

The Financial Stability Risks of Decentralised Finance

16 February 2023



The Financial Stability Board (FSB) coordinates at the international level the work of national financial authorities and international standard-setting bodies in order to develop and promote the implementation of effective regulatory, supervisory and other financial sector policies. Its mandate is set out in the FSB Charter, which governs the policymaking and related activities of the FSB. These activities, including any decisions reached in their context, shall not be binding or give rise to any legal rights or obligations.

Contact the Financial Stability Board

Sign up for e-mail alerts: www.fsb.org/emailalert

Follow the FSB on Twitter: [@FinStbBoard](https://twitter.com/FinStbBoard)

E-mail the FSB at: fsb@fsb.org

Copyright © 2023 Financial Stability Board. Please refer to the [terms and conditions](#)

Table of Contents

Executive summary	1
Introduction	4
1. Background on DeFi	5
1.1. The DeFi ecosystem	5
1.2. The distinguishing features of DeFi	7
1.3. Products and services provided by DeFi	13
2. DeFi vulnerabilities	16
2.1. Operational fragilities	17
2.2. Liquidity and maturity mismatches	19
2.3. Leverage	20
2.4. Interconnectedness, concentration and complexity	21
2.5. Other vulnerabilities	23
3. Interlinkages and transmission channels	24
3.1. Main transmission channels	24
3.2. Interlinkages and the scope for spillovers	25
3.3. Scenarios for the evolution of DeFi and financial stability implications	28
4. Monitoring the evolution of DeFi	31
4.1. Issues with existing data	31
4.2. Elements of DeFi monitoring	32
4.3. Tracking the evolution of DeFi markets	33
4.4. Tracking vulnerabilities	34
4.5. Tracking interlinkages and transmission channels	36
5. Conclusions	36
Annex: Illustration of typical DeFi applications	39
Glossary	41
Abbreviations	45

Executive summary

Within the crypto-asset ecosystem, so-called decentralised finance (DeFi) has emerged as a fast-growing segment. DeFi is an umbrella term commonly used to describe a variety of services in crypto-asset markets that aim to replicate some functions of the traditional financial system (TradFi) while seemingly disintermediating their provision and decentralising their governance. The DeFi ecosystem has a multi-layered architecture that includes permissionless blockchains, self-executing code (or so-called smart contracts), DeFi protocols and purportedly decentralised applications (DApps).

To date DeFi is mainly self-referential, meaning its products and services interact with other DeFi products and services rather than with the traditional financial system and the real economy, but TradFi players are beginning to enter the market. In addition, DeFi has integral connections to centralised crypto-asset trading, lending and borrowing platforms, through which participants exchange crypto-assets for one another or for fiat currency, often using stablecoins.

While the processes to provide services are in many cases novel, DeFi does not differ substantially from TradFi in the functions it performs. In attempting to replicate some of the functions of the traditional financial system, DeFi inherits and may amplify the vulnerabilities of that system. This includes well-known vulnerabilities such as operational fragilities, liquidity and maturity mismatches, leverage and interconnectedness. DeFi's specific features may result in these vulnerabilities playing out at times differently than in traditional finance, for example as a result of the risks of fire sales related to the automatic liquidation of collateral based on smart contracts, reliance on oracles for external information or dependence on infrastructure over which the DeFi developers may not have direct control (i.e. the underlying blockchain). The fact that crypto-assets underpinning much of DeFi lack inherent value and are highly volatile magnifies the impact of these vulnerabilities when they materialise, as recent incidents demonstrate.

Operational fragilities include unclear, opaque, untested or easy-to-manipulate DeFi governance frameworks, where the actual degree of decentralisation varies broadly; dependence on blockchain networks, which may become congested or are unreliable; oracles and cross-chain bridges, which can expose users to disruptions and thefts; and coding errors in smart contracts which are exacerbated given the immutability of DeFi transactions.

Arguably the most concerning vulnerabilities in DeFi relate to the different liquidity and maturity profile of liabilities and assets of relevant entities. Such mismatches can give rise to run risks with possible adverse spillovers to other parts of the financial system. In DeFi, these types of liquidity risks are particularly prominent in the case of stablecoins and lending protocols.

A key feature of crypto-asset markets, including DeFi, is the outsized impact of leverage on market dynamics. Due to pseudonymity, financial intermediation in DeFi largely rests on the use of collateral and on the leverage that such usage entails. The automatic liquidation of collateral in smart contracts, which can be applied unevenly among participants depending on the protocol design, is a primary reason why deleveraging dynamics in DeFi can be especially disruptive. In TradFi, such self-reinforcing dynamics can be alleviated via orderly liquidation at central counterparties or by market circuit breakers, but both of these mechanisms are absent in DeFi

today. Leverage in DeFi is also difficult to gauge, in part because borrowed funds are often used as collateral for other loans, giving rise to “collateral chains” (akin to re-hypothecation).

The DeFi ecosystem features a complex set of interconnections within DeFi and with outside entities – notably with other segments of crypto-asset markets (e.g. centralised finance, or CeFi) and to a lesser degree with TradFi, but also with third-party technology providers. The complexity of interconnections in DeFi gives rise to vulnerabilities relating to the composability of DeFi protocols; concentration of activity in a small number of protocols; and exposure to distress of centralised trading platforms and third-party providers.

Other vulnerabilities of DeFi, and crypto-assets more broadly, consist of market integrity issues (including the evasion of existing regulation); unsustainable business models that rely on continuous investor inflows to remunerate early adopters; and potential for cross-border regulatory arbitrage because of the opaqueness of DeFi organisational structures and lack of a clear domicile. DeFi may also contribute to currency substitution, especially in countries with weak macroeconomic conditions.

The extent to which these highlighted vulnerabilities can lead to financial stability concerns largely depends on the interlinkages and associated transmission channels between DeFi, TradFi and the real economy. These channels include financial institutions’ exposures to DeFi; confidence and wealth effects stemming from the involvement of households and firms in DeFi; and the extent to which DeFi applications may facilitate the use of crypto-assets for payments and settlement. To date, these interlinkages are limited, as shown by the modest impact of the May/June 2022 crypto-asset market turmoil and the November 2022 FTX collapse on TradFi. However, if the DeFi ecosystem were to grow significantly and become more mainstream as a result of the broader adoption of crypto-assets and the development of real-world use cases, then interlinkages would deepen and the scope for spillovers to TradFi and the real economy would increase.

Data on crypto-asset markets in general and DeFi specifically, lack transparency, consistency, and reliability. This is due to the difficulty in aggregating, reconciling, and analysing the vast amount of data available on distributed ledgers; the pseudonymous nature of information on public ledgers, which inhibits the ability to ascertain the types of crypto-asset investors; the large number of off-chain transactions and other off-chain data; complex ownership structures and loan/investment relationships; the lack of, or non-compliance with, reporting requirements producing consistent and reliable data; and the fact that some data providers (e.g. trading and lending platforms) may be incentivised to manipulate their data.

Notwithstanding the data limitations, the report identifies some indicators that can be used to incorporate DeFi developments in the broader financial stability monitoring of the crypto-asset ecosystem. These indicators help to gauge the overall size and evolution of DeFi; the identified financial vulnerabilities of DeFi; and the interconnections and possible transmission channels between DeFi, TradFi and the real economy, in order to gauge the scope for spillovers.

In light of these findings, several considerations are warranted. First, the FSB should proactively analyse the financial vulnerabilities of the DeFi ecosystem as part of its regular monitoring of the wider crypto-asset markets. In turn, the FSB’s crypto-assets monitoring framework should be complemented with DeFi-specific vulnerability indicators. Also, the FSB will explore the growth

of tokenisation of real assets as it could increase linkages between crypto-asset markets/DeFi, TradFi and the real economy.

Second, the FSB, in collaboration with standard-setting bodies (SSBs) and regulatory authorities, will explore approaches to fill data gaps to measure and monitor interconnectedness of DeFi with TradFi, with the real economy, and with the crypto-asset ecosystem. In the interim, consideration can be given to greater sharing of existing data and market intelligence and use of ad-hoc information collection methods.

Third, the FSB will explore the extent to which its proposed policy recommendations for the international regulation of crypto-asset activities may need to be enhanced to acknowledge DeFi-specific risks and facilitate the application and enforcement of rules. DeFi-specific risks may include, for example, the use of smart contracts; governance arrangements (including concentrated ownership); dependence on blockchain networks; and use of oracles and cross-chain bridges. The FSB, working with SSBs, could also consider potential policy responses to the risks stemming from DeFi's interconnectedness with the broader financial system and the real economy. Potential policy responses may include, for example, regulatory and supervisory requirements concerning traditional financial institutions' direct exposures to DeFi, as well as concerning other ways that such institutions may seek to become more integrated with DeFi (e.g. by serving as trustees or custodians, or by transacting with other firms engaging in DeFi).

As part of this work, the FSB could also consider, in coordination with the SSBs, assessing the regulatory perimeter across jurisdictions to determine which DeFi activities and entities fall or should fall within that perimeter (in which case enforcement of compliance with applicable regulations is warranted) or outside of it (in which case policies should be developed to achieve appropriate regulation of activities giving rise to similar risks). In this respect, a key element to consider would be the entry points of DeFi users (including retail investors and traditional financial institutions), such as through stablecoins and centralised crypto-asset platforms. The FSB may consider whether subjecting these crypto-asset types and entities to additional prudential and investor protection requirements, or stepping up the enforcement of existing requirements, could reduce the risks inherent in closer interconnections. SSBs can play an important role in such perimeter assessments, as well as in strengthening cross-border cooperation and data sharing together with the FSB.

Introduction

Crypto-asset markets are fast evolving and could reach a point where they represent a threat to global financial stability due to their scale, structural vulnerabilities and increasing interconnectedness with the traditional financial system.¹ Within the crypto-asset ecosystem, so-called decentralised finance (DeFi) has emerged as a fast-growing segment. DeFi is an umbrella term commonly used to describe a variety of services in crypto-asset markets that aim to replicate some functions of the traditional financial system by seemingly disintermediating their provision and decentralising their governance.² In DeFi, the role of financial institutions and market infrastructures is replaced to varying degree by self-executing code, or so-called smart contracts, deployed to public blockchains.³ DeFi emerges primarily as a crypto-based alternative and competitive peer-to-peer/pool marketplace of financial services, covering various activities like trading, borrowing, or lending, so far overwhelmingly within the crypto-asset space.⁴ The recent growth of DeFi has attracted the attention of various international organisations that have recently produced a number of reports providing an overview of the sector and its features, significant risks, and potential wide-ranging implications for traditional financial markets.⁵

The turmoil in crypto-asset markets and in DeFi in May and June 2022 exposed a number of features of DeFi applications that turned out to be vulnerabilities within DeFi and across crypto-asset markets more broadly.⁶ The November 2022 collapse of the crypto-asset trading platform FTX also exposed vulnerabilities relating to multifunction crypto-asset intermediaries. However, neither episode has resulted in significant contagion outside of crypto-asset markets. The results of these “stress tests” suggest that TradFi currently is not heavily exposed to DeFi or the crypto-asset ecosystem more broadly, reflecting in part a conservative supervisory and regulatory approach. That said, a forward-looking approach to the financial stability implications of DeFi seems warranted as the size of DeFi and/or its links with TradFi may grow over time, raising the potential for contagion. Not only will such a forward-looking perspective, which entails monitoring and the closing of data gaps, help authorities assess and adjust their regulatory stance and framework, but it will also help ensure they are ready to intervene if and when the financial stability risks from DeFi grow. It may also enable TradFi participants to assess risks as they consider participation in DeFi. This report aims to provide an overview of the main features and vulnerabilities of DeFi, to assess potential financial stability threats and draw policy implications.

The report is structured as follows: Section 1 introduces the DeFi ecosystem, its key elements and players as well as the main products. Section 2 discusses financial vulnerabilities of DeFi,

¹ See FSB (2022), *Assessment of Risks to Financial Stability from Crypto-assets*, February.

² With the exception of Graph 1 in Section 4, this report does not describe the recent evolution in DeFi markets.

³ This report uses the term ‘blockchain’ to refer to any type of distributed ledger technology (DLT) based network because blockchain is the most commonly used form of such networks. However, it should be noted that not all DLT-based networks are blockchains. Whereas DLT involves a database that exists across multiple locations, a blockchain is a form of distributed ledger that has specific technological features: 1) a block structure; 2) sequential; 3) proof of work (or an alternative validation mechanism); and 4) use of tokens.

⁴ In some cases, this report refers to specific crypto-assets or firms providing related services as examples. These examples are not exhaustive and do not constitute an endorsement by the FSB or its members for any crypto-asset, firm, product, or service.

⁵ See FSB (2019), *Decentralised financial technologies: Report on financial stability, regulatory and governance implications*, June; OECD (2022), *Why Decentralised Finance (DeFi) Matters and the Policy Implications*, January; IOSCO (2022), *Decentralized Finance Report*, March; OECD (2022), *Institutionalisation of crypto-assets and DeFi–TradFi interconnectedness*, May; and IIF (2022), *Decentralized Finance: Use cases, challenges and opportunities*, November.

⁶ See Box 1 in FSB (2022), *Promoting Global Financial Stability: 2022 FSB Annual Report*, November.

highlighting those that are manifestations of vulnerabilities familiar from TradFi as well as those that are potentially new. Section 3 sketches possible scenarios for the path that DeFi may take, with corresponding financial stability consequences. Section 4 discusses data gaps and steps to establish a monitoring framework for DeFi, and Section 5 concludes. Annex 1 illustrates typical DeFi protocols, followed by a glossary defining technical terms.

1. Background on DeFi

1.1. The DeFi ecosystem

1.1.1. *Key elements and players*

The DeFi ecosystem is a complex web of interconnections involving multiple players with varying interrelationships and interests. They include protocol creators and developers, so-called decentralised autonomous organisations (DAOs – see Section 1.2.3), funders (e.g. venture capital and private equity funds) and institutional and retail end-users, among others.

DeFi follows a multi-layered architecture⁷ wherein each layer has a distinctive purpose:

1. **Permissionless blockchains** are the backbone of the ecosystem in that they provide a ledger on which transactions are recorded and become immutable (settlement layer). Due to their public and permissionless nature, these blockchains are accessible to and can be edited by any potential participant, thus allegedly providing transparency and confidence over the legitimacy of its records in a similar manner to what a trusted third party does in the traditional financial system.
2. Self-executing code, or so-called **smart contracts**,⁸ lay on top of blockchains and fulfil the terms and conditions of a transaction in an automated manner.
3. The terms, conditions, and standards by which products and services are offered are set out in **DeFi protocols**, which govern particular activities and tasks, in part by combining various smart contracts and user interfaces. Protocols may involve a number of interrelated transactions.
4. Protocols further enable the creation of an application layer that allows users to interact with smart contracts via a set of graphical interfaces and other components. It is these **decentralised applications** (DApps) which in turn facilitate the provision of financial intermediation in DeFi.

Most protocols are permissionless and can be accessed by anyone anonymously (or pseudonymously),⁹ if they have access to the appropriate equipment and expertise, with minimal if any onboarding checks. Many DApps are funded by venture capital (VC) funds in exchange

⁷ See Schär (2021), *Decentralized Finance: On Blockchain and Smart Contract-based Financial Markets*, Review of the Federal Reserve Bank of St Louis, 103(2), pp. 153–174. Auer et al (2022), *The Technology of Decentralized Finance (DeFi)*, BIS Working Paper 1066 provides an alternative classification.

⁸ The ability to deploy smart contracts was arguably the main innovation of the introduction of the Ethereum blockchain in 2015. Being a first-mover allowed Ethereum to become over time the largest blockchain smart contract platform in use today in terms of user base, developer community and decentralised applications.

⁹ Pseudonymous data are data that cannot be attributed to a specific individual without additional information.

for governance or other tokens, and code for these DApps is written by protocol developers who might also retain governance or other tokens and administrative keys. This can mean that a purportedly decentralised protocol may in fact be controlled by a concentrated set of interests.

1.1.2. Commonalities and differences between DeFi and TradFi

The ultimate goal of an efficient and resilient financial system is to intermediate the allocation of resources to support real economic activities in the presence of risk and uncertainty. To achieve this objective, the financial system performs a number of interrelated functions:¹⁰

- It provides payment services for the exchange of goods and services or for the transfer of monetary value.
- It allows the pooling of funds to undertake large projects.
- It enables the transfer of resources through time and space.
- It allows economic agents to manage uncertainty and control risk.
- It provides price information to coordinate decentralised decision making.
- It reduces information asymmetries and incentive problems arising from one party having more information than the other in a transaction.

To date, DeFi is mainly self-referential, in the sense that DeFi products and services mainly interact with other DeFi products and services rather than with TradFi and the real economy. While the processes to provide services in DeFi are in many cases novel, DeFi does not differ substantially from TradFi in the functions it performs. For example, the ability to pool resources in support of large projects from a decentralised set of actors is the very essence of many DeFi protocols, while the ability to provide price information for various assets is inherent in the day-to-day operations of decentralised trading platforms. But while TradFi relies on a network of regulated intermediaries that need to be trusted to carry out these tasks (and where trust in these players relies on them being regulated), DeFi aims to replace this network with systems in which computer code and decentralised validators verify the legitimacy of transactions and the availability of funds to execute them, although these systems are in non-compliance with, or fall outside of, the regulatory perimeter at present. The means used to fulfil the functions are different, but the underlying incentives and nature of activities do not differ materially between TradFi and DeFi.

1.1.3. Drivers of DeFi development

There are a number of supply and demand factors behind the growth of crypto-assets and DeFi.

On the supply side, technological innovation such as efficient computing power and cryptography made the development of crypto-assets possible. For DeFi specifically, smart contract-provisioned blockchains like Ethereum have been crucial for its development, as well

¹⁰ See Merton, *A functional perspective of financial intermediation*, Financial Management (Summer 1995) for a discussion.

as the development of so-called stablecoins (typically referencing the US dollar), which aim to serve as a ‘stable’ instrument for the transfer and maintenance of value. While there are different stablecoin designs,¹¹ they provide a common mechanism to transact among the various DeFi protocols. As such, stablecoins, including those issued by a centralised entity like Tether or Circle, play an important role within the DeFi ecosystem through their use in purchasing, settling, trading, lending and borrowing other crypto-assets.

On the demand side, a number of factors are relevant. Arguably, a key push to develop decentralised alternatives to existing financial intermediaries was in part due to the lingering effects of the 2008 financial crisis. Crypto-assets and DeFi can appear to have attractive characteristics in this regard as some investors could turn away from traditional providers and find promises of an attractive yield in the crypto-asset space. Aside from the “true believers” and those with a “fear of missing out”, a sustained period of low interest rates following the 2008 financial crisis pushed investors to look for opportunities to invest in riskier assets offering higher yields. More recently, the perception of portfolio diversification benefits and/or inflation hedges may have also lured investors into this space, although recent analysis suggests that crypto-assets have started to show high correlation with financial assets such as equities.¹² However, given the changed interest rate environment against the backdrop of persistent inflationary pressures globally, the recent market turmoil that revealed fragilities in the crypto-assets markets, as well as reports of theft, fraud and market abuse, in addition to increasing regulatory attention, it is uncertain to what extent crypto-assets and DeFi will maintain their cycle-agnostic or counter cyclical appeal in the future.

The DeFi market is largely driven by institutional participants in advanced economies. In contrast, there is relatively little direct participation from retail investors and emerging or low-income economies. Accessing the DeFi ecosystem can be complicated, while transaction costs and the requirement for over-collateralization in many DApps is likely to limit the opportunity for less sophisticated or less well-capitalised participants to directly interact with the ecosystem.¹³

1.2. The distinguishing features of DeFi

1.2.1. *Unique operational features*

This subsection describes operational features and various components of DeFi, and how they interact among themselves and with external parties. A map visualising these interactions is in Figure 1.

¹¹ Some are (purportedly) reserve-backed, others rely on algorithms to maintain their peg. Some are issued centrally while others are issued by a DAO or DeFi protocol. See Baughman et al. (2022), [The stable in stablecoins](#), Federal Reserve Board, FEDS Notes, December.

¹² See Adrian et al. (2022), [Crypto Prices Move More in Sync With Stocks, Posing New Risks](#), IMF Blog, January.

¹³ See the [Chainalysis 2022 Geography of Cryptocurrency Report](#) and Carmona (2022), [Debunking the narratives about cryptocurrency and financial inclusion](#), Brookings report, October. These features imply that at present it is difficult to make the case that there are material financial inclusion benefits of DeFi.

Smart contracts

Smart contracts are the key innovation enabling the development of DeFi. Figure 1 highlights the central role played by smart contracts in DeFi as the foundation on which DApps are built.

Smart contracts are self-executing code deployed on a blockchain that fulfils the terms and conditions of a transaction in an automated manner. Automated programs that facilitate execution have been used in TradFi for many years but are typically confined to the intermediary and connecting institutions, or to specific processes in a transaction chain (e.g. trading or market-making algorithms). What is novel in the case of DeFi is the utilisation of blockchain technology and the fact that anyone who has the required crypto-assets used by the smart contract can participate in it. Once a DeFi protocol is developed, the underpinning smart contracts are deterministically deployed on each network node, typically by referring to an independent oracle that references the necessary data to determine whether the execution conditions are fulfilled. Their execution outcome is designed to be the same for any node that runs the smart contracts using the same set of programmed requirements.¹⁴

Smart contracts are supposedly tamper-proof¹⁵ once they are live. It is typical for a DeFi protocol to have a DAO or other governance arrangement which is utilised to reach consensus on certain changes to the protocol. That said, one should point out that the term ‘smart contract’ is a misnomer. They are not smart, in the sense that they do not react or change in response to external stimuli, but simply execute code when predefined conditions are fulfilled. They are also not necessarily contracts, in the sense that it is not clear whether they are enforceable in courts of law in most jurisdictions, though some jurisdictions are considering smart contracts’ place within their respective legal systems.¹⁶

Blockchain native tokens

In the absence of a trusted central authority, the security of a blockchain depends on the economic incentives of the entities (e.g. miners) who validate transactions. Validators are compensated with the blockchain’s native tokens (transaction fees, or ‘gas’) which, therefore, derive a certain amount of value from the activity that takes place around DeFi protocols. Native tokens are also held by investors who see intrinsic value in them, use them as collateral, or hold or trade them for speculative reasons. As such, these native assets – such as ether on the Ethereum blockchain – are essential to support DeFi’s functionality and provide incentives to participants in the DeFi ecosystem.

¹⁴ See Makarov and Schoar (2022), *Cryptocurrencies and Decentralised Finance (DeFi)*, NBER Working Paper 30006, April.

¹⁵ In theory, once the code is confirmed it cannot be modified without detection.

¹⁶ For example, see Osborne Clarke (2022), *Law Commission concludes English law supports smart contracts*, January and Werbach & Cornell (2017), *Contracts ex machina*, Duke Law Journal.

Composability

The open-source nature of DApps allows for components of the DeFi space to be pieced together by developers to create new and potentially highly sophisticated products.¹⁷ This feature is commonly termed as the DeFi “Lego”. As a result, a single token can potentially facilitate a variety of activities. Composability also creates a web of intricate interdependencies, by enabling the recycling of assets on different applications. This creates additional complexity and makes it harder to track, trace and detect those interdependencies, and it also introduces vulnerabilities due to interconnectedness (as discussed below). This is illustrated in Figure 1 through the arrows connecting different smart contracts and DApps.

Self-custody

To engage with DeFi protocols, participants typically maintain control of their crypto-assets and the ability to transact until they decide to lock their crypto-assets into a smart contract. However, such a course of action usually requires significant technical knowledge by the user, even though various solutions that differ in degrees of risk and complexity exist.¹⁸ Since the underlying settlement layer is immutable because of the use of blockchain technology, no third-party should, in principle, be able to control or censor recorded transactions.

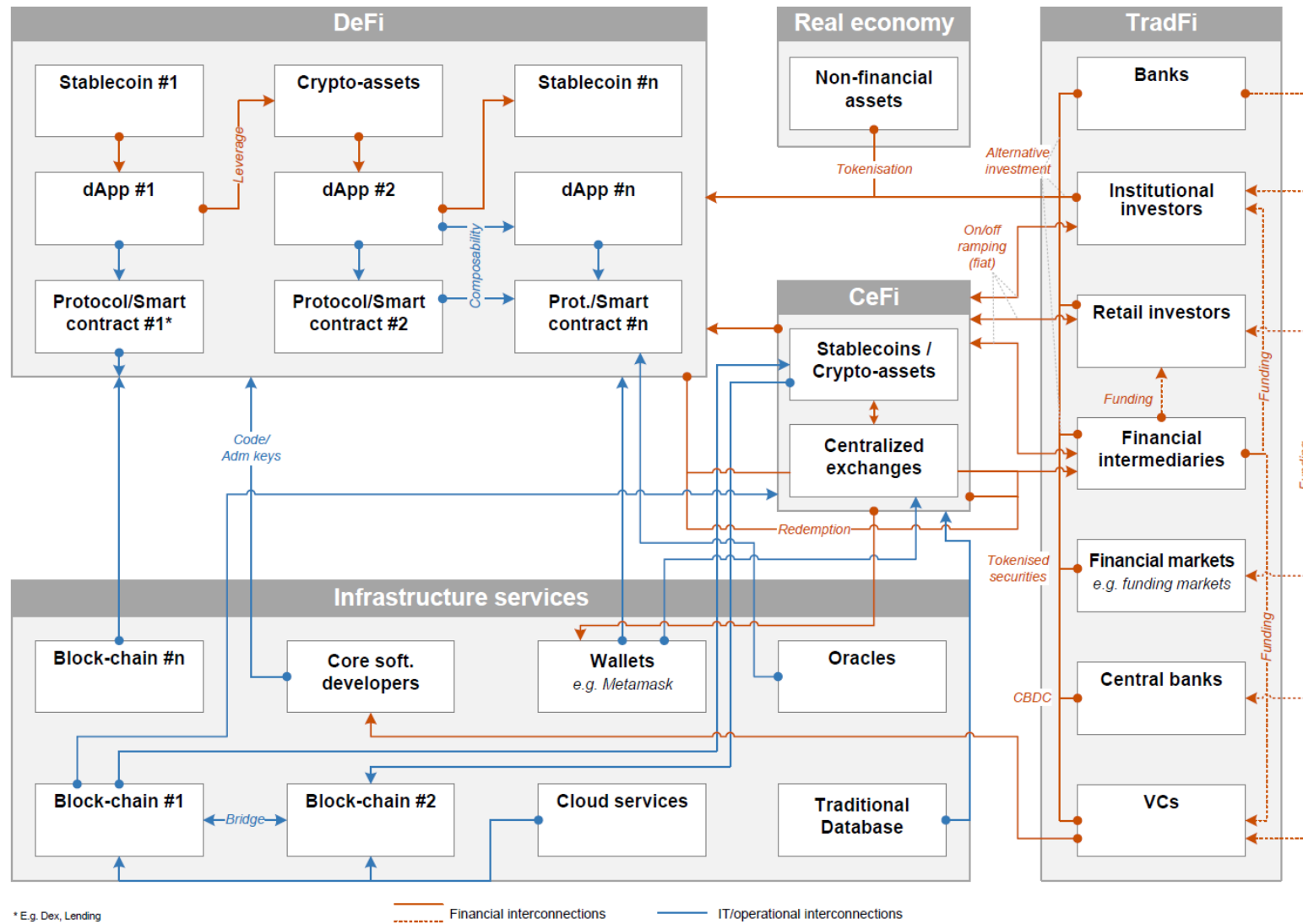
Oracles and bridges

Oracles and bridges provide critical mechanisms for large parts of DeFi activities to function. Oracles are services typically enabling blockchain smart contracts to access external (or “off-chain”), real-world data. Therefore, they are fundamental to the delivery of DeFi, as smart contracts may require up-to-date access to a variety of data feeds produced off-chain (i.e. outside of public distributed ledgers) or on a different chain, to meet their predefined conditions. Bridges in turn are an interoperability mechanism across blockchains, allowing for the creation of synthetic tokens that can represent a variety of native assets and other tokens on an entirely different blockchain, while purporting to maintain the underlying economic value. Bridges typically hold or store tokens from one chain and issue or release tokens for the same value on another chain, thus apparently allowing token holders to transact across chains. Such bridges, as pools of potentially very valuable amounts of crypto-assets, may and have become targets of attack, and attempts to misappropriate the tokens held in bridges have been successful. Figure 1 illustrates the role that bridges play in connecting different blockchains and the role that oracles have in supplying data to the DeFi ecosystem.

¹⁷ For example, a crypto-asset can be used as collateral in a DeFi loan protocol to help mint other crypto-assets, such as stablecoins. The latter in turn can be further locked into a so-called decentralised “money market” and further tokenised and subject to other uses.

¹⁸ It remains doubtful whether broad parts of the population indeed show a strong demand for decentralised self-custody of crypto-assets. There could hence be potential for independent custodians to offer services to DeFi users to facilitate this task to some extent. For example, in October 2022, BNY Mellon became the first major US bank custodian to announce they would custody bitcoin and ether – see WSJ (2022), *America’s Oldest Bank, BNY Mellon, Will Hold That Crypto Now*, October.

Figure 1: Stylised depiction of interconnections within the DeFi ecosystem and towards critical external players



1.2.2. External dependencies

DeFi relies largely on pre-existing technical infrastructures and intermediaries in the crypto-asset space, such as existing blockchain networks, off-chain infrastructures, centralised crypto-asset trading platforms (CEXs), oracles, bridges, and stablecoins. Concentration frequently is high on many of these dimensions. For example, smart contracts need first to be recorded on a public blockchain, which implies a dependency on its proper functioning and capacity constraints. Most DeFi applications are built on the Ethereum blockchain, which has often experienced congestion.¹⁹ This dependency has led many DeFi protocols to expand their services across multiple chains²⁰ to process operations in a less costly manner, albeit at the expense of fragmentation.²¹

External dependencies, although perhaps more muted, also exist in relation to other more traditional agents or markets. For example, traditional financial intermediaries provide a variety of standardised financial services to critical actors in the crypto-asset space including, among others, custody of a stablecoin issuer's reserve assets or the holding of fiat-based deposit accounts on behalf of stablecoin issuers. More generally, TradFi institutions such as specialized banks and crypto-asset CEXs support customers' funding and withdrawal needs to help facilitate their smooth on- and off-ramping into/from the crypto-asset ecosystem as well as channelling funds into DeFi (see Figure 1). In addition, growing levels of tokenisation of off-chain assets to serve as collateral for DeFi trades, and the potential utilisation of central bank digital currencies (CBDCs) if they were to be developed and used broadly, may create further interconnections, as could growth in institutional adoption and the reliance on third-party service providers.²²

1.2.3. The governance structure of DeFi protocols

The governance of a DeFi protocol refers to the scope of decision making as well as the process by which those decisions are made and implemented. DeFi applications purport to have decentralised ownership and governance structures if they have such structures at all. However, in some DeFi arrangements decision-making is centralised, and in practical terms, the actual degree of decentralisation among underlying DeFi organisational structures varies broadly (Figure 2). New forms of governance, known as decentralised autonomous organisations

¹⁹ The Ethereum blockchain processes between 10 and 15 transactions per second. By comparison, Visa processes around 1,700 transactions per second on average. The congestion problem can result in system failures that, in turn, could make the network susceptible to attacks, like the one that occurred during March 2020 when a manipulation of Ethereum's mempools allowed the theft of \$8M in MakerDAO Collateral – see Coindesk (2022), *Mempool Manipulation Enabled Theft of \$8M in MakerDAO Collateral on Black Thursday: Report*, July. Higher congestion also typically leads to higher transaction fees.

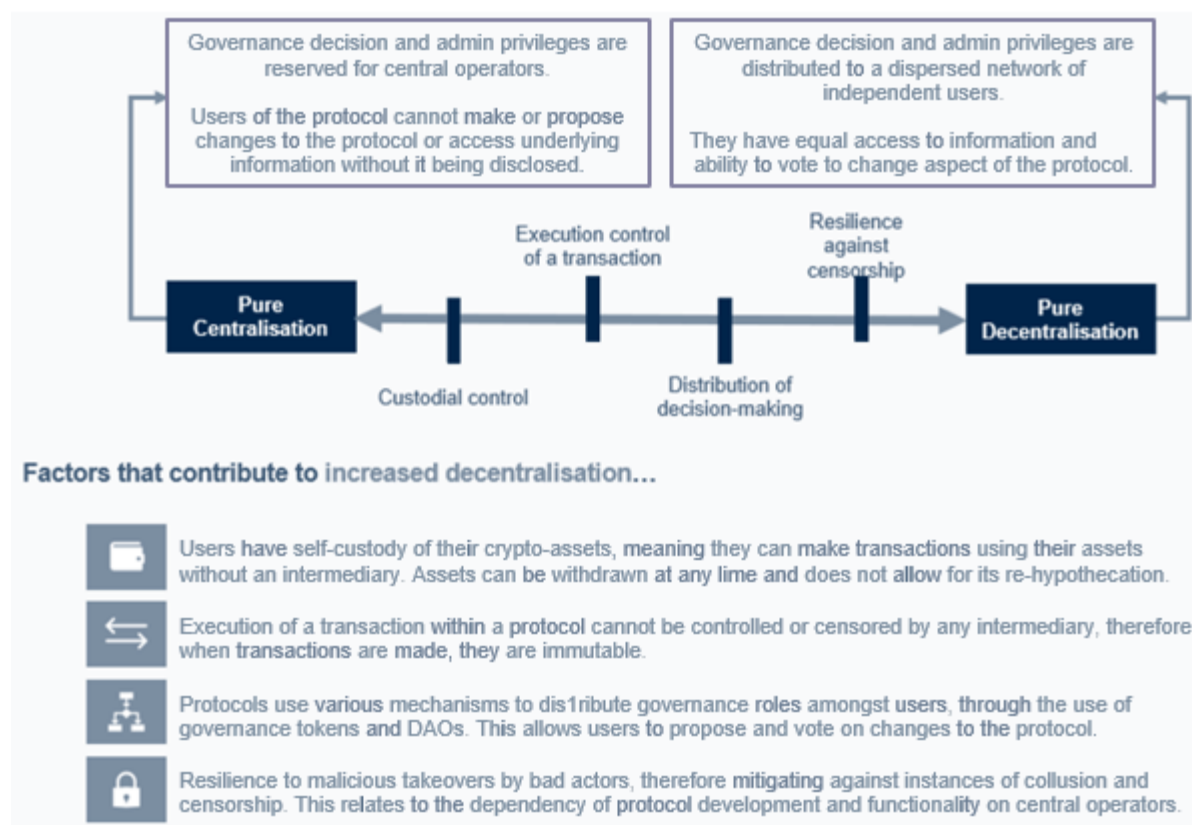
²⁰ For example, the Aave V2 protocol is available on 3 different DLT-based networks (Ethereum, Polygon and Avalanche) with a total value locked (TVL) concentration of 90% on Ethereum among these networks. Uniswap is available on 4 different DLT-based networks with a TVL concentration of 96% on Ethereum among these networks. Curve protocol is available on 10 different DLT-based networks with a TVL concentration of 87% on Ethereum among these networks. TVL refers to the total value of assets deposited on a DeFi protocol (see section 4.3).

²¹ See Boissay et al (2022), *Blockchain scalability and the fragmentation of crypto*, BIS Bulletins, no 56.

²² OECD (2022), *Institutionalisation of crypto-assets and DeFi–TradFi interconnectedness*, May.

(DAOs), have emerged, which purport to be, but often are not in reality, member-owned communities without centralised leadership.²³

Figure 2: Centralisation vs. decentralisation in the crypto-asset space: potential contributing factors



Source: FSB.

A DAO purports to be an entity governed by its community. In its purest form, there should not be a single authority or management team that decides the future of the entity, but it is instead determined entirely by members of the community.²⁴ Voting power is typically proportional to the holdings of the relevant DAO's governance tokens, which are in principle open to be acquired by anyone. In practice, however, as seen in Table 1 below, voting control can be highly concentrated and opaque. Some DeFi protocols are more consultative and engage the community more closely than others in the decision-making process. Some protocols also require a substantial participation in voting before developers may proceed with fundamental changes, and occasionally veto rights apply as well. These divergent approaches are often not fully transparent to market participants and regulators. Theoretically, a truly distributed decision-

²³ The degree of centralisation/decentralisation can vary across DeFi arrangements and can evolve over time. See OECD (2022), *Why Decentralised Finance (DeFi) Matters and the Policy Implications*, January. In fact, all governance mechanisms can potentially change the degree of decentralisation of a protocol and any of its components – see IOSCO (2022), *Decentralised Finance Report*, March.

²⁴ Anecdotal evidence suggests this is not always the case in practice. For example, the founding team and its investors often have large stakes in the protocol's governance token and are active in decision-making, while not all participants get to vote and in many cases voting is disconnected from the governance token itself (e.g. through delegation). Moreover, since governance tokens are freely tradeable in DEXs, and often on centralised trading platforms, any party can acquire significant or controlling voting stakes ahead of a vote to influence decision-making (including through the use of uncollateralised borrowing, voting and return of tokens in a single flash-loan type of transaction), or even propose and approve malicious proposals to the detriment of minority tokenholders - see OECD (2022), *Why Decentralised Finance (DeFi) Matters and the Policy Implications*, January.

making process contributes to greater decentralisation, becoming more dynamic and responsive to its community and stakeholders. But without a delegated decision-making authority, decisions may take much longer to be approved, making the process inefficient. As the software developer forgoes its control of the code in favour of the DAO, fixing an operational error, however small, may still require a decision of the DAO. This implies that software bugs or upgrades may not be addressed in a timely manner, as they depend on the efficiency of the protocol's decision-making process.

Table 1: Features of selected DeFi governance tokens as of June 2022

	Uniswap	PancakeSwap ²⁵	Aave	Compound	Ampleforth
DAO	Yes	No	Yes	Yes	Yes
Total number of wallets	3,438,910	1,305,747	111,203	111,183	73,992
Percentage of supply owned by top 100 addresses	86.74%	94.64%	85.89%	91.46%	92.19%
Percentage of votes required for proposal to go through	4%	Individually reviewed	Depends on type of proposal. Quorum and majority required vary.	Depends on type of proposal. Quorum varies.	5%

Source: FSB analysis.

1.3. Products and services provided by DeFi

Currently DeFi is primarily a self-referential system in that it does not provide services to the real economy. However, the crypto-asset services that DeFi provides are similar to TradFi functions: most commonly, facilitating DeFi lending and borrowing, trading (including on margin), asset management, and derivatives. Many DApps provide multiple functions which overlap with each other, and it is often not easy to clearly demarcate the limits of any one function.

1.3.1. Decentralised lending and borrowing

DeFi lending platforms, such as Aave, Compound and MakerDAO, are based on pooled assets provided by lenders in exchange for interest, and rely on collateral rather than an assessment of borrowers' creditworthiness. The identities of the participants are typically unknown. Most

²⁵ Based on BscScan data on May 26th, 2022, the data for PancakeSwap's transactions and holdings per wallet.

DeFi loans have no specified maturity (sometimes they are referred as being “perpetual”) and can be repaid at any time.

Because of the lack of a trusted counterparty relationship, a mechanism is necessary to ensure that loans are repaid and, thus, DeFi loans are almost always fully secured with crypto-assets as collateral.²⁶ In fact, lending platforms often require over-collateralisation by setting a collateral factor (typically up to 80% of the collateral value posted). Further, borrowers must meet the collateral requirements at all times within a predetermined range of hours or minutes and, if additional collateral is not provided, the collateral is automatically liquidated.²⁷

Another form of lending – which is unique to DeFi due to the settlement process on blockchains – is so-called “flash loans”, which enable users to instantaneously borrow, execute a transaction, and repay the loan within the same blockchain transaction. The transactions required for the flash loan to be executed are in a single block and either all or none of them are settled. This is usually referred to as ‘atomic settlement’. Such loans are of zero tenor²⁸ and do not require collateral. They have been used mostly for crypto-asset arbitrage and trading purposes. Given their features, flash loans can also be used by market manipulators and attackers (“flash attacks”) to borrow large amounts of crypto-assets and manipulate prices simultaneously on different platforms or exploit governance vulnerabilities of protocols.²⁹

1.3.2. Trading platforms

Crypto-asset trading platforms are marketplaces that allow users to exchange crypto-assets for one another or for fiat currency. They can be classified either as centralised (CEX)³⁰ or decentralised (DEX), the latter being a unique feature of DeFi. DEXs do not allow users to exchange crypto-assets for fiat currencies.

DEXs facilitate peer-to-peer or peer-to-pool trades that are settled atomically based on smart contracts while not requiring users to deposit funds with the trading platform operator, as occurs in CEXs. Two of the most prominent types³¹ of DEXs are order-book exchanges and automated market makers (AMM).³²

In order book exchanges, order books are usually maintained off-chain, while settlement occurs on-chain. This has a bearing on the actual degree of decentralisation. Buyers and sellers communicate their order to a third party (relayer) or DEX operator, who posts it to the order book and publishes that information so that an interested counterparty (taker) can match it.

AMMs are autonomous protocols that perform the role of traditional market makers, hence securing liquidity for crypto-asset trading pairs (e.g. ETH/USDT). As a result, users that demand

²⁶ See Aramonte et al (2021), *DeFi lending: intermediation without information?*, BIS Bulletins, no 57.

²⁷ Lehar and Parlour (2022), *Systemic Fragility in Decentralized Markets*, BIS Working Paper 1062, highlight how this gives rise to instability in DeFi.

²⁸ Such loans are due immediately upon issuance, a condition made possible by smart contract technology and by the relative slowness of blockchains. They do not require collateral.

²⁹ See Qin et al. (2020), *Attacking the DeFi Ecosystem with Flash Loans for Fun and Profit*.

³⁰ Examples of CEXs include Coinbase, Binance, and Kraken.

³¹ IOSCO (2022), *Decentralised finance report*, March.

³² An example of a DEX based use of an order book is [Serum](#), while that of an AMM is [Uniswap](#).

liquidity can tap the liquidity pools locked inside smart contracts. Pools are usually set up as trading pairs on the basis of deposits made by any entity or person interested in providing liquidity in exchange for a fee. Arbitrage opportunities arise between the assets' price in the pool and in the market when some amount of a token is removed from or added to a pool. Imbalances are addressed through arbitrage trading against the liquidity pool and tokens' prices adjust according to a predetermined formula.

1.3.3. Asset management and yield farming

Various DeFi protocols also offer asset management services. DeFi asset management protocols³³ use smart contracts to pool crypto-assets deposited by individuals into a portfolio. Fully decentralised on-chain funds use programmable code in place of a portfolio manager. The code can support automatic portfolio rebalancing and attempts to ensure that the fund adheres to a predefined strategy and acts in accordance with the coded rules and risk profile.

DeFi participants also often seek to maximise returns by lending or borrowing crypto-assets across various DeFi platforms, earning crypto-assets in return for their services in an activity known as "yield farming". While participants can engage in this practice independently, it is a manual and often tedious process. To facilitate this process, yield aggregators³⁴ have emerged that employ a range of strategies to distribute capital across different DeFi protocols. Aggregators automate the process of depositing assets in smart contracts and earning rewards by scanning across various protocols and strategies in a manner that seeks to maximise user profits while simultaneously reducing spending on gas fees. For a fee, aggregators facilitate complex strategies that typically involve the shifting of tokens around multiple different platforms.

1.3.4. Derivatives and synthetic assets

The creation of derivatives in DeFi takes the form of tokens, the value of which is contingent on fluctuations in the value of one or more referenced assets or another observable variable. For example, derivatives can reference a traditional stock or commodity, or another crypto-asset, cash flows on a business venture, or can be based on the predicted outcome of an event. Tokenised derivatives may not make use of an intermediary such as a dealer or a clearinghouse like in TradFi. Instead, governance, maintenance, and auto-liquidation of collateral for decentralised derivatives are usually controlled in part by programmable code. Some tokenised derivatives³⁵ may require reference to an oracle or a third-party information system to track information about the underlying asset or variable.

1.3.5. Margin trading

Some DeFi protocols offer users the possibility to carry out margin trading among the products and services that they offer.³⁶ A traditional financial intermediary (in this case, a broker) is replaced in part by smart contracts that reproduce the provision of this service purportedly in a

³³ Examples of asset management protocols include [Enzyme](#) and [DeFi Saver](#).

³⁴ Examples of yield aggregators include [Yearn Finance](#) and [Harvest](#).

³⁵ Examples may include commodities such as gold and silver where the price of the synthetic tracks the underlying commodity.

³⁶ The largest such derivative margin protocol is [dYdX](#).

decentralised and non-custodial way. Traders on these platforms can open a margin account, transfer their crypto-assets to it and use them to leverage (i.e. to borrow additional crypto-assets) in order to build up long or short positions. The level of leverage incurred is defined as the ratio between the borrowed funds and the margin (i.e. the funds contributed by the trader).³⁷ During the time the position is open, the margin acts as a guarantee (collateral). If at a certain point in time a trader's position evolves in such a way that the margin value falls below a certain threshold, the traders' collateral is automatically liquidated.

2. DeFi vulnerabilities

In identifying financial vulnerabilities in DeFi, this report builds on the FSB Financial Stability Surveillance Framework.³⁸ This framework has been designed for the analysis of vulnerabilities affecting the global financial system. By contrast, DeFi as a separate ecosystem – while sharing most of the vulnerabilities present in TradFi – is much less mature and is rapidly evolving. This fact, coupled with some of the novel technological features of DeFi, means that the surveillance framework must be applied in a more forward-looking way to DeFi.

A key message of this report is that DeFi – in attempting to replicate some functions of the traditional financial system – inherits and may repeat or amplify the vulnerabilities of that system. This includes well-known vulnerabilities such as operational fragilities, liquidity and maturity mismatches, leverage, and interconnectedness (see Figure 3). DeFi's specific features may result in these vulnerabilities sometimes playing out differently than in traditional finance, for example as a result of the risks of fire sales or other spill over effects related to the automatic liquidation of collateral based on smart contracts, the use of oracles, or dependence on the underlying blockchain. The amplification of known vulnerabilities comes from novel technological features, the high degree of structural interlinkages amongst the participants in DeFi and from non-compliance with existing regulatory requirements or lack of regulation.³⁹

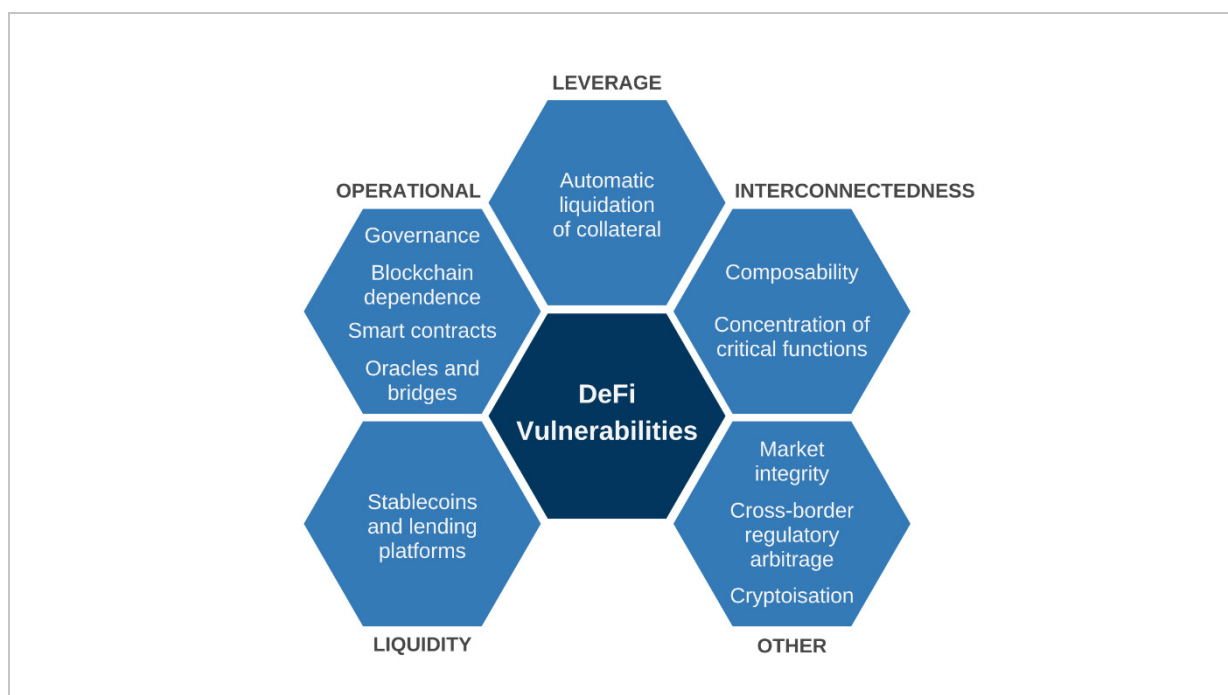
As recent incidents have shown, the vulnerabilities inherent in DeFi – while not at a level that represents a threat to global financial stability – will require ongoing monitoring as the ecosystem continues to grow and evolve. This section provides an initial assessment of these vulnerabilities, while the subsequent section analyses interlinkages and potential transmission channels between DeFi, TradFi and the real economy.

³⁷ The level of leverage allowed depends on the DeFi platform. For example, dYdX offers up to 5x in isolated margins. An isolated margin lets the trader leverage only a certain amount of funds, specifically deposited as collateral for a particular trade. dYdX also offers cross margin, which lets the trader leverage using all the assets in his account, the total of his account balances.

³⁸ See FSB (2021), *Financial Stability Surveillance Framework*, September.

³⁹ See also Allen (2022), *DeFi: Shadow Banking 2.0?*, William and Mary Law Review.

Figure 3: A summary of DeFi features and vulnerabilities



2.1. Operational fragilities

Operational fragilities refer to features of DeFi that may cause operational disruptions, outages or failures, intentional or otherwise, that may adversely impact the ability to deliver relevant services and products.

2.1.1. Governance arrangements

DeFi often employs novel governance arrangements with potential adverse consequences for financial stability. Unclear, opaque, untested and/or easy-to-manipulate governance frameworks can mislead users about claims and safeguards of DeFi activities.⁴⁰ For instance, developers and founders may lack the incentives to keep developing the DApps appropriately once they receive the initial investment. This may expose users to so-called “rug pulls”⁴¹ – a risk that is compounded by the fact that it is difficult to make developers and founders accountable for their actions (moral hazard) as their economic incentives are not always clear and almost always poorly disclosed.

Furthermore, the holding of voting powers across major DAOs and DeFi protocols is extremely concentrated, implying that in practice only a few controlling actors can propose, pass, or implement initiatives (see Table 1). Voting participation can also be low in some cases due to the staking of tokens or not being ‘on-line’ (e.g. because of governance tokens being held in

⁴⁰ A recent case is the Mango Markets episode allegedly involving manipulative trades to exploit a code vulnerability at the expense of the rest of the user community. See CoinDesk (2022), *DeFi Exchange Mango's \$114M Exploit Was 'Market Manipulation,' Not a Hack, Ex-FBI Special Agent Says*, October.

⁴¹ A rug pull is a crypto-asset market scam in which a development team attracts investors into a project before disappearing with the funds, leaving their investors with a valueless asset.

cold/offline wallets), or voting rights may be delegated to an entity that does not hold the governance token. Community disagreements about governance decisions can occur, leading to forks and network splits with potentially negative outcomes. These can lead to both losses for investors and a loss of confidence in DAOs or DeFi protocols which could spill over to other markets.

2.1.2. *Dependence on blockchain networks*

A DeFi-specific operational feature is that DeFi protocols depend critically on the blockchain infrastructure on which they are deployed. DApps are also subject to technical limitations that exist on their underlying blockchain. Disruptions to the blockchain caused by outages, network congestion⁴² or consensus failure can affect the cost, functioning and performance of the blockchain and of the DeFi services that rely on it and potentially result in forced liquidations and losses to DeFi users.⁴³ Despite these challenges, blockchain technology may also be a source of resilience in certain limited cases, for example by shortening custody chains and increasing transparency.

2.1.3. *Smart contracts*

There are a number of operational vulnerabilities associated with smart contracts. DApps use a variety of smart contracts that may be impossible to stop, modify, or reverse. Well-designed smart contracts need to account for many possible states of the world before they are deployed, creating complexity. Such complexity, in turn, increases the potential for coding errors and consequent unexpected behaviour.⁴⁴ Compounding this issue, smart contract code is widely re-used, such that seemingly independent contracts may suffer the same technological vulnerabilities. The immutability of DeFi transactions further implies that, should an error (or a fraudulent transaction) take place, it is not possible to undo it and reinstate the status before the error was made (or to do so would require agreement among affected parties and the consensus of blockchain validators). In addition, in contrast to TradFi, there is uncertainty over what ex-post remedial protections are available to participants in a DeFi protocol as it may be difficult to identify a legally cognizable party to hold accountable.⁴⁵

2.1.4. *Oracles and bridges*

The functioning of many DeFi protocols relies critically on oracles to execute off-chain operations or to retrieve data from off-chain sources. Oracles can also introduce dependencies on third-party providers and processes. The risk that an oracle does not behave as expected or is

⁴² Mitigating the risk of high congestion reportedly is driving several important developments in DeFi. See, for instance, the recent decision by dYdX to move its new version out of Ethereum, due to congestion issues, or the popularity of platforms like Polygon, which allows the creation of DApps based on Ethereum, but without the fee and congestion problems.

⁴³ For example, Solana experienced high network congestion in January 2022 due to an attack where bots overloaded the network and prevented users from topping up their collateral, resulting in the forced liquidation of their positions.

⁴⁴ Hackers may exploit code vulnerabilities, for example by triggering “suicide” instructions. These instructions are intended to allow the owner of the contract to cancel it. However, due to code errors some contracts may be killed by arbitrary addresses. Other examples include “greedy” contracts which lock up value that cannot be released anymore, and “prodigal contracts” which send value to an arbitrary recipient.

⁴⁵ In principle, smart contracts might have some potential benefits in terms of reducing counterparty risk due to their ability to conduct ‘atomic swaps’, i.e. the wallet-to-wallet exchange of two digital assets simultaneously and in a single operation.

corrupted is called ‘oracle risk’. Errors or attacks to their inputs may trigger actions in one protocol (e.g. liquidations, margin calls) with unanticipated negative consequences in other protocols (e.g. in algorithmic reserve assets or collateral management). Oracles themselves may also be subject to market manipulation, and conducting an exploit on a DeFi contract may be carried out by manipulating the oracle of the smart contract. Therefore, oracles could be critical in initiating or propagating a shock, especially when they are relied upon by a dominant protocol or when many protocols rely on a single oracle.

Another operational vulnerability relates to cross-chain bridges. Separate blockchains are often not interoperable, requiring bridges that connect protocols across various blockchains. Typically a bridge will hold/collect assets from one chain or protocol and issue or release assets (often referred to as ‘wrapped tokens’) on another chain or protocol for the same value. This allows asset holders to transact across chains or protocols but creates repositories potentially holding large amounts of assets, rendering them targets for theft and misappropriation. This represents yet another channel for the contagion of operational risks, which is further exacerbated by the fact that the consensus mechanism tends to be highly concentrated.⁴⁶ Compromised bridges may result in the loss or theft of the assets locked on the original chain and a collapse in the value of wrapped tokens on the destination chain.⁴⁷

2.2. Liquidity and maturity mismatches

Arguably the most concerning vulnerabilities in DeFi relate to liquidity and maturity mismatches⁴⁸ stemming from a different liquidity and maturity profile of liabilities and assets of relevant entities. Such mismatches can give rise to run risks with possible adverse spillovers to other parts of the financial system – this is a well-known risk in banking as well as in non-bank financial intermediation and a key reason for regulatory intervention in TradFi. In DeFi, as well as in crypto-asset markets more generally (as shown by the events of May/June and November 2022), these types of liquidity risks may especially arise in stablecoins or lending protocols and platforms.⁴⁹

The redemption run-risk of stablecoins arising from liquidity mismatches has been already widely documented and discussed.⁵⁰ As a manifestation of these risks, the June 2022 TerraUSD/Luna collapse had widespread effects beyond its closely linked DeFi lending protocol, Anchor. But the risk of redemption runs is not limited to algorithmic stablecoins like TerraUSD. Stablecoins where the issuer maintains “reserves” invested in less liquid traditional financial assets (such as commercial paper or certificates of deposit) are also subject to run risk, not dissimilar from the prime money market funds that have been a source of financial turmoil in the past.

⁴⁶ See Boissay et al. (2022), *Blockchain scalability and the fragmentation of crypto*, BIS Bulletins, no 56.

⁴⁷ See Forbes, *Over \$2 Billion Stolen This Year In Blockchain Bridge Hacks Expose DeFi's Achilles Heel*, (18 August 2022).

⁴⁸ As in TradFi, there could be issues associated with funding and market liquidity, but these seem less concerning in DeFi at present.

⁴⁹ See Aramonte et al (2022), *Non-bank Financial Intermediaries and Financial Stability*, BIS Working Paper No 972, January.

⁵⁰ See US President's Working Group on Financial Markets (2022), *Report on Stablecoins*, November; ECB (2022), *Stablecoins' role in crypto and beyond: functions, risks and policy*, Macprudential Bulletin article No. 18, July; and Arner et al (2020), *Stablecoins: risks, potential and regulation*, BIS Working Paper No 905, November.

Stablecoins that are acting in non-compliance with applicable regulations, are subject to limited or weak regulation, or are unregulated while performing liquidity transformation akin to traditional bank and non-bank entities⁵¹ could lose their peg, with broader repercussions for the DeFi ecosystem given their common usage within DeFi (see Section 1). In addition, such shocks could also be propagated to the markets of the assets in which stablecoins are invested, such as government bonds, corporate bonds and commercial paper.

Liquidity mismatches also arise in other segments of DeFi (and CeFi) intermediation, notably in the context of lending platforms. One way in which some lending platforms have offered higher yields is by promising investors immediate redemption, while investing proceeds from deposits in less liquid assets, often using the borrowers' collateral to borrow and invest more. When inflows exceeded outflows, the model allowed a fund or platform to benefit from a liquidity/maturity premium. But, when market sentiment turns and redemption demand rises, the fund or platform may struggle or fail to meet such redemptions.

A recent manifestation of this vulnerability in lending protocols is the shock that Lido experienced in May 2022. Lido ETH holders are able to 'stake' their ETH (i.e. pledge ETH holdings at term) while earning a yield. However, reports indicate that Lido's investors used their staked ETH (stETH) to boost their returns on the Anchor protocol, thereby creating a dependence between Lido's business model and Terra's blockchain.⁵² This in turn had knock-on effects on the CeFi lending platform Celsius, which offered depositors high returns on certain stETH and the possibility to redeem daily. After the collapse of TerraUSD and decline in the value of stETH relative to ETH, Celsius was forced to halt client withdrawals, placing further stress on the crypto-asset sector, including DeFi. Similar effects were observed after the collapse of FTX in November 2022, in response to which several other crypto-asset entities suspended withdrawals.

2.3. Leverage

A key feature of crypto-asset markets, including DeFi, is the outsized impact of leverage on market dynamics. Due to pseudonymity, financial intermediation in DeFi largely rests on the use of collateral and on the leverage that usage entails.⁵³

As in TradFi, the use of leverage leads to procyclicality and can trigger sharp adjustments in prices that have knock-on effects on other market participants. Specific features of DeFi relating to the management of leverage – in particular, the automatic liquidation of collateral – are a primary reason why deleveraging dynamics in DeFi can be especially vehement. This automated risk management tool serves to protect the lender but raises financial stability concerns for the DeFi ecosystem due to the externalities that stem from it. In these protocols, loans for which collateral falls in value below a certain threshold trigger an automatic liquidation. If these liquidations occur under stressed conditions, collateral may be forcibly liquidated into a market

⁵¹ Some authors argue that stablecoins issuers are essentially unregulated banks. See for instance Gorton and Zhang (2021), *Taming wildcat stablecoins*, University of Chicago Law Review Vol. 90 Forthcoming, September. In any event, stablecoins are subject to runs.

⁵² See Coindesk (2022), *Goldman Sachs Says DeFi's Interconnections Can Increase Systemic Risk*, May, and Decrypt (2022), *How the Celsius liquidity crisis crunch is linked to Lido's staked Ethereum*, June.

⁵³ See, for example, Aramonte et al. (2022), *DeFi lending: intermediation without information?*, BIS Bulletin no 57.

with low liquidity, pushing collateral prices down further, and spreading contagion. In TradFi, such self-reinforcing dynamics can be alleviated via orderly liquidation at central counterparties or can be arrested by market circuit breakers, but both of these mechanisms are absent in DeFi.

Leverage-induced boom-bust dynamics were on display during the turmoil in May and June of 2022. In the prior period, both institutional and retail investors had employed significant leverage to generate higher returns.⁵⁴ As crypto-asset prices fell, leveraged positions led to margin calls and/or automatic liquidations, amplifying price deterioration.

It is important to note that the exact amount of leverage deployed in DeFi is difficult to gauge. One reason is that in crypto-asset markets the borrowed funds are often used as collateral for other loans, giving rise to “collateral chains” (akin to re-hypothecation).⁵⁵ Better measurement of collateral re-use and the development of other measures of leverage would enable estimation of the degree of leverage in particular DeFi protocols and form an integral part of a monitoring framework of DeFi and crypto-asset risks (see Section 4).

2.4. Interconnectedness, concentration and complexity

As discussed in Section 1 and presented in Figure 1, the DeFi ecosystem features a wide set of existing and potential interconnections, both within DeFi as well as with outside entities (notably CeFi and other segments of crypto-asset markets, but also third-party technology providers). On the one hand, from a financial stability viewpoint, one could argue that diversity can bring benefits – if a shock hits one part of the system, the other part can compensate to help stabilise the system. On the other hand, the complex web of interconnections in DeFi may give rise to vulnerabilities, which are the focus of this subsection.

2.4.1. Composability

The composability of DeFi protocols – i.e. the DeFi “Lego” that proponents typically cite as an important source of efficiency – may lead to increased interconnectedness within the ecosystem. DApps often employ multiple smart contracts and interact with multiple protocols, which create strong interdependencies across smart contracts.⁵⁶ Therefore, technological failure in a single smart contract could generate adverse spillovers that can further propagate in the system. As such, composability can amplify the reach and speed of financial contagion within the DeFi ecosystem or could lead smart contracts to interact in unexpected ways.

2.4.2. Critical functions, concentration and complexity

Contrary to what decentralised finance proponents suggest, financial intermediation activities in DeFi often depend on a small number of critical intermediaries and systems to provide services which give rise to concentration risks. This is exacerbated by complex links with entities within and outside of DeFi that may not always be transparent. Currently, activity is concentrated in a

⁵⁴ There are also DeFi margin trading protocols, but trading volumes are less significant. [dYdX](#), a major margin trading protocol, currently appears to have only around \$30 million in open interest, down from around \$200 million in November 2021.

⁵⁵ See Aramonte et al. (2022), *DeFi lending: intermediation without information?*, BIS Bulletin no 57.

⁵⁶ See Amler et al (2021), *DeFi-ning DeFi: Challenges & Pathway*, January.

small number of protocols despite the existence of numerous applications. The aggregate total value locked (TVL) of the top four DeFi applications accounted for more than 75% of DeFi's TVL as of October 2022.⁵⁷ The failure of any large protocol could thus create spillovers that reverberate as, for example, the knock-on effects from each of the TerraUSD/Luna and FTX collapses illustrate. In addition, there is heavy concentration of activity on the Ethereum blockchain (about 60% of DeFi TVL). Hence, any disruptions from malicious activity or from infrastructure maintenance or upgrades affecting the Ethereum blockchain may impact the DeFi ecosystem as a whole.

DeFi platforms are also exposed to potential distress of CeFi trading platforms. The latter often provide more user-friendly interfaces that enable DeFi to reach more investors and enhance the liquidity of their products, and they often have counterparties across the crypto-asset/DeFi ecosystem.⁵⁸ While CEXs facilitate access and trading in DeFi protocols, they also exacerbate risks because of their outsized footprint in the market. Many platforms operate in non-compliance with or outside of supervisory and regulatory frameworks, increasing the likelihood of concentrated ownership, poor custody arrangements, illiquidity, and the potential for price manipulation, fraud, and other misconduct.⁵⁹ Further, CEXs often operate non-exchange related activities and may be linked with counterparties across the crypto-asset/DeFi ecosystem, for example through lending or investments in DeFi protocols. As such, concerns regarding possible conflicts of interest, comingling of customer funds and inappropriate combinations of business lines have regularly surfaced in the case of these platforms.⁶⁰ Such interlinkages between DeFi and CeFi platforms can give rise to two-way spillovers.

For example, the crypto-asset trading platform FTX had close ties to Solana's crypto-asset ecosystem and, in particular, the SOL token. It also had significant control over the DeFi trading platform Serum. The collapse of FTX in late 2022 raised investor concerns about the integrity of both Serum and the Solana blockchain more broadly, leading to significant price declines in associated tokens, and the termination of the Serum program.⁶¹

DeFi is also dependent on third-party providers for its functioning. Oracles are required for DeFi protocols to execute the code of their smart contracts and these oracles rely on off-chain data. But there are many other components of the DeFi ecosystem that are reliant upon third-party services to function, such as the underlying internet infrastructure or cloud service providers.

⁵⁷ Source: [The Block](#) as of 13 October 2022. This number is measured across all blockchains reflected in the data source. TVL refers to the total dollar amount of assets that is deposited in all DeFi protocols. It does not refer to transaction volumes or market cap of crypto-assets, but rather to the value of reserves that are "locked" into smart contracts. Reported TVL may vary depending upon the source and is prone to double counting.

⁵⁸ Such as Compound and Zora: see [Coinbase prospectus filing](#).

⁵⁹ Centralised crypto-asset platforms also often tend not to have measures in place such as circuit breakers to help mitigate the potential negative effects of large price swings. Many CEXs allow for extraordinary levels of leverage and may have non-standard margining practices or lack orderly liquidation mechanisms.

⁶⁰ See Aramonte et al (2021), [DeFi lending: intermediation without information?](#), BIS Bulletins, no 57; IOSCO (2022), [Decentralized finance report](#), March; and OECD (2022), [Institutionalisation of crypto-assets and DeFi–TradFi interconnectedness](#), May.

⁶¹ See Cointelegraph (2022), [Serum exchange rendered 'defunct' following the collapse of Alameda and FTX](#), November; and Decrypt (2022), [Binance Removes Trading Pairs for Solana-based Exchange Serum Token](#), November.

2.5. Other vulnerabilities

2.5.1. *Market integrity*

Market integrity issues are usually not directly connected to financial stability in TradFi. Shocks in this case are usually idiosyncratic and rarely propagate across the traditional financial system with sufficient magnitude and speed. However, given that DeFi is still nascent and evolving, severe market integrity issues could result in adverse confidence effects that may generate spillovers. These could potentially have an impact on financial stability should the sector grow further and become more interconnected with TradFi and the real economy.

An important market integrity issue that could have systemic consequences is the reliance of some DeFi products on continuous investor inflows to remunerate early adopters. These types of unsustainable business models have surfaced from time to time in financial markets. Given the technical complexities and opacity, coupled with retail investor participation, crypto-asset and DeFi markets have been a particularly fertile ground for such schemes. The demise of the Anchor protocol, which relied on the continuous growth of investors (as otherwise remuneration of lenders on the platform would have been unsustainable) and led to the collapse of TerraUSD, serves as an example of this vulnerability. As the TerraUSD/Luna meltdown and the subsequent bankruptcy of FTX have shown, the ensuing losses due to the collapse of such schemes can erode investor confidence and investor wealth, with potentially wide-ranging knock-on effects.

The provision of financial services by DApps directly or through synthetic structures in ways that do not comply with financial regulations, including regulatory evasion, expose retail and institutional participants to risks related to market manipulation or outright fraud. For instance, DeFi users are exposed to a manipulative practice unique to blockchain-based platforms reminiscent of front-running known as “miner extractable value” (also called “maximal extractable value”).⁶² Market participants are also exposed to the risk of fraud, hacks and theft and hence often risk losing a substantial share of their investment without any recourse.

2.5.2. *Cross-border regulatory arbitrage*

The cross-border nature of DeFi platforms and governance structures that make it difficult to identify appropriate legal ownership/control as well as relevant legal authorities, imply that DeFi cross-border interconnections are particularly opaque. DeFi arrangements often operate without a clear domicile and thus may assert that they are not subject to the jurisdiction of supervisors, regulators, or consumer protection and resolution authorities. DeFi protocols also operate across borders, requiring the cooperation of regulators in jurisdictions where the protocol is operated or used. If users engage with a protocol through virtual private networks, disguising their location, it may prove difficult to identify appropriate jurisdictions. In fact, certain DeFi arrangements may purposefully employ a cross-border architecture as a form of regulatory arbitrage, exploiting gaps in cross-border regulatory or legal coordination to avoid effective supervision and

⁶² As discussed in Section 1.3.2, within the AMM trading platform model, imbalances are addressed through arbitrage trading against the liquidity pool. This feature, alongside the fact that trades need to be added to the blockchain, allows validators to front-run large orders for higher trading profit.

regulation or enforcement.⁶³ Addressing these challenges requires global coordination among a broader range of financial authorities.

2.5.3. *Cryptoisation*

The growth of DeFi may also contribute to currency substitution, especially in countries prone to higher inflation, macroeconomic instability, weak central bank credibility and with an inefficient banking sector. Such a scenario may lead citizens of these countries to buy crypto-assets as a potentially more reliable store of value than their own national currency.⁶⁴ This phenomenon has been dubbed “cryptoisation”, which DeFi could accelerate if used more widely. As is the case for more traditional forms of currency substitution, cryptoisation may complicate the management of domestic monetary policy and ultimately compromise monetary sovereignty. In such a scenario, widespread adoption of crypto-assets may erode the efficacy of measures that the central bank may undertake to support the banking system in a crisis, for example introducing capital and foreign exchange controls.

3. Interlinkages and transmission channels

The extent to which the DeFi vulnerabilities described in Section 2 can lead to financial stability concerns largely depends on the interlinkages and associated transmission channels between DeFi, TradFi and the real economy.

Given the self-referential nature of DeFi, there is at present little risk of a shock originating in the DeFi ecosystem having significant effects on the real economy. That said, while interlinkages are currently minimal, the extent to which they may grow in the future constitutes a main factor in determining the possible transmission of financial stability risks from DeFi. After describing the main interlinkages and transmission channels, this section describes possible DeFi evolutionary scenarios. Should DeFi become more connected to TradFi, financial stability could be affected in different ways and expand transmission channels. A forward-looking perspective not only helps gauge the potential DeFi financial stability risks but may also be helpful in assessing suitable policy responses.⁶⁵

3.1. Main transmission channels

In its report on how crypto-asset markets could impact financial stability,⁶⁶ the FSB identified four potential transmission channels. These are: (i) financial institutions’ exposures to crypto-assets, related financial products and entities that are financially impacted by crypto-assets; (ii) confidence effects; (iii) wealth effects stemming from the fluctuations in the market capitalisation of crypto-assets; and (iv) the extent of crypto-assets’ use in payment and settlement.

⁶³ Parts of the industry however embrace the need for regulation. See GBBC Digital Finance (2022), *DeFi: Moving the Dialogue on Standards and Regulation Forward*.

⁶⁴ See IMF (2021), *The Crypto Ecosystem and Financial Stability Challenges*, Global Financial Stability Report, October.

⁶⁵ See Aquilina et al, (2023), *Decentralised Finance (DeFi): A Functional Approach*, CEPR Discussion paper 17810 for a discussion on how DeFi could be regulated.

⁶⁶ See FSB (2018), *Crypto-asset markets Potential channels for future financial stability implications*, October.

The materialisation of the vulnerabilities highlighted in Section 2 may interact with the identified transmission channels to create financial stability concerns. The exposures of financial institutions to DeFi are particularly important for the first transmission channel, as problems in DeFi could be transmitted to TradFi. On the other hand, confidence effects and market capitalisation are more relevant for households and corporates heavily exposed to DeFi. Finally, were DeFi tokens, and in particular stablecoins, to become a widely used means of payment, then their systemic importance may substantially increase.

3.2. Interlinkages and the scope for spillovers

This subsection describes how stress originating from DeFi could spill over to TradFi and the real economy via the above transmission channels.

3.2.1. Financial institutions' exposures to DeFi

Most important from a systemic perspective arguably are interlinkages with the core banking sector. Thanks to a conservative prudential approach, banks' exposure to crypto-assets and DeFi is currently minimal.⁶⁷ But some regulated financial institutions have invested directly in crypto-related companies, including companies that provide access to DeFi apps or services, exposing themselves to a potential loss of capital should these companies not perform.⁶⁸

In addition to direct investments, banks may be exposed to DeFi through various direct and indirect channels, including:

- *Lending to DeFi counterparts:* this could include direct lending to entities that are involved in DeFi, such as DApps or crypto-asset platforms.⁶⁹ Banks may also have exposures through loans to individuals, family offices, corporates or other financial institutions (including hedge funds) that invest in or are engaged in DeFi activities. These exposures may be secured by crypto-assets or real economy assets.
- *Market-making / clearing services:* banks could be involved in trading and clearing crypto-assets or derivatives on behalf of clients.⁷⁰
- *Facilitating activities in the DeFi ecosystem:* banks could also play a more direct and active role in the DeFi ecosystem, including as issuers of tokenised assets (e.g. tokenised deposits or settlement coins), validators, providing wallet services, acting as custodian for stablecoin reserves,⁷¹ providing depository services to crypto-asset participants involved in DeFi, or tokenising real world assets.⁷² Banks' direct or indirect

⁶⁷ The BCBS has recently finalised the prudential treatment of banks' crypto-assets exposures under the Basel framework. See BCBS (2022), *Prudential treatment of cryptoasset exposures*, December.

⁶⁸ For example, Blockdata (2022), *BNY's investment in Fireblocks or UBS' investment in ConsenSys*, August.

⁶⁹ For example, Coindesk (2022), *Siam Commercial Bank via Compound Treasury*, May.

⁷⁰ For example, Sygnum Bank is offering clients structured investment products, and Coindesk (2022), *Nomura is planning to offer clients exposure to DeFi and NFTs*, May.

⁷¹ See BCBS (2019), *Designing a prudential treatment for cryptoassets*, December for a comprehensive list of potential bank channels of exposures.

⁷² For example, Coindesk (2021), *SocGen refinancing through a tokenised covered bond on MakerDAO*, October and Coindesk (2022), *JP Morgan tokenisation of traditional assets to be used as collateral in DeFi pools*, June.

involvement in DeFi may also raise additional operational risk including fraud and cyber risks, legal and reputation risks, and AML/CFT and sanctions compliance risks.

- *DeFi lending to banks*: there are examples of banks receiving funding from stablecoin issuers,⁷³ and such funding could expand if DeFi grows in size.

An important way through which interlinkages could grow is the tokenisation of real-world assets (see Box 1). Banks' tokenisation of traditional assets and deposits on DeFi protocols would increase the pool of collateral available in DeFi markets, which could potentially bolster their growth. Such activity would also represent an entry of DeFi into financing real economic activity.

Should interlinkages of this kind grow, the risk that a shock originating in DeFi could be transmitted to the real economy would increase materially. Also, to the extent that these activities are being undertaken by institutions that are systemically important in traditional financial systems, this interlinkage could heighten concentration risks (across both DeFi and TradFi), the potential for contagion, and the importance of particular DeFi protocols.

Similarly, institutional investors, especially those with fewer constraints posed by regulations or their mandates (e.g. family offices and hedge funds) are the biggest group of TradFi players participating in DeFi. The crypto-asset market turmoil of May/June 2022 resulted in the collapse of Three Arrows Capital, a hedge fund with investments across the crypto-asset and DeFi ecosystems, highlighting the potential for contagion from hedge funds involved in DeFi.⁷⁴

Although data are scarce, market intelligence suggests that, in spite of the currently depressed crypto-asset market values, institutional investors continue to show interest in crypto-assets and DeFi. Notwithstanding the market turmoil, a number of asset managers have announced plans to gain direct exposure to crypto-assets, and such plans may be expanded to DeFi assets in the future.

As broader institutional investor interest in DeFi grows, offerings by DeFi platforms catering to their preferences will likely expand. This includes, for instance, the development of institutional versions of DeFi protocols using permissioned networks designed to comply with AML/KYC regulations. Such developments may spur greater institutional activity across DeFi by asset managers.⁷⁵ Such increased links may heighten the possibility of contagion, as investors are able to borrow in one system and invest the proceeds in the other.

⁷³ See for instance Euromoney (2022), *DeFi pioneer MakerDAO funds regulated US bank*, September.

⁷⁴ Voyager, a crypto-asset lender, filed for bankruptcy on 6 July following default by Three Arrows Capital on its loan obligations. Another crypto-asset lender, BlockFi, has also reported significant losses due to its exposure to Three Arrows Capital. The crypto-asset trading platform FTX won the bid to acquire Voyager and provided a credit line to BlockFi. However, FTX's own bankruptcy on 11 November led to the re-opening of the bidding process for Voyager, while BlockFi halted customer withdrawals on the same day due to uncertainty surrounding developments with FTX. Earlier in 2022, BlockFi settled with the SEC for offering crypto-asset lending products in violation of the US federal securities laws. BlockFi has since filed for bankruptcy.

⁷⁵ A major announcement in this area was Coinbase's partnership with BlackRock asset management and BlackRock's plans to provide access to spot bitcoin for U.S. institutional investors. See Financial Times (2022), *Asset managers bet big on crypto despite market rout*, August.

3.2.2. *Households and firms*

If retail involvement in DeFi were to grow, households' exposure to crypto-asset-related shocks would increase, with potential for wider repercussions through wealth and confidence effects. Faced with large losses, retail investors could curtail spending or reduce their investments in other businesses. A loss of confidence in DeFi platforms could also trigger investor redemption runs and sales of other assets, which could have broader implications.

Comprehensive data on DeFi adoption by retail users is lacking. However, available information indicates that household involvement in DeFi is currently minimal, suggesting limited linkages to date. Current barriers to increased retail DeFi adoption are its complexity, transaction costs, and the need to already be active in the crypto-asset ecosystem. However, these obstacles may decrease over time should interest in crypto-assets continue to grow and, for example, centralised trading or lending platforms make DeFi protocols more accessible.

Presently, the use of DeFi by non-financial companies is mainly focused on trade finance and invoice-backed credit.⁷⁶ But if non-financial businesses were to increase their access to DeFi, as a channel for investment or for raising funds, shocks in DeFi could further lead to losses for businesses and reduce investment. Excessive use of leverage could amplify the shock.

3.2.3. *DeFi and payments*

Applications of DeFi in the realm of payment and settlement are still at an early stage. Some existing stablecoins are purportedly managed by DAOs, such as the DAI and FRAX stablecoins. While these existing stablecoins perform a range of functions, including acting as a substitute for fiat currency in the crypto-asset ecosystem, their stated ambition is to become a cross-border means of payment. If they develop further, these could be additional sources of financial vulnerabilities, as they would likely increase the adoption of DeFi solutions by retail and corporate users as well as facilitate the adoption of crypto-assets as a means of payment.

3.2.4. *Failure of FTX and its implications for DeFi*

On 11 November 2022, FTX.com (FTX), one of the largest crypto-asset trading platforms, and a large number of affiliated companies including Alameda Research, a large crypto-asset hedge fund, filed for bankruptcy.⁷⁷ The full extent of the impacts of this failure, including on DeFi projects that were owned by FTX or depended on it for trading flows, will take time to become apparent given the lack of disclosure and transparency in these markets.

The FTT token, an unbacked crypto-asset issued by the FTX group,⁷⁸ does not appear to have been much used for collateral on DeFi platforms. Liquidations related directly to FTT have been

⁷⁶ Examples include InvoiceMate, Credefi and Centrifuge, which allow tokenised real-world assets – in particular invoices – to be deposited as collateral in on-chain credit transactions.

⁷⁷ See The Block (2022), *FTX files for Chapter 11 bankruptcy*, November. *FTX Trading Ltd. and 101 affiliated debtors each filed a voluntary petition for relief under Chapter 11 of the United States Bankruptcy Code in the United States Bankruptcy Court for the District of Delaware*. It should be noted that LedgerX LLC, doing business as FTX US Derivatives (LedgerX), an affiliate of FTX US, is a CFTC-registered Designated Contract Market, Swap Execution Facility, and Derivatives Clearing Organization. LedgerX is distinct from FTX.com's global operations and is excluded from the FTX bankruptcy filing.

⁷⁸ FTT entitled holders to discounts on fees on the FTX platform, along with other benefits such as increased referral rebate rates.

affecting primarily smaller participants. The major DeFi platforms have experienced some liquidations given the market turbulence, but so far to a lesser extent than during May/June 2022.

Some market participants have claimed that the failure of such a significant CEX could drive further adoption of DEXs, given the mismanagement of customer assets in the case of FTX.⁷⁹ Indeed, immediately after the FTX failure, some DEXs increased their market share as compared to major CEXs. However, as described in the previous section, DeFi protocols are subject to various operational and governance issues that may limit their reach and appeal vis-à-vis CEXs.

3.3. Scenarios for the evolution of DeFi and financial stability implications

DeFi's financial stability implications ultimately depend on how the sector develops. This subsection presents three potential scenarios that could inform policymakers on this issue. Which of these scenarios will materialise, and the extent to which DeFi could pose risks to financial stability, will depend, in part, on regulatory responses to the sector.

Scenario 1: DeFi remains a niche area

Under the first scenario, DeFi remains a niche sector within the crypto-asset ecosystem, its growth loses momentum and interconnectedness with TradFi remains limited. This could be driven by a number of factors. The first factor is the specialised nature of the sector itself and the technical expertise needed to participate. There simply may not be demand among the broader population for decentralised finance offerings. Second, increased regulatory and supervisory scrutiny of the crypto-asset sector may inhibit financial institutions from engaging with DeFi given the issues and vulnerabilities described in this report. Third, the appeal of novel financial services applications in the sector may dissipate if these applications do not ultimately deliver clear benefits compared to what is already available in existing markets. Fourth, the market forces that contributed to the growth in crypto-asset markets more broadly may weaken as interest rates increase in an inflationary environment and as investors that were previously attracted by yield considerations leave DeFi platforms, thereby reducing liquidity. Under such a scenario, the relatively small size and limited interconnectedness of the sector would not give rise to financial stability concerns.

Scenario 2: DeFi grows and becomes part of the mainstream

Under the second scenario, the DeFi ecosystem grows significantly and becomes more mainstream as a result of the broader adoption of crypto-assets and the development of real-world use cases for DeFi. The environment under which such developments occur will also be shaped to a significant extent by regulatory responses to the crypto-asset and DeFi markets.

The first driver, growth of the broader crypto-asset ecosystem, could be a continuation of the initial phase of growth in 2020-21, in which the DeFi sector grew in tandem with the overall crypto-asset ecosystem. The second driver, the development of new real-world use cases, could encourage greater participation. For example, the tokenisation of traditional assets for collateral

⁷⁹ See WSJ (2022), *FTX Tapped Into Customer Accounts to Fund Risky Bets, Setting Up Its Downfall*, November.

in financial transactions could allow DeFi to evolve beyond its current self-referential system to provide financial intermediation services to the broader economy (see Box 1). Both of these drivers will be substantially impacted by developments in the regulation and supervision of crypto-asset markets. In the first wave, increased regulatory attention is likely to focus on centralised trading platforms and crypto-assets including stablecoins. For the centralised players to comply with regulatory expectations, they will need assurance that their DeFi counterparties are also in compliance. Such a scenario will potentially accelerate DeFi's integration with centralised entities, at the likely cost of lower decentralisation of its activities and governance.

Under this scenario, DeFi's growth and greater connections with regulated markets would lead to a deepening of interlinkages between DeFi and the real economy. The scope for spillovers through the above identified channels would then increase, giving rise to potential financial stability concerns and requiring a proportionally greater policy response.

Box 1: The tokenisation of real-world assets

The tokenisation of real-world assets has the potential to substantially increase the interconnectedness of DeFi with TradFi.⁸⁰ The tokenisation of assets that exist off-chain is the act of creating a digital representation of an asset and placing it on a distributed ledger.⁸¹ This ledger could be either permissionless or permissioned. Similar to native tokens, a tokenised instrument may contain all information needed to exchange the underlying asset, e.g. asset type, ownership, legal framework, clearing, settlement and custody requirements.

Yet tokenisation is neither new nor limited to markets for crypto-assets. TradFi has used for a long time a physical tokenised representation of an asset to improve efficiencies and security. Nor does tokenisation of an asset need to take place on a distributed ledger. A digital representation of an asset can exist on a centralised ledger as well, for instance a cloud-based database.

There are certain financial assets more easily given to tokenisation than others. For instance, equities and liquid fixed income instruments (i.e. government bonds) are considered by most market participants to trade efficiently at this point in time. Replacing the current infrastructure to allow instruments to trade on a distributed ledger would be expensive and disruptive. Moreover, new infrastructure would need to generate positive network effects to become an effective alternative to the current platforms. Proponents of tokenisation instead view less liquid instruments, the markets for which may have multiple layers of intermediation, as better candidates for tokenisation in the near term, e.g. private equity, leveraged loans, real estate, intellectual property, and art. Proponents argue that tokenisation would improve such assets' liquidity, and placing these alternative instruments into a portfolio could provide investors with greater degree of diversification and potentially higher risk adjusted returns, while disintermediation may also allow issuers to realize potential efficiencies.

Tokenisation would significantly expand the set of assets that could be exchanged on distributed ledgers using the existing or new crypto-asset ecosystem tools and processes and could benefit the entire crypto-asset ecosystem, including both CEXs and DEXs, assuming these entities operate in compliance with applicable laws and regulations.⁸² On a CEX or blockchain-based trading platform operated by traditional financial institutions, investors potentially could, for example, purchase a tokenised equity in which the buyer has dividend rights, voting rights and can redeem the tokenised equity for the actual underlying stock. Pre- and post-trade operations potentially could take place off-chain, where the matching order book and post-trade custody and operations are serviced by traditional service providers. On a DEX, all activities might take place on-chain, where the order book is replaced by an AMM and post-trade operations are controlled by buyers and sellers. Unlike tokenised securities on a CEX and blockchain-based platforms operated by TradFi, tokenised shares on a DEX could be synthetic, i.e. while the price of the tokenised share may track the underlying actual shares, synthetic shares would not be redeemable for the underlying, nor would holders enjoy dividend or voting rights. The synthetic share would be instead backed by a stablecoin, which reflects the value of the underlying share determined through the use of smart contracts. DEX platforms may rely on oracles to access off-chain information sourced from outside the crypto-asset ecosystem, such as the price of the referenced asset. Ensuring the validity and accuracy of such information is crucial for DEXs and may have significant impact on the feasibility of tokenisation.

Proponents of tokenisation on CEXs argue that there would be certain benefits when compared to existing security transactions and to tokenisation on conventional DLT-based trading platforms. First, trading on a crypto-asset platform takes place 24/7, making for a continuous global trading marketplace. Second, fractionalised ownership of tokenised assets means investors do not need to own the entire share but can gain partial ownership, potentially expanding market participation. Third, on traditional exchanges settlement generally takes place 2 days after the transaction, while on a crypto-asset exchange settlement is instantaneous, although this is also achieved on conventional DLT-based trading venues and can be technically feasible in TradFi as well.

However, challenges to the wider use of tokenisation exist. For example, the legal framework for transitioning assets between the real and the crypto-asset ecosystem would need to be developed, complied with, or adjusted in many jurisdictions.⁸³ Second, the underlying distributed ledger infrastructure must be easily accessible to drive widespread adoption. Third, standardisation is needed in technology that supports tokenisation, which is a demanding task in a decentralised system. Finally, the demand for possible benefits that tokenization can potentially provide might never materialize.

Scenario 3: DeFi slowly fades, but a legacy of innovation remains

As the May/June 2022 market events illustrated, the DeFi sector has a number of vulnerabilities, which may ultimately cause interest in the sector to decline. However, as in other cases in the past, a legacy of useful financial innovation that could enhance the capabilities of TradFi may remain. These stem from the capacity to combine transactions and to execute the automatic settlement of bundled transactions in a conditional manner, building on programmability, smart contracts, and composability. These innovations could enable greater functionality and speed and reduce the cost of financial intermediation in TradFi.⁸⁴

4. Monitoring the evolution of DeFi

This Section describes data challenges in DeFi, as well as possible ways to overcome them. It also sketches out various indicators that – despite the current data limitations – could be usefully deployed to monitor the evolution of DeFi and the build-up of vulnerabilities. These indicators represent an initial, and in some cases still conceptual, step to incorporate DeFi developments as part of the broader financial stability monitoring of the crypto-asset ecosystem.

4.1. Issues with existing data

As already noted in other reports, data on crypto-asset markets in general, and DeFi specifically, lack transparency and consistency.⁸⁵ This also applies to data on the interconnections of DeFi with the traditional financial system. Data issues are largely due to the nature of crypto-assets and the associated blockchains as well as the incentives of market participants, in particular:

- (i) the **difficulty in aggregating and analysing the vast amount of data** available on distributed ledgers. Data available from public blockchains may be transparent and immutable in some respects, but they are generally difficult to collect and analyse.

⁸⁰ Oliver Wyman et al, (2022), *Institutional DeFi The Next Generation of Finance*, argue that DeFi's main value add will be in the tokenisation of real-world assets.

⁸¹ See Morgan Stanley (2022), *The Future of Tokenised Assets*, May. This is in contrast to tokenisation involving the issuance of “native” tokens built directly on-chain and existing exclusively on the distributed ledger and without reference to an ‘off-chain’ asset; see OECD (2020), *The Tokenisation of Assets and Potential Implications for Financial Markets*, January.

⁸² See PWC (2021), *Decentralised Finance: Defining the future of finance*, May.

⁸³ For a more in-depth discussion of regulatory challenges, see OECD (2021), *Regulatory Approaches to the Tokenisation of Assets*, January.

⁸⁴ See BIS (2022), *The future monetary system*, Annual Economic Report, Chapter III, June.

⁸⁵ See FSB (2022), *Assessment of Risks to Financial Stability from Crypto-assets*, February.

- (ii) the **pseudonymous nature of information** on public ledgers inhibits the ability to ascertain the types of investors in the crypto-asset ecosystem. While some transaction data at the wallet level are accessible, the lack of data about the identity of wallet owners makes the assessment of vulnerabilities much more challenging. These issues are further compounded by the cross-border nature of DeFi. In addition, there are a range of privacy-enhancing technologies (e.g. wallet mixers/tumblers/anonymity enhanced crypto-assets), which allow certain users to obscure transparency of transactions.⁸⁶
- (iii) the large number of **off-chain transactions**, i.e. those that occur outside of public distributed ledgers, and other off-chain data. As such, on-chain data may give an incomplete picture of the overall activity in the market. This is particularly important for DeFi transactions that take place on centralised platforms or bilaterally.
- (iv) the **lack of reporting** producing consistent and reliable data because parts of the crypto-asset ecosystem fall outside of, or are in non-compliance with, the regulatory perimeter at present. This means that crypto-asset market participants typically do not comply with common disclosure, recordkeeping and reporting rules covering entities in traditional finance, hampering data quality and comparability.⁸⁷
- (v) Some data providers, notably crypto-asset trading and lending platforms, may be **incentivised to manipulate their data** (e.g. through practices such as wash trading) to make their respective platforms appear more significant and attract additional volume or investment.⁸⁸ Market incentives for trading and lending platforms, coupled with participants acting outside of, or in non-compliance with, existing regulatory frameworks, increase the risk of market manipulation or data falsification.

Some attempts to overcome these shortcomings have been made by market data providers, such as blockchain analytics companies, but much of their source data is still subject to the problems described above. The deficiencies in private data collection call for a targeted approach by the public sector to enhance market transparency and risk monitoring.

4.2. Elements of DeFi monitoring

The first important ingredient in DeFi monitoring are indicators that can help to gauge the overall size and evolution of DeFi. The second key component are indicators that are specifically designed to gauge the financial vulnerabilities of DeFi identified in Section 2. The third set of

⁸⁶ In August 2022, the US Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned virtual currency mixer Tornado Cash. "Mixers" such as Tornado Cash receive a variety of crypto-asset transactions and mix them together before transmitting them to their individual recipients. While the purported purpose is to increase privacy, mixers are also used by illicit actors to launder funds, especially those stolen during significant heists. According to OFAC, Tornado Cash was used to mix more than \$7 billion worth of virtual currency since its creation in 2019. As a result of OFAC's action, all property, and interests in property of Tornado Cash in the US or in the possession or control of US persons is blocked and must be reported to OFAC.

⁸⁷ As parts of the DeFi ecosystem are outside of or in non-compliance with existing regulatory requirements, much of the available data is self-reported by industry participants. As such, there can be significant discrepancies across commercial data providers.

⁸⁸ For instance, in August 2022 it was reported that prominent developers of the Solana blockchain were artificially inflating Solana's TVL by counting the same crypto-asset multiple times. See Cryptotimes (2022), *Meet the people behind the fake TVL of 7.8B in Solana*, August. Some studies also find that much of the reported volume on unregulated crypto-asset platforms is due to "wash trading" – see Cong et al (2021), *Crypto Wash Trading* and Forbes (2022), *More Than Half Of All Bitcoin Trades Are Fake*, August.

indicators pertain to the tracking and assessment of interconnections between DeFi, CeFi, TradFi and the real economy in order to gauge the scope for spillovers.

It is important to note that monitoring should adapt flexibly as the crypto-asset and DeFi markets evolve. Furthermore, given the lack of comprehensive and reliable quantitative data on DeFi, monitoring should also incorporate qualitative analyses and insights from market intelligence.

Another important aspect of monitoring is the choice of frequency of updates. Some monitoring could take place at a fairly regular interval and concentrate on DeFi market conditions based on quantitative data. Other, more targeted monitoring could take place at lower frequencies and entail a deeper, forensic analysis of specific events or structural changes in markets (e.g. with respect to vulnerabilities stemming from specific DeFi arrangements).

4.3. Tracking the evolution of DeFi markets

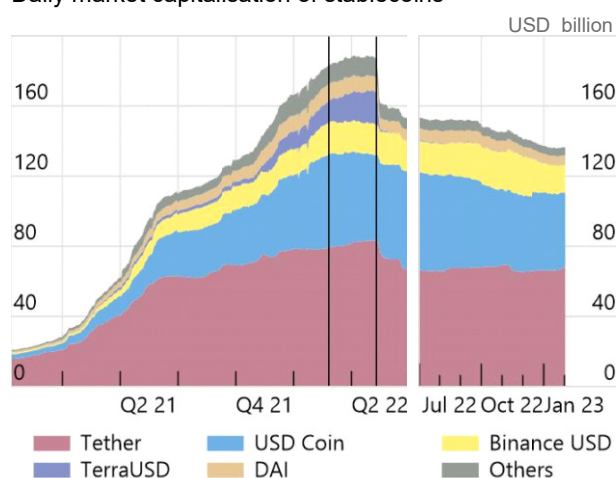
In general, there are currently at least four key metrics that can be used to monitor the evolution of the DeFi ecosystem (see Graph 1). First, the TVL purports to measure the total value expressed in USD “locked” in DeFi smart contracts and reflects the scale of DeFi market participation by blockchain and type of activity. Second, the number of DApps can be used as a proxy for the number of DeFi projects. The third metric is stablecoin market capitalisation, which may give an indication about the importance of stablecoins (particularly those that are native to DeFi protocols) within DeFi. Lastly, the number of DApps users based on the unique addresses in underlying blockchains can suggest the extent to which DeFi market participation is growing.

While seemingly simple indicators, their use introduces complexities when it comes to their interpretation. For instance, TVL estimates vary because of double counting issues. A new token created because of a smart contract could be counted in addition to the original token committed. Further, the TVL calculations may or may not include governance tokens. Stablecoins are often used for non-DeFi purposes and, thus, their market capitalisation growth might overstate DeFi growth. The number of DApps might depend on market structure, with a market characterised by a few dominant players having a low number of DApps. The number of unique addresses might depend on protocol design (e.g. users may be incentivised to create multiple unique addresses to take advantage of governance token “airdrops”). Operationalising the monitoring framework would therefore require developing measures that account for such complexities.

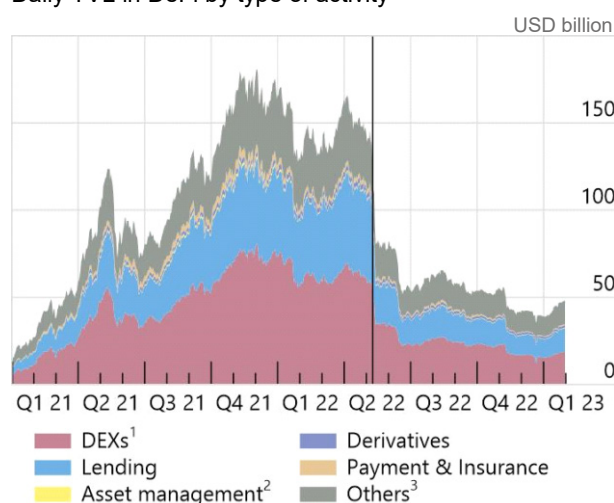
Evolution of DeFi markets

Graph 1

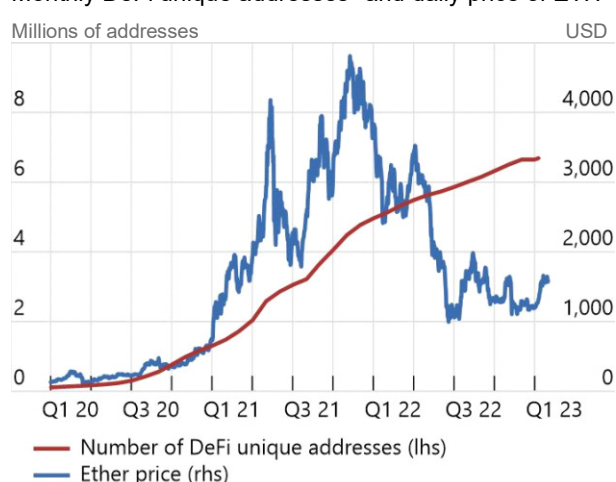
Daily market capitalisation of stablecoins



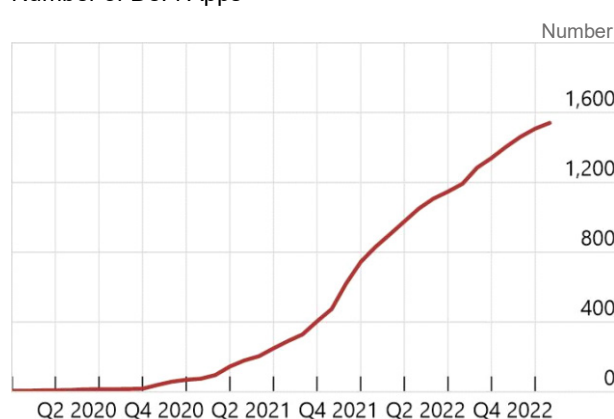
Daily TVL in DeFi by type of activity



Monthly DeFi unique addresses⁴ and daily price of ETH



Number of DeFi Apps⁵



The vertical lines in the top left panels indicate 23 February 2022, the day before the start of the Russia-Ukraine war and 9 May 2022, the day TerraUSD started to significantly decouple from its peg. The vertical line in the top right panel indicates 9 May 2022.

¹ DEXs stands for decentralized exchanges and include protocols which allow users to trade crypto-assets.

² Sum of Yield, Yield Aggregator and Indexes categories.

³ Others include all other protocols categorised by DeFiLlama such as Bridge, Liquid Staking, Collateralized Debt Position, Services, Algo-Stables and etc.

⁴ Number of unique addresses that either bought or sold a DeFi asset worldwide from December 2017.

⁵ The number of DeFi apps with positive TVL.

Sources: Coin Dance; CoinGecko; CryptoCompare; DeFiLlama; Statista; The Block; FSB calculations.

4.4. Tracking vulnerabilities

Section 2 discussed five types of core vulnerabilities in DeFi: (i) operational fragilities; (ii) liquidity/maturity mismatches; (iii) leverage; (iv) interconnectedness, concentration and complexity; and (v) other vulnerabilities. This subsection includes a non-exhaustive discussion on how the monitoring of these vulnerabilities could be approached.

One potential way to quantify fragilities emanating from **operational aspects of DeFi protocols** is by measuring the relative size of each particular source of fragility. For instance, data

measuring the size of individual DeFi protocols, oracles, and blockchains relative to the DeFi ecosystem (as measured by TVL) is available through publicly-available industry data providers.

Information on the **concentration of governance token ownership** is available through data providers and protocol websites. Ideally, this would not only show the concentration level but also the amount of tokens held in accounts linked directly to the protocol (e.g. developer team accounts), given that this type of information could provide insight into their role in the governance of the protocol. This type of information is only available in a very limited number of cases. Another important measure of governance-related risks is the voting percentage required to approve a proposal. This voting percentage could show how important the concentration of governance token holdings is for changing specific features of a protocol. In addition, information on whether the governance system includes token holders with veto power – so called “guardians” — or other gatekeeping features, can also provide material insights into the concentration of power.

Trying to measure the potential impact of an **outage or failure of a third-party service provider** is still more complicated. Individual third-party service providers may be utilised across a large number of DeFi protocols, and these providers fulfil multiple functions within the broader crypto-asset ecosystem. There does not appear to be a data provider that is collecting information on these third-party providers to enable an approximation of concentration within the DeFi sector. At present, only indicators relating to wallet providers can be analysed.

With respect to **liquidity and maturity mismatch** issues, stablecoins are a crucial area of focus. An understanding of the overall size of different types of stablecoins, differences in issuers, use cases and investors across stablecoins, as well as the quality of reserve assets referenced, is needed to assess and monitor the risk stablecoins pose to the crypto-asset ecosystem (including DeFi) and for the markets of TradFi assets in which they invest.⁸⁹ Issuer disclosures, audits and market data providers can give insights into some of these stablecoin-related issues. Certain providers also have data relating to the use of stablecoins in DeFi, at least for specific protocols or blockchains.

Measuring the amount of **leverage** deployed in DeFi and crypto-asset markets more generally is challenging. A variety of indicators may be informative, such as measures of collateralisation and the extent to which assets are re-hypothecated within the system. For instance, data from Chainalysis referenced by the Organisation for Economic Cooperation and Development (OECD)⁹⁰ show that many of the flows into DApps originate from within the DeFi space itself, and only a very small share of inflows comes from fiat converted into crypto-assets. This might suggest the high use of leverage by DeFi participants, who may create collateral chains by lending or investing assets initially received as collateral. Given the outsized role of leverage in DeFi and crypto-assets markets more broadly, as well as the potential for amplification channels due to automatic liquidations of smart contracts, the development of suitable leverage indicators should be a priority for monitoring.

⁸⁹ See FSB (2022), *Review of the FSB High-level Recommendations of the Regulation, Supervision and Oversight of “Global Stablecoin” Arrangements: Consultative Report*, October, for the proposed revisions to the FSB recommendations in this area.

⁹⁰ See OECD (2022), *Institutionalisation of crypto-assets and DeFi–TradFi interconnectedness*, May.

Interconnectedness among and **concentration** within the various components of DeFi (such as blockchains, protocols, oracles, bridges, and stablecoins) takes different forms and as such needs to be monitored using a variety of indicators. Evaluating new products and features in the DeFi ecosystem requires understanding of how they operate. As noted above, the failure of any large protocol could create spillovers that reverberate more widely. However, the safety and soundness of a single protocol cannot be analysed in isolation; influences of other protocols must also be considered. Monitoring such interconnectedness may be done by looking at the concentration activity in the underlying blockchains and in the TVL of the largest DApps.

As for **other vulnerabilities**, a number of indicators of **market integrity** issues may be used. The total miner extractable value represents a proxy of rent extraction by one set of “insiders”, which may come at the detriment of other investors. To monitor Ponzi-like dynamics, an assessment of the cash flow generated by DApps in comparison to the market capitalisation could be used, as well as a comparison of annual yield offered by DeFi protocols relative to alternative investments. Such quantitative information may be complemented by market intelligence to develop a good understanding about any fast-growing protocols that might have an unsustainable business model (as in the example of Anchor and Terra/Luna).

4.5. Tracking interlinkages and transmission channels

As noted above, the extent to which DeFi vulnerabilities result in financial stability issues largely depends on interactions with TradFi and the real economy. Monitoring such interactions is more complex, because it requires information both from the DeFi ecosystem and from other sources. In many cases, participants may be unwilling to disclose their activity in the DeFi space unless they are legally required to do so (current reporting and disclosure requirements for regulated firms do not generally provide adequate granularity in this area) and as the data to monitor these vulnerabilities are not on the blockchain it may be very difficult to gather them. In other cases, the aggregation of information will be impossible given wallet pseudonymity.

As for financial sector exposures, there are several areas to monitor. These include the growth of banks with business models tailored to the crypto-asset market and the participation of institutional investors in DeFi, especially if mainstream investment vehicles become more active. Other potentially useful indicators include household and corporate exposures, but there is little data currently available to measure these links.

5. Conclusions

As discussed in the report, while its purportedly decentralised processes to provide financial services are in many cases novel, DeFi does not differ substantially from the traditional financial system in the functions it performs. Furthermore, the actual degree of decentralisation among underlying DeFi organisational structures varies broadly, often deviating substantially from the stated claims of the founding originators. In attempting to replicate some functions of the traditional financial system, DeFi inherits and often amplifies the vulnerabilities of that system. The amplification comes from novel technological features, the high degree of structural interlinkages amongst the participants in DeFi, and from lack of regulation or non-compliance with existing regulatory requirements. Ultimately, the extent to which the vulnerabilities stemming

from DeFi can lead to financial stability concerns largely depends on the interlinkages between DeFi and traditional finance and the associated spillover channels.

One plausible scenario is that DeFi continues to grow in the future and becomes more interconnected with the real economy and the broader financial system. Thus, the vulnerabilities inherent in DeFi identified in this report and potential threats to financial stability require careful monitoring as the ecosystem grows and evolves. At present, the monitoring of its vulnerabilities is hampered by the absence or low quality of available data, lack of or non-compliance with reporting requirements, and market practices oriented towards operating in opaque and non-transparent ways that create challenges for accurate data collection and analysis.

In light of these findings, several considerations are warranted. First, the FSB should proactively analyse the financial vulnerabilities of the DeFi ecosystem as part of its regular monitoring of the wider crypto-asset markets. In this regard, the FSB crypto-asset monitoring framework should be complemented with DeFi-specific indicators of vulnerabilities. Relatedly, the FSB will explore the growth of tokenisation of real assets as it could increase interconnections between crypto-asset markets and DeFi with the broader financial system and the real economy.

Second, an effective analysis of whether vulnerabilities from DeFi could affect the financial system depends on the availability of data on the interconnectedness of DeFi (and the crypto-asset ecosystem in general) with TradFi (including both banks and other types of financial institutions) and with the real economy. The FSB, in collaboration with SSBs and regulatory authorities, will explore approaches to measure and monitor such interconnectedness. In the interim, consideration can be given to greater sharing of existing data and market intelligence as well as use of ad-hoc information collection methods (e.g. surveys).

Third, as both the use cases and regulatory approaches around DeFi are still evolving, the FSB will explore the extent to which its proposed policy recommendations for the international regulation of crypto-asset activities may need to be enhanced to take account of DeFi-specific risks and facilitate the enforcement of rules.⁹¹ DeFi-specific risks may include, for example, the use of smart contracts for transaction execution that can lead to automatic liquidation; opaque governance arrangements (including the possibility of concentrated token ownership); dependence on blockchain networks; and the use of oracles and cross-chain bridges that are susceptible to market manipulation and cyber thefts. The FSB, working with SSBs, will also consider potential policy responses to the risks stemming from DeFi's interconnectedness with the broader financial system and the real economy. Potential policy responses may include, for example, regulatory and supervisory requirements concerning traditional financial institutions' direct exposures to DeFi, as well as concerning other ways that such institutions may seek to become more integrated with DeFi (e.g. by serving as trustees or custodians, or by transacting with other firms engaging in DeFi). It also includes consideration of whether to address vulnerabilities within DeFi itself and its connection within the crypto-asset ecosystem if the sector grows but remains separate from TradFi.

As part of this work, the FSB could also consider, in coordination with the SSBs, assessing the regulatory perimeter across jurisdictions to determine which DeFi activities and entities fall or

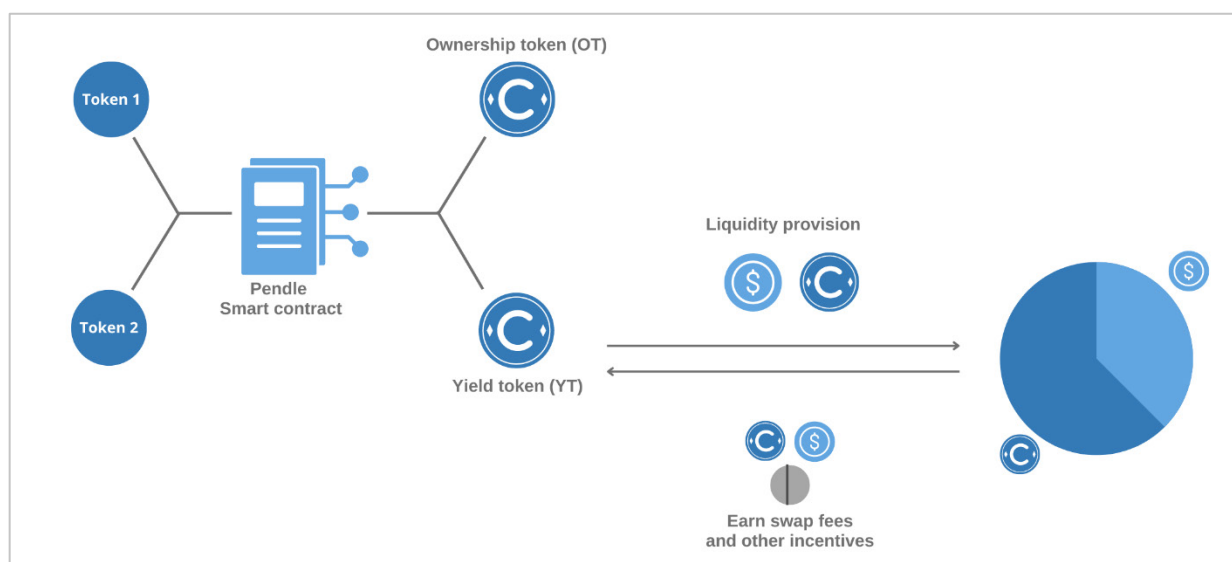
⁹¹ See FSB (2022), *International Regulation of Crypto-asset Activities: A Proposed Framework – For Consultation*, October.

should fall within that perimeter (in which case enforcement of compliance with applicable regulations is warranted) or outside of it (in which case policies should be developed to achieve appropriate regulation of activities giving rise to similar risks). In this respect, a key element to consider would be the entry points of DeFi users (including retail investors and traditional financial institutions), such as through stablecoins and centralised crypto-asset platforms. The FSB may consider whether subjecting these crypto-asset types and entities to additional prudential and investor protection requirements, or stepping up the enforcement of existing requirements, could reduce the risks inherent in closer interconnections.

If DeFi activities and entities are deemed to fall within the regulatory perimeter, the enforcement of compliance with applicable regulations is warranted. Enforcement actions should proceed, and members should collectively aim for a better understanding of enforcement and supervisory challenges. In instances where DeFi activities and entities fall outside the regulatory perimeter, the challenge would be to develop policies that achieve appropriate regulatory outcomes for activities giving rise to similar risks. SSBs can play an important role in such perimeter assessments, as well as strengthening cross-border cooperation and data sharing. The FSB is well-placed to analyse and advise on cross-sectoral and cross-border issues, including how to promote effective cooperation with respect to crypto-asset supervision and regulation.

Annex: Illustration of typical DeFi applications

Example 1: DeFi derivatives: pendle finance⁹²



To allow users to give up rights to their yield for a fixed period of time, users will deposit their yield token (YT) into a smart contract. Two tokens will be issued in exchange: a future YT and an ownership token (OT). Each YT represents ownership of the future yield, OT represents the underlying staked asset.

Users who have YT tokens can either sell them or add them to the YT liquidity pool in exchange for liquidity provider (LP) tokens to earn liquidity incentives.

YT can be traded until its expiry and has no value upon expiry. The OT holder can choose to roll forward to a new expiry and repeat the process or redeem the underlying tokens.

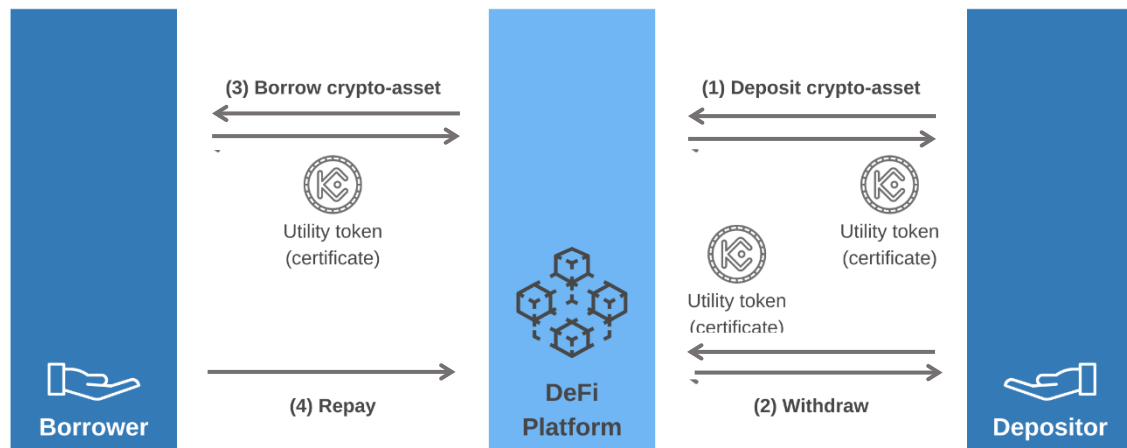
Redeeming an underlying token before contract expiry requires the possession of both OT and YT. The OT holder can obtain YT by either purchasing YT from the market or withdrawing YT from the liquidity pool.

⁹² See [the Pendle website](#).

Example 2: DeFi lending

DeFi lending platform receive crypto-assets as deposits and provide collateralised loans

The flow of a DeFi Lending Transaction



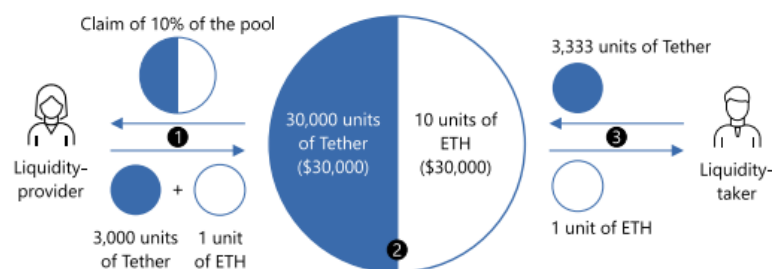
Most lending is against stablecoins backed by volatile crypto-assets

Example 3: Automated market maker

DEX – constant product function market-maker

Graph A

- ① Suppose 1 Tether = \$1, 1 ETH = \$3,000
Initially, 27,000 units of Tether and 9 units of ETH, each worth \$27,000



Transactions:

- ① A liquidity-provider "deposits" 3,000 units of Tether and 1 unit of ETH
- ② After this deposit, the pool contains 30,000 units of Tether and 10 units of ETH
Following the bonding curve, the constant equals 300,000 (= 30,000 * 10)
The liquidity-provider has a claim of 10% of the pool's crypto-assets
- ③ A liquidity-taker wishes to buy 1 unit of ETH
The price for 1 ETH is $(30,000 + x) * (10 - 1) = 300,000$
Thus, $x = 3,333$, which is the amount of Tether the taker pays for 1 ETH
End result: the pool contains 33,333 units of Tether and nine units of ETH

Liquidity-provider's value (10% of the pool)

Before trade
3,000 units of Tether
+ 1 unit of ETH
= \$6,000

After trade
3,333 units of Tether
+ 0.9 units of ETH
= \$6,033

Glossary

This glossary sets out a (non-exhaustive) list of terms used in the report as it relates to DeFi. The definitions are based primarily on previous reports by the FSB as well as by other international organisations and SSBs. The use of these terms in the report does not involve a judgment as to their appropriateness in all cases given the rapidly evolving crypto-asset markets.

51% attack: When a malicious actor is able to compromise more than half of the validators on the network, the actor can execute fraudulent transactions.

Asset-backed token: A crypto-asset that represents an interest in a physical asset.

Atomic Swap: Instant exchange of two crypto-assets, such that the transfer of one occurs only upon transfer of the other one.

Automatic Market Maker (AMM): A decentralized exchange protocol that relies on smart contracts to set the price of digital assets in accordance with a pre-established mathematical formula that may vary across DeFi protocols and whose goal is to provide liquidity to the ecosystem.

Blockchain: A form of distributed ledger in which details of transactions are held in the ledger in the form of blocks of information. A block of new information is attached into the chain of pre-existing blocks via a computerised process by which transactions are validated.

Bridge: A technique used to transfer crypto-assets between ecosystems by, typically, creating a synthetic representation of a blockchain-specific crypto-asset on a different blockchain.

Centralised exchange (CEX): A crypto-asset trading platform that facilitates the buying and selling of crypto-assets, either for fiat currencies, or for another digital asset. The platform functions as an intermediary and sometimes provides custody and other services.

Centralised finance (CeFi): Centralised intermediaries (for example lending or trading platforms) within the crypto-asset ecosystem that purport to offer some of the features of DeFi with some of the ease of use and security of traditional financial-services products.

Consensus mechanism: In DLT applications, the process by which validators agree on the state of a distributed ledger.

Crypto-asset: A type of private sector digital asset that is expressed primarily through cryptography and distributed ledger or similar technology.

Crypto-asset trading platform: Any trading platform where crypto-assets can be bought and sold, regardless of the platform's legal status.

Cryptography: The conversion of data into private code using encryption algorithms, typically for transmission over a public network.

Decentralised Autonomous Organization (DAO): In theory, a decentralised application consisting of rules of operation that dictate who can execute a certain behaviour or make an

upgrade. Code helps create an organisational structure intended to function without a centralised management structure.

Decentralised Applications (DApps): DeFi applications offering services such as lending or trading, predominantly between crypto-assets including stablecoins.

Decentralised exchange (DEX): Marketplaces built using distributed ledger or similar technology where transactions can occur directly between crypto-asset traders.

Decentralised Finance (DeFi): A set of alternative financial markets, products and systems that operate using crypto-assets and 'smart contracts' (software) built using distributed ledger or similar technology.

DeFi Liquidity pool: A smart contract that locks in a certain amount of digital assets in order to facilitate its underlying economic activity (e.g. trading or lending) to take place.

DeFi protocol: A specialized system of rules that creates a program designed to perform traditional financial functions.

Digital asset: A digital instrument that is issued or represented through the use of distributed ledger or similar technology. This does not include digital representations of fiat currencies. It is also called a coin or token.

Distributed ledger technology (DLT): A means of saving information through a distributed ledger, i.e. a repeated digital copy of data available at multiple locations.

Flash loan: A form of uncollateralized DeFi lending using smart contracts. If a loan is repaid within the transaction, it goes through and is immutably added to the blockchain ledger. If the loan is not repaid, the entire transaction is rejected.

FinTech: Technology-enabled innovation in financial services that could result in new business models, applications, processes, or products with an associated material effect on the provision of financial services.

Gas fees: Unit that relates to the amount of computational effort required to execute specific operations on the Ethereum network. Gas refers to the fee required to conduct a transaction on Ethereum.

Governance tokens: Tokens issued as an incentive, allowing the user the purported opportunity to become a partial owner and decision-maker in a DeFi protocol.

Miner extractable value (also called "maximal extractable value"): Value that is extractable by miners or others directly as crypto-asset profits. A particular source of MEV is the ability of miners to influence the order in which transactions on a blockchain take place and profit from such a re-ordering at the expense of other users.

Mining: One means to create new crypto-assets, often through a mathematical process by which transactions are verified and added to the distributed ledger.

Native Token: The base token of a blockchain which plays an integral part of the operation of the protocol it is issued on and that is created at its genesis. It is usually used to pay transaction fees.

On-ramp/Off-Ramp: procedure by which fiat money is converted into crypto-assets (on-ramp) or the other way around (off-ramp).

Oracle: A service that enables smart contracts to access, in real-time, relevant external or off-chain data by means of queries typically through crypto-asset exchange application programming interfaces and which provides inputs to smart contracts.

Order book exchange: A type of decentralised exchange (DEX) that uses smart contracts for transaction settlement and order books, which are usually held off-chain by a third party, for registration of buy and sell orders.

Proof of stake: A blockchain-specific consensus mechanism for validating entries into a distributed database and keeping the database secure based on validators' pledging or "staking" a certain amount of crypto-assets in order to have a chance to be chosen for the creation of a new block.

Proof of work: A blockchain-specific consensus mechanism for validating entries into a distributed database and keeping the database secure where potential validators compete with one another to solve cryptographic puzzles in order to be allowed to add transactions to the distributed ledger.

Pseudonymous data: Data that cannot be attributed to a specific individual, without the use of additional information.

Roll-up: A type of off-chain scaling solution that helps overcome capacity restrictions inherent to traditional blockchain networks and which works by executing transactions outside layer 1 and posting data to layer 1 once consensus is reached to benefit from the underlying blockchain's native security.

Rug pull: A crypto-asset market scam in which a development team attracts investors into a project before disappearing with investor funds, leaving investors with a valueless asset.

Side-chain: A type of off-chain scaling solution that helps overcome capacity restrictions inherent to traditional blockchain networks by leveraging a separate and independently run blockchain network that is connected to the original one by a two-way bridge.

Slippage: Difference between the expected price of a trade when the order is launched and the actual price at which the trade is executed.

Smart contract: A crypto-asset term that refers to self-executing applications that can trigger an action if some pre-specified conditions are met.

Stablecoin: A crypto-asset that aims to maintain a stable value relative to a specified asset, or a pool or basket of assets.

Staking: Is the process of locking up crypto-assets for a set period of time to help support the operation of a blockchain in return for a share of transaction fees.

Tokenisation: The process of creating a digital representation (token) of an asset and putting it on a distributed ledger. The information stored in tokenised form can include asset type, ownership details, valuation, legal framework, optionality, and settlement requirements, among other elements that enable significant customisation opportunities for issuer and owner to elect.

Total value locked: Industry-reported measure of the total value of assets deposited in a DeFi protocol.

Wallet: An application or device for storing the private keys providing access to the crypto-asset. Hosted wallets are typically held by a third-party provider, unhosted wallets by the user.

Wallet provider: A firm that offers storage services to investors in crypto-assets. These may be connected online ('hot' storage) or kept offline ('cold' storage).

Abbreviations

AMM	Automated Market Maker
BIS	Bank for International Settlements
CBDC	Central Bank Digital Currency
CeFi	Centralised Finance
CEX	Centralised Crypto-Asset Trading Platform
DAO	Decentralised Autonomous Organisation
DApp	Decentralised Application
DeFi	Decentralised Finance
DEX	Decentralised Crypto-Asset Trading Platform
DLT	Distributed Ledger Technology
FSB	Financial Stability Board
FTX	FTX.com
IMF	International Monetary Fund
IOSCO	International Organisation of Securities Commissions
LP	Liquidity Provider
OECD	Organisation for Economic Co-operation and Development
OT	Ownership Token
SSB	Standard Setting Body
stETH	Staked ETH
TradFi	Traditional Financial System
TVL	Total Value Locked
VC	Venture Capital
YT	Yield Token