile ETH transaction/validation fees, whereby high fees act as catalysts for declining transaction volumes involving crypto-assets, although causality is hard to infer (Carter, 2020[11]).

Figure 2.6. Ethereum daily transactions chart and transaction fees



Note: The cost of gas fluctuates with the supply and demand for processing power.
Source: Etherscan.io, bitinfocharts.

2.2.1. User base and motivations

The DeFi user base has followed a consistent growth pattern, reaching almost 3 million unique addresses using DeFi protocols as of June 2021 (Figure 2.7).[24] Although the number of unique addresses accessing DeFi has grown by c.65% since Q1 2021, active DeFi addresses still only represent 1.81% of all Ethereum addresses[25] (Consensys, 2021[12]). As some DeFi applications may fall out of the regulatory scope for many countries, DeFi markets are exposed to increased risk of fraud, illicit trading, and money laundering/terrorist financing. This could paradoxically make the market more attractive and favour adoption by criminals and other participants seeking to circumvent laws.

There are currently no statistics around the profile of DeFi users, given the pseudonymous or anonymous nature of their participation in such markets. Early adopters were mostly crypto-savvy users attracted by the novelty of DeFi and wishing to become part of the innovation brought by such applications, either as users or as contributors (given the open source nature of most protocols).

The DeFi summer in 2020 saw growing retail interest in DeFi, driven by speculation, fear of missing out and recycling of profits from other mainstream crypto-assets. Crypto-asset holders convinced that the value of their holdings will increase may wish to generate some yield by pledging them as collateral and through participation in liquidity pools. Other holders may also wish to postpone the monetisation of profits related to their crypto-asset holdings to escape taxation.

DeFi may follow other crypto markets in attracting an increasingly large number of retail investors: recent research by the UK FCA estimates that the number of UK consumers holding crypto-assets account now for 4.5% of the UK population, up from 3.8% in 2020 (FCA, 2021[13]). Nevertheless, retail investors are less likely to be specialists in crypto or in other asset classes, because they tend to invest in different products, and this could change market dynamics (e.g. day traders). However, there is a relatively high barrier to entry the DeFi market, as users must first hold crypto and understand how to use smart contracts. The lack of sophisticated knowledge by retail investors exposes them, at the same time, to high risks as they may not understand the risks involved or the exact mechanisms of the protocol operations (e.g. automated liquidations).

The possibility to engage in almost unlimited leveraged trading of crypto-assets has also attracted a large number of hedge funds and family offices investing proprietary funds into the DeFi space. Related to that, in recent months, the DeFi market is increasingly attracting institutional players, leading to the introduction of institutional or professional versions of some of the top DeFi protocols (e.g. Aave) to cater for their needs. The major novelty of such versions is the introduction of customer due diligence screening processes through the whitelisting of participants in what is then a permissioned DeFi application instead of a public permissionless one. Compound Finance has also recently launched the Compound Treasury, a new product designed for non-crypto native businesses and financial institutions to access the Compound lending protocol (the platform promises institutions to earn a fixed interest of 4% a year) (Liu, 2021[14]).

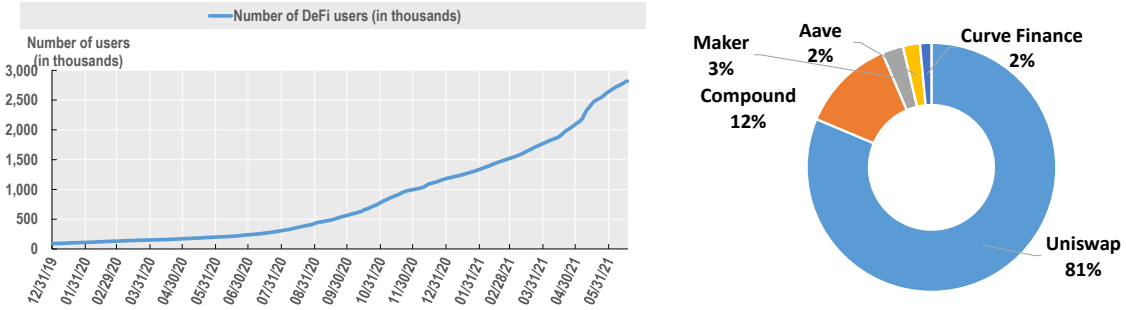
Recent surveys report that 21% of hedge funds are currently investing in digital assets with, on average, 3% of their total hedge fund AuM invested, with the vast majority of these (86%) reporting an intention to deploy more capital in to the asset class by the end of 2021 (PWC, 2021[15]). Another 26% of the same hedge fund manager survey respondents who are not yet investing in digital assets confirmed that they are in late-stage planning to invest or looking to invest (PWC, 2021[15]). The vast majority of investors in dedicated crypto hedge funds are either high net worth individuals (54%) or family offices (30%) (PWC, 2021[15]).

[24] It should be noted that one user can have multiple accounts through the use of digital wallets, which means that multiple addresses could correspond to the same user.

[25] Total Ethereum addresses stood at 161 million as of 1 July 2021.

Figure 2.7. DeFi users over time

Number of users in thousands, as of 18 June 2021 [LHS] and distribution of wallets by DeFi app [RHS]



Source: Dune Analytics.

2.3. Spotlight on lending protocols and yield farming

Lending is one of the largest DeFi markets, and at the time of writing of this report accounts for more than half of the TVL in DeFi applications (53% of total TVL in DeFi as of June 2021)[26]. Most such platforms entice users to provide liquidity to the platform by inviting deposits in crypto-assets, and rewarding them with tokens which are native to the platform. The rates at which users are rewarded depend on the demand and supply of liquidity, rather than the creditworthiness of the borrower on the other side of the transaction. Such platforms have automatic liquidation systems in place, which could be described as the margin call equivalent of blockchain-based finance, that programmatically liquidate positions that become undercollateralised. Recently, some of the top DeFi applications have introduced reserve funds which are intended to act as protection mechanisms in case of massive liquidations in order to protect the protocol's liquidity providers against default.[27]

Although many DeFi platforms market themselves as mere software providers, in this instance, platforms appear to be delivering banking services, i.e. accepting deposits, rewarding them, and, to some extent, onward lending them. It should be noted that, in some jurisdictions, such so-called deposit activities in return for a fixed or variable return may in fact constitute issuance of a debt instrument or an investment contract that may involve offers and sales of securities, rather than being traditional deposits. To the extent that these platforms perform similar financial activities to that of banks, it remains to be decided whether they should also have the same regulatory obligations. For example, according to recent guidance by the Financial Action Task Force (FATF), under certain circumstances software providers who undertake certain functions may meet the definition of a virtual asset service provider (VASP) and, as such, be required to comply with regulation for AML/CFT purposes (see Box 4.1). It is also unclear how the platforms' interest rate-setting mechanism would interact with monetary policy, and how central banks could affect it with traditional monetary policy tools.

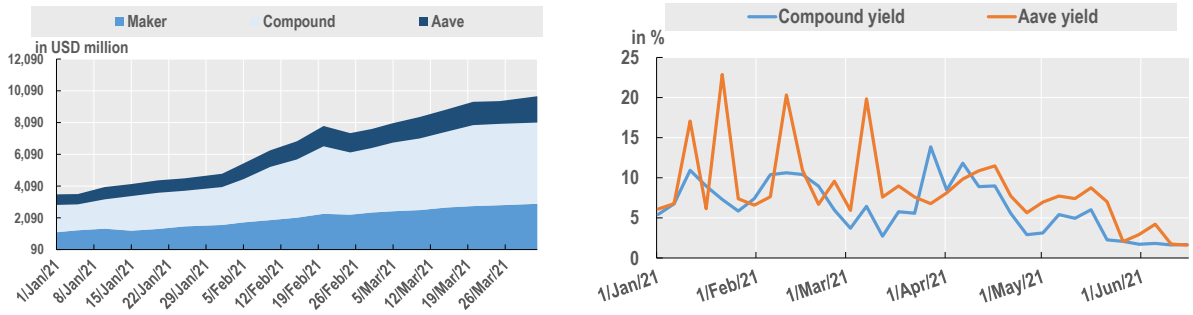
Although leverage is identified as one of the main risks involved in DeFi applications, until the writing of this report, DeFi protocols imposed very high collateralisation levels in order to protect against the massive volatility of crypto-assets pledged as collateral. These high levels of collateralisation are designed to

[26] Source: DeFi Pulse.

[27] For example, Compound uses 2.8% of the proceeds of any liquidation to fund the cToken reserves, which aims to reduce the risk of cascading liquidations rendering the protocol insolvent (see https://compound.finance/governance/proposals/49).

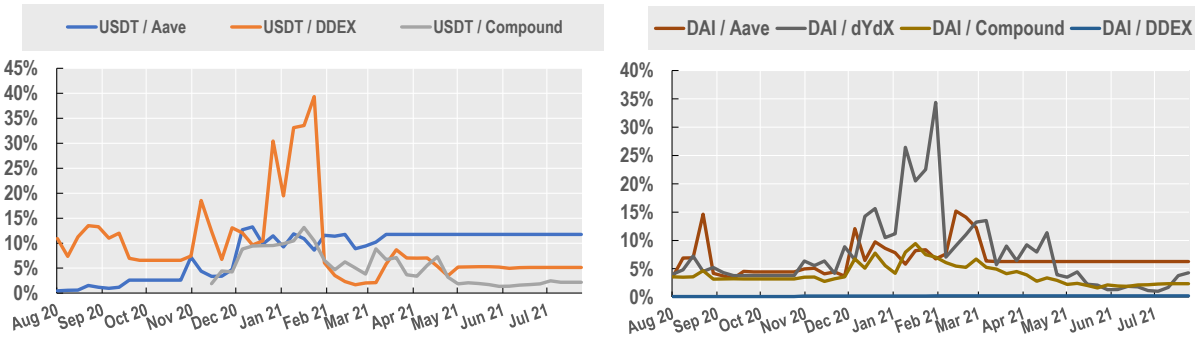
protect users pledging their crypto-assets from being automatically liquidated in case the value of the underlying collateral drops below a certain pre-defined level at which the automatic liquidation is triggered.

Figure 2.8. DeFi lending by top three protocols and lending yields



Note: Lending volumes for the period 01.01.2021 – 01.04.2021. Yields for lending USDC over the period 01.01.2021 – 16.06.2021.
Source: Consensys for lending volumes, loanscan.io for yields.

Figure 2.9. APR rates in DeFi lending protocols

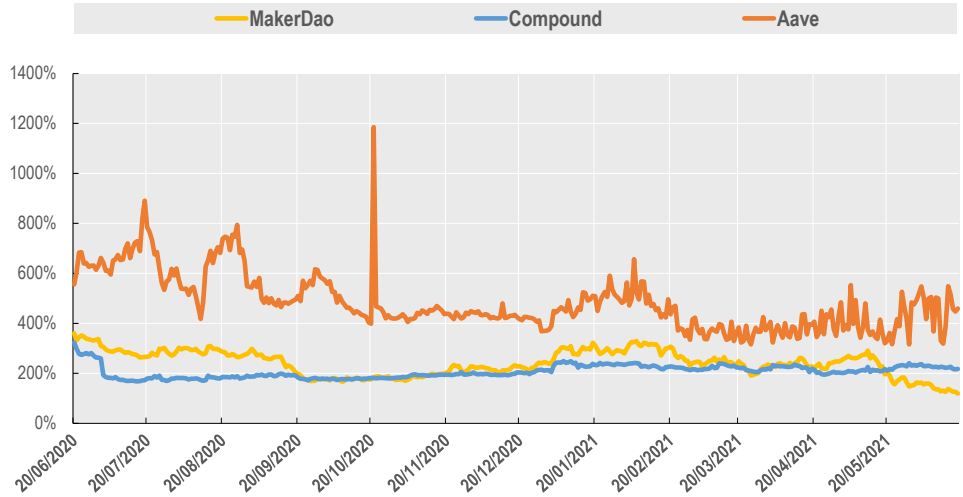


Source: https://app.defiscore.io.

The current high levels of collateralisation are onerous in terms of capital efficiency or in the need for excess loss absorbing buffers for the protocol itself. It could be expected that further growth of the DeFi market would bring down collateralisation levels to allow for better capital efficiency, as competition would put pressure on the tokenomics involved in DeFi protocols. Such an eventuality would come with commensurate risks for investors and financial consumers involved in this space, as the protection threshold for automatic liquidation would further thin. It should be noted that automatic liquidation happens instantly and without any notification to the investor, and it is up to the user to stay up to date with the value of the collateral at each point in time in order to avoid liquidation.[28]

[28]Certain applications are being built by third parties to allow for such notification of the users. For example, for Maker protocol, even if there is a smart contract called OSM (Oracle Security Module) that ensures that new price values propagated from the oracles are not taken up by the system until a specified delay has passed, there is no native notification features. External parties such as DeFi Saver enables to get a notification before your position gets liquidated, but there is still a requirement to know how to use them.

Figure 2.10.Collateralisation levels of top DeFi applications



Note: Collateralisation levels calculated on the basis of LTV ratios for each of the protocols for the period 20.06.2020-20.06.2021.
Source: Dune Analytics.

Borrowing and lending rates in DeFi lending protocols are much higher to those available for traditional financial products and are driven by supply and demand dynamics for each of the crypto-asset transacted (see Figure 2.11). Indicatively, providing USDC liquidity on the lending protocol Aave yields 6.27% APR as of 4 August 2021, and has been yielding 7.22% on average since the launch of the protocol (Codefi compare database). Such high rates have been an important driver of DeFi activity especially in a prolonged low-rate environment and a consequent search for yield by retail and institutional investors.

Figure 2.11. Borrowing and lending rates by major DeFi lending protocols

In percentages, as of 3 August 2021

Borrow rates (%)

	DAI	ETH	USDC	USDT	WBTC	LINK	ZRX	BAT	COMP	TUSD	REP	CRV	UNI	SNX
Maker	0.67	-	-	-	-	-	-	-	-	-	-	-	-	-
Compound	3.78	2.84	3.13	3.45	4.52	5.4	6.79	7.02	5.82	3.28	14.44	-	-	-
Aave	3.97	0.59	3.38	12.74	0.76	0.57	101.67	3.51	-	2.61	0.34	6.92	1.19	10.87
dYdX	5.58	1.29	5.47	-	-	-	-	-	-	-	-	-	-	-
Cream	7.97	4.12	10.61	14.38	5.23	1.91	-	-	8.04	-	-	17.40	1.79	5.94
DeFiner	3.21	1.77	2.59	2.93	1.21	7.18	4.34	4.50	-	-	-	-	-	-

Lending rates (%)

	DAI	ETH	USDC	USDT	WBTC	LINK	ZRX	BAT	COMP	TUSD	REP	CRV	UNI	SNX

Maker	0.01	-	-	-	-	-	-	-	-	-	-	-	-	-
Compound	2.37	0.18	1.77	2.15	0.38	0.57	0.76	0.84	0.69	1.95	0.00	-	-	-
Aave	3.52	0.02	2.55	5.43	0.02	0.00	1.85	0.54	-	0.91	0.03	2.46	0.07	2.40
dYdX	1.42	0.08	1.33	-	-	-	-	-	-	-	-	-	-	-
Cream	2.81	0.88	5.22	8.36	1.40	0.11	-	-	1.81	-	-	8.05	0.09	1.00
DeFiner	3.21	1.41	2.59	2.85	1.21	1.84	4.27	3.60	-	-	-	-	-	-

Source: Intotheblock.com.

Box 2.4. Flash loans in DeFi

Flash loans are one of the most interesting and noteworthy products of DeFi, as they demonstrate the level of sophistication of innovation and the emergence of new risks related to traditional financial services.

Flash loans are uncollateralised loans which enable users of DeFi to borrow without collateral, provided that they repay the loan to the pool in the same block on the blockchain. In other words, a user can borrow a crypto, arbitrage between exchanges, and then repay the loan with a fee, all in one block. The mechanism is based on software development that allows the packaging of all transactions and their submission as one single block. It aims to allow users to make profit by taking advantage of arbitrage opportunities between different crypto-assets and price disparities of such assets between decentralised exchanges.

Loans are mainly used for arbitrage opportunities, while they are also allowing the user to overcome a temporary liquidity squeeze or to acquire additional crypto-assets for leveraged exposure (Schär, 2021[3]).

At the same time, flash loans give rise to a number of very important risks: credit and liquidity risks, risk of high leverage if such practices were to expand, operational risks, risk of hacking and attacks, manipulation of prices and attacks on the code with no recourse or collateral. Examples of market manipulation through flash loans enabled by the unlimited leverage include the attack of Pancake Bunny in March 2021 (95% price drop) and of Alpha Homora protocol (USD 37m loss in February 2021) (Coinmarketcap, 2021[16]).

Flash loans involving governance tokens can also be used to undertake malicious governance attacks allowing bad actors to borrow governance tokens for the purpose of voting and return them in a single transaction and with no need for collateral.

3 Evolution and current state of DeFi markets

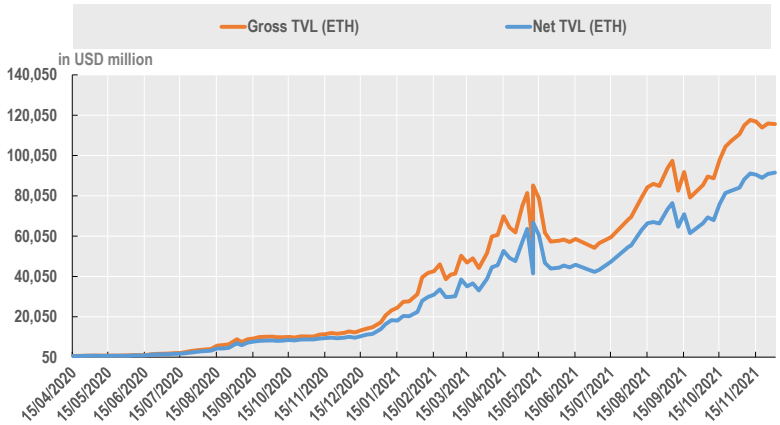
Decentralised projects came to the forefront in the past c.5 years (e.g. ETHLend lending platform established by the founder of Aave in 2017) but gained traction in the summer of 2020, when the market grew to over USD 50bn assets locked in DeFi protocol smart contracts. This section looks at the evolution of the market and its recent trends, discusses issuance and mechanics of governance tokens by DeFi protocols, provides an overview of trading activity in decentralised exchanges as well as analysis on the issuance and usage of stablecoins in the DeFi markets.

3.1. Market evolution and trends

The rapid growth of the DeFi market attention from market participants and policy bodies in the summer of 2020 (referred to as 'the DeFi summer'), when a number of DeFi applications appeared to gain traction with users, and has since grown to a multiple of its initial size. The gross total value of crypto-assets locked in ETH-based DeFi applications[29] (TVL) as of November 2021 reached USD 100bn up from USD 1.9bn on 2 July 2020 (50-fold increase, albeit from a very low base).

Alternative blockchains, such as the Binance Smart Chain and Polygon, are increasingly growing their presence in the DeFi space (19% and 9% of TVL respectively, as of 16 June 2021).

Figure 3.1. Gross and Net Total value locked (TVL) in DeFi (ETH)



Note: TVL (USD) is calculated by taking these balances and multiplying them by their price in USD. TVL in protocols built on the Ethereum blockchain only.
Source: Defipulse.com, theblock.com, as of 1 December 2021.

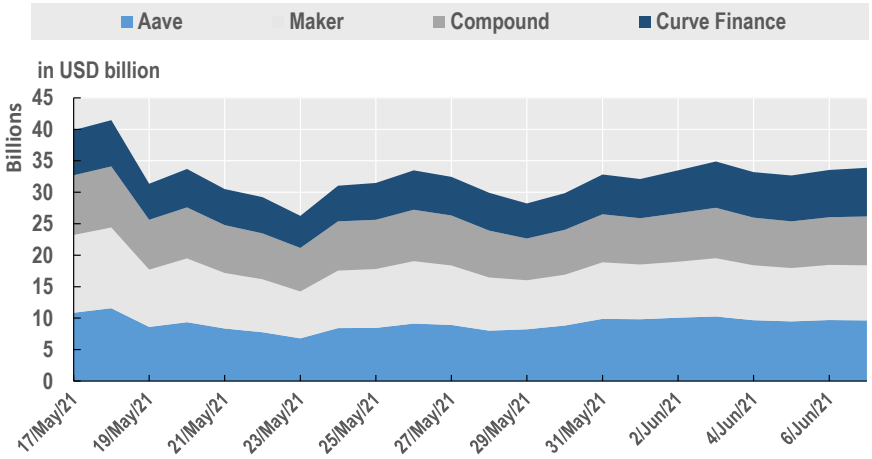
TVL is currently the best available proxy to ascertain the growth of this market, albeit with a lot of flaws associated with double-counting and miscalculations (see Box 2.1) as well as the lack of adjustment for the price effect linked to main crypto-assets.

[29] Total value locked calculated as total number of ETH and other ERC-20 tokens locked in the corresponding smart contracts of DeFi applications multiplied by the token price expressed in USD.

Net TVL is an attempt to refine the measurement of DeFi activity and address the issue of double counting, by excluding assets that are double-counted in multiple protocols. On average, c. 20% of value locked in smart contracts of DeFi applications seem to be double-counted at any point in time (Figure 2.1).

The DeFi market is currently highly concentrated in a small number of DeFi applications. The aggregated TVL of the top four DeFi applications accounts for almost half the TVL of the DeFi space as of May 2021 (see Figure 3.2).

Figure 3.2. TVL of top four DeFi applications accounts for roughly 50% of total TVL of the DeFi market



Note: Indicative calculation of gross TVL of top four DeFi applications for the period 17.05.2021 – 07.06.2021.
Source: intotheblock.com

The overall market value of DeFi tokens issued by the respective protocols stood at c.USD 72.3bn as of 17 July 2021[30], and is experiencing very wide volatility (8% drop over the last day in the above figure). The top five tokens account for c.35% of the total market capitalisation of DeFi-issued tokens (see Figure 3.2).

In addition to governance tokens, DeFi platforms issue crypto-assets or stablecoins aiming to support transactions in the app, on the back of transactions executed by users. They are described by the industry as DeFi's money supply and usually track the USD (e.g. DAI) or are representations of the crypto-asset deposited into the protocol's smart contract (e.g. WBTC, aETH).

The issuance of DeFi tokens has allowed for the development of yield farming or liquidity mining, a practice whereby participants lock their crypto-assets in a lending of market-making protocol (so called 'staking' of holdings[31]) in order to earn rewards (e.g. fees, new tokens).

Figure 3.3. Top 10 DeFi native tokens by market cap

NAME	PRICE (USD)	24hr %	7d %	Market Cap (USD m)	Volume (24hr) (m tokens)	Circulating supply (m tokens)
Uniswap (UNI)	18.71	-5.24	27.53	11,219	745	587

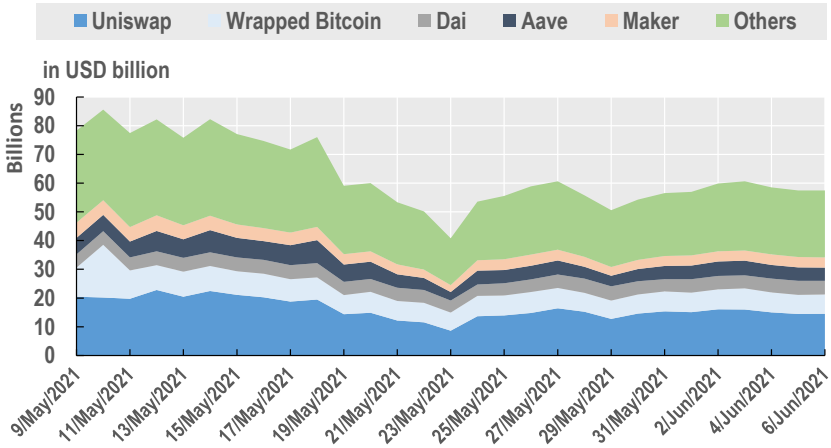
[30] https://coinmarketcap.com/view/defi/

[31] Different to staking for consensus purposes in proof of stake mechanisms.

Chainlink (LINK)	19.00	-0.33	38.07	8,576	1,364	441
Wrapped Bitcoin (WBTC)	38,107.87	-0.78	28.57	7,438	359	0.193
Dai (DAI)	1.00	-0.05	-0.09	5,567	535	5,561
Terra (LUNA)	9.26	3.45	58.51	3,953	446	417
Aave (AAVE)	300.27	-8.84	37.81	3,951	551	12
Pancakeswap (CAKE)	14.64	-1.25	31.09	2,985	375	201
The Graph (GRT)	0.57	-3.44	18.04	2,772	139	4,715
Maker (MKR)	2,651.88	-3.12	22.78	2,675	125	0.991
Compound (COMP)	394,13	-5.87	21.58	2,167	376	5,375

Note: As of 27 July 2021. This table includes self-proclaimed DeFi projects that may not be truly decentralised as per criterial defined in Section 2.1. of this report.
Source: https://coinmarketcap.com/view/defi/

Figure 3.4. Evolution of DeFi token market cap and dominant tokens



Note: Period 09.05.2021 – 06.06.2021.
Source: Intotheblock.

3.2. Governance tokens

In concept, governance tokens are a critical part of the DeFi ecosystem, as governance of DeFi protocols is to a large extent based on voting by tokenholders for any decision associated with the application. In practice, however, there are a lot of limitations to this. In concept, any member of the community can raise on-chain proposals to the community (e.g. to the DAO) and governance tokenholders are called to vote on proposals or other important decisions that need to be made. Proposals can include upgrades, changes in the mechanisms underlying the protocol, introduction of additional stablecoins for trading, change in the level of collateralisation or fees, but also allocation of treasury funds to developers or other users

contributing to the protocol, the hiring of staff and any other conceivable suggestion, such as the funding of a DeFi lobbying organisation[32]. Proposals are executable code, and are implemented if a majority votes for the proposal and a certain quorum is achieved, depending on the protocol. Some protocols compensate tokenholders for creating improvement proposals and/or for voting (e.g. Airswap).

In practice, however, at the current stage of development of the DeFi market, there are a number of limitations to governance through tokens. Not all participants get to vote and in many cases voting is disconnected from the governance token itself (e.g. through delegation). Not all protocol or smart contract changes occur due to votes of governance tokens, as some entities retain veto rights over the vote or control over discussion boards discussing protocol and smart contract changes. Software developers or venture capital investors financing the creation of the protocol in some cases retain controls related to voting, either through delegation or through the centralised holding of large governance token holdings. For instance, out of 15 of the largest voters in Uniswap's June 2021 governance proposal, six of the major voters were tied to university clubs, representing over USD 600m of tokens held (Bitcoin.com, 2021[17]).

Governance tokens are distributed in a variety of ways to users, including direct sales to the community, airdrops to platform users, or as rewards for providing liquidity to DeFi protocols. It should be highlighted, however, that in addition to their utility as voting tokens, these governance tokens are being traded in centralised and decentralised exchanges (DEXs) and the valuation of many of these native tokens has skyrocketed driven by speculative demand (for example, Yearn Finance is a governance token that started with a price of USD 6 and has reached USD 30,000 at its peak).

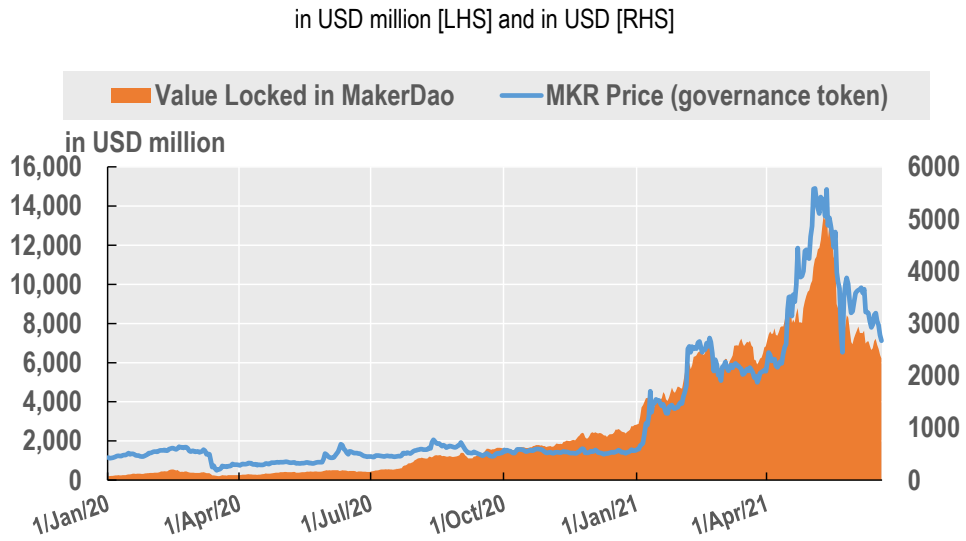
Governance tokens have some characteristics of securities/investment contracts and their issuance, promotion or trading in DeFi platforms could be considered non-compliant in many jurisdictions. In addition to being publicly traded, most DeFi tokens provide tokenholders with a reasonable expectation of profits to be derived from the efforts of other in the protocol. Tokens essentially endow tokenholders with either implicit or direct claims on cash flows generated through DeFi protocols (Carter and Jeng, 2021[18]).

Governance token ownership can be concentrated in a very small number of holders who are referred to as 'whales'. These can relate to the core software development team, the venture capital investors who receive such tokens as compensation for their investment or other investors who bought large parts of tokens in the market. In that case, users can make decisions that may be detrimental to the community, if there are economic incentives for them with negative repercussions for the rest of the tokenholders. Some protocols have imposed minimum thresholds of holding for tokenholders to be able to submit a proposal or for a vote to pass (e.g. Uniswap had until recently a proposal submission threshold of 2.5 million UNI and a vote requires 40 million UNI backing to go through).

The existence of governance tokens does not guarantee a robust governance process, on the contrary a number of risks emerge from the use of governance tokens for voting. Given that governance tokens are freely tradeable in DEXs, bad actors can get hold of important stakes of voting power ahead of a vote in order to influence the decision-making, or even propose and approve malicious proposals to the detriment of minority tokenholders. Flash loans (see Box 2.2) can also be used to undertake malicious governance attacks as they can allow bad actors to borrow governance tokens for the purpose of voting and return them within a single block and without the need for collateral. Added to that is the risk of potential exercising of voting rights by exchanges holding governance tokens and having no vested interest in the protocol's future.

[32] For more see: https://app.uniswap.org/#/vote/0/1

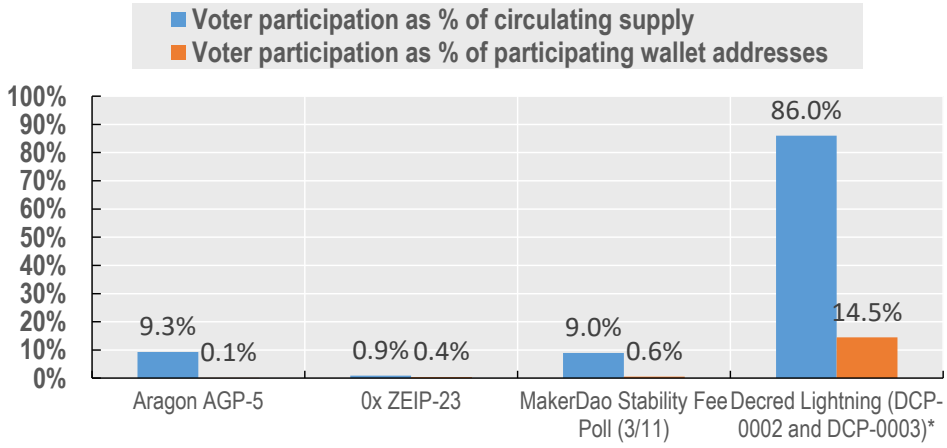
Figure 3.5. MakerDao value locked and native governance token price MKR evolution



Source: DuneAnalytics.

In addition, active governance in DeFi protocols is not guaranteed. In addition to potential questions around the distribution of tokens to the community and the risks related to the acquisition of voting power by malicious actors, the level of active involvement by tokenholders varies depending on the protocol or the proposal considered. Activist investors are rare and many tokenholders are unaware of proposals or unwilling to participate. Tokenholder apathy and lack of voter turnout is one of the large challenges around DeFi governance, with voting turnout levels being reported low (e.g. reported cases of proposals passing with as little as <1% of all outstanding votes). This, in turn, allows investors with a very small proportion of total supply of governance tokens to significantly swing the vote (Learner, 2019[19]) (see Figure 3.6).

Figure 3.6. Examples of voting turnout by weight of tokenholding vs. number of participants



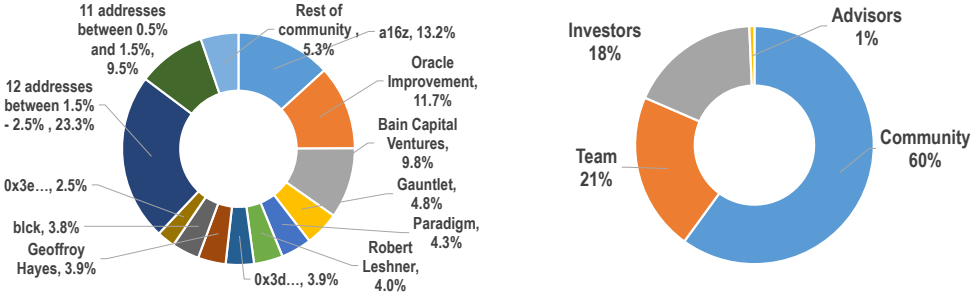
Note: Based on estimates.
Source: Foreground Capital, (Learner, 2019[19]).

Concentration of governance tokens by a handful of investors and/or the original core developers that built the protocol is another challenge for decentralisation. The developing team or venture capital funds

backing the initiation of the protocol can withhold a large proportion of governance tokens. VCs receive tokens in exchange for the funding provided to the project and core developer teams may get extra compensation for building the protocol in the form of tokens.

Figure 3.7. Voting weights in two of the top DeFi applications

Compound [LHS] and Uniswap [RHS]



Source: Application websites, as of 21 June 2021.

3.3. Trading activity in decentralised exchanges (DEXs)

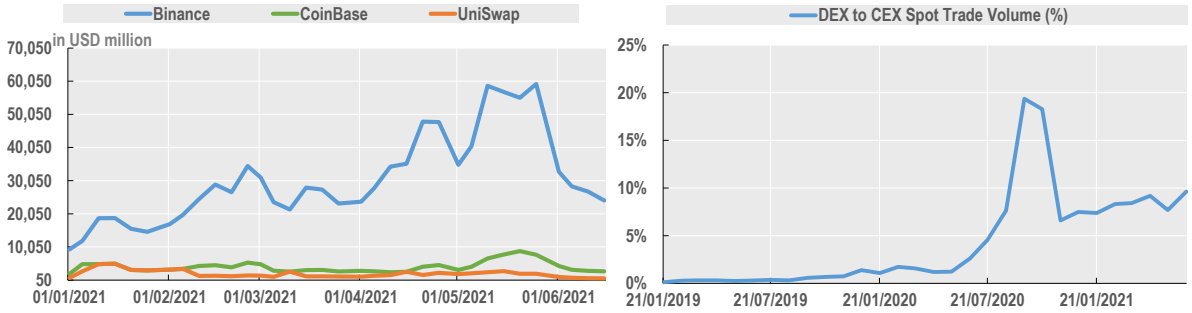
Decentralized exchanges (DEXs), automated market makers (AMMs), and token swapping aggregators are all types of decentralised exchanges that allow for P2P trading between users, while they maintain control of their funds in the self-custodian manner of DeFi protocols.[33]

Trading in DEXs recorded historical high volumes in Q2 2021, with total trading in Q2 2021 standing at USD 343bn (Consensys, 2021[12]). This compares against USD 335 billion of Coinbase's total trading volume in Q1 2021 and is noteworthy because DEXs enable trading only for EVM (Ethereum)-compatible assets, whereas 58% of Coinbase's trading is in Bitcoin (Consensys, 2021[12]). Uniswap and Sushiswap dominate the market for DEXs and account for c. 80% of trading volume as of June 2021.

The most important purported benefits of DEXs are atomic token swaps and real-time transparency to all users. Atomic settlement is one of the most important breakthroughs of blockchain-based financing with important implications for the post-trade of traditional financial securities (OECD, 2020[4]) (OECD, 2021[20]). In the case of DEXs, token swaps are simultaneous exchanges of crypto-assets that are compatible with the ERC-20 token standard and exist in the DeFi system. When it comes to real time transparency, the inherent public nature of public permissionless blockchains provides real-time access to all data related to transactions and crypto-assets. What is questionable though, is the extent to which the average retail user can make meaningful use or even understand such trade data.

[33] With the except of the time when tokens are locked into a protocol.

Figure 3.8. Trading volume in decentralised exchanges vs. centralised crypto-exchanges



Source: CoinGecko as of 30 June 2021.

3.4. The role of stablecoins

The role of stablecoins in DeFi markets is critical as such DLT-based fiat-backed tokens are some of the main types of collateral used to provide liquidity to DeFi applications. Total stablecoin supply stood at USD 73.5bn as of 30 June 2021, with Tether, USD Circle and Binance USD dominating issuance (see Figure 3.9). These three stablecoins are backed by fiat collateral, while DAI, MakerDao's stablecoin, is a crypto-collateralised stablecoin. Crypto-collateralised stablecoins, such as DAI, are backed by cryptoassets and are therefore less linked to the traditional financial system, although DAI still aims to maintain a (soft) peg to the USD, trading at or around 1 USD on average. In terms of market capitalisation of stablecoins, the above-mentioned collateralised stablecoins comprise 87% and DAI 5% of the market, respectively (as of August 2021) (see Figure 3.9).

Stablecoins are an indispensable ingredient of DeFi markets and one of the foundational basis of such markets; indicatively, it is estimated that DeFi lending protocols like MakerDAO, Compound, and Aave hold about 23% of the total USDC supply (Consensys, 2021[12]). Stablecoins are also used by participants in such markets as a way to hedge against crypto-asset volatility without having to convert their crypto-assets into fiat currency through a centralised exchange. Swaps between ETH and other ERC-20 tokens and stablecoins are one of the most frequent trading pairs that users access through MetaMask Swaps (Consensys, 2021[12]).

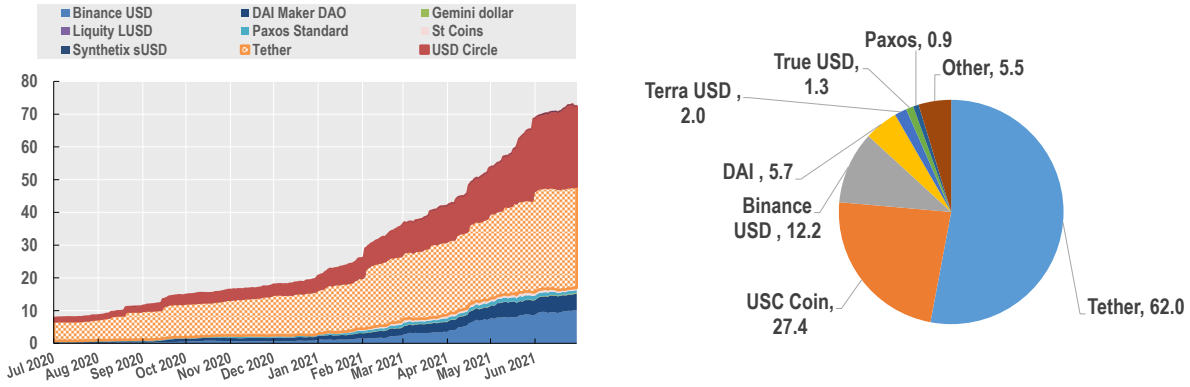
The use of stablecoins in DeFi protocols significantly increases interconnectedness between the DeFi and the CeFi worlds. Collateralised stablecoins are mostly USD-denominated tokens that purportedly are backed by financial assets held as reserves in a traditional financial institution and therefore, when used in DeFi applications introduce a close interlinkage between DeFi, the stablecoin issuer and traditional financial institutions acting as custodians of reserves underlying the stablecoins.

Centralised stablecoins expose users and the system to risks related to their trustworthiness associated with the auditability and reporting around their reserves, as well as with the composition of such reserves and stability of the custodian of such reserves. For example, Tether has been proven to have deceived clients by overstating reserves, making false statements about the backing of the stablecoin (CFTC, 2021[21]) (NY Attorney General, 2021[22]). In addition, stablecoins are reportedly increasingly investing in commercial paper as part of their reserves backing the crypto-asset issued. Indicatively, Tether claims to hold c.USD30bn in commercial paper, ranking as the 7th largest holder of such instruments globally, according to JPMorgan (Financial Times, 2021[23]). Stablecoins offering redemptions at par are exposed to liquidity risks and the possibility of 'breaking the buck'. In addition, any sudden risk aversion to certain stablecoins with significant holdings of such short-term debt instruments could cause significant disruption in CP and other short-term debt markets.

The increase in the use of stablecoins could potentially support mass adoption of DeFi, while at the same time constitute one of the greatest points of vulnerability of the DeFi market and a potential channel of risk transmission to the traditional financial markets. In a scenario where USDT or USDC loses its peg due to solvency issues of the issuers related to the reserves backing the stablecoin or its under-collateralisation, decentralised exchanges would go under severe stress and liquidity pools would be forced to mass liquidations. Investors exposed to losses in DeFi may have to close positions on traditional markets, too, propagating the shock. The ensuing risks of the wider use of stablecoins within and outside the crypto-asset space and their role as linkages between the DeFi and CeFi systems warrant an appropriate regulatory and supervisory framework and standards that will ensure appropriate protection levels for investors and financial consumers while supporting financial stability overall. It should also be noted that other risks present in DeFi markets (operational, cyber, governance, etc.) might also negatively impact investor confidence in the financial system.

Figure 3.9. Stablecoin supply per type of stablecoin and stablecoin market capitalisation

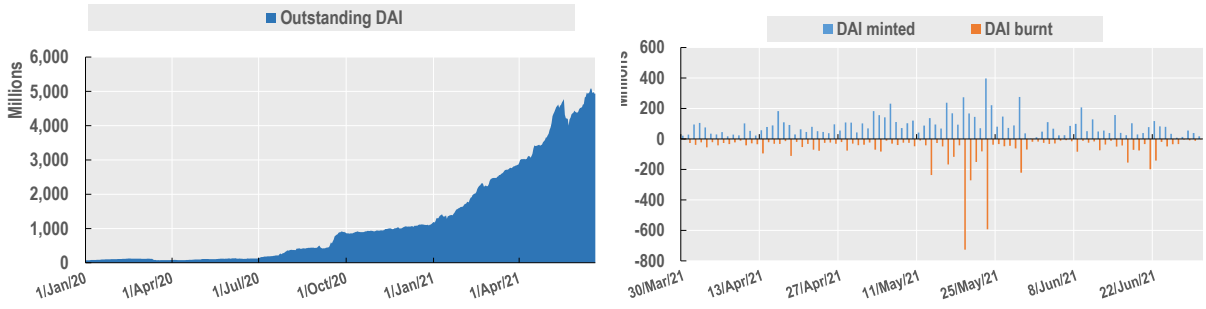
In USD billion [LHS] and in % [RHS]



Source: Dune Analytics (stablecoin supply LHS as of 30.06.2021), Coinmarketcap.com (stablecoin market cap, RHS, as of 01.08.2021).

Figure 3.10. Evolution of supply of MakerDao's stablecoin DAI

Outstanding DAI and evolution of issuance and cancellation of DAI



Source: MakerDao, Dune Analytics.

4 The benefits and risks of DeFi and DeFi/CeFi intersection

Although the size of the DeFi market itself is not large enough to be considered a risk to the stability of financial markets at its current level, its interconnection with the larger USD 3 trillion crypto-asset market suggests that it is worth closer scrutiny. The DeFi market is growing rapidly and attracts an increasing number of retail investors, exposing them to high risks. Increased interest and adoption of crypto-assets by institutional investors and other traditional financial service providers is leading to increased interconnections between traditional/centralised finance (CeFi) and the DeFi system through intersection or convergence points. What is more, the increasing use of stablecoins, tokenised and digital assets makes the boundaries of the two systems more porous and increases risks of spillovers to the traditional financial system and the real economy. Such risks are exacerbated by the recent price performance of main crypto-assets (BTC, ETH) and the recycling of profits in the DeFi space.

This section looks into the potential benefits of decentralised finance, the emerging challenges and risks for participants and the market overall, and discusses the possible transmission channels of those risks from the decentralised to the traditional financial markets.

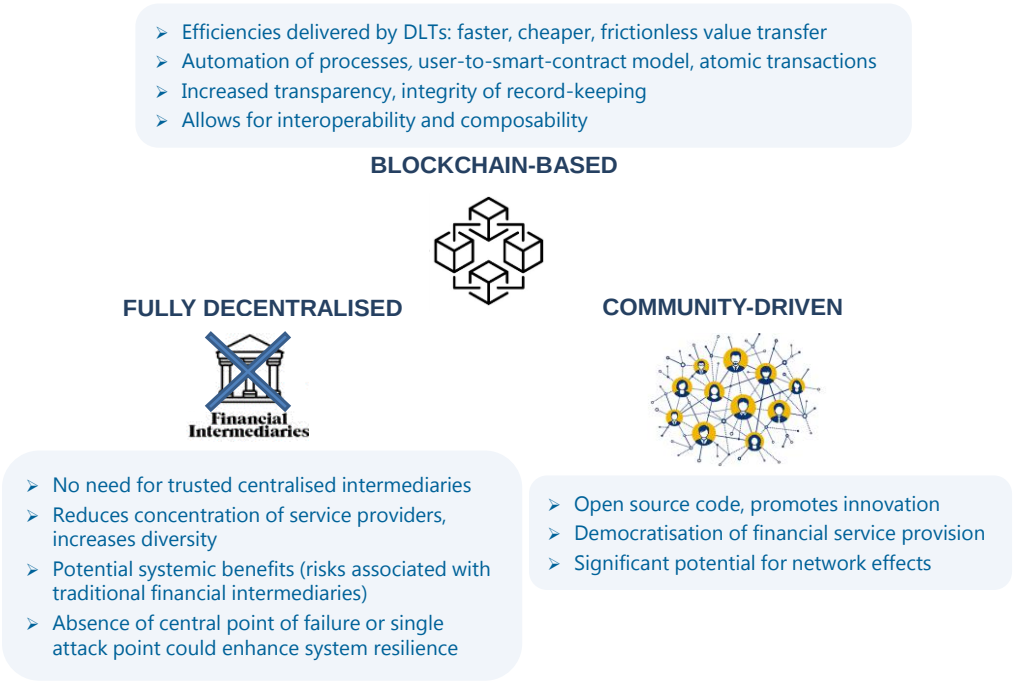
4.1. Potential benefits of DeFi

DeFi applications have the potential to deliver important efficiencies through the transfer of value without the need for trusted centralised intermediaries and through more efficient automation of processes. As with any tokenisation transaction, decentralised applications may result in faster, potentially cheaper and frictionless transactions driven by disintermediation and automation (OECD, 2020[4]). In addition, DeFi applications are building on the use of smart contracts, which could allow for cost reduction in issuance, administration, execution of transactions while also potentially reducing execution risk.

Transparency is promoted as all transactions are publicly available for everyone to analyse, although on a pseudonymous basis. The transparency offered by DLTs provides efficient auditing of solvency and proof of reserve (Carter and Jeng, 2021[18]).No human intervention is required in fully automated smart-contract-to-smart-contract mechanisms, and the transactions are triggered based on data feeds provided by the protocol or external nodes (such as Oracles).

Transactions in DeFi can be executed atomically, i.e. the wallet-to-wallet exchange of two digital assets simultaneously in a single operation or delivery versus payment instantaneously and without central counterparties (CCPs) to guarantee the transaction. Atomic settlement can provide benefits of speed and costs, as it eliminates the need for CCPs, collateral management and clearing. It should be noted, however, that similar benefits are realised in permissioned DLT-based systems for clearing and settlement and are not a privilege unique to DeFi markets. What is more, at least currently, transactions on Ethereum are much more expensive than in comparable legacy systems.

Figure 4.1. Potential benefits of decentralisation



Source: Author's illustration.

The application of distributed ledger technologies for the provision of financial services may reduce some of the financial stability risks associated with traditional financial institutions and intermediaries (FSB, 2019[2]). The decentralised nature and dispersion of financial service providers could increase diversity in the financial system and reduce the concentration of service providers. Decentralised networks for lending can reduce the reliance on existing intermediaries to channel short-term funding into lending, reducing solvency and liquidity risks for their balance sheets (FSB, 2019[2]).

The absence of a central point of failure or single attack point in a decentralised setting could enhance the resilience of the system. If appropriately secure, decentralised systems may be more resilient to cyber risk than highly centralised systems also in terms of the integrity of their record-keeping and service availability (FSB, 2019[2]).

Custody chains typically involved in traditional asset holdings could be shortened and their transparency increased, if DeFi users have self-custody of their assets. This, in turn, could decrease potential risks of liquidity problems arising in custodians in case of operational issues, financial distress or default.

Importantly, the code underlying the DeFi protocol is in most cases open source, so available for anyone to review and contribute to and such practice could constitute a source of democratised innovation by any participant of the ecosystem. The DeFi system's composability gives room for innovation in products and services that leverage on the accessibility of open source infrastructure to create new products. Such products can be the combination of multiple existing applications, built on top of existing applications. DeFi's promise of interoperability across blockchains, if achieved, could help diminish financial sector silos, promote innovation and build vibrant financial ecosystems (Carter and Jeng, 2021[18]).

Industry participants claim DeFi could be democratising financial services and could enhance global financial inclusion. Nevertheless, in practice, inclusion could be limited in this space if one considers the complexity of the technologies used and the technical capabilities and infrastructure that are required for such networks. It is, however, true that participating nodes in a DeFi network are – in most cases - given

governing rights to the network and can decide upon its future, which is not always the case in other financial services.

Increasing integration of decentralised finance with the conventional financial system, conceivable as a further stage of development, could have a beneficial impact on the traditional financial markets (Deutsche Bundesbank, 2021[24]). Such integration could result in stronger competition accompanied by lower transaction costs (Deutsche Bundesbank, 2021[24]). Such evolution would come with corresponding key risks that would need to be investigated and mitigated accordingly.

The development of DeFi markets could be seen as a testing ground for the use of DLTs in financial services. This is particularly relevant for jurisdictions such as the EU where initiatives are in place to introduce legal foundations for the pilot use of DLTs in traditional financial market infrastructure (e.g. European Commission's pilot regime for market infrastructures based on DLT) (European Commission, 2020[25]). In such cases, authorities could benefit from analysis of the functioning of DeFi markets in order to draw lessons for the broader use of DLTs in traditional finance, which would constitute a helpful contribution of DeFi to traditional finance.

Most of the DeFi benefits mentioned above are essentially associated with the purported benefits of DLT-based applications in finance and relate to efficiencies, transparency, resilience and reduction of friction. These benefits are however still to be proven for all types of blockchain-based financial applications. We are still in early days where it is difficult to assess whether these purported benefits will be achieved, and if so, whether they outweigh potential risks.

4.1.1. Financial inclusion

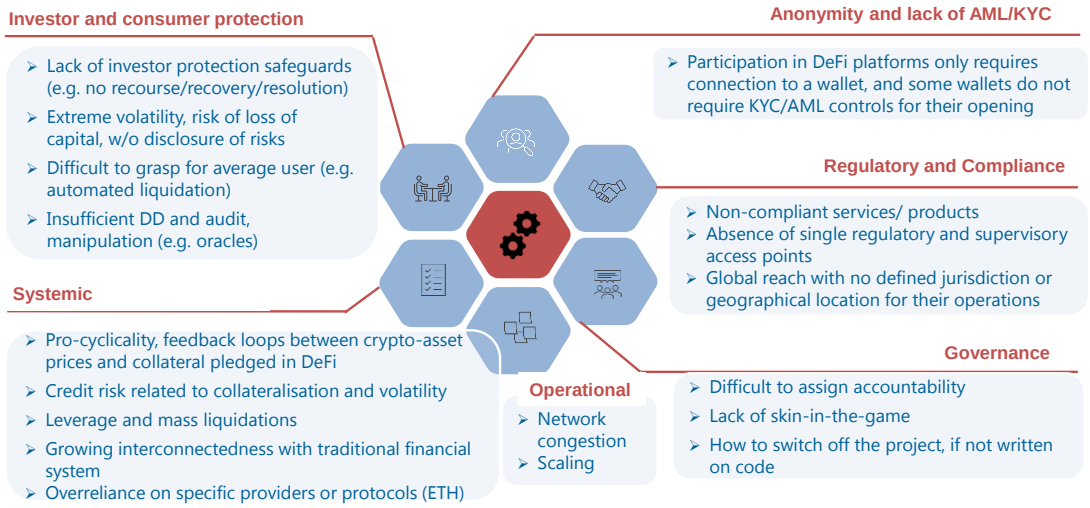
One of the most important purported benefits of DeFi is related to financial inclusion and the potential of DeFi to serve underserved parts of the population such as SMEs. According to proponents of such purported benefits, DeFi could replace onerous transaction banking services and overhaul the inflexibility of present processes, allowing SMEs to tap increased liquidity and alternative credit opportunities. By way of example, unbanked SMEs could use major DeFi exchanges to either make direct payments or convert payment amounts to USD-backed stablecoin for cross-border remittances or use DeFi lending protocols for their financing (WEF, 2021[26]).

At the same time, a number of arguments are counter to the financial inclusion narrative of DeFi proponents, particularly for retail investors and SMEs. Small business owners may not have the sophisticated knowledge and understanding of DeFi mechanisms or awareness of the impact of crypto-asset volatility on the functioning of such markets. Moreover, although decentralised finance provides trust through disintermediation and atomic (DvP/PvP) settlement, users are required to trust the author of the smart contract on the basis of which the transaction is executed. Unless the users have the technical capabilities to carry out the audit of the smart contract code themselves, they have to rely on software developers. Also, transactions costs at the current construct of the settlement layer may be prohibitive for small-sized transactions, particularly in moments of stress of the network, which may not be commensurate with the needs of small businesses (see Section 4.2.5 on network congestion and fees).

4.2. Key risks

DeFi applications and markets give rise to a number of risks, some inherent in DLT-based systems, and others stemming from innovations in the architecture and operations of such markets. This section gives a brief overview of regulatory and compliance-related risks; challenges around governance in decentralised networks; risks for investors and financial consumers; potential systemic implications of DeFi markets; and technology-related and operational risks.

Figure 4.2. A multitude of potential risks



Source: Author's illustration.

4.2.1. Regulation and compliance

Numerous DeFi applications (or part of their activities) are involved in non-compliant provision of regulated financial services and products, often reserved only for licensed entities. Regulators in most jurisdictions with active tokenised markets have adopted a technology-neutral approach to policies around DLT-based financial activity, with the same rules applying to the same types of activities and risks, irrespective of the technological medium through which the product/service or activity is provided (OECD, 2021[20]). As such, the use of DLTs or other technology does not affect the way these regulators assess whether or not the ensuing financial product/service or activity falls within the regulatory perimeter, and by consequence, whether it is regulated or unregulated.

Currently, numerous DeFi platforms deliver financial services in a non-compliant way, exposing participants and the market to significant risks. Despite their complexity, numerous DeFi applications, when broken down, could represent regulated activities for which comprehensive frameworks are already in place aiming at preserving financial stability, protecting financial consumers, promoting investor protection and market integrity, and mitigating illicit finance risks. Non-compliance of DeFi systems with existing frameworks gives rise to pronounced risks for participants and the market. Equally, other DeFi applications or activities currently falling outside of the regulated space in some jurisdictions raise risks that are left unaddressed by the existing rules (indicatively, issuance of crypto-assets that do not qualify as financial instruments or funds or e-money in the EU)[34].

Some of the characteristics of DeFi may be incompatible with existing regulatory frameworks, particularly given that the current framework is designed for a system that has financial intermediaries at its core. For example, frameworks are in place for the registration, licensing and supervision of intermediaries involved in issuance, brokerage/trading, custody and lending activities. The existence of intermediaries is contrary to the very essence of decentralised finance, and it is often difficult to even identify parties involved that can be assessed or regulated. Enforcement of existing regulation is also difficult to apply given the absence of a responsible entity. As such, it may also be the case that current regulatory frameworks may not be suitable to regulate decentralised networks in certain jurisdictions.

[34] For more information around the EU proposed framework for markets in crypto-assets (MiCA) see (European Commission, 2020[27]).

Potential regulatory gaps may appear for types of risks that arise in DeFi systems and which may stem from the novel characteristics of financial service provision in decentralised systems. Such potential gaps in the regulatory treatment of DeFi services could require further review, as they may give rise to regulatory arbitrage opportunities. For example, it could be argued that in the absence of prudential rules, DeFi is vulnerable to over-leveraging and other related financial risks. The experience of asset tokenisation has shown that policy makers could consider adjusting existing regulatory and supervisory frameworks and/or adopting new requirements to cover the novelties that DLT technologies bring and the new emerging risks that are stemming from the innovative nature of the technologies used (OECD, 2021[20]). The recent MiCA legislative proposal in the EU is an example of such need (European Commission, 2020[27]).

The absence of single regulatory and supervisory access points in decentralised DeFi networks is one of the key policy questions that remains to be overcome. Given the decentralised nature of the networks on the basis of which DeFi applications operate, and their community-driven governance, it is difficult to identify decision-making entities/actors that can be held accountable for the operation of the network. In some jurisdictions, policy makers may not currently have the legal basis for such access (e.g. to nodes participating in a system) even if access points were to be identified. This makes oversight, attribution of responsibility, and even communication with supervisors cumbersome, given that currently supervisory mandates are designed based on the existence of centralised decision-making bodies (e.g. financial intermediaries). Parties that are key for the development of the protocol, such as software developers or smart contract providers, may actually not even constitute nodes to the network, further reducing the scope for rendering them accountable. Composability adds to the difficulty of supervision and enforcement, given the complexity of products layered on top of each other, and the difficulty in assessing where the weak point is and who enabled it.

DeFi networks are global in reach and operation, with no defined jurisdiction and geographical location for their operations, which in turn increases jurisdictional uncertainty and challenges enforcement. This further obstructs oversight and regulatory compliance of such networks, particularly given the speed and ease with which financial service providers are able to change locations in response to actions of authorities (FSB, 2019[2]). Greater international policy collaboration and discussion can help overcome such challenges at the cross-border level.

Pseudonymity and lack of, or non compliance with, AML/CFT regulator requirements for some DeFi applications gives rise to risks of money laundering, terrorism financing, and other illicit use, facilitating misconduct. Participation in DeFi platforms only requires connection to a wallet, and some wallets do not require CDD or other AML/CFT controls for their opening. As such, nodes can remain pseudonymous without any link to the identity of the user, and with no controls as to the source of funds. The use of decentralised exchanges (DEX) is considered a prime example of the possibility of trading crypto-assets while staying under the radar of the supervisor, given the generalised absence of CDD checks.

Financial services provided in DeFi markets raise risks of regulatory arbitrage to the extent that they are not subject to regulation, or where there are important differences between the applicable regulatory frameworks between jurisdictions. At the national level, ‘going DeFi’ could be a way for market participants to try to avoid regulatory and supervisory costs, similar to other FinTech activities. Given the global reach and operation of DeFi networks, arbitrage opportunities may appear at a cross-border basis, and cooperation at the cross-jurisdictional level will be important to mitigate any such risks.

Regulators and supervisors may be exposed to reputational risks if consumers lose money on crypto-activity and DeFi and (wrongly) assume they have protection. Although regulators have explicitly highlighted the inherent risks of investing in crypto-assets on several occasions (e.g. (FCA, 2021[28]), they still carry the risk of being accused for not regulating crypto-assets more closely. As prudential requirements on crypto-assets are still being developed, in the event of a failing of a regulated institution as a result of their exposure to crypto (BCBS, 2021[29]), oversight from prudential regulators might be perceived as having been insufficient.

It should be also noted that in certain jurisdictions, such as the European Union, post-trading is not currently possible in a decentralised setting. Yet, possible interconnections between CeFi and DeFi do exist, adding to the complexity of the setting from a regulatory standpoint.

4.2.2. Challenges around governance of DeFi

The decentralised nature of DeFi gives rise to numerous challenges around governance of DeFi, with implications for consumer protection, oversight and enforcement. As mentioned above, the identification of decision-making entities/actors that can be held accountable is difficult, while at the same time impeding oversight and enforcement action by regulators and supervisors. Software operators or programmers who have provided the first cut of the protocol to the community have been suggested in some cases as the responsible entities/actors for the network. Could participants in a liquidity pool, or other node operators be held accountable for the operation of the network? And what about aggregators of applications, operators or user interfaces or other entities/actors facilitating transactions?

The provision of incentives for participation in the network, such as governance coins issued and distributed for free, could constitute security issuance depending on the jurisdiction.[35] Given that DeFi depends to a large extent on the creation and materialisation of network effects, for example for the accumulation of capital or liquidity, it is common practice for such networks to distribute free community tokens to participants. Most of these tokens have governance rights attached to them; however, they get upside from network expansion and can therefore not be considered as pure utility tokens. The distribution of governance tokens could actually be considered as offering of investment contracts, depending on the jurisdiction.

Given the decentralised character of the network, there is a risk of moral hazard and complete lack of accountability for the people who launch an open protocol for a DeFi project. In most cases, such projects are set up by individual programmers and are then shared as open protocols for the community to contribute to. What economic incentives exist for developers and others as a protocol transitions to being more decentralised? In most cases, initial VC funders, as well as core software developers, maintain part of the governance tokens as their compensation. The size of such holdings can be a critical factor in the operation of the protocol after its launch, and importantly, such holdings are not always known by users, nor by regulators and supervisors.[36]

Although no minority set of actors can manipulate most DeFi networks, depending on the governance structure, if most nodes decide to act in an unlawful or unfair manner, this can have repercussions on participating nodes. For example, if most nodes in a network decide to seize the assets of the network, this can be possible if there is no blocking mechanism for such eventualities built in the protocol.[37] Governance tokens are an important source of risk (see Section 3.2).

Lack of disclosure may be another impediment to the participation of tokenholders in votes, as, unlike regulated securities and issuers, there is no required communication.

[35] This will also depend on whether the tokens are created through mining, depending on the jurisdiction (e.g. under the proposed MiCA regulation in the EU).

[36] Although all holdings are publicly available on the chain, as these are reported on a pseudonymous basis there is no clear picture of shareholdings at an aggregate level available to the community (multiple addresses can belong to the same user).

[37] This example is made possible also due to the fact that DeFi relies on a non-custodial architecture. It should be noted, however, that this is driven by the use of permissionless systems and is not an inherent characteristic of DeFi itself.

Community splits on contentious decisions can also occur, leading to forks and network splits with potential repercussions for participants without the technical skills to understand such mechanisms. In proof-of-work systems like the Bitcoin or Ethereum[38] coordinated miners controlling more than 50% of the hashing power[39] of the network are effectively controlling the validation process and can therefore block transactions or decide upon the future of the chain. It is not clear across all DeFi projects whether and how changes in protocol that affect existing contracts can occur and whether such changes are decided by the community. Such lack of clarity exposes participants to future changes that affect them and which may be beyond their control.

It is unclear whether and how shutdown processes of DeFi applications are possible, in the event the protocol behaves in an unpredictable manner and its operation needs to cease. This is generally possible if someone holds an admin key to the protocol, which at the same time raises important risks for users, as admin keys can give control over user balances or protocol functioning. It is customary for some founders or software developer teams to retain an admin key at the early stages of the protocol life in order to be able to correct flaws or bugs at the protocol, upgrade or pause/shut it down (killer switch).[40] The inappropriate storing of keys, however, can allow malicious third parties to hack the application and compromise the smart contracts (Schär, 2021[3]). The founders or core developers themselves could also use the admin key to drain user funds, if compromised and motivated by significant monetary incentives.

Overall, despite the underlying decentralised nature of DeFi, human intervention in a centralised manner oftern remains present in governance, whether through concentrated holdings of governance tokens or through the existence of admin keys. Such centralised human intervention could be a control point for regulators (Ushida and Angel, 2021[5]).

4.2.3. Investor and financial consumer risks

In DeFi, the lack of traditional regulatory safeguards for investor protection, existing across the board of financial services regulation, leaves investors and financial consumers more exposed to forms of loss or erosion of value. Users have no recourse in case of default or failure of the DeFi protocol, and in most cases it is also difficult to identify a responsible party or central authority to turn to in case of consumer concerns. Additionally, there are no recovery schemes or resolution mechanisms, exposing participants to risks of total loss of investment in case of default. Related to that, DeFi projects can go live with little or no due diligence. Any software developer can launch a new project with zero audit or testing, and indeed, there have been numerous cases where the existence of bugs or other technological glitches were identified post-launch. This resulted in the malfunction or even collapse of the systems, with participants incurring significant monetary losses. In addition, the economic incentives of providing liquidity in order to get rewarded with governance tokens, encourages competitive and speculative behaviour which leads back to a centralised governance structure, since tokens slowly concentrate in a few hands.

Although it is true that DeFi democratises participation for all nodes and gives power to participants, there are many aspects of DeFi products and transactions that the average participant does not understand, exposing him/her to substantial credit and liquidity risks. For a non-programmer, it is very difficult to interact with the interfaces of DeFi if one is not familiar with blockchain technology, given the technical complexity of DLTs and composable DeFi financial services. Even when user-friendly web interfaces allow for an easier access to DeFi protocols, the average consumer of DeFi-based financial products is unable to fully

[38] Prior to the London hard fork upgrade, through which it migrated to a proof-of-stake mechanism.

[39] Hashing power is the power that a computer uses to run and solve different hashing algorithms. Such algorithms are used for mining, i.e. generating new cryptocurrencies and allowing transactions between them.

[40] As of 12 April 2021, the major DeFi protocols Synthetix, Yearn, Dharma, SushiSwap, Badger, Harvest, and Ren – containing user deposits of USD 10.58 billion collectively maintained admin keys enabling a discretionary freeze of user funds (Carter and Jeng, 2021[18]).

grasp the underlying complexity of a disintermediated system. Investors are therefore exposed to risk of full loss of capital through mechanisms whose functioning they do not understand, while it is also doubtful that participants are aware of the risks of full loss of capital. Similarly, the open source nature of the protocol's code is useless to the non-expert developer user who cannot read or review the code.

Consumer protection and awareness of risks involved in DeFi protocols and disintermediated environments are important challenges for regulators, particularly in a low interest rate environment that may have incentivised a search of yield also among retail investors. Participants in some of the lending DeFi protocols may not realise that they need to manage their accounts similar to open positions on margin. Although this can be a comfortable situation for a trader, retail investors may be ill equipped to understand and prevent the risk of liquidation of their positions as the price of crypto-asset collateral falls. Significant price volatility of the crypto-asset market exacerbates this challenge and exposes consumers to increased risk of loss of capital. Importantly, participants are not notified of such risks upon joining many of the DeFi marketplaces. Price disruptions and dislocations are extremely frequent and unlike other financial markets, where consumers may have had experience prior to entering DeFi. What is more, the immaturity of the security of DeFi protocols exposes participants to risks of hacks. In August 2021, the Poly network was hacked and c. USD 600m in various cryptocurrencies were stolen (FT, 2021[30]), on top of USD 474m lost to hacks and fraud in DeFi earlier in 2021 before the Poly network hack (Benson, 2021[31]).

Transparency around DeFi protocol mechanisms and the blockchains that host them does not necessarily translate into improved investor and financial consumer awareness of the nature of financial risks. Open source code, while transparent, would not be sufficient for the average retail investor that does not have the requisite level of technological and financial literacy to understand the implicit risks. Technically, users would require a combination of coding skills and financial literacy in order to fully understand the mechanism of the protocol as well as the implications of the code on financial and other (e.g. governance) risks.

A generalised trend of gamification of finance may increase the attraction of financial consumers to DeFi as an alternative to traditional finance, with important corresponding risks for those users. Several platforms provide a user-friendly experience to the DeFi protocol, which makes trading akin to interacting on social media or playing online games. This gamification of markets may attract an increasing number of unexperienced investors, who are more likely to trade irrationally or follow unsound financial advice and research. While these issues are more related to consumer protection, they could also change the way markets behave in aggregate, with potential financial stability implications. All the more so as the loss of confidence could result in the sale of assets in the traditional financial system.

The mechanisms put in place in financial markets to avoid market manipulation are lacking in non-compliant DeFi markets. As such, numerous manipulation cases have been observed, notably associated with manipulation of oracles. These are nodes feeding external data into the network, with significant consequences of erroneous information being introduced into the network: for example, if manipulated price data is fed into the network, it can trigger massive sell-offs, causing liquidations or margin calls that result in substantial losses incurred by participants. Similarly, the manipulation of price feeds provided by an oracle can create risk-free arbitrage opportunities if the attack involves the manipulation of the spot price of the crypto-asset used as collateral in the Dapp. The pseudonymous nature of public permissionless blockchains and the lack of effective regulatory oversight increases the risk of frauds, and the permanent nature of the blockchain renders them irreversible, even when they have involved oracle manipulation or other malicious activity.

4.2.4. Potential systemic risks

Despite its small size, the DeFi market is giving rise to risks and vulnerabilities that could, in the future, result or contribute to systemic risks, such as leverage, procyclicality, and increased interconnectedness with traditional financial markets. In its 2019 assessment, the FSB argued that the small size of crypto-

asset markets relative to the broader financial system do not pose a threat to financial stability (FSB, 2019[32]) (FSB, 2018[33]). This assessment could be currently transposed to DeFi given the size of that market at the current stage, however, DeFi could accelerate existing risks from crypto, should it continue to grow and gain prominence.

The sizeable growth of DeFi for financial services such as lending could lead to greater procyclicality (FSB, 2019[2]). The supply of credit on a peer-to-peer basis may exhibit larger and sharper swings in the provision of credit compared to traditional lenders, especially if relying on automation and the use of novel data/processes (FSB, 2019[2]). What is more, the performance of markets relying on novel data or models remains untested in a downturn.

Potential correlations between the sharply rising crypto-asset markets and the growth of less regulated DeFi markets allow for a rise in leverage through crypto-collateralised lending. Such leverage supports the valuation of crypto-assets, which in turn supports the collateral value against which lending is made and maintains – if not increases – the exuberance around crypto-asset valuation levels. By enabling unregulated leverage, DeFi protocols could incentivise elevated crypto-asset valuations through the positive feedback loops between the two markets. This is exacerbated in case of unlimited uncollateralised leverage through flash loans, with the caveat that the transactions are structured in a way that ensures repayment of the loan within the same transaction block.

Despite the decentralised architecture of DeFi systems, they can give rise to new forms of concentration risks (FSB, 2019[2]). Such risks are driven by the use of similar technology[41] and in the concentration of key operations (e.g. code development, crypto-asset mining) in the hands of a relatively small set of persons or entities (e.g. software developers, owners of mining hardware). At the current stage of development of the DeFi market, the activity is concentrated in a very small number of protocols, despite the existence of numerous smaller applications (e.g. the aggregated TVL of the top four DeFi applications accounts for almost half the TVL of the DeFi space as of May 2021 (see Figure 3.2)).

Concerns over amplification of risk in digital markets and possible financial stability considerations arise also with regards to the level of collateralisation of some of the DeFi applications. Although some applications, such as lending, require over-collateralisation, the large volatility of the underlying crypto-assets pledged can easily reduce (and possibly eliminate) collateral value and turn over-collateralised positions into under-collateralised ones in a matter of seconds. The magnitude of volatility that turns highly collateralised positions into substantially under-collateralised, which in turn contributes to forced asset sales, creates vulnerabilities in the system. Moreover, while currently, the collateralisation levels of lending DeFi platforms exceed 100%; these levels are not expected to persist. Most platforms currently require over-collateralisation of loans by more than 100%, given the volatility of crypto-asset valuations. Increased competitive pressures given the growth of the market will call for more efficient use of capital in DeFi, and as such, collateralisation levels could drop, exposing users to ever-greater risks of loss of capital.

Excessive leverage is another source of vulnerability in DeFi. Users can lever up in an app by using the borrowed crypto-assets as collateral for further borrowing on the same assets, or by moving from one application to another, levering up at each step of the process. Given the extreme volatility of crypto-assets, massive sell-outs or flash crashes are likely to occur and can be exacerbated by the excessive leverage in the system. Mass liquidations following a decline in crypto-asset prices are already the norm in DeFi and happen in an automated way, for example in liquidity pools, when the over-collateralisation ratio drops below a certain point. Such liquidations can have a domino effect on investor holdings across the board,

[41] At the same time it is worth noting that the concentration of DeFi services within one settlement layer (i.e. the dominance of Ethereum network which still prevails despite the emergence and growth of alternative networks) is understandable given the fact that one of the strongest selling points of DeFi is its composability, which is easiest to achieve with a common settlement layer.

and could have spill over effects in traditional markets given increasing interconnectedness between markets for crypto-assets and CeFi.

Growth in the holding and use of crypto-assets by traditional institutional and retail investors may create increased interconnections with the DeFi space (see Section 4.3). This could become even more pertinent if the use of stablecoins grows further and tokenisation of assets more broadly becomes mainstream. Increased interconnections between the two parallel systems would introduce systemic risks given the absence of most traditional regulatory safeguards in DeFi. The loss of confidence in the DeFi market could have spillovers in traditional markets and the real economy and to digital finance across digital assets, creating vulnerabilities to financial stability.

When it comes to financial stability, the implications might differ depending on the type of crypto-assets involved. For example, lending using Bitcoin as collateral would be different to similar operations using stablecoins or other tokenised assets, as the level of interconnectedness of the latter with the financial system is higher. The same holds for combined liquidity and maturity transformation, leverage, opacity and complexity of credit intermediation, and interconnectedness to a USD 3 trillion market for crypto-assets with a risk of a sharp unwinding of DeFi positions spreading to the wider crypto-asset market and, in turn, to traditional markets. It remains to be further analysed whether DeFi compounds existing vulnerability by adding digital leverage to traditional leverage, or adds new ones (e.g. the use of DeFi to create synthetic leverage through the digital markets, without violating fund regulations).

DeFi could also have implications for monetary policy transmission, as DeFi financial services may be less responsive to official sector interventions that have previously been used to remedy financial stability risks (FSB, 2019[2]). For example, liquidity facilities and lender-of-last-resort functions of the central banks are provided through traditional centralised structures. The efficacy of such tools is likely to be reduced in a decentralised setting.

4.2.5. Technology and operational risks

Similar to all types of DLT-based applications, DeFi projects give rise to technology-driven and operational risks with potential negative consequences for users and the marketplace. Technology-related risks are mostly associated with protocol flaws, for example errors in the code. Like all new technologies, DLTs are still immature in terms of their design and robustness. Audits and due diligence processes are rare in DeFi markets given the way governance is defused across the network, with no clear accountability anywhere in the system.

Operational risks also arise in relation to the quality assurance of smart contracts that enable DeFi protocols. Numerous examples of bug exploits leading to theft of crypto-assets show the impact of failures in this regard. The level of automation and dependence on the functioning of smart contracts and their underlying code intensifies the corresponding risks to users. The open source approach that is seen as a quality assurance technique by the proponents of DeFi has not proved to be efficient at ensuring quality. In addition, reliance on the efficient functioning of the underlying blockchain network (settlement layer) is also exposing users to operational risks as any disruption at this layer results in the disruption of services built on top of this.

Risks related to the underlying blockchain network come in two forms: network congestion due to lack of scalability, or absence of critical mass. Blockchain systems are very much based on the creation of network effects, and the underlying network is valuable as long as a critical mass of nodes on the network is attained so as to reach consensus, trade and transact. Early adopters take the risk of the network not reaching such critical mass. Lack of scale can also potential allow for node concentration and weakened security, making 51% attacks potentially easier to achieve.

Network congestion is one of the most pressing operational challenges of DeFi markets. As the number of DeFi applications have grown exponentially, and given that the vast majority of these applications run on

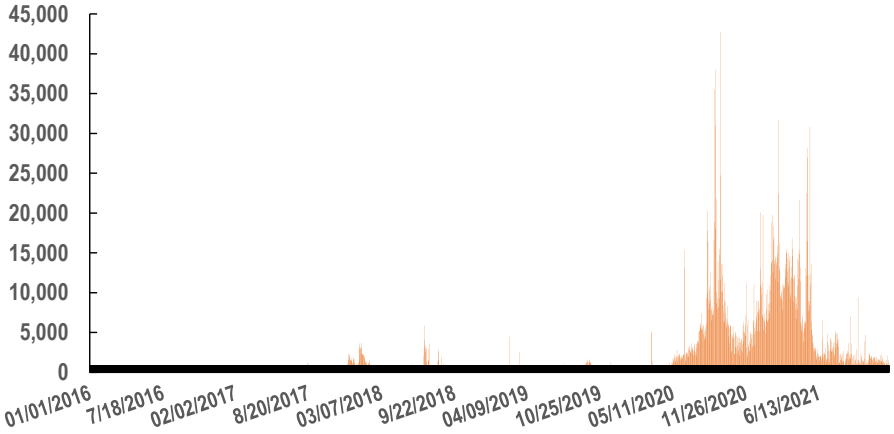
the Ethereum blockchain, the network has often experienced congestion, as each transaction needs to be validated before being added to the blockchain. This issue has been aggravated by the limited throughput of the Ethereum blockchain. Such congestion results in delays in the execution of transactions that may otherwise need to be settled real-time, in increased fees, also undermining market liquidity.

Layer 2 scaling solutions are a growing area of research and development in DeFi, as they promise to offer a way to reduce network congestion by increasing transaction throughput and lowering transaction fees. With Layer 1 being the Ethereum blockchain, Layer 2 is a term used to describe solutions designed to help scale applications by handling transactions off the main chain (on side-chains) and settle them once in a while on the main chain. Sidechains, sharding splits or rollups are all techniques that try to address scalability issues through transactional parsimony, by reducing a transaction into as few final bytes as possible (Carter and Jeng, 2021[18]). The use of Layer 2 solutions seems to take away the qualities of public transparency as well as the presence of a ledger that is updated in real-time, which are key propositions of public permissionless blockchain technology, and at the same time may be enabling market manipulation.

Related to the issue of network congestion is the problem of high gas fees paid by nodes as transaction costs, and which affects participants interacting with DeFi applications or transacting on DeFi. Similar to financial intermediary fees, each transaction on the Ethereum network incurs gas fees, as each transaction has to be validated by miners who are paid in gas in return for their services. As most of the DeFi activity sits on the Ethereum network, the price of gas cost, as denominated in gwei, has skyrocketed in the past year (see Figure 3.1) sometimes resulting in the cost of the transaction surpassing the value that is actually being transacted, rendering small transactions uneconomical.

Increased fees inhibit small transactions, as users are dis-incentivised to execute small-valued transaction when facing disproportionately high fees, effectively being priced out. This results in an increase in the size of transactions executed in response to a surge in fees, and with the consequent blocking of users' assets with disruptive effects to smaller retail investors, which is weakening the financial inclusion and democratisation of finance benefit proposed by DeFi. Transactions related to stablecoins like USDT also exhibit similar behaviour in response to high and volatile transaction/validation fees (Carter, 2020[11]). In addition, increased gas fees as a reaction to increased demand for transaction execution on the settlement layer tend to occur when users need it the most, as for example is the case when users need to interact with lending protocols to top up their collateral so as to avoid liquidation. Indicatively, gas fees reached 300 Gwei on May 18th or the equivalent of over USD 100. Since June 2021, the median gas fee has been on average 30 Gwei, or USD 1.33 for a simple transfer of crypto-assets (Consensys, 2021[12]). It is also worth noting that users do not earn gas fees if a transaction fails.

Figure 4.3. Ethereum network transaction fees (in Ether)



Source: Etherscan.io.

Over-reliance on one technology or infrastructure provider is another risk in DeFi markets. Currently, most of the activity in DeFi sits on the Ethereum blockchain, given that its code language is one of the earliest ones in the market to support smart contracts, as well as the fact that ETH is the only asset that can be used to pay transaction fees on Ethereum. The recent upgrade of the Ethereum blockchain (EIP 1559) implemented changes to the chain's tokenomics, including burning of transaction fees rather than paying them out to miners, which has also influenced the price of ETH[42]. Issuance of statements similar to the ones clarifying the status of ETH is expected to help diversify the use of other tokens or chains. The adoption of ETH by regulated financial institutions is also thought to have assisted in its use as a primary basis in DeFi.

Validator-based exploitations known as "miner extractable value" (MEV) involve the front running of transacting users or the selective transaction reordering by miners or validators at the expense of users (Daian et al., 2019[34]). The vast majority of observed MEV takes place on AMM exchanges, with validators gaining priority by outbidding users or reordering transactions if they are the miners. Given that MEV extractors do not have any obligation against the individuals they are outbidding or displacing, there are no natural limits to the exploitation of users by MEV (Carter and Jeng, 2021[18]). Similarly, inflation bugs, i.e. intentional manipulation which inflate the supply of coins ahead of a pre-agreed or expected schedule represent network-wide risks, can allow a 51% miner attack to cause inflation and destabilise a DeFi app (Carter and Jeng, 2021[18]).

Other operational risks in DeFi are similar to the ones arising in any DLT-based environment. Cyber risks, risk of hacking and various types of attacks or exploits (e.g. on smart contract code, on liquidity pools, oracles or smart contracts) are amplified by the immaturity of the market and the complexity of its applications, including through composability (OECD, 2020[4]), (OECD, 2021[20]). The risks of cyber attacks and exploits are more pronounced in DeFi settings given pseudonymity and numerous examples of market manipulation of voting and token prices have been observed. Other operational risks include network stability, risks related to interoperability, as well as business risks related to the achievement of settlement finality (OECD, 2021[20]).

[42] Some industry participants argue that reliance on ETH is also due to the fact that it is one of the very few crypto-assets that has been formally recognised as a commodity.

Box 4.1. Proof-of-work, proof-of-stake, energy consumption and the Ethereum Improvement Proposal (EIP) 1559

Energy intensive 'proof-of-work' consensus mechanisms, such as the ones applicable to the Bitcoin blockchain, require miners to solve complex mathematical puzzles to validate a new transaction, adding a block to the chain and permanently and irreversibly recording a new transaction. The proof-of-work validation mechanism is slow and highly energy-intensive given that the machines performing the 'work' are consume huge amounts of computing power for mining and render this consensus process unsustainable.[43]

Blockchain networks are increasingly shifting to 'proof-of-stake' mechanisms, and Ethereum began the process of transitioning to such a consensus mechanism (the EIP 1559) in January 2021, although transactions are still occurring on the original Ethereum main net that is proof-of-work (Ethereum.org, 2021[35]). The full migration to proof-of-stake will occur through a merging of the two and a migration to Ethereum 2.0 and to proof-of-stake, expected by Q2 2022. These are energy efficient alternative validation mechanisms for the verification of transactions/blocks without the need for expensive computations. Miners are replaced by validators and the choice of the validator in such mechanisms is based on the pledging of a stake (tokens) in the network.

Proof-of-stake mechanisms are also considered to be safer, as validators lock up their stake and put their capital at risk, given that they are slightly compensated for every validated transaction but harshly penalised for manipulation or attempted attack to the network. While in proof-of-work security comes from burning energy, in proof-of-stake security comes from putting up economic value at loss. Risks of high concentration of validators or collusion between validators exists in proof-of-stake mechanisms with ensuing risks of detrimental effects on end-users.

It should be noted, however, that neither proof-of-stake nor proof-of work models are immune to manipulation though a "51% attack". In the case of proof of stake models, an entity or a coalition of entities holding more than 50% of outstanding tokens can validate any transactions they wish, regardless of rules, including, in theory, double spends and misappropriation.

Source: (OECD, 2020[4]), (Ethereum.org, 2021[35]).

4.2.6. Other risks: legal framework for smart contracts, data availability and quality, energy consumption

Users of DeFi, similar to other blockchain-based applications, are not immune to the risk of fork or 51% attack, where miners or nodes who gain control of more than half a network's computing power can prevent the settlement of transactions or double-spend tokens. Risks of such forks or 51% attacks can occur irrespective of the type of consensus mechanism used by the protocol (see Box 4.1). Neither proof-of-stake nor proof-of-work models are immune to manipulation though a 51% attack. In the case of proof–of-stake models, an entity or a coalition of entities holding more than 50% of staked tokens can validate any transactions they wish, regardless of rules, including, in theory, double spends[44] and misappropriation.

Legal issues arise in regards to smart contracts that are the foundation of DeFi protocols, as these are currently incompatible with civil law in many jurisdictions. This relates to the fact that in most jurisdictions

[43] For more on bitcoin electricity consumption, see https://cbeci.org/.

[44] A single unit of currency is spent simultaneously more than once.

smart contracts are not contracts under civil law, and the interpretation of the provisions of civil law in the context of events in distributed ledgers remains to be defined (OECD, 2020[4]). Smart contracts are not legally binding in many jurisdictions, so any loss of investment due to operational or other reason related to such mechanisms cannot be brought to a court.[45] The application of the provisions on defects in declaration of will is an example of problems that may occur in that respect.

There is a general problem with the availability of reliable information and good quality data in the DeFi and crypto-asset space more broadly, which impedes the analysis of this market and may give rise to market manipulation. There are no reference prices for spot markets and each exchange operates as a silo, with trades executed on the prices for specific assets on each platform, presenting arbitrage opportunities. The lack of reliable information is particularly relevant given the social media element of crypto-asset platforms: many of the crypto news sites are owned by crypto players, with some (e.g. Coinbase) explicitly aimed at developing their research/content brand. There might be conflicts of interest in providing information and research that might be not as effectively managed as they are in traditional sell-side research providers.

When it comes to sustainability considerations and risks, the excessive energy consumption that is required to secure some decentralised networks is posing an additional risk depending on the consensus mechanism used by the network (see Box 4.1).

4.3. The intersection between DeFi and CeFi

Increased interest and adoption of crypto-assets by institutional investors and other traditional financial service providers is leading to increasing interconnections between centralised finance ('CeFi') and the parallel DeFi system. The DeFi summer in 2020 saw growing retail interest in DeFi, driven by speculation, fear of missing out and recycling of profits from other mainstream crypto-assets. Anecdotal evidence by market participants suggests that hedge funds and family offices have used DeFi as a tool to enable leveraged trading in crypto-assets.[46] Growing institutional interest in crypto-assets has led to the creation of DeFi protocols tailored to institutional investors. As such, the interaction between the two markets, DeFi and CeFi, is likely to further grow.

The increasing use of stablecoins makes the boundaries of the two systems more porous and increases risks of spillovers to the traditional financial system and the real economy. Issuers of stablecoins pegged to national currencies and backed by fiat collateral (i.e. not crypto-collateralised or algorithmic ones) are increasingly investing in commercial paper and other short-term assets as part of their reserve management strategies. One of the largest stablecoins in circulation, Tether (see Figure 3.9), purports to hold c.USD30bn in commercial paper, ranking as the 7th largest holder of such instruments globally, according to JPMorgan (FT, 2021[36]). A run or mass redemption event on stablecoins with significant holdings of such short-term debt instruments could cause significant disruption in CP and other short-term credit markets. Potential contagion risk resulting from spillovers to money market funds (MMF) could also result from sudden mass redemptions of such stablecoin arrangements if stablecoin issuers engage in fire sales of commercial paper also held by MMFs, affecting the stability of broader short-term credit markets. Authorities may be compelled to support dealers and prime MMF should stablecoin redemptions lead to or amplify a wider CP sell-off, pressuring market liquidity and impeding new CP issuance (Fitch Ratings, 2021[37]).

[45] In certain jurisdictions, such as Italy, this is assessed on a case-by-case basis. In the UK, the Law Commission has confirmed in November 2021 that the existing law of England and Wales is able to accommodate and apply to smart legal contracts, without the need for statutory law reform.

[46] Leverage opportunities are also available in exchanges that support leveraged trading.

New avenues for the use of crypto-assets by financial consumers have been opened by traditional payment service providers: Visa announced settlement of payments in USDC stablecoins on the Ethereum blockchain, partnering up with centralised crypto-exchange providers and other crypto-asset service providers (Forbes, 2021[38]). PayPal has started allowing users to spend their crypto-asset holdings at online merchants globally (Paypal, 2021[39]). Listed blue chip companies are expanding their direct crypto-asset holdings and are allegedly being used by investors as an indirect way to gain exposure to crypto like Bitcoin (e.g. Microstrategy, Square). Centralised exchanges and other FinTech players are offering user-friendly interfaces and products linked to DeFi protocols and/or the native crypto-assets issued in DeFi markets (e.g. Metamask wallet).

In parallel, the market has experienced growing institutional investor interest and the release of a number of financial products allowing sophisticated investors to get indirect access to crypto-asset risk. Based on a recent market survey, hedge funds expect to shift 7% of their assets to crypto in the next 5 years (FT, 2021[40]). CME has introduced bitcoin futures and options in 2021 (CME Group, 2021[41]), Goldman Sachs offers bitcoin investment vehicles (CNBC, 2021[42])and Morgan Stanley offers its private wealth management clients access to bitcoin and crypto funds (Bitcoin.com, 2021[43]). BlackRock added bitcoin futures as a potential non-principal investment for two of its funds (micro-allocations), while a number of incumbent investment banks are launching digital assets units (CNBC, 2021[44]). In October 2021, ProShares Bitcoin Strategy ETF was the first U.S. bitcoin-CME futures linked ETF to list in the US market (Proshares, 2021[45]). All that said, financial institutions have not yet gained significant exposure to the crypto market, let alone DeFi. While banks' exposures to crypto-assets are currently limited, the continued growth and innovation in crypto-assets and related services, coupled with the heightened interest of institutional investors, could increase risks to the banking system in the absence of a specified prudential treatment.

The identification of intersection or convergence points between DeFi and CeFi is necessary, as these would constitute transmission channels of risks identified in DeFi. At the current juncture, DeFi's most important interconnection with the traditional financial system is through the valuation of crypto-assets that are either used by traditional financial sector companies (e.g. in payments) or are underlying financial products offered by conventional players (e.g. crypto-funds, bitcoin futures). The valuation of financial products referencing crypto-asset prices is directly affected by price trends in the crypto-asset space. Similarly, feedback loops exist between the DeFi market and the main crypto-asset prices, given the recycling of profits in the DeFi space and the use of crypto-assets as collateral for leverage in DeFi, reinforcing the price volatility of such assets.

The boundaries between the two markets, DeFi and CeFi, are therefore becoming more porous and risks of spillovers to the traditional financial system and the real economy are starting to emerge (although small given current size of the market). In addition to price volatility and movements that directly affect traditional financial products referencing such assets, any rapid shifts in the behaviour of DeFi market participants or in the mechanisms underlying DeFi protocols would have an indirect effect on such CeFi products, driven by changes in supply/demand dynamics of DeFi applications and the impact that this would have in the crypto-assets used or minted by such DeFi applications. Similarly, changes in the regulatory or supervisory environment related to DeFi protocols and participants, or to crypto-assets circulated in such markets, are likely to be reflected in the valuation of referenced crypto-assets, which in turn will be transmitted to the CeFi space where such assets are referenced and their issuers. Given the high concentration of DeFi activity in few large protocols, failure of any such protocols could also affect the prices of crypto-assets involved and the impact could be diffused to CeFi through the same transmission channels. Equally, in case of generalized distress on DeFi markets, investors exposed to losses on crypto-assets may have to close positions on traditional markets, propagating the shock. Furthermore, DeFi increases the overall complexity of the crypto-asset market, which could further exacerbate existing risks.

At the moment, the linkages between DeFi markets and the traditional financial system appear to be weak, and risks to financial stability limited given their relatively small size. This, however, may change in the

future if crypto-assets' adoption reaches scale, and the linkages between the two markets may become more significant. Growth in the tokenisation of assets and the increasing use of stablecoins are likely to make the boundaries of the two systems, DeFi and CeFi, more porous, while increasing risks of spillovers to the traditional financial system and the real economy.

4.3.1. On-ramps, off-ramps and the potential role of exchanges as gatekeepers

The fiat conversion from and to crypto-assets via on-ramps and off-ramps can be considered the main point of convergence of DeFi with CeFi. Crypto on-ramps are the points of entry into crypto-asset markets and involve exchanges or other parties that allow investors to buy crypto/DeFi assets by converting fiat money to crypto. Off-ramps are the opposite mechanisms, where investors cash out by converting crypto-assets to fiat or by directly spending crypto to buy products or services in the off-chain world.

Currently the most easily identified gatekeepers to the DeFi space are exchanges offering on- and off-ramps through which fiat currency can be exchange for crypto-assets, including stablecoins, that are then deployed into DeFi applications. Payment providers (such as Visa or Paypal) facilitating acceptance of crypto-assets for payments outside crypto-asset space are more likely to be in fact a "currency conversion" service (i.e. same as paying a USD bill with a VISA card linked to an EUR account), in cooperation with an exchange company (e.g. Anchorage acting as a custodian for VISA for crypto-assets). This is why exchanges have been suggested by the industry as the regulatory check points for regulatory and supervisory purposes for the DeFi market, albeit insufficiently covering the activity that takes place within the DeFi space.

4.3.2. Institutional DeFi and the role of custodians

Interoperability of DeFi with CeFi is one of the ways to increase adoption and scale of DeFi applications. Given growing interest by institutional investors to hold crypto-assets, DeFi protocols have started launching institutional versions of their services; mainly by introducing compliance, including CDD processes (see Section 4.3.2). These are effectively permissioned versions of the application with whitelisting of participants in a compliant manner (see for example Aave Pro (Cointelegraph, 2021[46]).

Other DeFi or fintech firms create interfaces to allow their clients to access DeFi markets in a more user-friendly way. For example, the MetaMask Institutional wallet, launched by Consensys, is built to allow institutional investors to access DeFi while ensuring that they create safeguards by holding the keys to the assets, introducing reporting or promising enhanced protection against nefarious activity by fund managers having access to the digital assets. The absence of AML/CFT processes, including CDD collection, nonetheless restricts use of these funds, as funds cannot commingle their assets with assets from unverified sources in anonymous marketplaces.

Although contrary to the non-custodial nature of decentralised finance, custodians and custodial wallet services that maintain users' private keys are emerging for institutional and retail investors alike. Indeed, the loss of a user's private key is one of the most common risks of inexperienced retail users and translates into loss of access to all assets associated with the private key, as decentralised spaces do not allow for forced transfer mechanisms (OECD, 2020[4]). Multi-signature arrangements, often used in decentralised applications, require multiple keys to authorise a transaction, rather than a single signature from one key. It allows for the dividing up of responsibility among multiple parties, avoiding a single-point of failure, and making it more difficult for the wallet to be compromised.

Custodial wallet operators and other parties offering custodian services (e.g. Gemini, Bitgo, Coinbase) have to comply with the corresponding regulatory frameworks of their respective jurisdiction. According to the Updated Guidance of the Financial Action Task Force (FATF) on Virtual Assets and VASPs, where custodians need keys held by others to carry out transactions, these custodians may still have control of the asset, even in case of multisignature arrangements. Service providers acting on behalf of another

person that cannot complete transactions without a key held by another party are not inherently exempt from falling under the definition of a VAS (FATF, 2021[47]).[47]

Box 4.2. FATF updated guidance for a risk-based approach to virtual assets (VAs) and virtual asset service providers (VASPs) and DeFi

In 2019, FATF issued draft guidance on a risk-based approach to VAs and VASPs (FATF, 2019[48]). As part of this guidance, countries were required to assess and mitigate their risks associated with VA financial activities and providers; license or register VASPs and subject them to supervision or monitoring by competent national authorities. VASPs became subject to the same relevant FATF measures that apply to financial institutions.

In October 2021, the FATF updated its 2019 Guidance for a Risk-Based Approach to VAs and VASPs (FATF, 2021[47]). 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. However, creators, owners and operators or some other persons who maintain control or sufficient influence in the DeFi arrangements, even if those arrangements seem decentralised, may fall under the FATF definition of a VASP where they are providing or actively facilitating VASP services. This is the case, even if other parties play a role in the service or portions of the process are automated. Depending on its operation, there may also be additional VASPs that interact with a DeFi arrangement (FATF, 2021[47]).

4.3.3. Tokenisation, NFTs and the DAO ecosystem

Tokenisation of assets, i.e. the digital representation of real (physical) assets on distributed ledgers, or the issuance of traditional asset classes in tokenised form, could accelerate DeFi market growth, especially when it comes to institutional DeFi (OECD, 2021[20]). Tokenised assets could be used as collateral in DeFi protocols instead of mainstream crypto-assets or stablecoins in order to unlock liquidity and obtain leverage on pre-existing assets though a DeFi protocol. Indicatively, MakerDAO has tested the use of U.S. Treasury securities as the underlying collateral for borrowing DAI (Amico, 2019[49]). The platform now collaborates with third party asset originators who tokenise assets that are used as collateral on the protocol and allow the user to draw stablecoins and finance new loans (e.g. through its collaboration with Centrifuge (Schmitt, 2021[50])).

Similarly, Non Fungible Tokens (NFTs) have emerged as a way to prove ownership to art, collectibles or other digital items by guaranteeing the authenticity of tokens issued on the back of artwork and could be similarly pledged as collateral in DeFi protocols in order to finance new loans.[48]

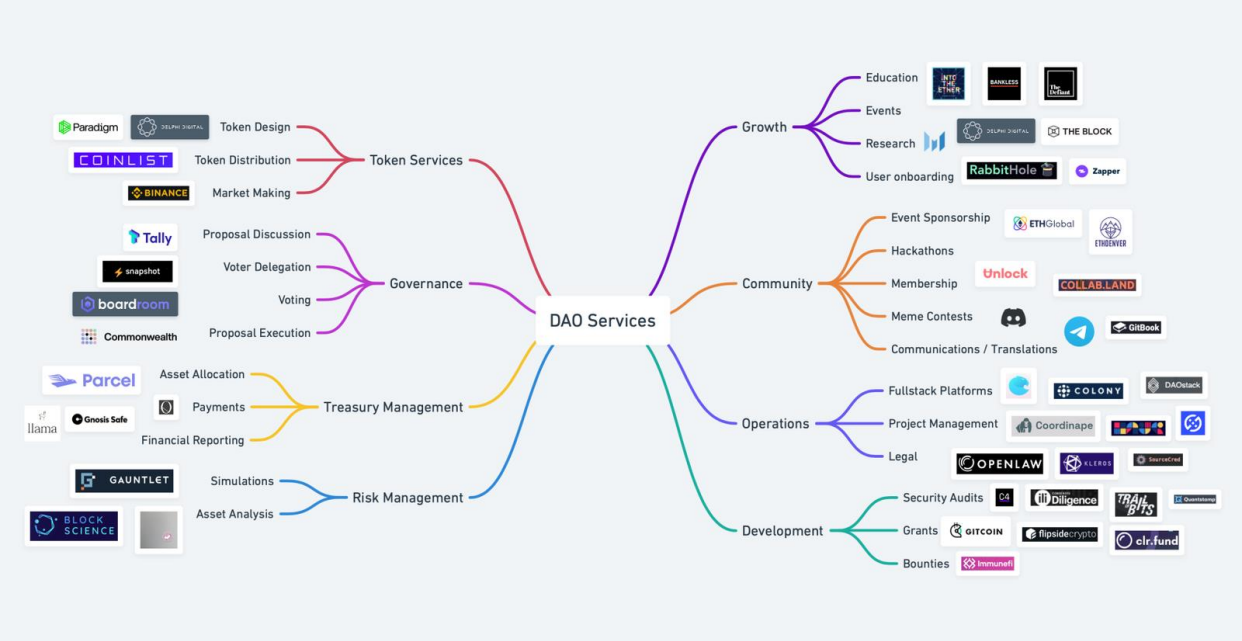
The emerging ecosystem that is being built around DeFi protocols and DAOs has been one of the drivers of growth of the DeFi market and will enable the flourishing of this space. This is particularly important given the network effects realised and materialised in blockchain-based systems (OECD, 2019[9]). FinTech firms providing user-friendly interfaces, custodians and wallet providers, operators of oracles and other service providers enrich the DeFi ecosystem and make it easier and more seamless for retail users to access DeFi platforms. This, of course, comes with risks, as the less savvy users may be exposed to high risks without fully understanding them. As the industry is still immature and FinTechs participating in the ecosystem are not financial services firms, there have been cases of platform employees engaging in conduct that would have been deemed illegal, had it been occurred in a traditional securities markets

[47] Regardless of the numbers, controlling power and any other properties of the involved parties of the signature.

[48] Depending on how NFTs are structured, they could be considered securities in certain jurisdictions.

setting (e.g. front-running clients in the case of OpenSea). Similarly, there have been cases where venture capital investors appeared to use inside information to launch Sybil attacks[49] to increase funds received during an upcoming airdrop.

Figure 4.4. The DAO ecosystem



Source: Corbin Page, Codefi.

[49] A Sybil attack is a kind of security threat on an online system where one person tries to take over the network by creating multiple accounts, nodes or computers. In the world of cryptocurrencies, a more relevant example is where somebody runs multiple nodes on a blockchain network .

5 Policy considerations

DeFi applications have the potential to provide benefits to financial market participants in terms of speed of execution and transaction costs. These efficiencies may be driven by leveraging DLT-technological innovation to disintermediate financial services replacing third parties with smart contracts. DeFi could possibly allow for a more equitable participation of users in markets depending on the design of governance arrangements and fees involved in settling transactions to the underlying DLT or blockchain. DeFi promotes innovation in financial services especially given the open source nature of protocols, and could have some potential to promote financial inclusion depending on the design and transaction arrangements (e.g. fees)[50]. Overall, the development of DeFi markets could be seen as a testing ground for the use of DLTs in financial services.

At the same time, DeFi applications give rise to important risks and challenges for participants and the markets, which call for policy consideration and possible action. The possibility to engage in conceptually unlimited leveraged trading of crypto-assets[51] is one of the main risks involved, and current high levels of collateralisation could decrease as the market evolves, translating into thinner protection threshold for automatic liquidations of users (the equivalent of margin calls for DeFi protocols). The volatility of crypto-asset prices intensifies the fragility of the DeFi market, and volatility spikes in the price of main crypto-assets (Bitcoin, Ether) pledged as collateral for borrowing and leverage or provided as liquidity for yield farming can induce massive automatic liquidations in DeFi protocols. Such liquidations can have a domino effect on investor holdings across the board, and may even have spill over effects in traditional markets. Investors exposed to losses in DeFi may have to close positions in traditional markets, too, propagating the shock. At the same time, stablecoins could constitute one of the greatest points of vulnerability of the DeFi market and a potential channel of risk transmission to the traditional financial markets. In a scenario where a major stablecoin loses its peg due to solvency issues related to the reserves backing the stablecoin or its under-collateralisation, decentralised exchanges would go under severe stress and liquidity pools would be forced to mass liquidations.

The sizeable growth of DeFi for financial services such as lending could lead to greater procyclicality and to new forms of concentration risks, potentially giving rise to financial stability risks, should DeFi reach a critical mass. The supply of credit on a peer-to-peer basis may exhibit larger and sharper swings in the provision of credit compared to traditional lenders, especially if relying on automation and the use of novel processes (FSB, 2019[2]). Risks of concentration relate to the technology used (e.g. Ethereum blockchain) and to the fact that key operations (e.g. code development, crypto-asset mining) are held in the hands of a relatively small set of persons or entities (e.g. software developers, owners of mining hardware). At the current stage of development of the DeFi market, the activity is concentrated in a very small number of protocols, despite the existence of numerous smaller applications (e.g. the aggregated TVL of the top four DeFi applications accounts for almost half the TVL of the DeFi space as of May 2021).

[50] For example, increased transaction fees linked to network congestion inhibit small transactions as users are dis-incentivised to execute small-valued transaction with disproportionately high fees, effectively being priced out.

[51] For example, a user can pledge ETH in one DeFi lending protocol in exchange for the protocol's stablecoin which he or she can then pledge on another DeFi protocol in exchange for a different stablecoin, and the process can be repeated indefinitely and is only limited by the level of the collateralisation ratio of the lending protocol for assets pledged as collateral.

Numerous DeFi applications (or part of their activities) are involved, at least for some part of their activity, in non-compliant provision of regulated financial services and products, often reserved only for licensed entities. Despite its complexity, DeFi activity 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 tokenised markets. Some DeFi applications, or part of their activities, may represent regulated activities for which comprehensive frameworks are already in place aiming at preserving financial stability, protecting financial consumers, promoting investor protection and market integrity, and mitigating illicit finance risks. For example, the issuance of governance tokens has some characteristics of securities/investment contracts and their issuance, promotion or trading in DeFi platforms could be considered non-compliant in many jurisdictions. Equally, when DeFi applications or activities currently fall outside of the regulated space in some jurisdictions, they raise risks that may be left unaddressed by existing rules. Additionally, anonymity or pseudonymity and lack of CDD by many DeFi applications gives rise to risks of money laundering, terrorism financing, and other use of illicit funds, facilitating misconduct.

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

The absence of regulatory/supervisory access points in decentralised DeFi systems is one of the key policy questions that remains to be overcome. As a first step, there may be a need to 'recentralise' DeFi in order to get some comfort from a regulatory and supervisory standpoint, without necessarily completely undermining decentralisation. Having one party accountable (e.g. developers of the protocol or other incentivised parties) can help balance between total absence of central controlling authority and full supervision. Similarly, regulatory and supervisory access points need to be defined by the community even though they may sound against the ethos of DeFi markets. Many of the challenges to the supervision of DeFi could be mitigated through forms of centralisation, such as organised governance (Deutsche Bundesbank, 2021[24]). Decentralised Autonomous Organisation (DAO) governance structures, where these exist, could serve as a potential control point for regulatory and supervisory purposes given their centralised characteristics such as the holding of the admin key or concentrated ownership of governance tokens (Ushida and Angel, 2021[5]). Similarly, holders of controlling shares of governance tokens or identified parties benefiting from the operation of DeFi services through profit sharing mechanisms or fees could be considered as potential regulatory access points. The legal basis for such access (i.e. the ability to force a node operator to give regulators information or to cease its activities) is not guaranteed in all jurisdictions.

In a hypothetical future scenario, there could be technological means for supervisors to participate as nodes in the network and/or intervene at the smart contract level. Similarly, supervisors could have access to all the data involved in the DeFi protocol 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. DAOs or similar governance arrangements could produce reporting for regulatory compliance purposes.

Box 5.1. Alternative DeFi policy approaches suggested by some policy makers and/or the industry

In order to address the lack of responsible entity in DeFi systems, some industry participants argue for a gatekeeper approach, which involves regulating entry and exit points (referred to as 'on-and-off ramps') to DeFi. This would render exchanges and/or other financial and non-financial service providers at the edges of DeFi the regulatory access point to the decentralised system, when fiat is converted to crypto-assets and vice-versa. The effectiveness of this, however, is limited as it would only cover the first and last transactions at the entry and exit points of DeFi, leaving all intra-DeFi activity unsupervised. It could be useful, however, as a way to tax income from such activity and counter the tax evasion aspect of DeFi participation.

Other proposals for decentralised projects include suggestions to provide network developers with a grace period within which, under certain conditions, they can facilitate participation in, and the development of, a functional or decentralized network, exempted from registration provisions of securities laws (Peirce, 2020[51]). The updated version of this particular proposal (referred to as Safe Harbour 2.0) includes enhanced token purchaser protections, with semi-annual updates to the plan of development disclosure and a block explorer, as well as an exit report requirement at the end of the three-year grace period.

Potential regulatory gaps may appear for new types of risks that arise in DeFi systems and which may stem from the novel characteristics of financial service provision in decentralised systems. Such potential gaps in the regulatory treatment of DeFi services need to be addressed, as they may give rise to regulatory arbitrage opportunities. For example, it could be argued that in the absence of prudential and investor protection rules, DeFi is vulnerable to over-leveraging and other related financial risks. Some of the regulatory tools applicable in centralised settings may need to be redesigned in order to be made interoperable and compatible with decentralised structures. Additional rules may need to be introduced to cover for the technological novelty of decentralised systems. For example, auditing of the code underlying the smart contracts by neutral external parties in specific intervals could help address the challenge that non-technical expert users are facing when required to trust the author of the smart contract based on which their transactions are executed.

The decentralised nature of governance in DeFi constructs gives rise to numerous challenges for users, with implications for consumer protection, oversight and enforcement. There is a risk of moral hazard and price manipulation related to undisclosed concentrated token holdings and complete lack of accountability for the people who launch an open protocol for a DeFi project. The economic incentives of developers and funding entities of protocols are not clearly understood or disclosed. A number of important risks relate to governance tokens, issued and distributed for free to users as an incentive for participation in the network, and which could constitute securities or investment contracts in some jurisdictions. As governance tokens are freely traded in decentralised exchanges, a (group of) bad actor(s) can purchase enough governance tokens to manipulate the outcome of a vote to the detriment of minority token holders. Such risk is exacerbated given the possibility of using uncollateralised flash loans to borrow such governance tokens for voting.

A few high profile DeFi applications have a tendency to centralisation of power in practical governance over time, which is visible through concentrations of governance tokens in the hands of only a few actors. This can have repercussions on participating nodes, for example, if parties holding the majority of governance tokens in a network decide to seize the assets of the network, if no blocking mechanism for such eventualities is built in the protocol. Community splits on contentious decisions can also occur, leading

to forks and network splits with potential repercussions for participants without the technical skills to understand such mechanisms.

The lack of traditional regulatory safeguards for investor protection, existing across the board of financial services regulation, leaves investors and financial consumers more exposed to forms of loss or erosion of value (e.g. absence of recourse in case of default or failure, lack of recovery or resolution mechanisms, market manipulation). As the list of risks for investors and financial consumers in DeFi is very long, users should be cognisant of the risks involved in such markets and which are not uncommon (loss of capital, manipulation, technical bugs, exploits, thefts, hacking, and loss of funds through user or protocol error). Anecdotal evidence suggests that the average consumer of DeFi-based financial products is, however, unable to fully grasp the technical complexity of the market, exposing him/her to substantial financial risks. A generalised trend of gamification of finance experienced in the markets may further increase the attraction of financial consumers to DeFi as an alternative to traditional finance. Therefore, regulatory bodies may want to consider encouraging or engaging in investor protection updates to raise financial consumer awareness of potential risks, thereby giving guidance to market participants to better articulate such risks to market participants. Financial education efforts and policies could also be instrumental in helping users understand the risks involved in decentralised finance products and protect themselves accordingly.

Improved disclosure in DeFi applications could be a first step towards greater protection of participants. Such disclosure can include governance token holding data and changes, similar to listed equity holdings. Disclosure around the existence of admin keys, their scope and the arrangements around them would also need to be encouraged for users to be aware of the potential risks involved. Details around the signers of those keys and the powers of the admin keys should be documented. Some of the protocols use multi-signature arrangements to enhance protection, as multiple signatures are required to execute an order. However, it should be noted that it is possible for the same person can be the only party holding all signing keys with significant risk of compromising the project.

The importance of user and market safeguards in DeFi increases given growing interconnections between CeFi and DeFi and growing transmission channels of risk from decentralised finance to traditional financial markets. Growing interest and adoption of crypto-assets by institutional investors and other traditional financial service providers (e.g. payments) has led to the creation of permissioned versions of DeFi applications with whitelisting of participants in a compliant manner.

The increasing use of stablecoins in DeFi protocols and beyond increase interconnectedness between the two parallel systems. Centralised stablecoins expose users and the system to risks related to their trustworthiness associated with the auditability and reporting around their reserves, as well as with the composition of such reserves and stability of the custodian of such reserves. Mass adoption of stablecoins could arguably support mass adoption of DeFi. The ensuing risks of the wider use of stablecoins within and outside the crypto-asset space and their role as linkages between the DeFi and CeFi systems warrant an appropriate regulatory and supervisory framework and standards that will support appropriate protection levels for investors and financial consumers while supporting financial stability overall.

The interaction and transmission channels between DeFi and CeFi is likely to further grow if interoperability of DeFi with CeFi is strengthened one of the ways to increase adoption and scale of DeFi applications. Given growing interest by institutional investors to hold crypto-assets, DeFi protocols have started launching institutional versions of their services, mainly by introducing compliance, including KYC processes. Increased interoperability of DeFi with CeFi is likely to further increase adoption and scale of DeFi applications. Such participation is likely to further grow with the introduction of tokenised assets as collateral in DeFi protocols instead of mainstream crypto-assets or stablecoins, allowing traditional financial institutions to unlock liquidity and obtain leverage on pre-existing assets though DeFi.

Investments in DeFi and mainstream crypto-asset products by financial intermediaries and credit institutions could benefit from prudential treatment that is aligned on the treatment of the holding of crypto-

assets. In this context, the Basel Committee on Banking Supervision (BCBS) has published a consultation on the prudential treatment of banks' exposures to crypto-assets (BCBS, 2021[29]). This will eventually lead to a set of minimum standards that national regulators will need to implement for banks in their regulatory frameworks.

Should DeFi continue its rapid growth and use of leverage, it may be useful for policy makers to monitor the evolution of this market, not least so as to better understand its mechanics, potential benefits and underlying risks. While traditional finance - and lending in particular - involves credit risk and the regulatory scrutiny of loan quality, in DeFi, crypto-assets placed as collateral replace risk management and supervisory guidance. As DeFi becomes more interconnected with CeFi, regulators are strengthening their knowledge of DeFi markets and products in order to evaluate emerging benefits and risks and how to mitigate such risks in order to support an orderly and reliable market for decentralised finance. A better understanding of the mechanics of the DeFi market will also allow policy makers to assess whether potential policy gaps may exist, whether new regulatory approaches may be required or existing frameworks may need updating in order to ensure that similar activities are subject to similar regulation, and whether risk management practices are in place to encourage the safe functioning of these markets.

Given the novelty of the DeFi market and the rapid growth it experienced in 2020 and 2021, further exploration of potential risks from DeFi to the safety and soundness of regulated financial institutions and to the resiliency of the financial system, as well as in order to protect consumers, is warranted, in line with the mandate of financial regulators and supervisors. The availability and quality of data and actionable information is one of the aspects of DeFi and crypto-asset markets that needs to be further explored in preparation for any possible future policy intervention.[52] Good quality data improve the visibility and measurement of risks, as well as gauge the potential for spillovers on other markets. While data appear to be available, it is hard to know whether the unregulated nature of DeFi markets means that data quality is poor, or whether there are gaps that prevent the effective monitoring of risks.

Another reflection goes back to the fundamental question of whether policy makers aim to regulate DeFi applications or not, and if so, at which level should rules be applied. Some jurisdictions argue that the underlying protocol and the DeFi applications coming on top of such protocol could be seen as a general-purpose information communications technology (ICT), similar to the Internet or telephone lines. Also, where should policy be applied? The protocol is just software, and the underlying blockchain is the infrastructure network, the interface that allows users to communicate with the protocol is one entry point, and the community of users or nodes to the network another, in addition to the core developer community having created and launched the protocol. The concept of the secondary liability may also be developed in that cases and organisations that provide web-tools, applications, interfaces or other means to access the DeFi market might become subject to obligations and/or to the requirement to provide assurances to users.

Possible ways for regulators to limit risks that could emerge in and from DeFi, as well as ways to enforce existing regulation in decentralised structures, need to be further explored. Importantly, 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. DeFi is fuelling innovation (conventional and disruptive) and leading established market infrastructures and players to review existing processes to make them more efficient (e.g. rethinking of post-trade processes and financial intermediation).

[52] The lack of reliable data is one of the paradoxes of DeFi markets. Despite the plethora of data, it is still unclear how reliable they are. Blockchain transaction and wallet information is not actionable information without other methods to attribute and triangulate it, even if its integrity is not an issue.

In addition, DeFi networks are truly global in reach and operation, with no defined jurisdiction and geographical location for their operations, which in turn increases jurisdictional uncertainty and challenges enforcement. This further obstructs oversight and regulatory compliance of such networks, particularly given the speed and ease with which financial service providers are able to change locations in response to actions of authorities. Greater international policy collaboration and discussion can help overcome such challenges at the cross-border level.

Further collaboration is warranted between all stakeholders involved in decentralised finance and policy makers could benefit from actively playing a role towards establishing a cooperative environment among stakeholders. The engineering and software developing communities should be involved in such dialogue, given that the code embedded in DLT systems could inform the discussion of the appropriate oversight on the activities of a blockchain-based financial ecosystem despite often disparate incentives and mind sets of such communities (Yuta Takanashi et al., 2020[52]).

References

Amico, J. (2019), *Introducing The Tokenized Asset Portfolio — A Model to Leverage Real World Assets in DeFi Credit Facilities | by Jeffrey Amico | Fluidity | Medium*, https://medium.com/fluidity/introducing-the-tokenized-asset-portfolio-7710e4239ab6 (accessed on 17 August 2021). [49]

BCBS (2021), "Basel Committee on Banking Supervision Consultative Document Prudential treatment of cryptoasset exposures", http://www.bis.org (accessed on 9 August 2021). [29]

Benson, J. (2021), *DeFi Has Lost $474 Million to Hacks and Fraud in 2021: Report - Decrypt*, https://decrypt.co/78146/defi-has-lost-474-million-hacks-fraud-2021-report (accessed on 17 August 2021). [31]

Bitcoin.com (2021), *Blockchain Groups From Major Universities Are Powerful Voters in Defi Governance Protocols – Bitcoin News*, https://news.bitcoin.com/blockchain-groups-from-major-universities-are-powerful-voters-in-defi-governance-protocols/ (accessed on 7 December 2021). [17]

Bitcoin.com (2021), *Morgan Stanley Making 3 Bitcoin Funds Available to Clients – Finance Bitcoin News*, https://news.bitcoin.com/morgan-stanley-bitcoin-funds/ (accessed on 12 April 2021). [43]

Carter, N. (2020), *Public blockchain fee cyclicality and negative feedback loops | by Nic Carter | Medium*, https://medium.com/@nic__carter/public-blockchain-fee-cyclicality-and-negative-feedback-loops-1620141a8a87 (accessed on 2 August 2021). [11]

Carter, N. and L. Jeng (2021), *DeFi Protocol Risks: the Paradox of DeFi*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3866705. [18]

CFTC (2021), *CFTC Orders Tether and Bitfinex to Pay Fines Totaling $42.5 Million | CFTC*, https://www.cftc.gov/PressRoom/PressReleases/8450-21 (accessed on 7 December 2021). [21]

CME Group (2021), *Bitcoin Overview - CME Group*, https://www.cmegroup.com/trading/equity-index/us-index/bitcoin.html (accessed on 12 April 2021). [41]

CNBC (2021), *BlackRock has 'started to dabble' in bitcoin, says Rick Rieder*, https://www.cnbc.com/2021/02/17/blackrock-has-started-to-dabble-in-bitcoin-says-rick-rieder.html (accessed on 12 April 2021). [44]

CNBC (2021), *Goldman is close to offering bitcoin to its clients*, https://www.cnbc.com/2021/03/31/bitcoin-goldman-is-close-to-offering-bitcoin-to-its-richest-clients.html (accessed on 12 April 2021). [42]

Coinmarketcap (2021), *What Are Flash Loan Attacks?* | *CoinMarketCap*, https://coinmarketcap.com/alexandria/article/what-are-flash-loan-attacks (accessed on 2 August 2021). [16]

Cointelegraph (2021), *Aave price hits 3-week high as 'Aave Pro' debuts for institutional lending*, https://cointelegraph.com/news/aave-price-hits-3-week-high-as-aave-pro-debuts-for-institutional-lending (accessed on 17 August 2021). [46]

Consensys (2021), *DeFi Report Q2 2021*, https://consensys.net/reports/defi-report-q2-2021#DeFi-Economy (accessed on 4 August 2021). [12]

Daian, P. et al. (2019), "Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges", https://arxiv.org/abs/1904.05234v1 (accessed on 2 August 2021). [34]

Dale, B. (2021), *DeFi Liquidations Up 14X in Broad Crypto Sell-Off - CoinDesk*, Coindesk, https://www.coindesk.com/defi-liquidations-up-14x-in-broad-crypto-sell-off (accessed on 3 August 2021). [53]

DeepDAO (2021), *Deep DAO - Insights for a Decentralized World*, https://deepdao.io/#/deepdao/dashboard (accessed on 4 August 2021). [6]

Deutsche Bundesbank (2021), "Crypto tokens and decentralised financial applications". [24]

Ethereum.org (2021), *Proof-of-stake (PoS)* | *ethereum.org*, https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/ (accessed on 16 August 2021). [35]

European Commission (2020), *Draft regulation of the European Parliament and of the Council on Markets in Crypto-assets (MiCA) (Text with EEA relevance)*. [27]

European Commission (2020), *Proposal for a regulation of the European Parliament and of the Council on a pilot regime for market infrastructure based on a distributed ledger technology EUR-Lex - 52020PC0594 - EN - EUR-Lex*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0594 (accessed on 19 July 2021). [25]

FATF (2021), "October 2021 Updated Guidance for a risk-based approach - Virtual assets and virtual asset service providers", https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html (accessed on 7 December 2021). [47]

FATF (2019), "Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers". [48]

FCA (2021), *FCA warns consumers of the risks of investments advertising high returns based on cryptoassets* | *FCA*, https://www.fca.org.uk/news/news-stories/fca-warns-consumers-risks-investments-advertising-high-returns-based-cryptoassets (accessed on 9 August 2021). [28]

FCA (2021), *Research Note: Cryptoasset consumer research 2021* | *FCA*, https://www.fca.org.uk/publications/research/research-note-cryptoasset-consumer-research-2021 (accessed on 3 August 2021). [13]

Financial Times (2021), *Tether's commercial paper disclosure places it among global giants | Financial Times*, https://www.ft.com/content/342966af-98dc-4b48-b997-38c00804270a (accessed on 2 August 2021). [23]

Fitch Ratings (2021), *Stablecoins Could Pose New Short-Term Credit Market Risks*, https://www.fitchratings.com/research/fund-asset-managers/stablecoins-could-pose-new-short-term-credit-market-risks-01-07-2021 (accessed on 7 September 2021). [37]

Forbes (2021), *Visa Will Start Settling Transactions With Crypto Partners In USDC On Ethereum*, https://www.forbes.com/sites/ninabambysheva/2021/03/29/visa-to-start-settling-transactions-with-bitcoin-partners-in-usdc/?sh=b7a80785228c (accessed on 12 April 2021). [38]

FSB (2019), *Crypto-assets: Work underway, regulatory approaches and potential gaps - Financial Stability Board*, https://www.fsb.org/2019/05/crypto-assets-work-underway-regulatory-approaches-and-potential-gaps/ (accessed on 16 August 2021). [32]

FSB (2019), *Decentralised financial technologies: Report on financial stability, regulatory and governance implications*, http://www.fsb.org/emailalert (accessed on 28 September 2020). [2]

FSB (2018), "FSB Chair's letter to G20 Finance Ministers and Central Bank Governors", https://www.fsb.org/2018/03/fsb-chairs-letter-to-g20-finance-ministers-and-central-bank-governors/ (accessed on 16 August 2021). [33]

FT (2021), *China steps up crackdown on bitcoin mining industry*, Financial Times, https://www.ft.com/content/7526f514-9f36-4dbb-94ee-beb061f5cc52 (accessed on 4 August 2021). [8]

FT (2021), *Hackers siphon $600m in digital tokens, crypto network says | Financial Times*, https://www.ft.com/content/47329261-afec-4cf7-840e-5eee0c70ba61 (accessed on 17 August 2021). [30]

FT (2021), *Hedge funds expect to hold 7% of assets in crypto within five years | Financial Times*, https://www.ft.com/content/4f8044bf-8f0f-46b4-9fb7-6d0eba723017 (accessed on 17 August 2021). [40]

FT (2021), *Tether's commercial paper disclosure places it among global giants | Financial Times*, https://www.ft.com/content/342966af-98dc-4b48-b997-38c00804270a (accessed on 17 August 2021). [36]

Learner, R. (2019), *Blockchain Voter Apathy. Governance is a key area of exploration… | by Roy Learner | Wave Financial | Medium*, https://medium.com/wave-financial/blockchain-voter-apathy-69a1570e2af3 (accessed on 4 August 2021). [19]

Liu, C. (2021), *Announcing Compound Treasury, for Businesses & Institutions | by Calvin Liu | Compound | Jun, 2021 | Medium*, https://medium.com/compound-finance/announcing-compound-treasury-for-businesses-institutions-83d4484fb82e. [14]

Medium (2021), *Black Thursday for MakerDAO: $8.32 million was liquidated for 0 DAI | by whiterabbit | Medium*, https://medium.com/@whiterabbit_hq/black-thursday-for-makerdao-8-32-million-was-liquidated-for-0-dai-36b83cac56b6 (accessed on 9 April 2021). [10]

NY Attorney General (2021), *Attorney General James Ends Virtual Currency Trading Platform Bitfinex's Illegal Activities in New York | New York State Attorney General*, https://ag.ny.gov/press-release/2021/attorney-general-james-ends-virtual-currency-trading-platform-bitfinexs-illegal (accessed on 2 August 2021). [22]

OECD (2021), *Regulatory Approaches to the Tokenisation of Assets*, https://www.oecd.org/finance/regulatory-approaches-to-the-tokenisation-of-assets.htm. [20]

OECD (2020), *The Tokenisation of Assets and Potential Implications for Financial Markets*, https://www.oecd.org/finance/The-Tokenisation-of-Assets-and-Potential-Implications-for-Financial-Markets.htm. [4]

OECD (2019), *Initial Coin Offerings (ICOs) for SME Financing*, https://www.oecd.org/finance/initial-coin-offerings-for-sme-financing.htm. [9]

Paypal (2021), *Cryptocurrency on PayPal - FAQs*, https://www.paypal.com/us/smarthelp/article/cryptocurrency-on-paypal-faq-faq4398?app=searchAutoComplete (accessed on 12 April 2021). [39]

Peirce, H. (2020), *Running on Empty: A Proposal to Fill the Gap Between Regulation and Decentralization*, SEC.gov, https://www.sec.gov/news/speech/peirce-remarks-blockress-2020-02-06 (accessed on 5 August 2021). [51]

Proshares (2021), *ProShares Bitcoin Strategy ETF | BITO | Overview | ProShares ETFs*, https://www.proshares.com/funds/bito.html (accessed on 7 December 2021). [45]

PWC (2021), *3rd Annual Global Crypto Hedge Fund Report 2021*, https://www.aima.org/educate/aima-research/third-annual-global-crypto-hedge-fund-report-2021.html (accessed on 4 August 2021). [15]

Schär, F. (2021), *Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets | St. Louis Fed*, https://research.stlouisfed.org/publications/review/2021/02/05/decentralized-finance-on-blockchain-and-smart-contract-based-financial-markets (accessed on 2 April 2021). [3]

Schmitt, L. (2021), *DeFi 2.0 — First Real World Loan is Financed on Maker | by Lea Schmitt | Centrifuge | Medium*, https://medium.com/centrifuge/defi-2-0-first-real-world-loan-is-financed-on-maker-fbe24675428f (accessed on 17 August 2021). [50]

The Block (2021), *DeFi exploits total $680 million so far in 2021*, https://www.theblockcrypto.com/post/123030/defi-exploits-total-680-million-so-far-in-2021 (accessed on 29 November 2021). [1]

Ushida, R. and J. Angel (2021), *Regulatory Considerations on Centralized Aspects of DeFi managed by DAOs*. [5]

Walch, A. (2019), *Deconstructing 'Decentralization': Exploring the Core Claim of Crypto Systems*, https://papers.ssrn.com/abstract=3326244 (accessed on 2 August 2021). [7]

WEF (2021), *How decentralized finance will transform business financial services | World Economic Forum*, https://www.weforum.org/agenda/2021/07/decentralized-finance-transaction-banking-smes/ (accessed on 4 August 2021). [26]

Yuta Takanashi, D. et al. (2020), “Call for Multi-Stakeholder Communication to Establish a Governance Mechanism for the Emerging Blockchain-Based Financial Ecosystem, Part 1 of 2”, *Stanford Journal of Blockchain Law & Policy*, Vol. 3/1, https://stanford-jblp.pubpub.org/pub/multistakeholder-comm-governance/release/1. [52]

www.oecd.org/finance