Decentralised Finance – A Policy Perspective

Dr Anton N Didenko
Senior Lecturer, Faculty of Law and Justice, UNSW Sydney

ISBN: 978-1-922690-40-1

2022 Edition.
CPA Australia Ltd Level 20, 28 Freshwater Place Southbank VIC 3006 Australia

Author

Dr Anton N Didenko

Anton is a Senior Lecturer at the Faculty of Law and Justice of the University of New South Wales (UNSW Sydney) specialising in banking and finance law, with a focus on FinTech, RegTech and cyber security.

Anton has over 10 years of experience in financial regulation. Prior to joining UNSW Sydney, he worked as head of legal support of international operations in major commercial banks in Russia, as a senior associate at a law firm in London and as a research fellow at the British Institute of International and Comparative Law.

He also specialises in the area of secured transactions law and transnational commercial law: he is the author of a monograph on the documentary history of the Cape Town Convention on International Interests in Mobile Equipment (Hart, 2021) and the general editor of the Cape Town Convention Journal.

Anton holds several law degrees from Russia and the United Kingdom, including a DPhil (Doctor of Philosophy) from the University of Oxford. At the time of writing, Anton's research at UNSW Sydney was funded by the Australian Government through the Australian Research Council (project FL200100007 'The Financial Data Revolution: Seizing the Benefits, Controlling the Risks').

Table of contents

1. Introduction

The concept of 'DeFi' (decentralised finance) has gained prominence in recent years. Enabled by technological developments – in particular blockchain and smart contracts – DeFi mimics the more traditional, centralised finance ('CeFi') 'in an open, decentralised, permissionless way'.[1]

The underlying computing technology enables delivery of financial services and products in new ways that can minimise (or even eliminate) the need for trusted intermediaries or human discretion in financing transactions.

Although the size of the DeFi market remains relatively small, the latter has grown considerably over a short period, experiencing explosive growth between May 2020 and November 2021: during this time, the total value locked ('TVL')[2] increased from less than USD 1 billion to over USD 170 billion.[3]

Nonetheless, it remains to be seen whether a similar growth pattern will continue in the future, considering the more recent steep decline of the TVL throughout 2022 to less than USD 55 billion at the time of writing. Massive rapid swings in the total value of assets in the DeFi ecosystem suggest that decentralised finance remains a volatile and risky environment for investors.

While DeFi applications have the potential to deliver important efficiencies in the financial services sector, they also pose significant risks. This report analyses the main benefits, risks and mechanics of the DeFi ecosystem to identify regulatory gaps and explores a range of policy responses that may be introduced to tackle the many challenges presented by DeFi and its links to centralised finance.

[1] OECD, *Why Decentralised Finance (DeFi) Matters and the Policy Implications* (Report, 19 January 2022) 15.

[2] TVL represents the total value of crypto assets locked in DeFi applications.

[3] According to the data available at **https://defillama.com**. Another resource commonly used as a source of TVL data – **https://www.defipulse.com** – ceased publishing TVL statistics at the time of writing.

2. Boundary problem

As a relatively new concept, DeFi 'is not widely understood by many market participants and policy makers.'[4] The underlying technical complexity may be particularly challenging for unsophisticated investors and is likely to obscure the relevant risks.

However, DeFi's distinguishing characteristics relate not so much to the nature of the products and services classified as 'DeFi', but rather to the new ways of delivery of those products and services.[5]

As some DeFi mechanics can also apply in traditional finance, this creates a '*boundary problem*': it may be challenging to distinguish different forms of DeFi applications from their CeFi counterparts. It is therefore unsurprising that the boundary problem can be, and indeed has been, abused by market participants seeking to promote applications with questionable levels of decentralisation:

'Given the recent exuberance around DeFi, a lot of start-ups and projects *arbitrarily market themselves* as DeFi without necessarily being true DeFi projects, for marketing and other purposes.'[6]

The emergence of self-proclaimed DeFi service providers of dubious quality raises an important question: what is considered 'true' DeFi? Despite a number of attempts to exhaustively define this concept, there is a demonstrated lack of conceptual clarity.

The authors of a comprehensive World Economic Forum report offer a 'functional description to distinguish DeFi from traditional financial services and auxiliary services'[7] that identifies four characteristics that should be present in a DeFi protocol, service or business model: (i) an offering of financial services or products, (ii) trust-minimized operation and settlement, (iii) non-custodial design and (iv) programmable, open and composable architecture.[8]

However, the same authors also acknowledge that these characteristics essentially 'represent the *aspirations* for DeFi' and in practice '[b]usinesses will exhibit each of these characteristics to *varying degrees*, and this may be fluid over projects' lifetimes'.[9]

This approach presents obvious challenges if used in the regulatory context – as regulation needs to apply on the basis of *actual*, existing risks and *current* functionality of the relevant product or service, rather than the features that the activity may (or may not) exhibit at some indeterminate time in the future.

A recent OECD (Organisation for Economic Co-operation and Development) study has similarly focused on the non-custodial nature and composable architecture of DeFi applications, as well as their self-governed and community-driven operation.[10]

However, this approach similarly represents the high-level aspirations for what DeFi is *expected* to be:

'Rather than relying on centralised parties for trust, DeFi markets are community-based networks *seeking ways* to automate the factors that contribute to trust in centralised institutions, and operating in a global, borderless way.'[11]

Zetzsche et al propose a definition based on a literal interpretation of DeFi as a 'decentralised' form of finance: '*the decentralized provision of financial services* through a mix of infrastructure, markets, technology, methods, and applications'[12] – which means 'provision by multiple participants, intermediaries, and end-users spread over multiple jurisdictions, with interactions facilitated, and often in fact enabled in the first place, by technology'.[13]

[4] OECD, *Why Decentralised Finance (DeFi) Matters and the Policy Implications* (Report, 19 January 2022) 16.

[5] Sirio Aramonte, Wenqian Huang and Andreas Schrimpf, 'DeFi risks and the Decentralisation Illusion' (2021) *Bank for International Settlements Quarterly Review* 21, 24.

[6] OECD, *Why Decentralised Finance (DeFi) Matters and the Policy Implications* (Report, 19 January 2022) 19 (emphasis added).

[7] World Economic Forum, *Decentralized Finance (DeFi) Policy-Maker Toolkit* (White Paper, June 2021) 6.

[8] Composability in this context refers to the possibility to combine different elements of DeFi networks, including the underlying digital assets and smart contracts, to form new DeFi applications.

[9] World Economic Forum, *Decentralized Finance (DeFi) Policy-Maker Toolkit* (White Paper, June 2021) 6 (emphasis added).

[10] OECD, *Why Decentralised Finance (DeFi) Matters and the Policy Implications* (Report, 19 January 2022) 18.

This approach helpfully focuses on the key aspect of *decentralisation* (which gave DeFi its name) – yet it remains unclear at which point the delivery of a financial service becomes decentralised. Is it sufficient that a service is provided by two, five or perhaps ten entities? If not, what is the threshold between CeFi and DeFi?

Other commentators have focused on the underlying technology, treating blockchain as an unalienable part of DeFi:

'The key difference between DeFi and CeFi lies in whether the financial service is automated via smart contracts on a blockchain or is provided by centralised intermediaries.

While *DeFi records all the contractual and transaction details on the blockchain* (ie on-chain), CeFi relies on the private records of intermediaries, such as centralised exchanges and other platforms (ie off-chain).'[14]

It is hardly disputed that decentralisation can be enabled by a particular technology – like the blockchain, which appears to be prevalent in today's DeFi architecture. Indeed, authors from different disciplines analyse DeFi mainly through the lens of decentralisation achieved through this database structure.[15]

Nonetheless, it is questionable whether blockchain should be viewed as a *necessary* element of DeFi, at least for two reasons. First, as observed elsewhere,[16] 'decentralised' in DeFi does not necessarily mean 'distributed' – and thus, strictly speaking, decentralisation could be achieved using other, non-DLT[17] databases.

Second, more importantly, a long-term perspective suggests that a more advanced technology may replace blockchain in the future – and from that perspective a technology-neutral approach would enable a more robust and future-proof policy and regulatory decision-making.[18]

Yet another conceptual challenge stems from the fact that decentralisation – even when enabled by blockchain – is rarely absolute and generally exists along the spectrum. Indeed, some degree of centralisation can be found in many seemingly decentralised applications:

'A number of self-proclaimed DeFi projects are hybrid in nature. Such projects consist of a combination of a centralised front-end business set-up with a DeFi architecture at the back end of the application.'[19]

Once this is accepted, 'the tricky question is determining the point of decentralization, on the spectrum of decentralization, achieved by the protocol from the day it was launched into the world'.[20] The degree of control exercised by the developers of a protocol (for example, by controlling the keys granting administrative privileges that authorise the key holder to amend or shut down the protocol) may signal incomplete decentralisation – essentially making DeFi characterisation reliant on human judgment.

[11] Ibid 16 (emphasis added).

[12] Dirk A Zetzsche, Douglas W Arner, Ross P Buckley, 'Decentralised Finance' (2020) 6 *Journal of Financial Regulation* 173-174.

[13] Ibid (emphasis added).

[14] Sirio Aramonte, Wenqian Huang and Andreas Schrimpf, 'DeFi risks and the Decentralisation Illusion' (2021) *Bank for International Settlements Quarterly Review* 21, 23 (emphasis added).

[15] See, e.g., Iwa Salami, 'Challenges and Approaches to Regulating Decentralized Finance' (2021) 115 AJIL Unbound 425; Chris Brummer, 'Disclosure, Dapps and DeFi' (2022) 5.2 Stanford Journal of Blockchain Law and Policy 137, 140; Johannes Rude Jensen, Victor von Wachter and Omri Ross, 'An Introduction to Decentralized Finance (DeFi)' (2021) 26 *Complex Systems Informatics and Modeling Quarterly* 46, 46; Sirio Aramonte, Wenqian Huang and Andreas Schrimpf, 'DeFi risks and the Decentralisation Illusion' (2021) *Bank for International Settlements Quarterly Review* 21, 23.

[16] Dirk A Zetzsche, Douglas W Arner, Ross P Buckley, 'Decentralised Finance' (2020) 6 *Journal of Financial Regulation* 173.

[17] DLT stands for distributed ledger technology.

The multifaceted nature of DeFi can be illustrated by ubiquitous applications of decentralisation at different operational layers:

'The *settlement layer*, supported by blockchains like Ethereum and Solana, handle the settlement of transactions between parties interacting through the DeFi application.

The code and smart contracts comprise the *protocol layer*, which governs how the protocol operates. The *application* layer comprises the consumer facing operations of the protocol, which usually happens via an app or landing page on the world wide web. Some DeFi operations additionally have application layer functionalities enabling assets and products to be used and combined without explicit agreement or permission.' [21]

The resulting complexity raises a number of questions that policymakers seeking to regulate DeFi are likely to grapple with. How decentralised should a service become to be considered 'DeFi'? Is incorporation of decentralised technology on top of a partly centralised operational layer sufficient to treat the entire application as 'DeFi'? If absolute decentralisation is not achievable in practice and some centralisation unavoidably remains, then does 'true DeFi' remain a purely theoretical construct?

Overall, while there appears to be a broad consensus about some of the key features of DeFi (such as disintermediation and composability), upon a closer look there appears to be a clear lack of certainty regarding the boundaries of this concept – namely the features that would enable various stakeholders to clearly distinguish DeFi from other forms of traditional finance.

This uncertainty needs to be acknowledged for the purposes of the remaining sections, as it is likely to impact whether and how policymakers may seek to regulate DeFi applications.

[18] See, e.g., Lyria Bennett Moses, 'How to Think about Law, Regulation and Technology: Problems with "Technology" as a Regulatory Target' (2013) 5(1) *Law, Innovation and Technology*.

[19] OECD, W*hy Decentralised Finance (DeFi) Matters and the Policy Implications* (Report, 19 January 2022) 20.

[20] Iwa Salami, 'Challenges and Approaches to Regulating Decentralized Finance' (2021) 115 *AJIL Unbound* 427.

[21] Chris Brummer, 'Disclosure, Dapps and DeFi' (2022) 5.2 *Stanford Journal of Blockchain Law and Policy* 137, 142 (citations omitted).

3. Main DeFi applications

In the light of the preceding discussion, 'true DeFi' may end up being merely a theoretical concept. Nonetheless, existing attempts to provide early forms of DeFi taxonomy distinguish several groups of DeFi applications:

- stablecoins;
- exchanges;
- lending;
- derivatives;
- insurance;
- asset management; and
- auxiliary services.

Stablecoins are crypto assets designed to preserve their value by maintaining a peg to another asset (or group of assets) and for this reason they are frequently used as collateral to provide liquidity within the DeFi ecosystem. Integration of stabilisation mechanisms aims to boost the ability of crypto assets to function as a store of value – which explains why stablecoins tend to be associated with reduced volatility and used to hedge crypto investments against volatility without relying on the more traditional assets, such as fiat currencies.[22]

Stablecoins implement varying levels of decentralisation that depend largely on the underlying stabilisation mechanism and the asset types used to maintain their value. Many are backed by non-crypto assets, such as fiat currency or short-term liquid securities, and are managed off-chain whereby 'a designated intermediary manages issuance and redemption as well as the reserve assets backing the stablecoins'.[23]

These stablecoins are sometimes referred to as 'CeFi stablecoins' due to their built-in reliance on intermediaries.

CeFi stablecoins link the DeFi ecosystem to traditional finance (including the banking system through bank deposits) and can be a source of interconnectedness and spill-over (and potentially even systemic) effects.

At the other end of the decentralisation spectrum lie 'DeFi stablecoins' that 'record all transacting histories directly on-chain, without the involvement of centralised intermediaries.'[24] Since DeFi stablecoins dispense with third-party intermediation, their stabilisation mechanics differ substantially. Some seek to retain their value by maintaining an overcollateralised pool of crypto assets, allowing stablecoin holders to seize the collateral when the collateralisation ratio reaches a certain threshold. In contrast, others eliminate collateral as the main stabilisation mechanism and instead seek to rely on algorithmic management of supply of stablecoins relative to their demand[25] – a process which challenges their characterisation as 'stablecoins' in the first place (or, conversely, calls for a rethinking of the broadly accepted definition of 'stablecoin').

Decentralised exchanges ('DEX's) enable trading of crypto assets between users while minimising (or eliminating) reliance on intermediaries taking custody of those assets. Like other DeFi applications, DEXs continuously evolve. Their early implementations essentially mimicked the traditional central limit order book on a decentralised platform, but the underlying cost structure limited the attractiveness of trading due to front-running: arbitrageurs could offer a higher fee to incentivise miners to pick a transaction that could exploit the next state change in the order book.[26]

The introduction of automated market-maker ('AMM') protocols sought to address some of the underlying coordination problems by locking crypto assets provided by liquidity providers and relying on mathematical formulas to determine trade prices.[27]

[22] OECD, *Why Decentralised Finance (DeFi) Matters and the Policy Implications* (Report, 19 January 2022) 37.

[23] Sirio Aramonte, Wenqian Huang and Andreas Schrimpf, 'DeFi risks and the Decentralisation Illusion' (2021) *Bank for International Settlements Quarterly Review* 21, 25.

[24] Ibid.

[25] Ibid.

[26] Johannes Rude Jensen, Victor von Wachter and Omri Ross, 'An Introduction to Decentralized Finance (DeFi)' (2021) 26 *Complex Systems Informatics and Modeling Quarterly* 46, 49-50.

[27] Sirio Aramonte, Wenqian Huang and Andreas Schrimpf, 'DeFi risks and the Decentralisation Illusion' (2021) *Bank for International Settlements Quarterly Review* 21, 26.

Lending is one of the largest segments of decentralised finance that attracts investors by offering more attractive interest rates compared to traditional bank deposits or money market funds.[28] DeFi loans share the fundamental characteristics of traditional loans, except the fact that the crypto assets used to fund the loans are provided to 'a peer-to-peer protocol receiving continuous interest payments'.[29]

DeFi lending platforms operate on a pseudonymous basis, which makes it impracticable to borrow purely on credit (since creditworthiness of the borrower cannot be easily verified). To address this problem, the common practice of DeFi platforms is to 'overcollateralise' the loan by posting as collateral different crypto assets with a value exceeding the loan amount.[30] Therefore, DeFi lending effectively reverses the mechanics of traditional unsecured lending: disintermediation implies that lenders have no access to credit reporting data (which is traditionally held by credit reporting agencies), significantly limiting the ability of creditors to make informed decisions – thereby generating what some authors have dubbed 'disintermediation without information'.[31]

Overcollateralisation limits the attractiveness of DeFi lending: 'At present, the need for crypto collateral stands in the way of lending to households and businesses, eg for house purchases or productive investment.'[32]

The need to post collateral is a significant barrier for wider adoption: 'collateral-based lending only serves those with sufficient assets, excluding those with little wealth'.[33]

While some platforms have implemented forms of unsecured lending to eliminate the need for collateral, the relevant solutions often require off-chain relationships and thus reintroduce elements of centralisation and reliance on third-party data.

A notable exception is the novel concept of so-called 'flash loans' – i.e., unsecured loans that must be borrowed and repaid in the same block on the blockchain:

'In other words, a user can borrow a crypto, arbitrage between exchanges, and then repay the loan with a fee, all in one block. The mechanism is based on software development that allows the packaging of all transactions and their submission as one single block. It aims to allow users to make profit by taking advantage of arbitrage opportunities between different crypto-assets and price disparities of such assets between decentralised exchanges.'[34]

Derivative instruments (such as options and forwards) are being introduced to expand the range of financing tools within the DeFi ecosystem – and, just as in traditional finance, they can be used for hedging or speculative purposes. As with the other types of DeFi applications, derivatives can implement varying degrees of disintermediation. While some can be largely managed on-chain, others rely on external data feeds to verify that the event triggering the relevant payment obligations has in fact occurred.[35]

Similar issues are likely to arise in the emerging area of DeFi **insurance** – particularly considering the functional similarities between insurance and certain types of derivatives (such as credit default swaps).

[28] Sirio Aramonte et al, *DeFi Lending: Intermediation Without Information?* (Report, 14 June 2022) 1.

[29] Johannes Rude Jensen, Victor von Wachter and Omri Ross, 'An Introduction to Decentralized Finance (DeFi)' (2021) 26 *Complex Systems Informatics and Modeling Quarterly* 46, 50.

[30] Ibid.

[31] Sirio Aramonte et al, *DeFi Lending: Intermediation Without Information?* (Report, 14 June 2022) 1-2.

[32] Sirio Aramonte, Wenqian Huang and Andreas Schrimpf, 'DeFi risks and the Decentralisation Illusion' (2021) *Bank for International Settlements Quarterly Review* 21, 27.

[33] Sirio Aramonte et al, DeFi Lending: Intermediation Without Information? (Report, 14 June 2022) 2.

[34] OECD, *Why Decentralised Finance (DeFi) Matters and the Policy Implications* (Report, 19 January 2022) 30.

[35] See Fabian Schär, 'Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets' (2021) 103(2) *Federal Reserve Bank of St. Louis Review* 166-167.

Asset management in the DeFi ecosystem mimics the traditional practice of allocating financial assets in accordance with a particular long-term strategy. In line with the DeFi's disintermediation objective, this practice does not involve a custodian:

'Instead, the cryptoassets are locked up in a smart contract. The investors never lose control over their funds, can withdraw or liquidate them, and can observe the smart contracts' token balances at any point in time.'[36]

The main types of asset management applications are yield aggregators and crypto asset indices.

External data feeds (sometimes known as 'oracles') are a form of **auxiliary services** used in the DeFi ecosystem as a source of trusted information – but, by definition, they serve as trusted intermediaries, thus generating external third-party dependencies.[37] While there have been attempts to overcome the limitations of these dependencies, some proposed solutions are likely to push the DeFi ecosystem even further away from its disintermediation objectives – e.g., if dispute resolution systems are introduced to adjudicate attempts to manipulate oracle data feeds.

[36] Ibid 167.

[37] Johannes Rude Jensen, Victor von Wachter and Omri Ross, 'An Introduction to Decentralized Finance (DeFi)' (2021) 26 *Complex Systems Informatics and Modeling Quarterly* 46, 51.

4. Prospective benefits of DeFi services for the real economy

DeFi proponents have linked DeFi to a whole range of positive impacts on the real economy:

'It replicates existing financial services in a more open and transparent way. In particular, DeFi does not rely on intermediaries and centralized institutions. Instead, it is based on open protocols and decentralized applications (DApps). Agreements are enforced by code, transactions are executed in a secure and verifiable way, and legitimate state changes persist on a public blockchain. Thus, this architecture can create an immutable and highly interoperable financial system with unprecedented transparency, equal access rights, and little need for custodians, central clearing houses, or escrow services, as most of these roles can be assumed by "smart contracts".'[38]

Nonetheless, given the relatively early stages of development of most DeFi applications, many of the assumed benefits are yet to be fully realised.

As long as DeFi does not (at least at the current stage of its development) generate fundamentally novel financial products and services, its perceived benefits largely stem from the underlying technology that enables new modes of delivery of financial services. While the number of different types of DeFi applications continues to increase, thus generating new opportunities for end-users, at the time of writing DeFi is mainly associated with the following key potential benefits:

- improved efficiency;
- enhanced resilience;
- greater transparency;
- increased accessibility and inclusivity; and composability.

The expectation of improved efficiency stems from DeFi's 'techno-utopian vision of finance without the dominance of concentrated intermediaries',[39] whereas some commentators treat disintermediation as the main defining characteristic of DeFi:

'The term DeFi is a financial system without the requirement of traditional, centralized intermediaries.'[40] Disintermediation is expected to reduce counterparty risks and, in doing so, promote end-users' trust:

'While much of the traditional financial system is trust based and dependent on centralized institutions, DeFi replaces some of these trust requirements with smart contracts. The contracts can assume the roles of custodians, escrow agents, and CCPs. For example, if two parties want to exchange digital assets in the form of tokens, there is no need for guarantees from a CCP. Instead, the two transactions can be settled atomically, meaning that either both or neither of the transfers will be executed.'[41]

DeFi may reduce some of the costs and frictions associated with the design, distribution, trading and settlement of financial products. Smart contracts used in DeFi asset management applications can streamline the relevant processes by enforcing a pre-defined set of rules and risk profiles and, potentially, even some of the regulatory requirements. As a result, 'on-chain asset management may lead to lower fund setup and auditing costs.'[42] Some of the projected cost savings include compliance costs, perhaps assuming that the relevant DeFi-enabled activities will remain unregulated. Further potential benefits include increased transaction speed due to automation,[43] reduced concentration of financial service providers and lowered insolvency and liquidity risks (as a result of greater availability of credit).[44]

[38] Fabian Schär, 'Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets' (2021) 103(2) *Federal Reserve Bank of St. Louis Review* 153.

[39] Dirk A Zetzsche, Douglas W Arner, Ross P Buckley, 'Decentralised Finance' (2020) *6 Journal of Financial Regulation* 177.

[40] Christoph Wronka, 'Financial Crime in the Decentralized Finance Ecosystem: New Challenges for Compliance' (2021) *Journal of Financial Crime* 1.

[41] Fabian Schär, 'Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets' (2021) 103(2) *Federal Reserve Bank of St. Louis Review* 169.

[42] Ibid 167.

[43] OECD, *Why Decentralised Finance (DeFi) Matters and the Policy Implications* (Report, 19 January 2022) 39.

[44] Ibid 40.

Enhanced resilience could be achieved by reducing or eliminating end-users' dependencies on external factors, including counterparty risks:

'Custody chains typically involved in traditional asset holdings could be shortened and their transparency increased, if DeFi users have self-custody of their assets. This, in turn, could decrease potential risks of liquidity problems arising in custodians in case of operational issues, financial distress or default.'[45]

Decentralisation helps reduce concentration risks in the financial system, which may be caused by limited competition or arise naturally in the wake of certain regulatory reforms (such as the introduction of central counterparties or other trusted intermediaries to facilitate financing transactions):

'The absence of a central point of failure or single attack point in a decentralised setting could enhance the resilience of the system. If appropriately secure, decentralised systems may be more resilient to cyber risk than highly centralised systems also in terms of the integrity of their record-keeping and service availability.'[46]

The recent successful attempts by various governments to weaponise the financial system, using it as a tool to suppress and coerce non-allied countries (e.g., in the form of unilateral freezing of another sovereign's reserves)[47] can make DeFi particularly attractive as a tool for maintaining resilience from external political intervention. In this context, DeFi may enable a financial system to persevere amidst significant geopolitical risks of the ongoing deglobalisation and at least partly insulate finance from arbitrary intervention by the key financial centres, since its 'objective is to develop systems which use technology to eliminate borders, jurisdiction, and the necessity of centralized control including governments'.[48]

Many DeFi applications offer greater transparency, which can be generated by the publicly observable data on the blockchains, as well as by the open (non-proprietary) coding implemented in smart contracts used to facilitate financing transactions. The resulting public availability of transaction data may simplify monitoring and macroeconomic analysis:

'In the case of a crisis, the availability of historical (and current) data is a vast improvement over traditional financial systems, where much of the information is scattered across a large number of proprietary databases or not available at all. As such, transparency of DeFi applications may allow for the mitigation of undesirable events before they arise and help provide much faster understanding of their origin and potential consequences when they emerge.'[49]

Wider availability of transaction data is particularly valuable considering the evolving nature of DeFi applications, some of which may carry novel risks that may be hard to quantify – not unlike the obscure levels of exposure to derivatives that facilitated the Global Financial Crisis of 2008.

DeFi's increased accessibility can promote financial inclusion by granting access to financial services to the unbanked and underserved individuals and SMEs:

'By default, DeFi protocols can be used by anyone. As such, DeFi may potentially create a genuinely open and accessible financial system. In particular, the infrastructure requirements are relatively low and the risk of discrimination is almost inexistent due to the lack of identities.'[50]

Pseudonymity of DeFi applications facilitates diversity in the financial system through inclusion 'without having to fulfill onerous requirements, as is currently the case in traditional finance.'[51]

[45] Ibid.

[46] Ibid.

[47] Douglas W Arner et al, 'Ukraine, Sanctions and Central Bank Digital Currencies: The Weaponization of Digital Finance and the End of Global Monetary Hegemony?' (2022) **<https://dx.doi.org/10.2139/ssrn.4133531>**.

[48] Dirk A Zetzsche, Douglas W Arner, Ross P Buckley, 'Decentralised Finance' (2020) *6 Journal of Financial Regulation* 184.

[49] Fabian Schär, 'Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets' (2021) 103(2) *Federal Reserve Bank of St. Louis Review* 169.

[50] Ibid (emphasis added).

[51] Iwa Salami, 'Challenges and Approaches to Regulating Decentralized Finance' (2021) 115 *AJIL Unbound* 425.

Structural flexibility (sometimes referred to as 'composability') of DeFi applications is facilitated by the functional interoperability of different layers of the DeFi ecosystem:

'The layers build on each other and create an open, highly composable and interoperable infrastructure that allows everyone to build on, propose amendments, or use other parts of the stack.'[52]

Composability of DeFi is sometimes compared with Lego pieces (whereby financial primitives are viewed as individual construction blocks):

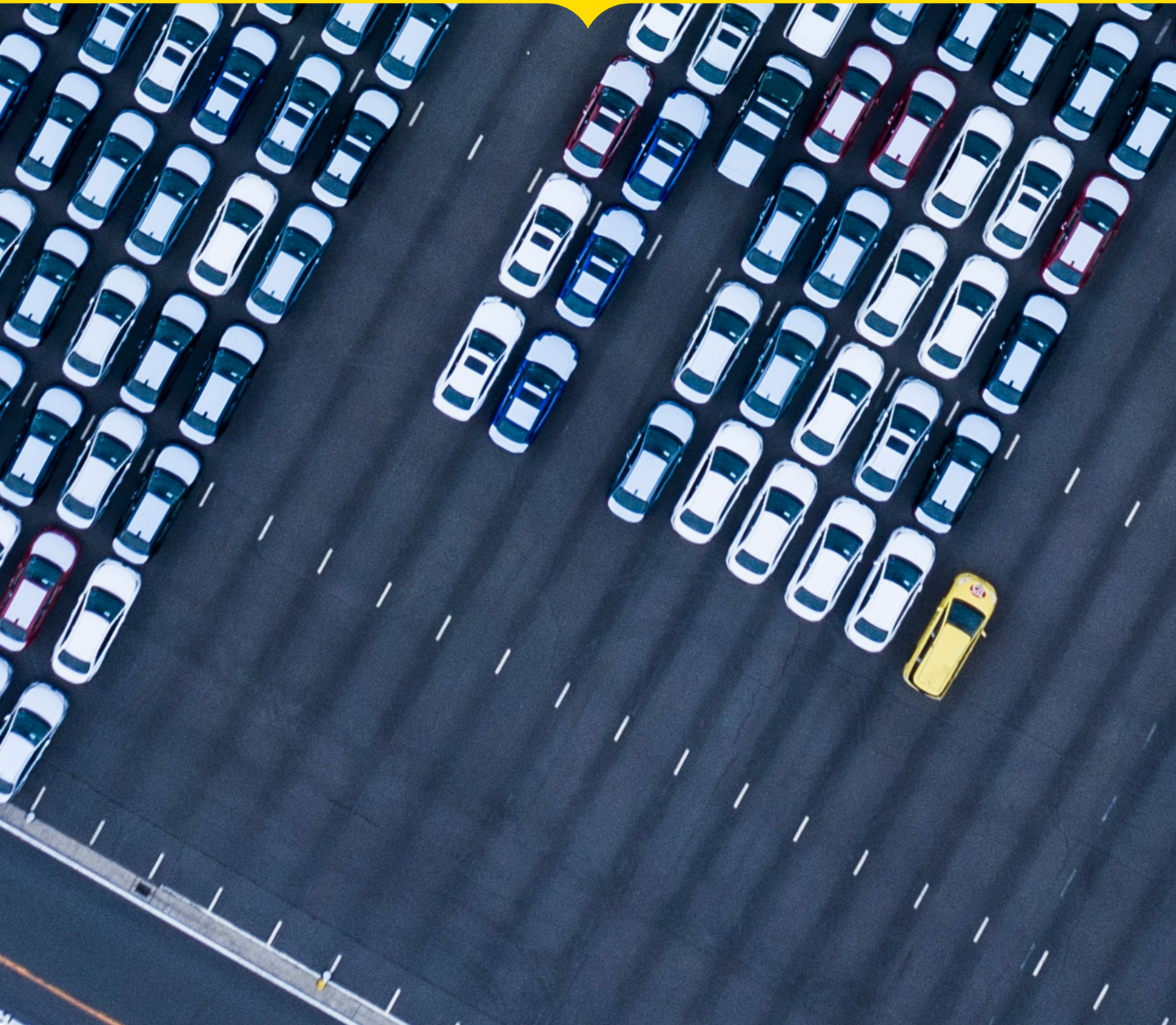
'The shared settlement layer allows these protocols and applications to interconnect. On-chain fund protocols can make use of decentralized exchange protocols or achieve leveraged positions through lending protocols. Any two or more pieces can be integrated, forked, or rehashed to create something entirely new.'[53]

Composability, when coupled with the transparency of publicly observable smart contract code and the borderless nature of blockchains, enables innovation, including the development of new ways to access financial products and services. This, in turn, could help break the traditional silos within the financial sector. In addition, DeFi applications can be integrated with the established CeFi ecosystem – thus providing end-users with a greater variety of financing options, while also increasing the mutual dependencies between DeFi and traditional finance.

[52] OECD, *Why Decentralised Finance (DeFi) Matters and the Policy Implications* (Report, 19 January 2022) 17.

[53] Fabian Schär, 'Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets' (2021) 103(2) *Federal Reserve Bank of St. Louis Review* 169 (emphasis added).

5. Risks of DeFi for the traditional financial system



DeFi applications present a wide array of risks for traditional finance – however their exact magnitude and relevance is difficult to evaluate at the time of writing, considering their emergent nature and changing characteristics. On the one hand, these risks could create major regulatory challenges that affect both retail and institutional investors, some of which may well have systemic implications in the long run. On the other hand, the DeFi infrastructure has not yet achieved the scale required to present a meaningful challenge to traditional finance:

'In principle, DeFi has the potential to complement traditional financial activities. At present, however, it has few real-economy uses and, for the most part, supports speculation and arbitrage across multiple cryptoassets. Given this self-contained nature, the potential for DeFi-driven disruptions in the broader financial system and the real economy seems limited for now.'[54]

At the time of writing, a comprehensive analysis of the risks posed by DeFi remains challenging due to the rapidly changing design of DeFi applications and the quick pace of innovation in the DeFi space. While some of the new forms of decentralised finance could be designed to reduce (or eliminate) the existing risks, others could propagate them further – or even introduce yet undocumented and obscure risks.

DeFi is enabled by the proliferation of crypto assets that are actively making forays into the 'traditional' financial system – as more and more incumbents (including banks, payment service providers and fund managers) are engaging with digital currencies like Bitcoin and Ether.[55] Although crypto assets have been around for years, attempts to strike a regulatory balance between promoting innovation and protecting end-users (especially consumers) have proven to be particularly challenging even for the most developed economies.

Many of the risks associated with crypto asses remain unresolved even in the CeFi setting – and will only proliferate as part of decentralised finance. Indeed, while DeFi represents a substantial shift in the way financial services are provided, the recent surge of crypto-asset activity signifies a highly speculative market:

'The exponential growth of the DeFi market has a lot of the characteristics of the 2017-18 crypto-asset bull market associated with the Initial Coin Offering (ICO) boom in terms of its drivers (OECD, 2019). Similarities exist also in terms of associated complexities and risks for participants.'[56]

There have been limited attempts to develop a taxonomy of DeFi risks. Carter and Jeng classify DeFi risks into five groups: '(i) interconnections with the traditional financial system, (ii) operational risks stemming from underlying blockchains, (iii) smart contract-based vulnerabilities, (iv) other governance and regulatory risks, and (v) scalability challenges.'[57] The World Economic Forum white paper provides another classification of risks breaking them down into five (financial, technical, operational, compliance and emergent) categories.[58]

This section presents an alternative risk classification that distinguishes the following groups of vulnerabilities:

- technology and operational risks;
- financial stability risks;
- legal risks; and
- market integrity and governance risks.

[54] Sirio Aramonte, Wenqian Huang and Andreas Schrimpf, 'DeFi risks and the Decentralisation Illusion' (2021) *Bank for International Settlements Quarterly Review* 21, 21.

[55] Nic Carter and Linda Jeng, 'DeFi Protocol Risks: The Paradox of DeFi' (2021) 2 **<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3866699>**.

[56] OECD, *Why Decentralised Finance (DeFi) Matters and the Policy Implications* (Report, 19 January 2022) 22.

[57] Nic Carter and Linda Jeng, 'DeFi Protocol Risks: The Paradox of DeFi' (2021) 6ff **<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3866699>**.

[58] World Economic Forum, *Decentralized Finance (DeFi) Policy-Maker Toolkit* (White Paper, June 2021) 13.

A. Technology and operational risks

Analysis of operational risks of DeFi, which largely stem from the technical limitations of the underlying technology, is complicated by 'uncertainties in future developments and the novelty of the technology'.[59]

(i) Protocol limitations

While blockchain designs continuously evolve – as demonstrated by the recent transition of Ethereum to a proof-of-stake architecture replacing the previous proof-of-work consensus algorithm – distributed platforms used in most DeFi applications pose significant risks.

DeFi applications (particularly at the early stages of development) may suffer from insufficient scalability – i.e., inability to achieve, or loss of, a critical mass of nodes to efficiently execute the consensus algorithm. Insufficient scale facilitates abuse of the blockchain mechanics through node concentration, which could enable so-called 51% attacks and is at odds with the fundamental characteristics of decentralised finance.[60]

To compensate miners for their use of computing resources to add new blocks to the blockchain, many DeFi applications enable transacting parties to pay additional fees 'in the effort of incentivizing miners to select their transaction for inclusion in the next block'.[61] In periods of network congestion (i.e., periods when the number of transactions exceeds the network's capacity), this may lead to substantial increases of transaction fees, which are nearly always paid by the end-users.[62]

The problem can be exacerbated even further in DeFi platforms utilising algorithms to adjust the relevant fees automatically:

> 'If a period of network congestion coincides with a period of volatility, the application design may suddenly impose excessive fees or penalties on otherwise standard actions such as withdrawing or adding funds to a lending market'.[63]

It is worth stressing that the network congestion risks of DeFi represent a vulnerability that has been largely eliminated in traditional payment systems. Recording transactions onto the blockchain effectively acts as the final – settlement – stage of a bank-to-bank payment process, whereby the accounts of the payer's and payee's financial institutions are debited and credited as a conclusive record of a completed money transfer. Real-time gross settlement ('RTGS') platforms ensure that payments are processed without delay – and the introduction of fast payment systems (such as Australia's New Payments Platform ('NPP')) operating in a 24/7 mode makes payments seamless.[64] Legal rules on settlement finality, including the so-called 'zero hour rule', further insulate payments made through traditional payment systems from roll-backs caused by external factors, such as initiation of bankruptcy proceedings.

This comparison makes DeFi applications seem like a step back compared to payment mechanisms commonly used in traditional finance. The former become even less attractive, considering that the act of recording a transaction on a blockchain cannot guarantee its finality – since malicious actors may launch a 51% attack and overtake the 'true' chain of transactions, effectively nullifying the block containing the earlier payment.

[59] Johannes Rude Jensen, Victor von Wachter and Omri Ross, 'An Introduction to Decentralized Finance (DeFi)' (2021) 26 *Complex Systems Informatics and Modeling Quarterly* 46, 52.

[60] OECD, *Why Decentralised Finance (DeFi) Matters and the Policy Implications* (Report, 19 January 2022) 48.

[61] Johannes Rude Jensen, Victor von Wachter and Omri Ross, 'An Introduction to Decentralized Finance (DeFi)' (2021) 26 *Complex Systems Informatics and Modeling Quarterly* 46, 52.

[62] Ibid.

[63] Ibid. See also Daniel Perez et al, 'Liquidations: DeFi on a Knife-edge' (2021) **<https://arxiv.org/abs/2009.13235>**.

[64] In Australia, settlement of NPP payments is processed on an RTGS basis, although the same may not always be true for other fast payment systems.

(ii) Basic infrastructure

The increasing number of DeFi applications may create the false impression that the DeFi ecosystem is, as a whole, not concentrated and decentralised, whereas '[a]t the current stage of development of the DeFi market, the activity is concentrated in a very small number of protocols'.[65]

Another source of concentration in DeFi stems from the very limited number of providers of basic infrastructure:

'Currently, most of the activity in DeFi sits on the Ethereum blockchain, given that its code language is one of the earliest ones in the market to support smart contracts, as well as the fact that ETH is the only asset that can be used to pay transaction fees on Ethereum.'[66]

Incumbent financial institutions have also adopted Ether in their own applications – further entrenching Ethereum as the foundational element of the DeFi infrastructure.

Reliance on a single major provider of basic infrastructure makes end-users vulnerable to platform downtimes in the absence of redundancy platforms. Despite its perceived resilience, Bitcoin – arguably the most well-known and secure decentralised crypto asset – experienced several rollbacks throughout its history, resulting in the removal of roughly 15 hours' worth of transactions from the blockchain.[67] Integration of additional intermediaries on top of the basic infrastructure generates even more dependencies:

'Ethereum is arguably more fragile to outages since most users do not run nodes but instead rely on service providers like Infura to query and index the blockchain and broadcast transactions. When these service providers experience downtime, as was the case with Infura during an unplanned chain split in 2020, intermediated transactions ground to a halt.'[68]

(iii) Inflexibility of smart contracts

Despite the many perceived benefits of smart contracts (such as their deterministic mode of execution), reliance on self-executing code on a blockchain presents substantial risks for users of DeFi services. In particular, as a result of coding errors or malicious attacks, end-users' crypto assets could be irreversibly destroyed or permanently immobilised. While history knows a number of cases when blockchains were hard forked to roll-back to the state that existed prior to a successful cyber-attack, some DeFi platforms are reported to have no such functionality:

'In the case of certain irrevocable smart contracts - like Uniswap, developers have no ability to take down a smart contract once it is deployed. Upgrading such a smart contract would be a matter of deploying an alternative and persuading users to use it. As long as the underlying Ethereum blockchain remains intact, certain classes of smart contracts will remain operable regardless of administrator or user behavior.'[69]

In other words, the deterministic nature of smart contracts means that DeFi end-users may lose their investment without recourse:

'The irreversible or, 'immutable' nature of transactions in a blockchain network has led to significant loss of capital on multiple occasions, most frequently as a result of coding errors, sometimes relating to even the most sophisticated aspects [of] virtual machine and programming language semantics'.[70]

These risks are exacerbated by other design features of DeFi applications, some of which routinely request from end-users 'permissions to transfer an infinite number of tokens on behalf of the user' to simplify future transactions.[71] Inability to recover funds in those circumstances may result in a total (and uncontrolled) loss of one's investment.

[65] OECD, *Why Decentralised Finance (DeFi) Matters and the Policy Implications* (Report, 19 January 2022) 47.

[66] Ibid 50.

[67] Nic Carter and Linda Jeng, 'DeFi Protocol Risks: The Paradox of DeFi' (2021) 14 **<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3866699>**.

[68] Ibid.

[69] Ibid 22.

[70] Johannes Rude Jensen, Victor von Wachter and Omri Ross, 'An Introduction to Decentralized Finance (DeFi)' (2021) 26 *Complex Systems Informatics and Modeling Quarterly* 46, 52.

[71] Fabian Schär, 'Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets' (2021) 103(2) *Federal Reserve Bank of St. Louis Review* 170.

Inflexibility of smart contracts is yet another example of how DeFi may struggle to deal with matters that pose little challenge for traditional finance, where technical and financial support can be provided to affected end-users through a variety of tools, from emergency liquidity assistance to deposit protection schemes.[72]

Conceptually, however, the rigidity of smart contract code and the difficulties with obtaining recourse make it rather poorly suited for non-speculative use cases. Inability to reverse clearly fraudulent transactions is likely to make the other perceived benefits of DeFi obsolete for most end-users, since as long as the platform prioritises the integrity of the code over the elementary notions of fairness and common sense, it effectively protects criminals and opportunists at the expense of honest participants.

(iv) Technical complexity

Substantial technical complexity of DeFi applications and their underlying infrastructure consisting of multiple layers creates major obstacles for informed decision-making, particularly by unsophisticated investors, such as individual consumers. The above discussion about the rigidity of smart contract code that may lead to a permanent loss of funds demands that prospective DeFi investors have the ability to ascertain the risks of their investment:

'Users have to be aware that the protocol is only as secure as the smart contracts underlying it. Unfortunately, the average user will not be able to read the contract code, let alone evaluate its security.'[73]

It is worth stressing that the complexity of smart contract code for non-expert end-users differs substantially from the complexity of analysing the provisions of legal contracts (some of which may also be complex for non-specialists). Legal contracts are written in natural language – and therefore are likely to raise only occasional difficulties with certain complex provisions or vaguely defined terms, which may lead to misunderstanding a particular term or clause (or failure to appreciate the relevance of a particular disclaimer).

In contrast, smart contracts are fragments of programming code, which would be impossible to understand in its entirety without special training.

In this context, the often-cited transparency of smart contract code implemented in DeFi applications offers little benefit to the vast majority of (non-expert) investors, who do not possess the skills to read and independently verify the integrity of the code in order to make a genuinely informed investment decision. If public availability of the smart contract code is the main source of trust in its quality, retail investors would have to make their investment decisions based on other factors, such as third-party endorsements or disclosures from the platform developers.

Yet again, if we continue our analogy with traditional finance, the latter establishes numerous safeguards preventing particularly complex financial products from reaching non-sophisticated investors. In other words, regulation dispenses with the idea that all end-users always act rationally and make sensible decisions if provided with sufficient information to make an informed decision. The recent introduction of the design and distribution obligations for financial products in Part 7.8A of the Corporations Act 2001 (Cth) is particularly noteworthy in this context. It requires developers to consider whether a particular financial product is objectively consistent with the likely objectives, financial situation and needs of retail clients comprising the target market for that product.

(v) Cyber security

Cyber-attacks on the DeFi infrastructure are common and financially attractive. The losses to investors from only a handful of security exploits in DeFi protocols reported in 2020 and 2021 exceeded USD 200 million.[74] Cyber-attacks in the DeFi ecosystem come in a variety of forms, including reentrancy attacks, integer manipulation or single- and multi-transaction sandwich attacks.[75]

[72] Dirk A Zetzsche, Douglas W Arner, Ross P Buckley, 'Decentralised Finance' (2020) 6 *Journal of Financial Regulation* 191.

[73] Fabian Schär, 'Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets' (2021) 103(2) *Federal Reserve Bank of St. Louis Review* 170.

A large number of attacks have been enabled by simple programming errors and propagated by the deterministic nature of smart contract execution:

'While logical bugs are by no means unique to smart contracts, but common to any type of software, the consequences for smart contracts, where immutability underpins the system, can be much more severe than for many other genres of software and result in unrecoverable financial losses.'[76]

One of the most common vulnerabilities of this kind is known as 'inflation bugs' – errors enabling the inflation of supply of crypto assets on the blockchain ahead of the scheduled development plans:

'Since DeFi protocols are highly automated, run continuously, and operate with minimal (or in some cases, no) human oversight, inflation bugs on the underlying native protocols can significantly destabilize DeFi applications. Inflation bugs are among the most severe threats that blockchains face, and remediation often requires halting or rolling back the blockchain, which would impair the assurances of any smart contracts relying on the underlying blockchain.' [77]

Cyber security of external data sets is another major vulnerability in the DeFi ecosystem, which routinely relies on so-called 'oracles' as a source of outside trusted data (such as market prices of various assets) to a smart contract. Oracles play an important role in facilitating DeFi lending (by enabling timely liquidations and deleveraging), derivatives (through margin calls) and asset management.[78] Consequently, manipulation of oracle data can have catastrophic consequences, allowing attackers to influence the reference prices of collateral, enabling riskless arbitrage opportunities and triggering liquidations.[79] As a result, oracles represent a critical vulnerability in the DeFi ecosystem that stems from incomplete disintermediation.

Overall, cyber security presents a unique challenge for the DeFi ecosystem. On the one hand, open access and excessive transparency of smart contracts offer virtually no direct benefit to the vast majority of consumers, who lack the necessary expertise to analyse the programming code. On the other hand, transparency provides excellent opportunities for coding experts. Some of them may seek to improve the code – especially if they have a stake in the underlying crypto asset or have been engaged by the platform developer for audit purposes. Other experts, however, will seek to exploit vulnerabilities and profit from coding errors.

Ironically, the decentralised nature of DeFi applications can make them particularly vulnerable to cyber threats. In a truly decentralised system, operational decisions are made by a large number of independent stakeholders by consensus or majority vote, either of which generates delays in decision-making. Cyber criminals, on the other hand, are not bound by such limitations: upon identifying a vulnerability, they can initiate an attack immediately. Similarly, a platform that engages cyber security experts to identify vulnerabilities on an ongoing basis is likely to be a step behind cyber attackers, as the decision to implement a patch would need to be approved by the decentralised community. In other words, fully decentralised governance appears to be at its weakest when the need to act is urgent – which is exactly when cyber breaches are identified.

[74] Sam Werner et al, 'SoK: Decentralized Finance (DeFi)' 8 **<https://arxiv.org/pdf/2101.08778.pdf>**.

[75] Ibid 6ff.

[76] Ibid 7.

[77] Nic Carter and Linda Jeng, 'DeFi Protocol Risks: The Paradox of DeFi' (2021) 21 **<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3866699>**.

[78] Ibid 23.

[79] Ibid.

This is particularly challenging in the context of ransomware attacks, which can generate disagreement as to the best course of action: to pay ransom or reject the attackers' claims (bearing in mind that the decision would be particularly problematic if a majority vote can bind the minority).

Clearly, DeFi platforms could be designed in a way that enables developers to act quickly and implement patches and deal with vulnerabilities on a day-to-day basis. However, such a platform is, by definition, recentralised – as long as it can be unilaterally modified by a trusted third-party intermediary.

Yet another potentially problematic aspect of DeFi in the context of cyber risk management relates to the deterministic nature of smart contract execution. Modern approaches to the management of cyber risks embrace the 'assume breach' approach, which acknowledges that impenetrable cyber fortresses do not exist and that every system will be breached at some point. In other words, a cyber breach is only a matter of time. As long as DeFi smart contracts continue to execute the same pre-set lines of code and the blockchains remain truly immutable, the 'assume breach' logic presents an existential challenge to the DeFi ecosystem, since it effectively implies that each DeFi is not only unsafe, but also unrecoverable in the event of an unavoidable cyber breach. Admittedly, 'assume breach' is a long-term oriented regulatory logic – which implies that it may take years or even decades for some applications to be breached. But even then, the resulting status quo is hardly acceptable (as it is more likely than not to promote the opportunistic 'get in, get out quickly' mentality among investors – instead of positioning DeFi as a long-term counterpart to traditional finance).

B. Financial stability risks

Decentralised finance has the potential to become a source of substantial financial stability risks for the traditional financial system in the future, even if, as argued by some experts, the current size of the DeFi market 'is not large enough to be considered a risk to the stability of financial markets at its current level'.[80]

There are multiple sources of financial stability risks in DeFi. These are discussed in sub-sections (i) to (iii) below.

(i) Excess volatility and costs

The DeFi ecosystem is highly susceptible to fluctuations in the valuation of crypto assets used as collateral. The volatility of such crypto assets remains so significant that it 'can easily reduce (and possibly eliminate) collateral value and turn over-collateralised positions into under-collateralised ones in a matter of seconds'.[81] The resulting liquidations of collateral can be near instantaneous and are likely to put further downward pressure on the valuation of relevant crypto assets, with a risk of creating downward spirals. Furthermore, collateral volatility is likely to make transfers across DeFi platforms more cumbersome, which may negatively impact the overall 'composability' of the DeFi ecosystem that relies on the ease of connecting different applications and operational layers.[82]

Even the safest forms of collateral used in the DeFi ecosystem – stablecoins – are not insulated from volatility, although the source of that volatility largely depends on the types of underlying assets.

[80] OECD, *Why Decentralised Finance (DeFi) Matters and the Policy Implications* (Report, 19 January 2022) 39.

[81] Ibid 47.

[82] Sirio Aramonte, Wenqian Huang and Andreas Schrimpf, 'DeFi risks and the Decentralisation Illusion' (2021) *Bank for International Settlements Quarterly Review* 21, 31.

Stablecoins backed by other crypto assets (like Bitcoin or Ether) are vulnerable to market risks, which can quickly depreciate the value of those assets, whereas stablecoins backed by non-cash reserves (such as short-term securities) are subject to liquidity mismatches, to the extent that fire sale of those reserves may be insufficient to maintain the stablecoin's declared peg to the stabilisation asset.[83] In this context, the example of Tether (the world's most prominent stablecoin) is illustrative: the investigation by the Office of the Attorney General of the State of New York has revealed that the stablecoin's issuers experienced severe liquidity issues that starkly contrasted the very positive public-facing updates and assurances.[84]

The high volatility of stablecoins backed by traditional assets can set off investor runs in the race to be the first to recover the collateral. In contrast, the traditional financial system largely mitigates similar issues (i.e., bank runs) through deposit insurance arrangements that guarantee the recovery of bank account balances (typically up to a certain amount), thus effectively removing the first mover advantage.

One of the main perceived benefits of decentralised finance – increased efficiency – includes reduced costs of transacting within the DeFi ecosystem. However, in recent years, the transaction fees on the leading Bitcoin and Ethereum blockchains have grown considerably and can be seen as yet another source of volatility:

'Due to relatively inelastic blockspace combined with volatile demand for blockchain resources, fees are highly volatile. For instance, on February 23, 2021, mean per-transaction Ethereum fees reached $38 while mean Bitcoin fees reached the equivalent of $25.146 For comparison, in 2019, Bitcoin and Ethereum per-transaction fees averaged the equivalent of only $1.24 and $0.13, respectively.'[85]

This additional source of volatility in the DeFi ecosystem is a direct result of incomplete disintermediation. Despite the technical innovations meant to reduce the reliance on intermediaries in the financial system, the operation and growth of the blockchain (used to finalise and settle the relevant transactions) depends on the actions of validators that combine transaction data into individual blocks. The gas fees are meant to compensate these intermediaries and, as is not uncommon in traditional finance, these costs of intermediation are generally offloaded onto DeFi investors. Increasing fees make the DeFi ecosystem more expensive to use – potentially pricing out smaller (especially retail) investors (who refuse to trade at such fee levels) and effectively locking their balances:

'As fees rise on the base layer, retail users can no longer economically engage in DeFi operating on the base layer, affecting liquidity in decentralized exchanges.'[86]

Coupled with the high technical complexity (discussed above), increasing costs and volatility may further entrench DeFi applications as financing instruments intended for a small group of expert investors, rather than the average consumer.

[83] Ibid.

[84] See *In the Matter of Investigation by LETITIA JAMES, Attorney General of the State of New York, of iFINEX INC., BFXNA INC., BFXWW INC., TETHER HOLDINGS LIMITED, TETHER OPERATIONS LIMITED, TETHER LIMITED, TETHER INTERNATIONAL LIMITED*, available at **<https://ag.ny.gov/sites/default/files/2021.02.17_-_settlement_agreement_-_execution_version.b-t_signed-c2_oag_signed.pdf>**.

[85] Nic Carter and Linda Jeng, 'DeFi Protocol Risks: The Paradox of DeFi' (2021) 33 **<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3866699>** (citations omitted).

[86] Ibid 34 (citations omitted).

(ii) Systemic risks

Interoperability and composability are the key perceived benefits of the DeFi ecosystem. Seamless integration of multiple layers is necessary for the operation of different financial products. As an example, withdrawal from a DeFi fund leads to a sale of the relevant assets on a decentralised exchange:

'When the investor decides to close out the investment, the fund tokens get burned, the underlying assets are sold on a decentralized exchange, and the investor is compensated with the ETH-equivalent of their share of the basket.'[87]

This close integration between different elements of DeFi infrastructure can cause a domino effect in the event of a seemingly localised disruption:

'An increasing degree of contagion between applications may introduce systemic risks, as a sudden failure or exploit in one application could ripple throughout the network, affecting stakeholders across the entire ecosystem of applications.'[88]

Systemic effects are observable during periods of high volatility, such as 12 March 2020 (known as 'Black Thursday') when a drop in the valuation of collateral led to the liquidation of borrower accounts within MakerDAO.[89]

Interestingly, the composability of the DeFi ecosystem and the resulting systemic risks have a lot in common with the systemic implications caused by the proliferation of derivatives in traditional finance. Just as derivatives can be used to create multiple new financial products linked to a single underlying financial asset, so too can DeFi products involve the creation of new tokens linked to other crypto assets ad infinitum.

Examples include so-called 'liquidity shares' received by liquidity providers on a decentralised exchange that can be redeemed for the corresponding share of the overall liquidity pool. These fungible shares can be traded on a secondary DeFi market, which may similarly involve issuing new (second generation) liquidity shares and so on.

However, since the value of such liquidity shares is ultimately based on the value of the underlying base asset, excess volatility in the price of that asset 'may trigger a sequence of cascading liquidations, as the market struggles to price in any rapid changes in the price of the source asset'.[90] In this setting, the number of times the original asset gets 'repackaged' propagates the risk of the domino collapse.

So-called wrapper tokens can obscure the true levels of exposure of investors in the DeFi ecosystem – similar to how the opacity in the over-the-counter derivatives markets prevented financial regulators from adequately assessing the exposure of traditional financial institutions in the run-up to the Global Financial Crisis of 2008, eventually leading to a range of derivatives reforms facilitated by the G20.

Another source of vulnerability of the DeFi ecosystem to systemic risks is the absence of a stable lender of last resort that could help absorb short-term shocks by providing emergency liquidity. This was aptly demonstrated by the collapse of an algorithmic stablecoin TerraUSD, which used another floating-rate crypto asset, Luna, to maintain its peg to the US dollar. Attracted by a lucrative opportunity to obtain a high (20%) return on the lending protocol Anchor, investors actively purchased Luna tokens in order to acquire TerraUSD tokens.

[87] Fabian Schär, 'Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets' (2021) 103(2) *Federal Reserve Bank of St. Louis Review* 168.

[88] Johannes Rude Jensen, Victor von Wachter and Omri Ross, 'An Introduction to Decentralized Finance (DeFi)' (2021) 26 *Complex Systems Informatics and Modeling Quarterly* 46, 53.

[89] Iwa Salami, 'Challenges and Approaches to Regulating Decentralized Finance' (2021) 115 *AJIL Unbound* 426.

[90] Johannes Rude Jensen, Victor von Wachter and Omri Ross, 'An Introduction to Decentralized Finance (DeFi)' (2021) 26 *Complex Systems Informatics and Modeling Quarterly* 46, 53. See also Daniel Perez et al, 'Liquidations: DeFi on a Knife-edge' (2021) **<https://arxiv.org/abs/2009.13235>**.

When the value of the latter fell sharply, the reverse process began: investors switched to withdrawing TerraUSD balances from Anchor to mint Luna hoping to sell it and make a profit. However, amidst substantial volatility there was insufficient demand for Luna – which led to the rapid depreciation of its value. As both TerraUSD and Luna were used as collateral for DeFi loans, their collapse triggered a spike in liquidations, effectively resulting in a 'platform run'.[91] In the absence of a lender of last resort, no immediate liquidity was available within the DeFi ecosystem, leaving individual investors to fend for themselves in a run to be the first to exit the collapsing crypto asset.

Interconnectedness, which is widely considered to be a pre-requisite for DeFi's growth, also increases systemic risks. This conclusion is important from a regulatory perspective, since the expansion of the DeFi ecosystem is likely to be both horizontal (by expanding the range of financial products and services) and vertical (by increasing the systemic dependencies between different layers in the DeFi ecosystem). This important dynamic demonstrates yet another potential deficiency of DeFi, when compared to traditional finance. The latter, when faced with systemic risks, seeks to mitigate and insulate them by imposing prudential regulation on the critical intermediaries (such as banks and providers of critical infrastructure). In contrast, the overall thrust of DeFi towards decentralisation seeks to reduce the number of intermediaries. Nonetheless, at least at the time of writing, this form of decentralisation often leads to the replacement of one type of intermediaries with another (as demonstrated in section 5(D) below), which leaves systemic risks intact but obscures liability when things go wrong.

Despite its unique features, the DeFi ecosystem does not exist in a vacuum and has established connections to traditional finance that can become a conduit for the transmission of systemic shocks. These connections may come in different forms but at present appear most noticeable in the pricing of crypto assets:

> 'At the current juncture, DeFi's most important interconnection with the traditional financial system is through the valuation of crypto-assets that are either used by traditional financial sector companies (e.g. in payments) or are underlying financial products offered by conventional players (e.g. crypto-funds, bitcoin futures).'[92]

While at present spill-overs between DeFi and CeFi may appear relatively insignificant,[93] they are likely to increase in the future, as banks and other traditional intermediaries increase their exposure to crypto assets or serve as keepers of non-crypto asset collateral (such as fiat currency) supporting the value of stablecoins. These interlinkages operate both ways. On the one hand, stablecoin issuers may engage in opportunistic issuance of liabilities backed by illiquid assets in the absence of a corresponding regulatory framework – which, in the event of financial distress, may result in the stablecoin losing its peg to the relevant assets, triggering mass liquidation of collateral on DeFi platforms. On the other hand, in the event of a platform run, stablecoin issuers may be forced to liquidate the reserves in the traditional financial system, putting downward pressure on their prices. If those reserves include liquid securities, a rapid firesale may cause a downturn in the stock market.[94]

[91] Sirio Aramonte et al, *DeFi Lending: Intermediation Without Information?* (Report, 14 June 2022) 4.

[92] OECD, *Why Decentralised Finance (DeFi) Matters and the Policy Implications* (Report, 19 January 2022) 53.

[93] Sirio Aramonte, Wenqian Huang and Andreas Schrimpf, 'DeFi risks and the Decentralisation Illusion' (2021) *Bank for International Settlements Quarterly Review* 21, 31.

[94] Iwa Salami, 'Challenges and Approaches to Regulating Decentralized Finance' (2021) 115 *AJIL Unbound* 426.

(iii) Excessive leverage

Excessive leverage is a characteristic feature of the current DeFi ecosystem and an important source of financial stability risks. DeFi's composability can make reusing borrowed funds as collateral for further borrowing seamless. Overcollateralisation, which is commonly used as a tool for reducing counterparty risk, offers little protection against over-leveraging: 'While loans are typically overcollateralised, funds borrowed in one instance can be re-used to serve as collateral in other transactions, allowing investors to build increasingly large exposure for a given amount of collateral.'[95] Excessive leverage becomes particularly dangerous during economic downturn:

'High leverage in crypto markets exacerbates procyclicality. Leverage allows more assets to be purchased for a given amount of initial capital deployed. But when debt eventually needs to be reduced, eg because of investment losses or depreciating collateral, investors are forced to shed assets, putting further downward pressure on prices.'[96]

Reliance on collateral as the sole shock absorbing instrument makes the DeFi ecosystem unattractive compared to traditional finance, wherein commercial banks, supported by central banks as lenders of last resort, act as shock absorbers in times of increased volatility.

C. Legal risks

Conceptually, decentralised finance may present substantial challenges to the ability of governments to regulate the economy and enforce the law on their territory:

'In terms of the rule of law, DeFi poses a direct challenge to state-based systems, in that in its strong form (as fully decentralized finance) it seeks to eliminate the role of the state as rule-maker and enforcer. In its purest expression, DeFi thus serves as the ultimate form of 'code is law', with technology replacing state-based legal systems.'[97]

The reality, however, is far from this long-term ambition of DeFi proponents. As noted previously, DeFi applications – at least at the current stage of their evolution – represent innovative, technology-enabled ways of delivering traditional financial products and services. This means that technology-neutral regulatory frameworks may treat DeFi applications as regulated activities (by examining their functional characteristics, rather than their form). Such regulatory frameworks may include, among others, licensing requirements for providers of financial services, consumer, investor and privacy protection frameworks, market integrity, as well as anti-money laundering and counter-terrorism financing (AML/CTF) laws. Failure to comply with the relevant obligations may lead to substantial penalties and may negatively impact end-users' confidence in the DeFi ecosystem.

An exhaustive review of all possible legal implications of DeFi applications is outside the scope of this report. Nonetheless, certain key challenges should be noted.

[95] Sirio Aramonte, Wenqian Huang and Andreas Schrimpf, 'DeFi risks and the Decentralisation Illusion' (2021) *Bank for International Settlements Quarterly Review* 21, 29.

[96] Ibid.

[97] Dirk A Zetzsche, Douglas W Arner, Ross P Buckley, 'Decentralised Finance' (2020) 6 *Journal of Financial Regulation* 184.

(i) Regulatory access points

Even if a particular activity (such as lending or creating a market for trading crypto assets) offered through DeFi platforms is regulated, disintermediation within the DeFi ecosystem could make it difficult to determine the 'regulatory access point' – namely, the entities to which existing laws should apply. As an example, financial services licensing requirements are built on the assumption that the regulated activity (such as distribution of financial products) is performed by a clearly identifiable entity. These requirements can be poorly suited in the DeFi setting whereby the service is performed by multiple, and often pseudonymised, participants.

The absence of a clearly identifiable regulated entity can create perverse incentives for developers of DeFi platforms and promote irresponsible risk-taking by irrational customers. Indeed, elimination of prudential controls and conduct restrictions could deprive customers of meaningful legal recourse options, including in cases of outright fraud.

At the same time, DeFi applications are rarely fully decentralised, which makes it possible to identify individuals or groups of individuals empowered to exercise operational control of the relevant protocols:

'Even if there are no corporations or firms officially underwriting these decentralized protocols, virtually all of these protocols have an entity, whether codified or not, effectively managing the protocol.'[98]

The relevant governance challenges are discussed in greater detail in section 5(D) below.

(ii) Securities laws and disclosure obligations

Another example of legal uncertainty affecting decentralised finance is the question whether the relevant DeFi transaction falls within the ambit of securities laws.

In the United States, the application of the federal securities laws 'turns on whether the economic realities of a transaction comprise in their totality an "investment contract"' – a test (named after the seminal case of SEC v Howey Co) that involves an analysis 'whether there is 1) an investment of money 2) in a common enterprise, and whether investors, in their 3) pursuit of profits, are 4) dependent on the efforts of others'.[99] As discussed by scholars, the application of each of these prongs to DeFi transactions may raise complications.[100]

Traditional disclosure requirements equally pose substantial challenges when faced with the decentralised financing model, as they often predate the introduction of platforms with distributed decision-making, management and ownership (such as decentralised autonomous organisations, or 'DAO's). It is thus unsurprising that disclosure forms aimed at 'typical' securities issuances may 'fail to anticipate decentralized architectures, and are both over- and under-inclusive in terms of the disclosure requirements that one would expect of issuers of blockchain-based securities'.[101] As an example, disclosure forms may fail to recognise that the blockchain governance mechanism is typically embedded in the code of the underlying smart contract – as opposed to a voting process by directors of a company. Similarly, the number of participants involved in the management of the blockchain (including miners and code developers etc) may not be easily reported. The same is true of DAOs, which represent a major departure from a centralised corporate management structure – towards a disperse community of stakeholders.[102]

[98] Nic Carter and Linda Jeng, 'DeFi Protocol Risks: The Paradox of DeFi' (2021) 31 **<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3866699>**.

[99] Chris Brummer, 'Disclosure, Dapps and DeFi' (2022) 5.2 *Stanford Journal of Blockchain Law and Policy* 137, 144-145.

[100] Ibid 145.

[101] Ibid.

[102] See generally ibid 146-149.

(iii) AML/CTF laws

While some aspects of DeFi applications (such as records of transactions recorded on the blockchain) are designed to be transparent, others (like control of blockchain nodes) are often specifically engineered to remain obscure. Indeed, many DeFi applications offer limited traceability – as historical records of transactions are not 'linked to the actual world identity'.[103] As a result, network pseudonymity of blockchains may be abused for illicit purposes in the absence of mandatory customer due diligence checks. Decentralised exchanges are particularly attractive for parties willing to escape supervision, considering the relatively slow rollout of new laws seeking to regulate crypto markets and their overall focus on CeFi exchanges.

Despite the apparent difficulties with applying AML/CTF laws in a pseudonymous setting, regulators have proven that enforcement against decentralised protocols is possible (albeit not without limitations) – as demonstrated by the inclusion of Tornado Cash into the US Office of Foreign Assets Control ('OFAC') Specially Designated Nationals and Blocked Persons ('SDN') list on 8 August 2022.[104] The unusual characteristic of this action by OFAC is that Tornado Cash is not a legal entity or individual, but a crypto currency mixer (essentially a decentralised non-custodial platform built on Ethereum permitting different users to deposit Ether into pools of crypto currency for subsequent withdrawal). As a result, the sanctioned entity is mostly defined by a long series of digital addresses on the Ethereum blockchain[105] – rather than any personally identifying information about a person or company.

According to OFAC, Tornado Cash 'facilitates anonymous transactions by obfuscating their origin, destination, and counterparties, with no attempt to determine their origin' and was used to launder over USD 7 billion worth of crypto assets .[106] While it remains to be seen whether sanctions against computer code will become more commonplace, at least in the short term the designation appears to have had the desired effect of substantially reducing the amount of crypto assets processed by Tornado Cash.[107]

(iv) Consumer protection

Consumer protection rules are rarely concentrated in a single legal instrument – they tend to be spread across different legal frameworks (e.g., financial products and services laws, securities and privacy laws and many others). However, for the purposes of this report, it is worth stressing that consumers are likely to be particularly vulnerable to fraud and abuse within the DeFi ecosystem, considering their lack of specialist knowledge required to make genuinely informed decisions about investments in crypto assets.

This conclusion is supported by the recent study by the Australian Securities and Investments Commission ('ASIC') which revealed that only 20 per cent of surveyed retail crypto investors considered their investment as risky.[108] The lack of adequate understanding of the underlying risks was identified as a critical issue by ASIC's chairman Joseph Longo: 'My concern is that consumers and investors are not fully understanding the risks of this activity and ... not fully understanding what they're investing in as well.'[109]

[103] Christoph Wronka, 'Financial Crime in the Decentralized Finance Ecosystem: New Challenges for Compliance' (2021) Journal of Financial Crime 4.

[104] U.S. Department of the Treasury, 'U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash' (8 August 2022) **<https://home.treasury.gov/news/press-releases/jy0916>**.

[105] U.S. Department of the Treasury, 'Cyber-related Designation' (8 August 2022) **<https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20220808>**.

[106] U.S. Department of the Treasury, 'U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash' (8 August 2022) **<https://home.treasury.gov/news/press-releases/jy0916>**.

[107] J P Koning, 'How to Stop Illegal Activity on Tornado Cash (Without Using Sanctions)' (30 September 2022) **<https://www.coindesk.com/layer2/2022/09/29/how-to-deal-with-tornado-cash-without-using-sanctions/>**.

[108] Australian Securities and Investments Commission, '22-215MR ASIC Releases Research about Investment Behaviour' (11 August 2022) **<https://asic.gov.au/about-asic/news-centre/find-a-media-release/2022-releases/22-215mr-asic-releases-research-about-investment-behaviour/>**.

[109] Dominic Powell, '"Very concerned": ASIC Chairman Sounds Alarm over Crypto Investing Boom' (The Sydney Morning Herald, 11 August 2022) **<https://www.smh.com.au/business/markets/very-concerned-asic-chairman-sounds-alarm-over-crypto-investing-boom-20220811-p5b91y.html>**.

(v) Data protection and privacy laws

Fully decentralised DeFi applications raise significant challenges from the perspective of data protection and cyber security: in addition to making the same data accessible from a greater number of access points, they obscure the identity of the entity responsible for effective data control.

(vi) Regulatory arbitrage

DeFi applications create a range of jurisdictional issues directly related to their dispersed pseudonymous cross-border nature, which complicates the analysis of geographical application of domestic laws. This jurisdictional uncertainty obstructs monitoring and oversight by individual national regulators. Furthermore, the lack of harmonised international approaches to the regulation of DeFi applications facilitates regulatory arbitrage, as investors and platform developers alike seek to stay below the radar:

'Financial services provided in DeFi markets raise risks of regulatory arbitrage to the extent that they are not subject to regulation, or where there are important differences between the applicable regulatory frameworks between jurisdictions.'[110]

This challenge is further reinforced by the reluctance of even the more advanced legal systems to attempt regulating decentralised finance. As an illustration, the most recent text of the Markets in Crypto-Assets (MiCA) Regulation of the European Union available at the time of writing expressly excludes from its scope crypto asset services 'provided in a fully decentralised manner without any intermediary'.[111]

(vii) Enforcement

The foundational characteristics of DeFi (in particular, decentralisation and pseudonymity) may significantly complicate legal enforcement: 'If a DeFi protocol has achieved a high degree of decentralization, it becomes very challenging to hold anyone accountable for failures and errors from the operation of the protocol.'[112]

More specifically, regulatory enforcement in the DeFi ecosystem is hindered by a range of factors.

First, automation through smart contracts and their deterministic execution obscures the decision-making process, making it difficult to identify the person or persons ultimately responsible for the operation of DeFi applications.

Second, regulators may deem their mandates insufficient to permit enforcement against decentralised networks without a clearly distinguishable responsible entity.

Third, composability of DeFi applications makes it more difficult for regulators to identify the responsible entity in complex multi-layer products.[113]

Fourth, DeFi applications tend to operate on a borderless basis, which may complicate the territorial application of domestic laws and identification of responsible regulators.

Fifth, crucially, from the enforcement perspective, the ability to identify the responsible entity may not be as important as having the tools to effectively curb unlawful activities, since 'even when operators can be identified, they may lack the ability to modify DeFi services or stop transactions because of the decentralized nature of the protocols'.[114]

These challenges, while substantial, do not imply that regulators are disincentivised to seek ways to enable enforcement within the DeFi ecosystem. On the contrary, regulators still bear reputational risks and may be considered at least partially responsible when DeFi investors (especially consumers) repeatedly face unlawful practices that are considered unacceptable in traditional finance – such as misleading and deceptive conduct prohibited under section 12DA of the Australian Securities and Investments Commission Act 2001 (Cth) and section 1041H of the Corporations Act 2001 (Cth).

[110] OECD, *Why Decentralised Finance (DeFi) Matters and the Policy Implications* (Report, 19 January 2022) 43.

[111] See paragraph 12a of the Preamble to Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 annexed to Information Note by the General Secretariat of the Council of the European Union dated 5 October 2022 No 13198/22 (Interinstitutional File: 2020/0265 (COD)).

[112] Iwa Salami, 'Challenges and Approaches to Regulating Decentralized Finance' (2021) 115 AJIL Unbound 427.

[113] OECD, *Why Decentralised Finance (DeFi) Matters and the Policy Implications* (Report, 19 January 2022) 43.

[114] World Economic Forum, *Decentralized Finance (DeFi) Policy-Maker Toolkit* (White Paper, June 2021) 22.

D. Market integrity and governance risks

The thrust towards complete disintermediation leaves the DeFi ecosystem open to abuse. If the regulatory controls restricting market manipulation in traditional finance do not apply, legitimate investors are effectively left one-on-one with unscrupulous market participants without the assistance of the usual signposts of credibility and professional qualifications, such as regulator-issued licences. To make matters worse, even if some end-users have the capacity to conduct risk assessment of their prospective counterparties or other stakeholders facilitating transactions on the blockchain (like miners), the pseudonymous character of blockchain operation makes such assessment inefficient (if not unrealistic).

In this context, it is important to recall that – despite the many attempts to achieve disintermediation, decentralisation is rarely absolute and generally exists along a spectrum. As a result, upon a closer examination, intermediaries continue to facilitate DeFi transactions – even if those intermediaries operate quite differently compared to the more centralised traditional finance. This confusing status quo may catch many end-users off guard – as long as they make their DeFi investment decisions by applying their knowledge (however limited) of traditional finance. At the same time, the least sophisticated DeFi investors – consumers – may be swayed by the promise of security offered by self-executing smart contracts devoid of emotion and human control, and thereby fail to recognise the many different forms in which intermediation can continue to exist (and be abused) in the DeFi ecosystem. As a result, the main trusted features of the DeFi ecosystem may, in fact, not be worthy of trust.[115] Below is a brief outline of several main DeFi features that may facilitate market abuse.

(i) Limited incentives to be a repeat player

Interestingly, DeFi's key features – decentralisation coupled with pseudonymity – largely nullify one of the main factors that curb market manipulation in traditional finance: major market participants tend to be repeat players that value their reputation and therefore are disincentivised to abuse the system.

(ii) Validators as intermediaries

Validators are indispensable in DeFi applications due to their role in assembling individual transactions into blocks on the blockchain. As a result, it would not be an exaggeration to say that the integrity of the DeFi market largely depends on the faithful observance of the order of execution of transactions reflected on the blockchain – and especially the incentives the DeFi ecosystem creates for validators to act in good faith.

In practice, validators tend to engage with the blockchain motivated by self-interest and expectation of financial gain and are able to pick and reorder transactions to be added to the next block, while market participants seek to incentivise validators by attaching higher remuneration in the form of fees. This setting creates multiple opportunities for market manipulation, such as abusing the time lag between placing a trade order and its execution on the blockchain. This practice is known as 'front-running' and enables validators and other market participants to make additional profits in the form of 'miner extractable value' ('MEV').

There have been attempts and proposals to mitigate the potential for market abuse associated with MEV (such as encryption of transactions while they are broadcast to the network of miners or facilities enabling miners to auction off their reordering rights), however in the absence of clear and uniformly applicable and enforceable regulatory controls (with a trusted regulator evaluating the risks associated with those alternatives), it is likely that the risks and benefits of such alternative systems can only be fully ascertained by expert investors – since the less sophisticated end-users risk simply replacing one source of vulnerability with another.

[115] On the interplay between the concepts of 'trust' and 'trustworthiness' in this context, see, e.g., Onora O'Neill, 'How to Trust Intelligently' (TED Blog, 25 September 2013) **<https://blog.ted.com/how-to-trust-intelligently/>**; David Spiegelhalter, 'Should We Trust Algorithms?' (2020) 2(1) *Harvard Data Science Review* **<https://doi.org/10.1162/99608f92.cb91a35a>**.

(iii) Manipulation using flash loans

The unique characteristics of flash loans not only enable large-scale risk-free arbitrage, but also create market manipulation opportunities: 'an attacker can, for instance, manipulate the number of tokens in an AMM [automated market-maker] – which is a critical parameter in determining the prices of such tokens'.[116]

(iv) Governance implications

From the governance perspective, DeFi applications can be a source of obscure liability and unclear incentives. Decision-making in the DeFi ecosystem tends to be more complicated not only because multiple stakeholders are involved, but because the technology layer can obscure the decision-making process itself. As a result, it may be unclear (i) who controls the relevant crypto assets, (ii) who controls the platform and (iii) who ultimately receives the financial benefit (including the benefit from platform manipulation).

These aspects can be particularly complicated in DeFi, since the governance model often changes over the course of the project's development: 'The initial implementation is typically centralized governance, where the operator controls and implements changes directly'.[117] Subsequently, however, DeFi platform developers may announce their intention to relinquish some of that control in favour of collective decision-making. Whether and how this is implemented in practice is not always clear and verifiable:

'DeFi developers often describe a trajectory from centralized governance at the outset to partially and then fully decentralized governance as the service reaches maturity. At this early stage of the market, however, there are few if any examples of this process unfolding from start to finish. The token-based voting systems that have been implemented are immature, and governance votes of major services have failed due to insufficient turnout.'[118]

Despite multiple attempts to market DeFi applications as fully disintermediated, the degree of influence exercised by developers of DeFi platforms can be significant, often amounting to effective (and centralised) control. There are two main sources of such control.

Concentration risks

First, platform developers may have effective veto power due to large holdings of governance tokens. When privately developed platforms are shared with the wider community as DeFi applications, the original developers and investors can retain a large amount of such tokens. In this context, from the governance perspective, the perceived transparency of the blockchain is essentially rendered meaningless through pseudonymity:

'Although all holdings are publicly available on the chain, as these are reported on a pseudonymous basis there is no clear picture of shareholdings at an aggregate level available to the community (multiple addresses can belong to the same user).'[119]

Furthermore, even where the design of a DeFi platform is genuinely inspired by the intention to create a fully decentralised infrastructure, economic incentives of concentrated voting power push strongly in the opposite direction – by facilitating the creation of cartels, particularly in proof-of-stake systems whereby one's governance power is proportional to one's share of the tokens on the blockchain (further enabled by the ability to freely trade governance tokens, pseudonymously, on decentralised exchanges).[120]

The resulting concentration can create significant opportunities for DeFi market manipulation, allowing large validators to 'congest the blockchain with artificial trades between their own wallets ("wash trades"), steeply raising the fees that other traders pay them.'[121]

[116] Sirio Aramonte, Wenqian Huang and Andreas Schrimpf, 'DeFi risks and the Decentralisation Illusion' (2021) *Bank for International Settlements Quarterly Review* 21, 27.

[117] World Economic Forum, *Decentralized Finance (DeFi) Policy-Maker Toolkit* (White Paper, June 2021) 9 **<https://www3.weforum.org/docs/WEF_DeFi_Policy_Maker_Toolkit_2021.pdf>**.

[118] Ibid.

[119] OECD, *Why Decentralised Finance (DeFi) Matters and the Policy Implications* (Report, 19 January 2022) 44 (emphasis added).

[120] Nic Carter and Linda Jeng, 'DeFi Protocol Risks: The Paradox of DeFi' (2021) 19 **<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3866699>.**

[121] Sirio Aramonte, Wenqian Huang and Andreas Schrimpf, 'DeFi risks and the Decentralisation Illusion' (2021) *Bank for International Settlements Quarterly Review* 21, 28-29.

Coupled with composability of the DeFi ecosystem, the tradability of fungible governance tokens may well become the source of systemic risks:

'…yield farming may lead to centralization creep by allowing an already well-established protocol to assume a significant portion of a relatively new protocol's governance tokens. This may create large meta protocols whose token holders essentially control a considerable portion of the DeFi infrastructure.'[122]

Administrator-level control

Second, developers may have no formal duty to implement all decisions of the decentralised community – effectively retaining control over the development of the system. In the absence of a mechanism to override it, the 'control' of the decentralised community is only nominal and superficial – as when the interests of developers and platform users collide, administrator permissions enable developers to go rogue. Reportedly, with very limited exceptions, the operation of DeFi platforms remains subject to effective control by software developers and administrators, including kill-switches:

'Many DeFi protocols retain the discretionary option for administrative teams or other entities to shut them down, upgrade them, pause the contract, and in some cases, drain user funds.'[123]

Major DeFi platforms today also maintain administrative keys.[124] The existence of these keys, even if introduced for legitimate reasons (such as to preserve the ability to fix software bugs) effectively recentralises control of DeFi platforms in the hands of whoever holds them, creating perverse incentives:

'If the keyholders do not create or store their keys securely, malicious third parties could get their hands on these keys and compromise the smart contract. Alternatively, the core team members themselves may be malicious or corrupted by significant monetary incentives.'[125]

At the same time, the very fact that administrative keys do, in fact, exist on a particular platform can be difficult, if not impossible to verify – particularly for the less sophisticated investors. If such crucial information can be easily withheld, a genuine investment via a DeFi platform may effectively turn into a gamble, with limited or no recourse to those who may rig the system (considering that, unlike traditional finance, DeFi platforms tend to be pseudonymous, which obscures the identities of all actors – and not just the investors).

Overall, the substantial degree of control exercised by different actors is a clear sign of centralisation often hidden behind the DeFi façade. The economic incentives for maintaining control, as well as for seizing it, appear to be simply too strong to seriously expect DeFi platform developers to readily relinquish administrative keys, at least at the time of writing. This status quo essentially nullifies the foundational premise of DeFi – the removal of intermediaries – leaving prospective investors to deal with risks they do not understand on platforms controlled by persons they do not know, all while the many legal protections of traditional finance do not apply.

[122] Fabian Schär, 'Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets' (2021) 103(2) *Federal Reserve Bank of St. Louis Review* 170-171.

[123] Nic Carter and Linda Jeng, 'DeFi Protocol Risks: The Paradox of DeFi' (2021) 25 **<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3866699>**.

[124] Ibid 26.

[125] Fabian Schär, 'Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets' (2021) 103(2) *Federal Reserve Bank of St. Louis Review* 170.

6. Regulatory tools and policy options to enable safe integration of DeFi in traditional finance

The policy (and in particular, regulatory) implications of DeFi are determined by the risks generated by DeFi applications. As discussed previously, these risks stem mostly from the innovative ways of delivering traditional financial products and services using blockchain and smart contracts. Since the products and services themselves remain largely unchanged – and only their delivery changes – DeFi serves as a useful litmus test of the resilience of national (and in some ways, international) regulatory frameworks and its preparedness for technological change.

This section explores the regulatory and policy tools and factors that can facilitate safer integration of DeFi into the wider economy.

A. Functional approach to regulation

As a starting point, regulation should be able to see through the technology to identify the pressure points, such as access to complex financial products by unsophisticated and vulnerable investors without adequate regulatory controls in place to prevent abuse. This technology-neutral approach, already adopted in multiple jurisdictions, usefully applies the same rules to (functionally) the same activities, regardless of the underlying technology: 'As such, the use of DLTs or other technology does not affect the way these regulators assess whether or not the ensuing financial product/service or activity falls within the regulatory perimeter, and by consequence, whether it is regulated or unregulated.'[126]

Since the risks are not entirely new, we can look at traditional finance for regulatory approaches to curb the same risks: 'Since the main challenges in DeFi resemble those in traditional finance, established regulatory principles can serve as a compass. The basic tenet "same risks, same rules" should apply, not least to counter regulatory arbitrage.'[127]

Nonetheless, a technology-neutral approach is rarely enough due to substantial costs associated with effective monitoring and supervision of a dispersed community, many of whom may 'contribute only gradually and partially to the overall service'.[128] Just like DeFi changes how the same financial services are offered to end-users, so too the law may need to change how it applies to those financial services.

Despite the disintermediation aspirations of DeFi platform developers, the preceding analysis in section 5(D) demonstrates not only that complete disintermediation is hardly achievable, but also that regulatory access points can be realistically identified through a holistic examination of DeFi protocols focusing on the governance mechanics. Even though the perceived attractiveness of automation via smart contracts used in DeFi applications is the elimination of the human factor (particularly human discretion), in most cases some element of human discretion remains – whether in programming or governance, or both.

B. DeFi as a developing concept

At the time of writing, the DeFi ecosystem remains significantly underdeveloped: 'At present, it is geared predominantly towards speculation, investing and arbitrage in crypto assets, rather than real-economy use cases.'[129] Nonetheless, DeFi's potential to rapidly evolve is undeniable. From a policy perspective, however, it is hardly a consolation that the DeFi ecosystem will continue to evolve and, with enough trial and error, may one day eliminate or substantially mitigate the risks observed today. Even if the overall size of the DeFi ecosystem has not yet reached a level that is sufficient to pose meaningful systemic challenges to traditional finance, many of the issues (particularly those concerning unsophisticated investors) cause immediate harm and, therefore, need to be immediately addressed.

[126] OECD, *Why Decentralised Finance (DeFi) Matters and the Policy Implications* (Report, 19 January 2022) 42.

[127] Sirio Aramonte, Wenqian Huang and Andreas Schrimpf, 'DeFi risks and the Decentralisation Illusion' (2021) *Bank for International Settlements Quarterly Review* 21, 33.

[128] Dirk A Zetzsche, Douglas W Arner, Ross P Buckley, 'Decentralised Finance' (2020) 6 *Journal of Financial Regulation* 185.

[129] Sirio Aramonte, Wenqian Huang and Andreas Schrimpf, 'DeFi risks and the Decentralisation Illusion' (2021) *Bank for International Settlements Quarterly Review* 21, 32.

Potential future developments aside, the many risks generated for DeFi investors currently outweigh the benefits, many of which remain unrealised. Against this background, regulatory intervention seems necessary – both to prevent immediate harmful consequences for investors, and to promote end-users' trust (not by fostering uncontrolled use of DeFi applications, but by encouraging those practices which improve upon traditional finance).

While some commentators have stressed the importance of attempts to 'differentiate between legitimate decentralized protocols and projects that only claim to be decentralized',[130] the boundary problem discussed in section 2 above suggests that it may be virtually impossible to distinguish DeFi meaningfully from traditional finance in the absence of agreed functional characteristics of decentralised finance and considering that decentralisation exists on a scale and is rarely absolute. Once this is accepted, the growing connections and dependencies between DeFi and CeFi present two more immediate concerns worthy of policymakers' attention: (i) consumer protection and (ii) systemic risks.

C. Consumer protection as a regulatory priority

As demonstrated above, as an alternative to traditional finance, DeFi still has a lot of teething problems that need to be dealt with in the future iterations of DeFi applications. This is understandable. However, the immediate risks to the least sophisticated investors (particularly consumers) should not be ignored. Simply put, DeFi developers should be free to continue to improve upon their early designs and develop new ones – as long as this development does not turn out to be an experiment at the expense of those who engage with the DeFi ecosystem because they cannot understand the underlying risks. Even if customers trust something, it does not mean they do not need to be protected from the risks they do not see.

Consumers represent perhaps the most vulnerable group of DeFi investors due to the high technical complexity of DeFi mechanics and limited expert knowledge and resources to make informed investment decisions.

Information disclosures are a common tool used to permit consumers to make informed decisions that could be used for DeFi applications – since DeFi developers generally seek to make their platforms accessible by prospective investors through a variety of tools, from blogs to dedicated web sites, to social media. However, there is a substantial difference between a disclosure that seeks to provide a simple but genuine representation of the risks of a DeFi application, on the one hand, and a vague and misleading description pursuing a single objective – to induce investors to part with their money – on the other.

Disclosures relating to DeFi platforms need to provide an accurate description of the corresponding risks. A notable concern here is that 'entrepreneurs are usually not expected, or even supposed to disclose all risks to investors, but are tasked with identifying which risks are most likely, or if unlikely, would have the greatest impact on the operation of the DeFi project'.[131]

[130] Fabian Schär, 'Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets' (2021) 103(2) *Federal Reserve Bank of St. Louis Review* 172.

[131] Chris Brummer, 'Disclosure, Dapps and DeFi' (2022) 5.2 *Stanford Journal of Blockchain Law and Policy* 137, 154.

In the light of the previous discussion in section 5, efficient DeFi disclosures would likely contain information about:

- the degree of centralisation of different functions of the DeFi application – with a clear description of all elements that are, or may be considered, centralised (this will include, among other things, administrative keys and concentrated holdings of governance tokens);
- the level of control and the economic and governance stake of platform developers and any of their affiliated entities (whether through a single node on the blockchain or multiple different nodes);the existence of conflicts of interest (actual or perceived) between platform developers/administrators and end-users;
- checks implemented on the DeFi application to prevent manipulation and abuse of control over the platform;
- an explanation of token mechanics (basic economics, factors impacting their market and value – taking into account the governance and incentives they have and whether they may differ from those of investors);[132] and
- specific technical and risks, including network congestion, extra cyber security risks of open software and liquidity crunches.

The relevant disclosures would have the most practical value if drafted in non-technical language that is accessible by non-experts. Another crucial feature of DeFi disclosures relates to the mode of their delivery to investors, which may come in different forms.[133]

A more radical method of minimising consumers' exposure to DeFi applications could involve the introduction of a blanket restriction for DeFi applications to interact with non-expert investors – akin to the sophisticated (or qualified) investor regime found in securities laws.

D. Systemic risk prevention as a regulatory priority

The systemic risks discussed in section 5(B)(ii) above require regulators to focus attention on the intersection of DeFi with traditional finance. While in theory the DeFi ecosystem could be structured as a crypto asset-enabled infrastructure completely isolated from traditional finance, some commentators have argued that harnessing of DeFi's true potential is impossible without interlinkages with traditional finance:

'First, DeFi lending must engage in large-scale tokenisation of real-world assets, unless it wants to remain a self-referential system fuelled by speculation. Representing assets such as buildings or capital equipment on the blockchain, so that it can serve as collateral underpinning loans, would be particularly beneficial for SMEs, which have more limited access to finance. Oracles, ie the mediators that communicate real-world information to blockchain-based DeFi applications, are essential to achieving this objective. But oracles must be reliable and trustworthy, lest they be used to corrupt the system by inducing smart contracts to take action based on manipulated information.'[134]

Once this is accepted, the natural starting point for addressing potential contagion effects between DeFi and traditional finance could be the intersection between the two systems. In this context, Schär suggests that regulators should pay special attention to the facilities that enable exchanges to and from fiat currency:

'Fiat on- and off-ramps are the interface to the traditional financial system. Whenever people want to move assets from their bank account to the blockchain-based system or the other way, they have to go through a financial service provider.'[135]

[132] Ibid 156-157.

[133] See, e.g., ibid 165ff.

[134] Sirio Aramonte et al, *DeFi Lending: Intermediation Without Information?* (Report, 14 June 2022) 6.

[135] Fabian Schär, 'Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets' (2021) 103(2) Federal Reserve Bank of St. Louis Review 172.

This is a helpful proposal, particularly as a means of combating tax evasion.[136] At the same time, DeFi's intersection with traditional finance is not limited to conversions into fiat currency. As an example, traditional financial institutions may interact with the DeFi ecosystem directly, by operating nodes on DeFi platforms (or having a subsidiary or another group member do so). To minimise the contagion effects of DeFi's intersection with traditional finance, the prudential requirements for incumbent institutions should incorporate clear guidance on dealing with exposures to the DeFi ecosystem – such as rules on exposure to crypto assets. An important step in this direction is the publication of the second public consultation on the prudential treatment of crypto asset exposures by the Basel Committee on Banking Supervision in June 2022.

As a result, a more comprehensive examination of points of contact between DeFi and CeFi (such as stablecoins) is warranted. Such examination would be particularly helpful if performed on a continuing basis, along with the evolution of DeFi platforms and their technical features.

E. Importance of ex ante regulation

While the fast-changing nature of DeFi applications may understandably lead some regulators to favour a 'wait-and-see' approach, regulatory intervention at an early stage has two important benefits.

First, it appears to be the most efficient option, considering that a typical cycle of development of DeFi applications is one of continuous decentralisation (i.e., transition from a closed centralised system towards an open decentralised platform):

'There will typically be an identifiable group of protocol developers (although it might operate under the umbrella of an open-source development community, non-profit foundation or association or the DAO). Once the protocol is published, multiple teams might develop it into services and market it to users, representing a combined deployment stage. Those services might later be forked by different teams. The operation of the service will largely be automated by the protocol and smart contracts, perhaps moderated by decentralized governance processes.'[137]

As a result, regulatory intervention is likely to be most effective earlier in the lifecycle of a DeFi application.

Second, earlier interaction between regulators and developers can help steer the development towards enhanced consumer protections and may help remedy some of the issues identified in the earlier sections of this report. Incidentally, such earlier engagement can be facilitated by the development of regulatory sandboxes aimed at DeFi applications.

F. A regulatory sandbox for DeFi development

A regulatory sandbox[138] for developers of DeFi applications offers a number of advantages. If designed as a form of interactive regulator-led engagement of developers with a limited number of real investors, a sandbox will provide an opportunity for the regulator to monitor the development of the platform's trajectory towards full decentralisation. It seems worthwhile to require DeFi developers participating in the experiment to give the responsible regulator administrative privileges, to enable immediate shutdown and rollback of the protocol should the need arise.

It is possible that some regulators may go further than that – and, in the absence of a better alternative – rethink what a regulatory sandbox means in the DeFi context, turning it from an optional testing facility on the way towards authorisation to a necessary mandatory step in the development of approved decentralised platforms (where the risks can be verified by the regulator ex ante).

[136] See OECD, *Why Decentralised Finance (DeFi) Matters and the Policy Implications* (Report, 19 January 2022) 59.

[137] World Economic Forum, *Decentralized Finance (DeFi) Policy-Maker Toolkit* (White Paper, June 2021) 23.

[138] For a comprehensive analysis of the concept, design and implications of regulatory sandboxes, see Anton N Didenko, 'A Better Model for Australia's Enhanced FinTech Sandbox' (2021) 44(3) *UNSW Law Journal 1078*.

G. Three drivers to support responsible DeFi regulation

Regulation of DeFi requires long-term planning and should be supported by three key drivers.

(i) Informed decision-making by policymakers

Continuous monitoring of the DeFi market is a resource-intensive task – but one that appears unavoidable, considering the increasing interconnectedness of the DeFi ecosystem with traditional finance. The availability and quality of relevant data will determine the ability of policymakers to react quickly to particularly dangerous developments, such as increased risks to consumers and systemic spill-overs to CeFi. At the time of writing, the need for such reliable data appears acute: 'While data appear to be available, it is hard to know whether the unregulated nature of DeFi markets means that data quality is poor, or whether there are gaps that prevent the effective monitoring of risks.'[139]

(ii) International regulatory coordination

DeFi's cross-border nature strongly suggests that international regulatory coordination is needed to address the most damaging aspects of DeFi (such as fraud) and to facilitate the circulation of reliable data on the state of the DeFi ecosystem between policymakers. Long-term goals may as well include the development of global standards, as suggested by some commentators.[140] Such standards could target the key elements of the DeFi ecosystem creating spill-overs into traditional finance, such as stablecoins. In the short-to-medium term, however, a wider international coordination among various stakeholders – one that is not limited to policymakers alone – can help generate sufficient knowledge to enable further reform.

While full-scale international coordination on DeFi is yet to emerge, regulators are increasingly exploring new opportunities for joint work in this area.

Notably, 2022 marked the launch of a Fintech Task Force ('FTF') under the auspices of IOSCO (International Organization of Securities Commissions) chaired by the Monetary Authority of Singapore. The FTF's two initial workstreams focus on crypto and digital assets and decentralised finance, respectively.[141] The DeFi workstream will be led by the United States Securities and Exchange Commission and seeks 'to develop a shared understanding among IOSCO members of emerging DeFi trends and risks while providing guidance to IOSCO members on how to manage these risks within their regulatory frameworks'. The Financial Stability Board (FSB), in turn, has recently launched a consultation on a proposed set of recommendations for the regulation and supervision of crypto-asset activities, which, among other things, has the potential to significantly impact the regulatory expectations for stablecoins that link DeFi with CeFi.[142]

(iii) End-user education and capacity-building

It is hardly questionable that well-informed end-users can better appreciate the many risks posed by DeFi. Yet, the ease of access to the DeFi ecosystem observed today significantly surpasses the levels of end-user awareness. On the one hand, most end-users – particularly consumers – would clearly lack the capacity to verify the integrity of computer code used in DeFi applications. On the other hand, many DeFi investors are likely to fail to recognise even the most fundamental sources of underlying risks and mechanisms of their transmission – in the light of ASIC's eye-opening conclusion that only 20 per cent of surveyed cryptocurrency owners appreciated the riskiness of their investment.[143]

[139] OECD, *Why Decentralised Finance (DeFi) Matters and the Policy Implications* (Report, 19 January 2022) 61.

[140] Iwa Salami, 'Challenges and Approaches to Regulating Decentralized Finance' (2021) 115 *AJIL Unbound* 429.

[141] International Organization of Securities Commissions, 'IOSCO Crypto-Asset Roadmap for 2022-2023' (7 July 2022) 1 **<https://www.iosco.org/library/pubdocs/pdf/IOSCOPD705.pdf>** 1.

[142] Financial Stability Board, 'International Regulation of Crypto-asset Activities: A Proposed Framework – Questions for Consultation' (11 October 2022) **<https://www.fsb.org/wp-content/uploads/P111022-2.pdf>**.

[143] Australian Securities and Investments Commission, '22-215MR ASIC Releases Research about Investment Behaviour' (11 August 2022) **<https://asic.gov.au/about-asic/news-centre/find-a-media-release/2022-releases/22-215mr-asic-releases-research-about-investment-behaviour/>**.

DeFi's characteristics make some of the traditional signposts of risky investments largely redundant. After all, mandated disclosure requirements widely used in centralised finance – even if implemented for DeFi applications – are likely to be effective only as long as they can be meaningfully enforced in a decentralised ecosystem (see section 5(C)(vii)).

This brings to the forefront the need for greater customer (especially consumer) education delivered directly by (or on behalf of) regulators:

'Therefore, regulatory bodies may want to consider encouraging or engaging in investor protection updates to raise financial consumer awareness of potential risks, thereby giving guidance to market participants to better articulate such risks to market participants. Financial education efforts and policies could also be instrumental in helping users understand the risks involved in decentralised finance products and protect themselves accordingly'.[144]

[144] OECD, *Why Decentralised Finance (DeFi) Matters and the Policy Implications* (Report, 19 January 2022) 60.

7. Conclusion

Although DeFi mimics traditional finance, more often than not the latter produces similar results more cheaply, efficiently and with fewer risks for the less sophisticated end-users. The need for a regulatory response to the risks of DeFi is palpable but designing such a response is a complex challenge for a number of reasons.

a) This report has shown that the *efficiencies* of removing intermediaries in DeFi are often cancelled out by the *inefficiencies* generated by the removal of those intermediaries. Disintermediation, while welcome in a number of scenarios, reduces the opportunities for adequate regulatory oversight, timely intervention and effective enforcement.

b) The lack of precision regarding the exact scope of DeFi and the associated boundary problem could refocus the policymakers' attention towards the functional characteristics of DeFi, as opposed to underlying technologies. As DeFi applications continuously evolve, attempts to regulate DeFi 'as it is now', by reference to the current level of technology will likely result in a whack-a-mole-style approach that would invariably lag behind the technology, potentially generating an endless catch-up race between the regulators and the regulated.

c) DeFi applications experience major teething problems, as they struggle with the issues that have already been resolved in traditional finance. Disintermediation eliminates the efficiencies generated by credit reporting (thus leaving DeFi investors to make poorly informed investment decisions based on the perceived benefits of overcollateralisation and faith in the overall health of the DeFi ecosystem that cannot be assumed) or legally enforceable dispute resolution (thus asking DeFi investors to trust third party 'oracles' whose trustworthiness can be misplaced – not to mention the fact that oracles are, by definition, intermediaries which DeFi seeks to eliminate).

d) Evaluation of the balance of interests of different stakeholders in the DeFi ecosystem will inform the policy responses to the risks of DeFi. As an example, policymakers would need to determine which of the two conflicting objectives of DeFi should take priority: the deterministic and irrevocable nature of execution in smart contracts or the fairness achieved by the ability of aggrieved investors to recover stolen funds in the event of fraud or market manipulation. This report posits that the lack of effective recovery mechanisms in DeFi makes it clearly unsuitable for non-sophisticated retail investors.

e) The transparency of smart contracts widely implemented in the DeFi ecosystem – while attractive – offers little to no benefit for non-expert users who will continue to rely on intermediaries to interpret or evaluate the programming code for them or improve the usability of DeFi applications (e.g., by offering an intuitive user interface).

f) When applied within the DeFi context, the 'assume breach' logic commonly used in cyber security controls presents an existential challenge to the entire decentralised finance ecosystem. If investors cannot recover their funds after a cyber breach (due to the deterministic nature of smart contract execution), the inevitability of cyber incidents, coupled with purely nominal (as opposed to meaningful) transparency of DeFi protocols makes DeFi investments more akin to gambling in the eyes of unsophisticated investors.

g) Since the risks of DeFi appear particularly pronounced for unsophisticated investors (especially consumers), this report posits that policymakers should prioritise insulating such investors from the risks of DeFi.

h) The risks of systemic disruption generated by DeFi applications create strong incentives for policymakers to prevent spill-over effects within traditional finance. This can be achieved by (i) targeting the cross-points between decentralised and traditional finance (such as crypto currency exchanges and stablecoin issuers) and (ii) regulating the providers of critical infrastructure underpinning the basic layer of the DeFi ecosystem.

i) Despite its many *currently* observable risks, DeFi remains a rapidly evolving concept – which calls for a long-term strategy to build responsible DeFi regulation. Such a strategy should be underpinned by three key pillars: (i) informed decision-making by policymakers, (ii) international regulatory coordination and (iii) end-user education and capacity-building.

cpaaustralia.com.au

CPA AUSTRALIA