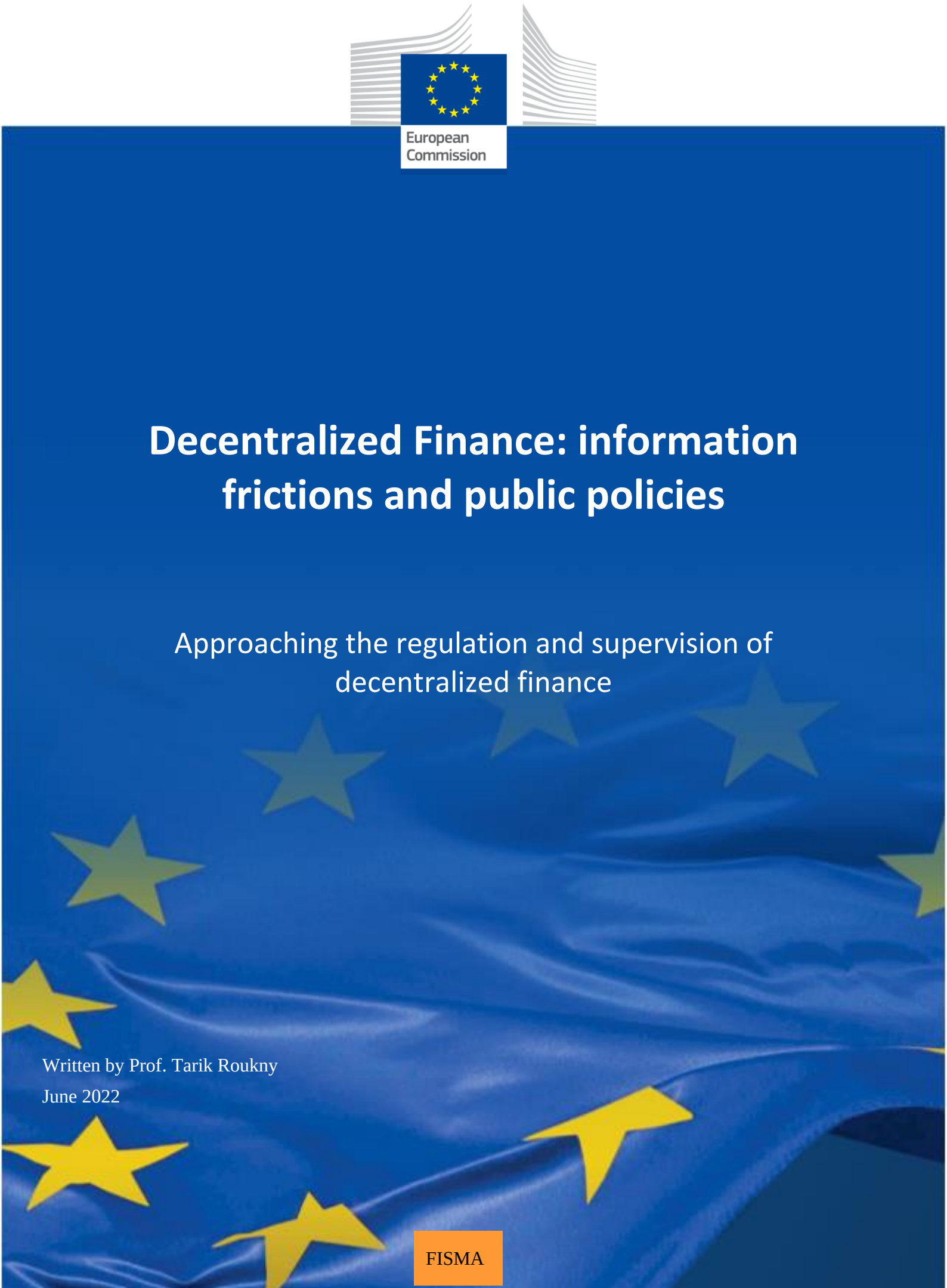


Decentralized Finance: information frictions and public policies

Approaching the regulation and supervision of decentralized finance

Written by Prof. Tarik Roukny

June 2022

FISMA

EUROPEAN COMMISSION
Directorate-General for Financial Stability, Financial Services and Capital Markets
Directorate B – Horizontal policies
Unit B4 – Digital Finance
Contact: FISMA-B4@ec.europa.eu
European Commission
B-1049 Brussels

Decentralized Finance: information frictions and public policies

Approaching the regulation and supervision of decentralized finance

LEGAL NOTICE

Manuscript completed in June 2022

Luxembourg: Publications Office of the European Union, 2022

PDF ISBN 978-92-76-56387-7 doi:_10.2874/444494 Catalogue number EV-07-22-933-EN-N

Abstract

At its core, Decentralized Finance is an effort to disintermediate financial markets through a combination of cryptographic solutions and incentive compatible designs. While still in early development, DeFi applications have grown rapidly over the last years. As a result of the large volumes of associated capital, policy makers and financial authorities are turning their attention to the risk and opportunities posed by this trend. Are DeFi services fundamentally different from traditional finance? Should policy frameworks adapt to the specific nature of DeFi systems? How could public actions promote synergies and ensure sustainable interactions between DeFi, traditional finance and the real economy? In addressing those questions head on, this report provides a rationale for the presence of public support in the DeFi ecosystem. Building on standard arguments from the literature on the origins and consequences of financial intermediation, the report establishes a set of key distinctive features between traditional financial markets and DeFi. The conceptual contribution of the report is to position the treatment of information at the center of analysis and to show how such a process differs between traditional and decentralized financial systems. Relying on this information framework, the study highlights conditions under which specific public initiatives may be warranted from a welfare perspective and feasible from a technological perspective. As a result, the report proposes implementable solutions to foster economic growth and financial stability for DeFi systems as well as promoting complementarities between DeFi and the economy as a whole.

Acknowledgements

Raphael Auer, Andreas Park, Co-Pierre Georg, Hannah Halaburda, Ioana Surpateanu, Julien Prat, Bruno Colmant, Agostino Capponi, Markus Brunnermeier, Kevin Werbach, Mathias Dewatripont and Brian O'Hagan.

Contents

1. Introduction

Applications in Decentralized Finance (DeFi) rely on automated protocols to produce financial services including exchanges, credit, derivatives and portfolio management. In contrast with traditional venues, the specificity of DeFi is that protocols are (i) encoded in public digital contracts universally accessible and (ii) maintained by an open pool of pseudonymous agents rather than a unique legal entity.[1]

As with any new technology, DeFi services combine great opportunities and severe risks to the economy. On the one hand, openness and transparency bear promises to remove threats of abusive market power, promote innovation and facilitate financial inclusion. On the other hand, aspects such as pseudonymity, limited formal leadership and restrained control over contracting processes bear the risk of attracting illicit activity, exposing customers to great harm and generating new sources of financial instabilities.

One of the prime objectives of public policies is to ensure that benefits from innovation do not come at an irremediable cost. However premature and inadequate attempts to regulate nascent technologies may hinder substantial future welfare gains. In view of this balance, this report proposes a framework to evaluate the positive role that appropriate public policies can have on the development of the DeFi ecosystem and its contribution to the economy.

Growth of DeFi

Compared to other trends initiated following Bitcoin's success - such as centralized crypto-exchanges and initial coin offerings - DeFi is a relatively young branch of the crypto-economic system family. Activity in DeFi gained traction at the turn of the last decade: the total amount of value locked (TVL) in DeFi services went from $600 millions in January 1st 2020 to a peak around $315 billions on the 26th of December 2021, yielding a growth of 524% in two years.[2] This period of 2020-21 is commonly referred to as the 'DeFi Summer'. In the first quarter of 2022, TVL dropped but remained well above $250 billion. In March 2022 the market capitalization of the 100 largest assets related to DeFi services was still averaging close to $100 billions.[3] However, volatility and instability have progressively gained power, particularly during the second quarter of 2022. A case in point was the crash of the once-popular stablecoin TerraUSD and its sister token Luna during the month of May 2022 which led to hundreds of billions of losses in market capitalisation across crypto-markets and a halving of TVL in DeFi in the span of a week.[4]

In recent years, several institutions have initiated efforts to assess and manage the implications of DeFi activity to the rest of the economy. IOSCO (2022) published a report highlighting several sources of risk and economic frictions inherent to DeFi protocols. The World Economic Forum (2021) has proposed a policy toolkit to support policy makers in their attempt to assess how risks from DeFi protocol should be addressed. The Financial Action Task Force (2021) also included guidance on DeFi activity for crypto service providers to combat money laundering and criminal activities. Furthermore, the IMF (2021), the OECD (2022) and the Financial Stability Board (2022) all recently issued warnings that an increase of interactions between DeFi activity and the traditional financial system could pose significant threats to financial stability and systemic risk. In a recent report, BIS (2021) shows that while banks have so far retained limited direct exposure to DeFi activity - in part due to conservative regulatory constraints - investment by traditional

---

[1] We define a DeFi protocol as the set of rules that govern the smart contract of a given DeFi application or service.

[2] The Total Value Locked (TVL) is a common metric to estimate economic value in the DeFi ecosystem. It corresponds to the sum of assets stacked in DeFi protocols. Note that figures can differ from one provider to the next. In this report we use data from DeFi Llama (https://defillama.com), a leading source with the largest coverage of DeFi protocols. Other providers include DeFi Pulse and Coingecko. While absolute values differ, growth rates are broadly similar across providers.

[3] Source: https://defimarketcap.io

[4] "Terra $45 Billion Face Plant Creates Crowd of Crypto Losers" – Bloomberg News, May 2022.

(non-bank) investors grew tenfold between 2018 and 2021. Importantly, the authors show that this trend is mainly driven by family offices and hedge funds which often receive funding from major dealer banks, thereby exposing the banking sector indirectly.

In a geographical analysis of DeFi activity, Chainanalysis (2021) highlights that in contrast to other trading trends in crypto-economic systems, a large part of the DeFi growth has been driven by professional and institutional investors from advanced economies including several European countries such as The Netherlands and France. The report concludes that 'Central-North-Western Europe has become the world's biggest cryptocurrency market, and its growth over the last year was largely driven by institutional investors and other whales moving into DeFi'.

The above evidence suggests a tight link between DeFi activity and the European financial sector. As a result, policy institutions such as the European Commission may hold a key role in shaping the future of DeFi and its interactions with the rest of the economy.

Challenges to standard policies

While public attention to the regulation and monitoring of DeFi systems is growing, the very nature of service provisioning in DeFi poses a general challenge to standard policy frameworks. At the center of this challenge lies the absence of clearly delineated legal entities - both on the supply side and the demand side - upon which policy institutions have traditionally enforced their requirements. More precisely, the combination of permissionless access to the consumption and provision of financial services by (legally) unidentified agents through automated protocols constitute an unprecedented setting where standard intervention tools may simply not be appropriate nor implementable. Consider for instance a policy which would prevent anyone from creating and deploying her own protocol at scale on a blockchain such as Ethereum. This would not constitute an implementable policy rule by virtue of the permissionless access of Ethereum. As such legacy regulatory approaches may be ill-suited to the task at hand. Importantly, the value of policy interventions in DeFi needs to be weighted against their economic needs and technological feasibility.

This report

The present work aims to address the challenge of implementing public actions in DeFi services. Our approach consists of identifying whether, when and how public policies may be both warranted and feasible in the DeFi ecosystem.

Our first contribution is to rationalize the need to adapt policy frameworks by focusing on a key deviation which DeFi services exhibit vis-à-vis traditional financial systems, that is, a fundamental shift in the underlying information structure upon which financial services are provided. Leveraging the literature on traditional financial intermediation, we source the existence of traditional intermediaries to the presence of information frictions inherent to financial interactions. In traditional financial systems, financial intermediaries produce welfare gains to the economy by addressing these frictions. Implicitly, this rationale relies on a specific form of information structure which has in turn supported the design of several standard policy frameworks in place for traditional financial markets today. We show how DeFi protocols rely on different information structures, thereby making several standard policies inadequate to the treatment of DeFi services.

Building on this information view of financial intermediation, we next propose a simple taxonomy of DeFi protocols based on their underlying information structure requirements. We differentiate between three categories of protocols: autarkic, crossing and off-chain. We show - and illustrate when possible - that the implicit information space upon which a protocol relies strictly determines its economic scope of application. Following this classification, we revisit sources of market failures in DeFi related to each information setting. We identify which sources

of risk and inefficiency may not be fully addressed by private solutions, thereby opening up opportunities for warranted public support.

Finally, we consider a set of candidate policy approaches to implement such public actions. These policies are selected and discussed in light of their technological implementability. Our list consists of four proposals: regulating activity of legal entities, a voluntary compliance framework, a public observatory and the treatment of off-chain markets (i.e., oracles).

Approach and limitations

By design, the study of DeFi systems is an interdisciplinary one. Not all aspects of such a rich ecosystem can nor should be tackled all at once, especially when they relate to the delicate question of policy enforcement. In this report, we therefore limit our focus to the economics of information in decentralized solutions and their policy implications with a strong emphasis on the constraints imposed by the set of core DeFi principles. DeFi is a rapidly growing area with new developments occurring at a high pace. A comprehensive listing of all protocols and their related solutions is therefore not realistic within the scope of this report. Instead, our approach attempts to essentialize major activities and services to their core economic value in order to propose a first cohort of policy approaches upon which future work will be required to integrate contemporaneous developments. By the same token, several legal and institutional specificities surrounding DeFi are also omitted from our analysis. When appropriate, we direct the interested reader to dedicated material produced by parallel initiatives that this report aims to complement.[5]

[5] In particular, we adjust our analysis to comparatively under-developed areas of policy research in DeFi. For instance anti-money laundering and know-your-customer policies are currently at a distinctively more advanced stage of development regarding DeFi policy frameworks compared to financial stability and market efficiency issues. Accordingly, we allocate more attention to the latter set of issues.

2. Traditional financial intermediation

On the origins of financial intermediation

The origins of financial intermediation have traditionally been rooted in information sharing frictions either because of technological costs or privacy preferences. In an ideal world of frictionless and complete financial markets, investors and borrowers are able to obtain optimal trading and risk sharing allocations. However, once financial interactions exhibit frictions in their transaction technology, the optimal outcome is no longer feasible. It is within this imperfect context that financial intermediaries enter the picture in order to address transaction costs and generate welfare gains (Freixas and Rochet, 2008).

In economics, an intermediary is typically depicted as an agent buying and selling goods and services from producers down to consumers when there exist transaction costs such as transportation technologies. In finance, intermediation includes banks issuing deposits and originating loans, broker-dealers taking both buy and sell positions between opposite customers orders and clearinghouses standing between each leg of a duplicated derivative contract. In contrast to traditional markets, the main sources of transaction cost in finance results from information frictions. In particular, two forms of information asymmetries limit market efficiency.

The first source of friction relates to *information that requires technological investment in order to be efficiently collected*. Such a setting involves monitoring and screening technologies to assess risk levels among investment opportunities. For example, in a classical model of delegated monitoring, Diamond (1984) shows that investors may prefer to first lend to intermediaries who then lend to borrowers, instead of lending directly. The reason for this is the presence of information friction when a borrower's incoming cash flows are private information. It is therefore the borrower's decision to truthfully reveal cash flows to her investors, or not. She could for instance choose to reveal lower global returns in order to reduce the share of investors' return. By investing in a costly monitoring technology, a financial intermediary can observe the realized cash-flow while economizing on monitoring costs. Leveraging monitoring activity, economies of scale and diversification benefits, intermediation therefore reduces deadweight losses caused by asymmetric information.

A second friction relates to *types of information that require relationship and reputation investment to be voluntarily shared*. Such a setting involves trust building capacity to enable bilateral sharing of proprietary information between contracting parties. For instance, results from Bhattacharya and Chiesa (1995) and Yosha (1995) show that in presence of proprietary information, borrowers may prefer to engage with financial intermediaries (e.g., bank-client specific relationship) rather than entering multilateral trading in order to avoid disclosing private information which may leak to competitors.[6]

The ensemble of solutions to these information frictions broadly relates to ex-ante monitoring in order to minimize adverse selection, interim monitoring in order to minimize moral hazard and ex-post monitoring in order to reduce costly state verification. Intermediaries therefore contribute to the economy by specializing in reducing one or several of these frictions because, doing so, they can improve the overall allocative efficiency in financial markets.

Note that the literature on financial intermediation traditionally contrasts the role of institutions with the role of capital markets. DeFi however implies a wider range of intermediation services: it encompasses any form of activity that stands between end-customers of a financial contract and that could exert economic power over them. This broader definition therefore includes market infrastructure services like payments as well as portfolio and risk management services.

---

[6] Similar arguments can be found in general for private individuals unwilling to make private information public, as documented in the literature review on privacy by Acquisiti, Taylor and Wangman (2016)

In this report, we harmonize this distinction by arguing that market failures due to information frictions hold in any type of financial interaction. For instance, payment systems also feature information frictions when clients value the privacy of their payment activity. Payment intermediaries therefore constitute solutions to a transaction cost problem. As such, we consider that information frictions sources the existence of all forms of intermediation - albeit at different intensities.

The cost of intermediated financial markets

The economics of intermediation often features economies of scale and scope (Bergera and Mesterm, 1997).[7] As such, the structure and organization of intermediated markets is naturally driven towards concentration and centralisation.

For financial products relying on *costly verification and monitoring technologies*, such technologies typically feature large investment costs and private information, leading to natural oligopoly conditions for specialized (incumbent) entities. In a model of asymmetric information in banking, Dell'Ariccia (2001) for example shows that banks gather proprietary information about their clients, acquiring an advantage over potential entrants. Contrary to traditional models of horizontal differentiation, the resulting market structure is characterized by a finite number of banks even in the absence of exogenous fixed costs.[8]

For financial products relying on *sensitive and private information*, reputation building and switching costs can be high. The number of entries once markets mature may therefore become naturally limited. Worse, markets may simply not exist when such cost is too high. An important additional implication of sensitive information - in payments for example - is the emergence of strong network effects (i.e., the increased benefit for users to join the system with the largest pool of other users): because information sharing is costly, everyone could benefit from coordinating with the same intermediary. Under simple conditions, this solution minimizes the cost of sharing information while maximizing economic interactions. Such an outcome can further exacerbate switching costs and natural monopoly conditions.[9]

In each of the cases reviewed above, the risk that a limited number of financial intermediaries end up accumulating large market power is high and often realized. By limiting entry of newcomers and competition overall, the resulting market structure may in turn reduce incentives to innovate and limit market efficiency, thereby lowering the overall growth potential of financial systems. In payment systems for instance, Li, McAndrews, and Wang (2020) have recently documented that the large market power accrued to credit card providers was key to the relatively low historical rate of adoption in digital payments both because of the rent extracted from merchants and the lack of investment in research and development by incumbents payment platforms.

In addition to the costs of concentration from a pure competition perspective, intermediation also complicates the overall economic picture because of financial stability concerns: while promoting greater competition may be good for (static) efficiency, its effect on financial stability is ambiguous. The underlying reason is that competition might push intermediaries to seek extremely risky investments in order to compensate for losses in rent-extraction capacities.[10] As stated in the seminal work of Allen and Gale (2004): “In general, the relationship between competition and stability is complex: sometimes competition increases stability. In addition, in a second-best world, concentration may be socially preferable to perfect competition and perfect

---

[7] Further details on the role of monitoring technologies in economies of scale and scope are provided in Section 2.1 from Freixas and Rochet (2008).

[8] For a review on the literature on information acquisition and financial market structure see Chapter 4 in Vives (2016).

[9] Payments systems are a standard example of multi-sided platforms with strong network effects and severe consumer welfare concerns. A landmark reference in this area is the work of Rochet and Tirole (2003). See Rysman (2009) for an extensive overview on the topic and Tirole (2015) for a public policy discussion.

[10] For a full introduction to this tension, see Vives (2016).

stability may be socially undesirable". The rise of too-big-to-fail financial institutions and the policy conundrum regarding their treatment epitomizes the financial stability trade-off imposed by the gains and risks associated with large financial intermediaries.[11]

While the nature of information frictions in financial markets requires the presence of financial intermediaries, the resulting market structure introduces complex interactions between market efficiency and financial stability. As such, a long history of policymaking has been devoted to the implementation of intervention in order to strike the adequate trade off between market failures and systemic collapse.

Traditional policy approach to financial intermediation

Historically, government intervention and public policies have been the main solution to limit market failures and promote growth, integrity and stability in financial markets. In particular, financial intermediaries - as a result of the ambiguous role discussed above - have generally been the main focus of public authorities. A standard approach to the regulation and supervision of financial markets has therefore been the setting of rules to guide and delimit the scope and behavior of financial intermediaries. Classic examples include capital requirements, liquidity ratios, rate controls, know-your-customer rules and anti-money laundering detection settings.

From an information perspective, regulation therefore assigns financial intermediaries as (1) prime holders of verification and monitoring technologies and (2) licensed collectors and holders of private information (e.g., payment history and personal data) - which they can only disclose to designated authorities or on under their clients' consent. In turn, an important part of both regulation and supervision has been devoted to ensuring a proper treatment of such information by intermediaries.

[11] See Strahan (2013) for a global overview of the causes, consequences and policy implications of too-big-to-fail financial institutions.

3. The rise of Decentralized Finance

Demand for and supply of alternative solutions

Over the past few decades, two forces - one of demand and one of supply - have paved the way for an alternative setting to the traditional financial system. The first can be seen as a demand-side force driven by numerous crises (financial, political, etc.). The globalization of the modern economy and some of its adverse effects have indeed fueled concerns and fears about the accumulation of arbitrary power by financial and political institutions. The main sources of concern include: financial exclusion, market manipulation, process opacity, inefficiency of financial payments and rent extraction (cross border, credit card etc.), centralized control (custody of assets etc.) and systemic risk.[12]

The second force can be seen as a supply-side positive shock following progress in digital technologies. Research and development in technologies such as telecommunication - both infrastructures and communication protocols - data management and cryptography have produced ground breaking solutions for the treatment of information friction problems in general leading to massive drops in transaction costs.

Demand for rethinking the role of intermediaries is therefore meeting technological opportunities to address traditional failures of financial markets, in particular, the frictions of the kind discussed in the previous section. It is according to this context that financial services relying on distributed ledger technologies such as Bitcoin and Decentralized Finance protocols enter the picture.

Decentralized Finance (DeFi) relies on publicly distributed ledgers and automated digital (smart) contracts to provide financial services without requiring the presence of intermediary agents. As such it offers an alternative view to the traditional model of financial intermediation which grants central authorities privileged rights such as controlling access to markets, information and asset holding. Supporters of DeFi argue that such an alternative should alleviate demand-side concerns such as financial exclusion, market manipulation and opacity (Harvey, Ramachandran and Santoro, 2021).

Principles of DeFi

Below we present an overview of the basic principles of DeFi and review the main current applications.[13]

Distinguishing features

DeFi is distinguishable from traditional finance in at least four fundamental ways:

1. Universal access: No single entity has authority to bar entry of any participant. This applies to all sides of a financial service including users, developers, validators, etc. This feature contrasts with several traditional financial services which require screening of customers or licensing of service providers. In particular, DeFi services rely on pseudonymous identities which therefore allow anyone to create an address at zero cost and preserve it in order to participate in services without facing discriminatory rules against their real identity.[14]
2. Transparent and deterministic rules: Contracts and infrastructures supporting DeFi solutions are coded in public and autonomous scripts (i.e. smart contracts). This feature contrasts with traditional finance where contracts can be private and rules subject to arbitrary decisions.

---

[12] See Chapter 1 in Harvey, Ramachandran and Santoro (2021).

[13] More extensive presentations on the matter are provided by Harvey, Ramachandran and Santoro (2021), WEF (2021), Schar (2021) and IMF (2021).

[14] For more information, see Narayanan et. al, (2016).

3. Non-custodial services: Holders of crypto-assets in a DeFi process have full control over the treatment of their assets once they are associated with holders' public addresses. This feature contrasts with the traditional use of custodial services by financial intermediaries to manage their clients' portfolios.
4. Interoperable and composable protocols: DeFi protocols can be combined and interfaced at will to generate new solutions. The capacity to freely interoperate digital services and seamlessly interface protocols is intrinsic to the open and public nature of DeFi protocols. This feature is inherited from the legacy of open source systems in computer science. As such, there is no direct mirror of such a dynamic in the traditional financial system.

It is relevant to note at this stage that three out of these four features imply a change in the organization of information when compared to traditional financial services. Pseudonymity entails a change in identification and activity consolidation. Contract transparency translates into a strictly public means of operating financial services. In turn, universal access and public information allows for composability and integration of financial services by freely interconnecting protocols according to their exact mechanisms which are publicly accessible. We investigate further the implications of such structural shifts in the next Section. Before that, let us first illustrate the role of DeFi's four distinguishing features by reviewing the main areas of application for DeFi services.

Main financial services

The main DeFi services are currently structured around the following products:

- Stablecoins: Specific crypto assets which maintain a stable value vis-à-vis a given asset (e.g., US dollar). Major protocols include USDT by Tether[15], USDC by Circle[16] and Dai by MakerDAO[17].
- Decentralized Exchanges: Automated market makers which allow users to trade tokens and supply liquidity to trading pools through smart contracts. Major examples include Uniswap[18], Sushiswap[19] and Curve[20].
- Credit: Credit services mainly provided by pools of liquidity which are either collateralised or instantaneous (flash loans)[21]. Major protocols include Compound[22] and Aave[23].
- Derivatives/Insurance: Derivatives services including futures, perpetuals and synthetic exposure to crypto or real assets. Similar to credit, most of these services are provided by liquidity pools with collateralised positions. While insurance services are less developed at the time of writing, the initial offering follows from similar mechanisms based on the identification of a predetermined event. Major protocols include dYdX[24] and Synthetix[25].
- Portfolio management: Asset management services allowing customers to integrate pools of assets - so-called 'vaults' - governed and managed by predetermined rules encoded publicly into smart contracts. Major protocols include Set Protocol[26] and PieDAO[27].

---

15 https://tether.to/
16 https://www.circle.com/en/usdc
17 https://makerdao.com/en/
18 https://uniswap.org
19 https://www.sushi.com
20 https://curve.fi
21 Instantaneous loans are called *flash loans*. They are loans for which both issuance and reimbursement take place within the same validation block.
22 https://compound.finance
23 https://aave.com
24 https://dydx.exchange
25 https://synthetix.io
26 https://www.tokensets.com
27 https://www.piedao.org

The DeFi stack

The structure and composability potential of DeFi applications can be illustrated through a stack decomposition (Schär, 2021). In the context of this report, the layers of interest are:

- Settlement layer which manages the ledgers by recording changes to the state of the blockchain (e.g.,payments) and sets incentives for validators to maintain the chain (e.g., process transactions).
- Token layer where crypto-assets are created. This includes fungible and non-fungible tokens like stable coins, governance token, etc.
- Application layer where most DeFi protocols are integrated as they rely on both settlements and token layers to execute their associated smart contracts. This layer contains applications for services such as credit, decentralized exchange, asset management and derivatives.[28]

[28] According to Schär (2021), there are separate application layers for frontend and backend solutions. While backend solutions exist in the form of smart contract protocols, frontend solutions exist in the form of software applications and aggregation services. This report focuses on the backend aspect of application (i.e., the economic design). It is however important to note the existence of additional areas of development in the frontend part of applications which are not covered in our analysis. More information can be found in Schär (2021) and WEF (2021).

4. An information view of DeFi

Section 2 of this report has argued that financial interactions are subject to information frictions leading to market failures. As a result, financial systems have traditionally relied on specialized entities (i.e., financial intermediaries) to acquire information and remedy such frictions. The determination of market efficiency and stability was therefore shown to require an understanding of the information structure upon which financial intermediaries rely. In general, this connection between information structure and market dynamics has provided a rationale for the design of regulatory frameworks in standard financial settings.

Following this traditional approach and in view the nature of DeFi systems presented in Section 3, a natural question arises: how do DeFi services differ in their treatment of information frictions? We address this question by analyzing the information design underpinning DeFi protocols and the deviations from traditional structures. Doing so provides us with an integrated view of both traditional and DeFi systems. Furthermore, this information centric approach will support an assessment of the potential role DeFi holds with standard public policy targets such as economic growth, market integrity, consumer welfare and financial stability

The economics of information in DeFi protocols

DeFi leverages distinguishing information features such as pseudonymity and transparency in order to produce financial services that do not require the presence of financial intermediaries. The resulting shift in information structure sheds light on the scope of DeFi applications, their risk and the appropriate policy approaches.

In a traditional economic setting, the execution of contracts is determined by the set of observable and verifiable information upon which contracting parties can rely. A standard template would for instance consider the following scheme: should event X occur, party A receives Z EUR from party B, where X is an observable and verifiable event. The verifiability of information on event X matters to guarantee outcomes: in case of a dispute among parties, the court will verify information on X to fix the situation and execute a final judgment. Note that in traditional settings, this information could initially be either public or private. As long as the information can ultimately be accessed by the court, the contract can be implemented.

In contrast to this template, DeFi settings require that the execution of contracts be objective, automated, final and free from any central authority's arbitrary decision. Such smart contracts therefore require information that is strictly publicly verifiable and immediately accessible at the time of execution. As a result, the scope of application for DeFi smart contracts (i.e., contracting space) is directly bounded by the information structure they rely upon.

Contracting spaces and information structure

In order to generate contractible information (i.e., public and verifiable), DeFi leverages a combination of cryptographic technologies and incentive compatible designs. For example, cryptographic signing solutions allow one to publicly prove ownership of an asset without having to reveal her own identity. The resulting pseudonymous system bears a binary information structure: either information is public and verifiable (e.g., transactions history recorded in the blockchain) or information is not observable nor verifiable (e.g., private identity). Formally, this information structure gives rise to a ‘smart contract challenge’ (Gans, 2019). On the one hand, permissionless distributed ledgers (e.g., Blockchain) reduce the cost of verifying information stored on the ledger (Catalini and Gans, 2020). On the other hand, information outside the ledger

becomes infinitely costly to verify, in principle. As a result, the cost distribution among observable and verifiable information determines the contracting space for DeFi protocols.[29]

As a result, the contracting space of smart contracts is theoretically bounded by information stored on the ledger. Such information structure is in stark contrast with the one financial systems traditionally rely upon, that is, where verifiable information may be hidden from the public yet privately accessible by a given authority for execution or in case of dispute. Much of the development of DeFi services hinges on the capacity to generate as much public and reliable information as possible while satisfying constraints such as privacy and verifiability.

The table below illustrates the distinctive contracting spaces upon which traditional finance and DeFi systems rely. Information is split according to three sets: public information accessible to everyone, private information with conditional access and private information with no external access. We obtain the following difference between traditional finance and DeFi.

- By virtue of pseudonymity, identity-related information cannot be contracted upon in DeFi.
- By virtue of transparency, any activity on DeFi is public and can be contracted upon.

Note further that most of the contracting activity in traditional finance takes place in the private yet conditionally accessible part. In contrast, DeFi contracts strictly occur in the public space.

TABLE 1 - Information structure and contracting spaces

	Information		
	Private		Public
	Not accessible	Conditionally accessible	
Traditional		Contracting space	
Examples	Effort	Identity, Transactions	Price
DeFi			Contracting space
Examples	Effort, Identity	∅	Transactions

Differences in the structure of information have deep implications in terms of market dynamics, some structures allowing for economic forces absent in other settings. To illustrate the effect of the information shift on the economics of financial markets, let us revisit the first embryonic DeFi application: the Bitcoin payment system.

The role of information structure: the case of digital payments

Implementing a digital payment system requires the following capacities:[30]

- Compute account balances
- Prevent stealing: only the sender can initiate payment
- Prevent denial of service: no one can prevent a valid payment request
- Prevent double spending

To satisfy this agenda, a digital payment system therefore requires information on:

- Sender and receiver account addresses
- Signatures to certify origin sender

[29] An interesting parallel exists with the co-development of smart contracts and the internet of things (IoT). Halaburda and Bakos (2019) extend the arguments of Gans (2019) and show the impact of changes on verifiability on the contracting space for smart contracts.

[30] See Narayanan et al. (2016) for a detailed presentation of payment system requirements and the bitcoin solution. Note that we here envision the strict minimum requirement for a payment system and abstract from KYC/AML types of requirements

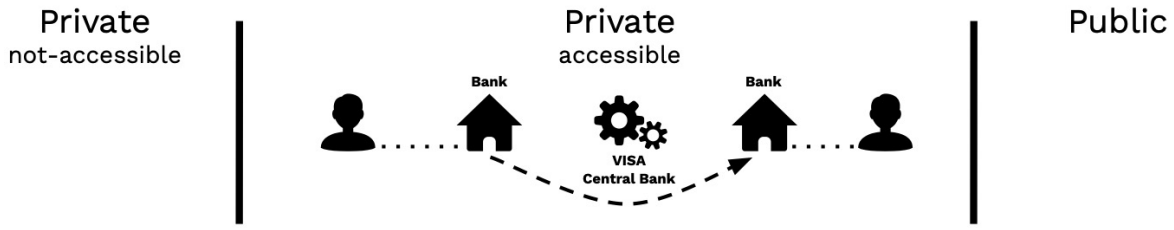
- Transaction history to compute balances and prevent double spending

The first historical application of crypto-economic systems and a precursor to the rise of DeFi has been the so-called Bitcoin payment system. One of the fundamental value propositions introduced in the Bitcoin White Paper has been the way information could be re-organized to enable digital transfers while retaining privacy in absence of a centralized authority (Nakamoto, 2008).

In fact, a key friction to digital payment systems lies in the privacy value of transaction information: the default scenario should assume that users do not want their entire transaction activity to be public. Traditional payment systems and the Bitcoin model offer two different solutions to this problem.

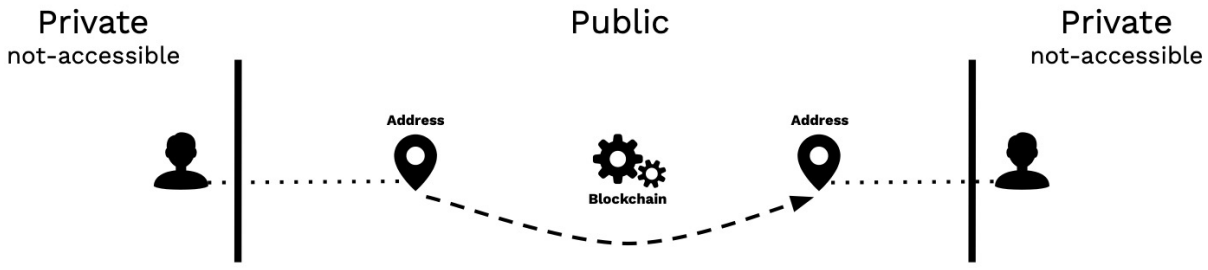
- In a traditional digital payment, the information is concealed to the parties involved along the payment chain (i.e., sender, sender's bank, payment system, receiver's bank, receiver). Information on a given transaction is not accessible to third parties unless permission is granted (e.g., government intervention or client release of information to third party apps). The information structure is illustrated in Figure 1.

FIGURE 1 - Information structure in traditional digital payments



- In Bitcoin, the information is split into two distinct sets. On the one hand, all transaction-based information is public and stored on the distributed ledger. As such, everyone can observe and verify information about a transaction (e.g., value, timing, sender and receiver addresses). A payment service is therefore possible and implementable according to our list of information requirements. On the other hand no one can observe any other form of information (e.g., identity of parties, items purchased, etc.). Figure 2 below illustrates the related information structure.

FIGURE 2 - Information structure in the Bitcoin payment



The distinct approaches followed by traditional payments and Bitcoin solve the privacy problem in different ways: the former relies on a trusted third party to hide information from public access while the latter segments between public activity and strictly not-accessible private identity.

Importantly, this shift in information structure has implications for the organization of payment markets. While the traditional solution allows more information to be stored in the system and therefore to be contracted upon, it provides natural avenues for the service provider to exert market power and extract rent at the expense of consumers. In fact, unregulated markets for

traditional payment are text-book cases of market failure in terms of competition and consumer welfare.[31] Importantly, the lack of market contestability is particularly driven by the fact that transaction information is traditionally held exclusively by the payment provider and that payment systems are in general not interoperable. Several public interventions have taken place across the world - in particular Europe - to prevent market abuses and consumer harm in such industries.[32]

Bitcoin offers a contrasting solution. Because all the necessary information to run payments is public, the provisioning of payment services (e.g., validating transactions) can be done in a competitive setting with (theoretically) free entry, while benefits from network effects still accrue to users (Catalini and Tucker, 2019). The price for validating transactions is no longer determined by a single entity but rather subject to competitive forces in the market for miners (i.e., validators).[33] Such vertical disintegration of payment service necessarily requires a distributed ledger with public information on transactions (Aymanns, Dewatripont and Roukny, 2020). Note however that even though distributed ledgers might enable competition for services which traditionally were conceived of as natural monopolies, this is not a guaranteed outcome. Continuous increase observed in the concentration of mining power in Bitcoin illustrates that distributed ledgers are a necessary but not sufficient condition to obtain strong competition in those markets (Bakos, Halaburda and Mueller-Bloch, 2021).

Comparing both payment systems, the following Table 2 showcases how each approach generates different implications vis-à-vis the tension between information structure and efficiency:

TABLE 2 - Comparing traditional payments and Bitcoin

	Solution to information friction	Welfare gains	Welfare losses
Traditional Payments	Private information only accessible to authorized service providers	- Liability of parties in case of wrongdoing - Dispute resolution and remediation possible	- Market power and centralized control - Lack of innovation
Bitcoin	Transaction information is public while residual information is private and not accessible.	- Competition forces to reduce service rent - No arbitrary control - Incentives to innovate	- No dispute resolution - No access to private information

Building on the achievement of Bitcoin, next generation protocols under the DeFi umbrella are deploying alternative solutions to the rest of the financial domain. In fact, since the introduction and wide adoption of smart contract frameworks introduced by Ethereum, DeFi designers are now able to attach an infinite set of conditions to future payment flows between multiple parties. These opportunities constitute the fundamental ingredients of most financial products and

[31] As discussed in Section 2, the strong network effects associated with payments give rise to natural monopoly conditions.

[32] See Tirole (2015) for a discussion on the policy implications of network effects in payment systems and the policy interventions in the EU. Further details on the modeling and economics of such markets can be found in Belleflamme and Peitz (2021).

[33] For instance, Prat and Walter (2021) show that free entry places competitive pressure on miners. In another work, Aymans, Dewatripont and Roukny (2020) study how competition in the provisioning of payment services affects consumer welfare when compared to traditionally 'integrated' payment systems.

services including market making, credits, derivatives, insurances, etc. However, while Bitcoin has demonstrated that a digital and disintermediated environment could replicate payment services in a more competitive setup, it does not directly hold that all other types of financial activities will follow suit. In particular, information requirements for other forms of financial activities may strongly differ from the ones required for payments.

Below, we present a classification of DeFi protocols according to their information structure and discuss how such constraints affect their scope of applications.

A taxonomy of DeFi protocols

In view of the role played by information frictions in determining the feasibility and efficiency of financial services, we propose to classify DeFi protocols according to their underlying information structure. Information structure here is defined as the ensemble of data required by validators to execute a given smart contract. In other words, the relevant information set is the necessary input required to prove an outcome according to the rules of a given protocol.

Given the rich and complex state of the DeFi ecosystem, a protocol's information structure can presumably be articulated at different levels. For instance two protocols might differ because they operate on different chains (e.g., settlement layers) or because they relate to different applications attached to the same chain (e.g., different tokens on the same settlement layer). Yet both types of protocols might conceptually implement the same class of information structure. As such, when we compare protocols from an information viewpoint below, we focus on the nature of the data they require for the proper execution of their related smart contracts.

Our simple taxonomy considers three categories of protocols:[34]

- Autarkic protocols which strictly rely on verifiable information produced under their own activity
- Crossing protocols which strictly rely on verifiable information produced by a set of protocols
- Off-chain protocols which weakly rely on unverifiable information

Such a classifier allows for a separation between different forms of economic and financial activity which in turn will help identify different forms of market failure and support appropriate roles for public action.

Autarkic protocols

Autarkic protocols are *internally consistent protocols* which rely strictly on information produced under their own activity, which is therefore fully verifiable. To execute contracts, validators collect information strictly accessible through the protocol's ledger of past transactions. In other words, the protocol only trusts itself. Financial services are in turn produced by exploiting three features of DeFi: transparency (for validation and consensus), universal access (using pseudonymous identities) and non-custodial ownership (through the account of ownership in the distributed ledger). This class of protocol typically applies to on-chain settlement layers.[35]

Example: The leading figure of autarkic protocols is Bitcoin as previously discussed in this Section.

[34] Systems described below could in principle be permissioned or permissionless. Given the scope of this report, we consider a permissionless setting by default.

[35] Another case of autarkic protocol is a protocol that issues a token on a settlement layer (e.g., an ERC 20 token on the Ethereum blockchain) but restricts validation to its own set of rules and where these rules would strictly rely on fully verifiable information from the point of view of the protocol itself. As such the protocol's ledger constitutes a subset of the settlement layer's main chain filtered by changes which can only be sourced from the protocol's own activity. The protocol is therefore autarkic because it would reject any activity which relies on information stored in the settlement layer that would have been produced by any other protocol.

Discussion: The information required to implement Bitcoin rules is self-contained in the ledger that the Bitcoin protocol operates and maintains. All validating parameters are internal to the protocol. For instance, the consensus protocol requires verification of transactions in previous blocks of the ledger. Also incentives for validation (e.g., block reward) are computed from the ledger's own activity (e.g., hash rates).

Autarkic systems can proceed with few information requirements (e.g., the information set required by a minimal payment system discussed previously in this Section). From the protocol's perspective, the main limitation is that information has to be produced and collected under the protocol's own ledger (which may constitute a filtered version of a larger chain). This has a cost when it comes to the scope of application for autarkic protocols. For instance, autarkic protocols cannot handle identity information nor can they handle price information. The former also implies that reputation schemes are not implementable because of the cost-free entry of pseudonymous identities (e.g., sybil attacks). The latter is not feasible because it requires exchange information related to the end-purchase of transactions which is not verifiable from the ledger.

From this information-based analysis, it results that protocols relying exclusively on information which is only recorded under their own activity and authority have limited applications and contributions to provide the economy and the digital finance ecosystem.

Figure 4 illustrates the information structure of autarkic protocols and Table 3 summarizes the scope of application of these protocols. We next consider two extensions that unlock opportunities for financial contracting and growth.

FIGURE 4 – Information structure of autarkic protocols

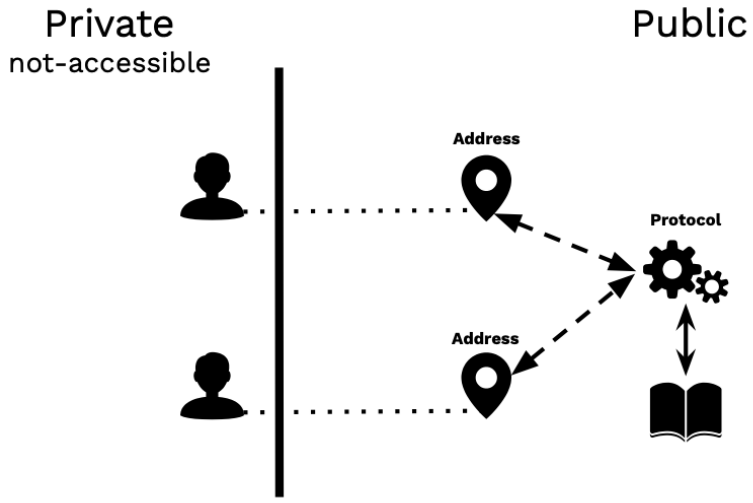


TABLE 3 - Contracting space for autarkic protocols

Autarkic protocol		
Financial service	Feasible	Not feasible
Payment and exchange	Payment with native token Example: Bitcoin	Any exchange* Requirement of at least two assets to swap Any stable coin Requirement of price information
Credit	∅**	Any Requirement of either liability or collateral

Derivatives and insurance	∅***	Any Requirement of information on price or external event
Asset management	∅	Any* Requirement of at least two assets to manage

* We assume that an autarkic protocol can credibly commit to operate through a unique token
** Flash loans are theoretically feasible in an autarkic system but their value is unclear which limits their applicability.
*** Derivatives and insurance contracts are theoretically feasible in an autarkic system but their value is unclear which limits their applicability.

Crossing protocols

Protocols can expand their contracting space by increasing the underlying set of publicly verifiable information. This is achieved when a protocol crosses information with other protocols. In this setting, the protocol accesses information stored in a network of information sets (e.g., ledgers) operated by a set of other protocols and its own. The other protocols can either be crossing protocols themselves or autarkic protocols which ensures that any information they produce can be publicly verifiable. Formally, such protocols can be defined as *λ-consistent protocols* where λ indicates the set of protocols from which the protocol sources all contractible information, that is, all the information required to validate the execution of a transaction/contract is accessible from the union set. This family of protocols applies at different levels:

- A protocol may be a *crossing* protocol because it is a multi-chain or a cross-chain protocol, that is, it relies on information stored in multiple chains (e.g., multiple autarkic protocols).
- A protocol may also be a *crossing* protocol because it integrates information stored by other protocols on the same chain (e.g., tokens on the same settlement layer or aggregation layer as per Schär (2021))

In both cases, the protocol extends its information structure by integrating activity from other protocols, thereby expanding its contracting space compared to an autarkic protocol while ensuring that all information remains publicly verifiable.

This category of protocols exploits the DeFi features of autarkic protocols and the interoperability of DeFi to interface with outputs from other protocols.

Example: Decentralized Exchange (DEX) designs such as the first version of Uniswap are examples of crossing protocols.[36] These systems allow users to swap between pairs of tokens held in a common pool. Such protocols integrate other protocols such as the protocols related to each exchangeable token and their respective ledgers. Importantly, Version 1 oft Uniswap DEX is a Constant Product Automated Market Maker (CPAMM) where the pricing is internally determined through a constant product function:

$$x * y = k,$$

*w*here *x* and *y* are quantities of two different tokens and *k* is a constant parameter. The price for each token is derived from the formula to maintain quantities accordingly.

[36] These DEX correspond to the initial Reddit proposal made by Vitalik Buterin on the construction of on-chain automated market makers with constant product function.

Uniswap is an example of on-chain *crossing* protocol where the set of protocols are all related to the same settlement layer (Ethereum). Other applications like Anyswap[37], follow the same principle applied cross-chain, that is, across multiple settlement layers including Bitcoin, Ethereum, Litecoin and Ripple.

Discussion: The information required to validate activity on a Constant Product Automated Market Maker (CPAMM) relates to

1. At least two tokens (x and y) for which crossing access to the ledger is granted in order to verify ownership and execute transfers
2. An arbitrary constant variable set by the protocol (k)

Price adjustments are expected to be achieved through the participation of arbitrageurs. Hence no external pricing information is required on the part of the protocol. As such, these protocols are based entirely on public and verifiable information produced by an ecosystem of protocols including themselves.[38]

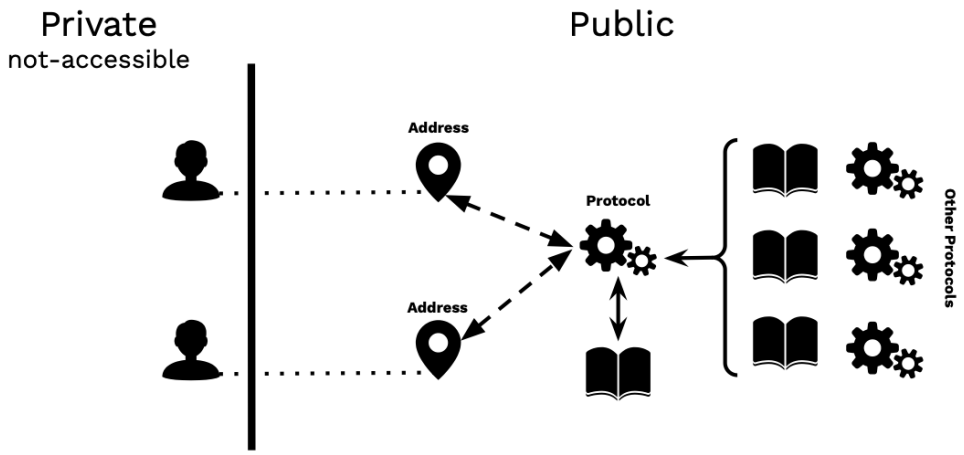
Compared to autarkic systems, crossing protocols extend the possibilities of financial application by extending the information set to the aggregate information produced by multiple protocols in terms of activity, ledger or tokens. Doing so allows crossing protocols to

- Verify ownership of multiple tokens
- Execute transfers and exchanges, thereby producing price information where the price has to be associated bilaterally among the λ-tokens
- Verify more complex events such as default, liquidation, etc.

While the scope of financial products that can be created through crossing expands the autarkic case in depth and complexity, it however remains limited to activities whose information remains publicly verifiable. In addition, crossing protocols are similar to autarkic protocols in that they remain strictly pseudonymous and therefore cannot handle identity information nor can they handle external price information. In fact, from the point of view of validators within the crossing protocol, both such items remain unverifiable information.

Figure 5 illustrates the information structure of crossing protocols and Table 4 summarizes the scope of application of these protocols.

FIGURE 5 - Information structure of crossing protocols



[37] https://anyswap.exchange/

[38] Recent studies formally assess the inefficiencies and vulnerabilities as well the opportunities present in CPAMM protocols, e.g., Park (2021), Capponi and Jia (2021) and Lehar and Parlour (2021)

TABLE 4 - Contracting space for crossing protocols

Crossing protocol		
Financial service	Feasible	Not feasible
Payment and exchange	Payments and exchanges within and across the λ-protocols Example: Uniswap V1	Exchange Which requires token outside the set of λ protocols Stable coin* Which is backed by fiat and other securities which requires unverifiable information
Credit	Flash loans Example: Aave	Loans** Which requires external collateral or external price information or counterparty risk
Derivatives and insurance	(limited) any contract contingent on an event in the set of λ-protocols	Any contract Which requires event information outside the set of λ protocols
Asset management	(limited) any management strategy among the assets of the the set of λ-protocols	Any management Which requires return information outside the set of λ protocols
* Stable coins are theoretically feasible in a crossing system with algorithmic stability pegged to a λ-consistent value. However their value is unclear which limits their applicability. ** Collateralized loans are theoretically feasible in a crossing system with assets attached to the set of λ-protocols. However their value is unclear which limits their applicability.		

Off-chain protocols

So far, contracting spaces have been mainly limited by the constraint that information had to be publicly verifiable. Off-chain protocols do not abide by this limitation. In this setting, the protocol accesses information publicly verifiable - as a crossing protocol would - as well as information submitted by external providers whose input cannot be formally verified on the ledger. Such a protocol is *δ-conditionally consistent* where the conditional validity of unverifiable information relates to δ external sources. External sources of unverifiable yet contractible information are referred to as *Oracles.* Note that off-chain protocols exploit the same DeFi features as for crossing protocols (transparency, universality, non-custodial and composability) but lose consistency in their verification power.

Example: Decentralized lending protocols such as Compound are an example of off-chain protocols. In such a setting, a pool of liquidity is provided by suppliers of tokens in exchange for earning interest (i.e., lenders). Borrowers obtain credit from the pool by posting collateral in the form of another token. Granting loans is conditional upon the relative value between collateral posted and borrowed funds.There is no maturity. As long as the collateral ratio is above a certain threshold determined by the protocol, usually around 200%, the loan is maintained and interest accumulates. Therefore a loan terminates either when the borrower reimburses the principal and the interest, or when the collateral ratio is below the threshold. In

the latter case, the position is liquidated. While computation of the interest rate is internal,[39] tracking of the collateral ratio requires pricing information on the value of both the collateral token and borrowed token. As such the protocol's smart contract interfaces with price feed oracles to acquire the input necessary to identify liquidation events.

Discussion: Granting a loan with positive maturity is feasible in this protocol because it can access collateral. Hedging counterparty risk is guaranteed as long as the relative value of the supplied collateral satisfies the given threshold. However, the economic value of the collateral is subject to changes that are exogenous to the system (e.g., demand in the real economy). Therefore the protocol interfaces with external information providers. As such, the pricing information becomes observable and contractible. However, it is not verifiable at the moment of execution.

When protocols interface with oracles (i.e., off-chain inputs) the scope of financial activities that can be replicated in the DeFi economy becomes theoretically unbounded. However, off-chain mechanisms introduce a new factor to consider growth, welfare and stability: the treatment of oracles.

Oracles can be of many forms as long as their outputs are machine readable: information scraper, human analysts, IoT sensor, public documentation, etc. For off-chain protocols, the capacity to develop new financial contracts becomes complementary to the development of efficient oracles to feed in the necessary information. In contrast with validators, oracles cannot be programmatically prevented from cheating because the information they provide cannot be verified by validators. As such the economics of oracles in turn requires careful attention. Furthermore, a decentralized system depending on a centralized source of information is subject to important threats of manipulation and misbehavior.

Note that, conceptually, several other services can be mapped into an oracle-based service. For instance the onboarding of users by centralized exchanges and wallet providers embeds with them an oracle information on their information credentials. As such the KYC and AML value of customers can be transmitted to protocols. More generally, initiatives to support the development of KYC-token are forms of oracle interfaces which link protocols to the off-chain classification. We discuss this aspect further in the next sections.

In terms of application scope, off-chain systems theoretically entail everything that exists in the real world provided that an oracle system allows for it. Figure 6 illustrates the information structure of crossing protocols and Table 5 summarizes the scope of application of these protocols.

[39] Interest is determined by the amount of supplied and borrowed tokens in a particular market. Interest paid by borrowers equals interest earned by lenders and rates are calculated per block. A standard way to compute interest follows the equation Borrowing Interest Rate = a + Borrows /(Supplies +Borrows)*b where a and b are ratio parameters whose exact value is determined through the protocol governance. More information on https://compound.finance/documents/Compound.Whitepaper.pdf

FIGURE 6 - Information structure of off-chain protocols

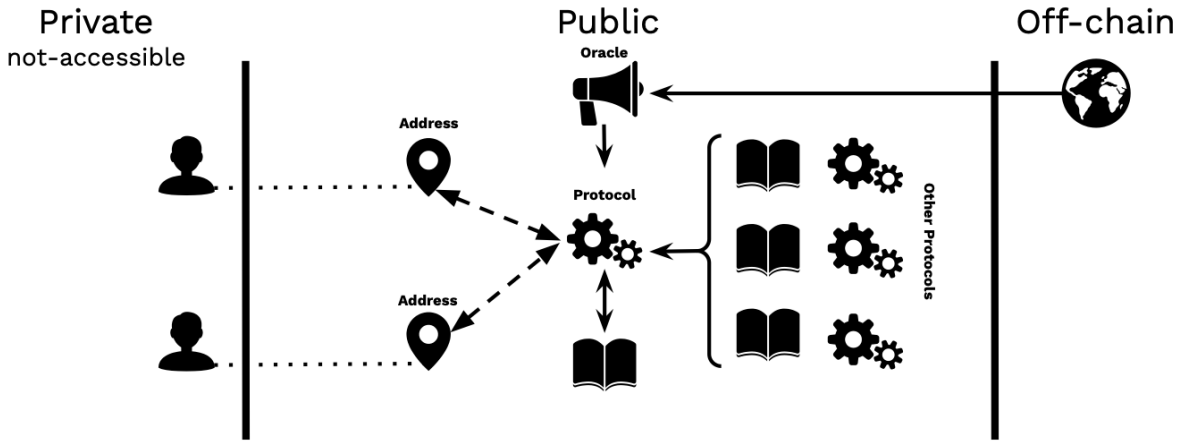


TABLE 5 - Contracting space for off-chain protocols

Off-chain protocol		
Financial service	Feasible	Not feasible
Payment and exchange	Any Example: DAI stablecoin, Bancor V2	∅
Credit	Any Example: Compound	∅
Derivatives and insurance	Any Example: dYdX	∅
Asset management	Any Example: Set Protocol	∅

5. Sources of risk and inefficiency in DeFi

Having established the importance of information structures in financial interactions - both for traditional finance and DeFi - we now investigate how information structures relate to different sources of risk and inefficiency for DeFi protocols.

Given the early stage of development in DeFi services, a comprehensive listing of all risks and inefficiencies is premature and unrealistic. In fact, the DeFi ecosystem is expanding rapidly with new challenges and opportunities emerging constantly.[40] This report focuses efforts on identifying clear cases where information frictions generate negative externalities that may in turn result in market failures for DeFi services. Our goal is therefore to demonstrate how the information-centric framework introduced previously can be used to assess when public action may be both warranted and feasible.

- By 'warranted' action, we mean to stress that several sources of risk and inefficiency do not necessarily require public intervention. In fact several major sources of risk in DeFi are continuously being addressed through solutions produced within the DeFi ecosystem itself. As in many other industries, the private sector may constitute a more suitable and efficient vehicle to develop adequate solutions than external interventions. Hence we are here interested in configurations where there is a limit to the production of private solutions and where services exhibiting market failures would likely benefit from public support.[41]
- By 'feasible' action, we mean to stress that only a subset of theoretically warranted actions are possible under the technological constraints imposed by the nature of DeFi protocols. In light of the taxonomy provided above, we will observe that certain treatments may be implemented on a given information structure while not on others.

Importantly, note that the following results are not definite. Rather they constitute a building block to a common effort to identify and organize sources of risk and inefficiency that may exist under different DeFi information structures and design policy proposals that may be adequate to address them.

We proceed in this section by presenting and mapping sources of risks and inefficiency according to our protocol taxonomy. We further discuss frictions and market failures which may call for public support. Importantly, it will be shown that the common thread behind the rationale for public action relates to fundamental information frictions which are unlikely to be treated efficiently by private solutions.

The incremental nature of our taxonomy implies that features and discussions are inherited from one class of protocol to the next. That is, results for autarkic protocols apply to crossing and off-chain protocols as well. By the same token, features of crossing protocols apply to off-chain protocols which also rely on a crossing of protocols. Results from this section are then complemented in the following section by considering candidate policies to address the set of listed issues.

Autarkic protocols

Private solutions

Prominent autarkic protocols are found at the settlement layer (e.g., Bitcoin). In such protocols, there exist several important risks related to the safety and efficiency of the underlying distributed ledger. Settlement risk for example relates to the risk that a given public and valid trade does not

---

[40] For the interested reader, numerous other works provide listings of multiple sources of risk and inefficiency facing DeFi applications including - but not limited to - Harvey, Ramachandran and Santoro (2021), WEF (2021), Schär (2021), IMF (2021), BIS (2021) and IOSCO (2022).

[41] A complementary dimension relates to the possibility of self-regulation inside the DeFi industry. While this configuration exists in many other industries, the private serving benefits have been shown to inefficiently protect the public in absence of any external pressure. However, limited public oversight such as the threat of government enforcement can substantially improve the efficiency of self-regulating organizations (DeMarzo et al., 2005).

get included in any block of the ledger. Congestion risk exists when trading activity increases faster than the supply capacity to process and validate trades in the ledger. Risk of congestion thus implies a level of settlement risk as well as sharp - and potentially unexpected - increases in the cost of validating transactions.

Given the welfare cost of such risks, there is an active community searching to reduce the related frictions. First, the open nature of the DeFi ecosystem means free entry for new solutions to build on previous limitations and directly compete with less efficient or more risky incumbent solutions. New protocols are proposed with encoded solutions to scaling and fee-state designs. Solana[42] and Avalanche[43] are two such protocols with settlement solutions aimed to outcompete Ethereum: both outperform Ethereum settlement speed by orders of magnitude while maintaining transaction fees orders of magnitude lower.

Second, the open source and composable nature of DeFi also allows for technological solutions to patch limitations on incumbent protocols themselves. Layer 2 solutions, for instance, are a family of protocols built on top of Ethereum - which in turn constitutes a Layer 1 protocol - in order to fix settlement and congestion issues. The Lightning Network protocol[44] for Bitcoin or Polygon[45] for Ethereum both propose solutions to speed up transaction settlement and decrease fees leveraging technologies such as *side-chains* and *roll-ups*.

Finally, protocols coded by human beings are always subject to bugs and vulnerabilities. In addition, the transparency of protocols makes the threat of cyber attacks particularly severe. As such, security risk in the implementation of a smart contract is never fully eliminated. This implies both the risk of severe losses and a lack of uptake by risk averse customers even when protocols have high levels of safety. In this context, the growing habit of auditing protocols before deploying constitutes a major step in minimizing risk and fostering adoption. Most major protocols today interact with crypto auditing companies. For instance OpenZeppelin[46] provides security support for the Ethereum Foundation and Compound; ConsenSys Diligence[47] conducts audits for Aave and Bancor; Runtime Verification[48] and Certora[49] have provided formal verification services to Sushiswap, Algorand, Aave and Makey. Growth in supply and demand for such service is a positive sign of sustainable development to continuously address sources of security risk. This practice also increases trust and rates of adoption thereby increasing the efficiency of some activity given the large network effects of several financial services, specially in autarkic protocol cases (e.g., payments).

Market failures

The previous discussion showcases how several sources of friction in autarkic DeFi protocols can and have been addressed by privately generated solutions. However, there remains a number of issues where public action may be uniquely adequate, in particular those where information frictions are key.

One of the major shifts in information structure compared to traditional finance is the pseudonymity of activity in DeFi protocols. Lack of identification limits liability and commitment which in turn reduces the efficiency of contracting mechanisms. Furthermore, pseudonymous features also imply risk in terms of manipulation and abuse that cannot always be treated with cryptographic or decentralized technologies.

As such, rug pulls have been a major source of risk. They also constitute a limiting factor in the widespread adoption of DeFi protocols. Simply put, rug pulls are a type of manipulation where

---

42 https://solana.com
43 https://www.avax.network
44 https://lightning.network
45 https://polygon.technology
46 https://openzeppelin.com/security-audits/
47 https://consensys.net/diligence/
48 https://runtimeverification.com
49 https://www.certora.com/

developers abandon a project and divest investor's money. In their yearly crypto crime report, Chainalysis (2022) estimated that rug pulls constituted the biggest threat to trust in DeFi systems. In fact, such scams accounted for a total of $2.8 billions in 2021, constituting 37% of total identified illicit revenues, up from 1% in 2020.

More generally, the lack of commitment in pseudonymous systems creates a risk that maintenance and upgrade of protocols might be discontinued, irrespective of the intention. Note that here discontinuation costs might be direct or simply triggered by the possibility of *forks*. For instance, disputes over protocol upgrades may lead to versioning conflicts, confronting both users and miners with potential losses should they decide to adopt a least popular fork. For instance, Bitcoin Cash was a fork of Bitcoin which resulted from a long dispute among developers regarding the size of each block in the Bitcoin blockchain. Kwon et al. (2019) showed that this split introduced security and welfare concerns on the least popular fork because of inefficient mining allocations.

Resulting from the lack of commitment is a form of contract incompleteness that limits welfare gains where agents which might benefit from participating in the protocol are reluctant to engage in the first place because of concerns about the future governance of the protocol. Several DeFi protocols attempt to address the issue by decentralizing control. In general however, decentralizing governance can have ambiguous effects. In the presence of contract incompleteness, governance structure and ownership allocation become crucial for welfare. This incompleteness argument directly follows from the seminal work of Grossman and Hart (1986) and subsequent work by Hart and Moore (1990).[50] McAfee and Brynjolfsson (2017, Chap 12) presents a compelling analysis of the role of contract incompleteness for the infamous governance failure of the Decentralized Autonomous Organization (DAO).[51]

Such governance risks are further amplified by the risk of unobservable concentration of power in pseudonymous systems. In fact, for DeFi protocols where governance is operated via governance token, pseudonymity means that while tokens may be held by different public addresses, a single entity may in theory possess all such addresses and therefore all governing power. Other users would have no formal means to detect such underlying concentration directly.

In each case discussed so far, the lack of verifiable information on entities behind public addresses constitutes a barrier to mitigating risks and improving economic efficiency. While it is unclear how private solutions can address and solve these problems, issues of market failures due to lack of committing devices and contract incompleteness have a long history of public policy action. Leveraging such experience for the design of DeFi solutions appears therefore warranted. We discuss this further in Section 6.

In addition, there also exist cases where private and public solutions may be complementary. For instance, dispute resolutions may benefit from both private solutions and public support. Private solutions in the form of incentive compatible mechanisms have been proposed to prevent defection in absence of liability.[52] While such solutions can be compatible with the autarkic design of protocols, allowing for public interactions could help resolve disputes by supporting off-chain verifiable information into the resolution mechanism. Note that some private solutions exist with a recourse to a court-like system (e.g., Chainlink's adjudication systems proposed by Breidenbach et al. (2021) and Kleros' decentralized arbitration service[53]).

Another prevalent concern with DeFi protocols, in particular at the settlement layer, is wash trading. In fact, in absence of private information regarding trades, validators and protocols may be incentivised to issue, promote or be complacent with 'fake trades' in order to induce a false

---

[50] A general presentation of the role of contract incompleteness for governance structure can be found in Hart (1995).

[51] Wald (2016) and BIS (2021) offer additional views on the incompleteness of smart contracts and DeFi protocol governance.

[52] See for example Gans (2019) which adapts a 'simple sequential mechanism' (Moore, 1992) as a mechanism design solution to a smart contract problem with costly verification.

[53] https://kleros.io

sense of demand activity. The result is an increase in prices which may benefit validators, protocol developers and participants all together. Researchers are developing tools to expose such patterns. For example, Cong et al. (2021) study several dozens of centralized exchanges both regulated and unregulated. They identify multiple wash trading patterns depending on the design and regulation of the exchange. In unregulated settings, crypto wash trading accounts for about 70% of the reported volumes. Moving the analysis to purely decentralized protocols increases the identification challenge though. While DeFi protocols provide rich and public data on trading activity, the lack of verifiable information on private information (e.g., trade and address metadata) implies that preventing wash trading purely on the basis of the information structure of autarkic protocols will have limited power. Furthermore, benefits on the part of validators, protocol participants (developers, owners, users) and/or members of the DeFi ecosystem as a whole might also distort incentives to exert the necessary efforts on the part of the private sector to address this issue. Public intervention might therefore be warranted in this case as well.

Finally, activity in DeFi relies on the capacity of entities to prove their ownership of a given public address, typically by signing messages with a private key. The mismanagement of private keys can therefore be detrimental to the well-functioning of DeFi markets. Key management risks such as loss or theft of private keys indeed limit the sustainability and growth of DeFi protocols. In 2018, it was estimated that around 20% of all Bitcoins in circulation were lost in part due to mismanagement of private keys.[54] While there exists a number of private solutions including hardware keys, so called cold wallets such as Ledger[55] and Trezor[56] or crypto-wallet solutions such as DeFi Wallet[57] or Zengo[58], making sure some addresses can recover their private key in a secure way also bears systemic importance. Akin to the systemic role played by certain financial institutions in traditional systems, some addresses might be conceived of as too-big-to-lose. For instance, should a public address accumulate ownership of a significant amount of a protocol's tokens, losing the associated private key would de facto freeze those tokens indefinitely. This would in turn have a significant impact on the protocol's monetary or token issuance policy and disrupt its fully diluted valuation,[59] potentially creating a panic on the protocol performance with no fundamental grounding. Another case would be the impact of a key loss from a major holder of governance tokens or admin key holder which would in turn endanger the well functioning and sustainability of the associated protocol. To solve this issue private technological progress may propose solutions. However, public actions to support an ultimate key management backstop in extreme systemic cases may also play an important part in promoting confidence, efficiency and stability of the DeFi ecosystem.

Crossing protocols

Crossing protocols rely on a set λ of other protocols including themselves to source information into their contracts. This set of protocols can be composed of crossing and autarkic protocols. While the aggregation of protocols generally increases contracting spaces, crossing protocols add sources of risk and inefficiency to the autarkic set through their composability, internal dependencies and layering complexity.

Private solutions

A prime area of development in crossing protocols has been decentralized exchanges (DEX). Current designs for such protocols have been shown to exhibit inefficiencies in pricing (e.g., Parks (2021) and Capponi and Jia (2021)), on top of being prone to front running (Capponi, Jia and Wang, 2022). The rapid pace of protocol upgrades and active academic research in these

---

54 'A fifth of all Bitcoin is missing' – The Wall Street Journal, July 2018
55 https://www.ledger.com
56 https://trezor.io
57 https://crypto.com/eea/defi-wallet
58 https://zengo.com
59 The fully diluted valuation of a DeFi application corresponds to its total market capitalization if all tokens are put in circulation.

domains bears witness to the demand and search for improved solutions. Interestingly, several upgrades to DEX protocols imply a transition from on-chain (crossing) to off-chain protocol classifications (see e.g. version 3 of Bancor and version 2 of Uniswap).

More generally, exchange activity across protocols gives rise to Miner Extractable Value (MEV) risk which is a form of front running intimately linked to the transparent nature of DEX protocols (Dayan et al., 2020). Given the adverse effect of such risk on economic value - as users become reluctant to engage in fear of getting their trading opportunity stolen - several initiatives are under way in different protocols to fix it. For instance, Automata[60], a privacy middleware, recently introduced Conveyor[61], a solution which sidelines standard transaction broadcasting by implementing First-In-First-Out (FIFO) transaction batches to DEXs in order to prevent any form of front-running, back-running or sandwiching by standard miners.

In our view, it is unclear how public actions may address the issue of MEV. Similar to autarkic protocols, the virtues of open market competition, open source protocols and composability may be the best ingredients to address these frictions.

Market failures

The composability of protocols in DeFi allows crossing protocols to build on top of each other and interface multiple services to generate new opportunities and solutions. The richness of such mechanics however entails layering dependencies which in turn create risks of contagion and crossings of vulnerabilities. In absence of ring fencing or explicit buffering procedures, one protocol at risk may expose others directly or indirectly through the network of λ protocols.

A major lesson from the Global Financial Crisis (GFC) of 2008 was that the stability and security of interconnected financial systems required policymakers to beware of the composite fallacy: in a networked system, ensuring the stability and security of each node independently is not sufficient to guarantee the stability and security of the system as a whole. In the case of traditional finance prior to the GFC, micro-prudential approaches had traditionally been the main focus of regulators and supervisors. The experience from the crisis pushed regulatory frameworks to integrate macro-prudential approaches to complement the picture and avoid falling prey to the composite fallacy in the future.

Similarly, layering dependencies in DeFi and the risk of interdependent vulnerabilities, may call for systemic measurements of security and stability in addition to auditing protocols individually. Private initiatives however might not be guaranteed to achieve such goals efficiently. In fact, while we acknowledge the benefits of private auditing for the case of autarkic protocols, private incentives for auditing crossing protocols do not - in principle - include the treatment of negative externalities (e.g., contagion) to the rest of the DeFi ecosystem. As such public actions meant to treat systemic externalities might be warranted.

Another lesson from the GFC has been the cost of complexity usually associated with interdependent and layered contracts. On the one hand, such cost can materialize as an amplifier of shocks and distress (see for example Gai, Haldane and Kapadia (2011), Caballero and Simsek (2013) and Battiston et al. (2016)). On the other hand, complexity of overall processes bears an opacity risk for participants' bounded rationality (Brunnermeier and Oehmke, 2009) and social planners (Roukny, Battiston and Stiglitz, 2018). Such risk entails moral hazard, manipulation, phishing, etc. Importantly, the adverse effects of complexity also apply to developers and protocol designers. Mirroring the ways in which Collateral Debt Obligation (CDO) contracts were mishandled by each side of the trade,[62] developers and protocol designers are both subject

---

60 https://www.ata.network

61 https://www.ata.network/conveyor

62 A masterful illustration of the multilateral opacity of complex financial products is provided in the bestseller The Big Short by Michael Lewis (Lewis, 2011).

to the risk of mishandling and excessive risk taking when protocol complexity becomes larger and more interconnected.

In standard settings, when information becomes too hard to process, private third parties specialize in servicing aggregated information. In several financial markets, credit rating agencies play such a role. While similar private solutions are emerging in DeFi (e.g., DeFiSafety[63] and Prime Rating[64]), systemic issues with the inefficiency of rating agencies - once again tragically illustrated during the GFC - may hold in DeFi as well. For instance Bolton, Freixas and Shapiro (2012) study how the market for credit agencies can exhibit inefficient aggregation of information. The authors show that the effect of market structure is ambiguous because the revenue of rating agencies is determined by the institutions they need to screen and rate. In response to the crisis, several public institutions were constituted to prompt better monitoring of systemic risk and management of financial crises. These institutions include among others the European Systemic Risk Board and the Financial Stability Board. As such, policy efforts to complement private solutions with public research institutions insulated from incentive frictions may also be warranted in the DeFi ecosystem.

Off-chain protocols

Compared to strictly on-chain protocols (autarkic and crossing), off-chain protocols expand the underlying information structure and the related contracting space by interfacing with external sources of information. However, strict verifiability of such information at the moment of execution is not achievable in principle. Furthermore, interfacing protocols with off-chain sources enables two-way flows: protocols may benefit from external information but they can also generate input to real world outcomes.

Given the early stage of development and the steep learning curve of this class of protocols, a clear distinction between private and public areas of frictions and solutions is not straightforward. As such we here formulate major sources of risk and inefficiencies in off-chain protocols and identify the potential value of public action with milder distinctions on the efficiency of private solutions.

A direct implication of off-chain protocols is the increase of layering dependency issues. In addition to the issues raised with crossing protocols, new off-chain layers involve vulnerability in the nature and quality of the information that is collected. The lack of formal verifiability of off-chain information re-introduces an intermediary dependence (intermediation risk) that entails risks of manipulation and reluctance to engage on the part of distrusting users. The intermediary here is the oracle which forms an interface between the on-chain and off-chain world.

In general, oracles constitute a source of risk and inefficiency that is specific to off-chain protocols. As such, the growth and development of off-chain protocols is intrinsically complementary to the state of stability and efficiency of oracle markets. A dysfunctioning oracle service might impact financial transactions in multiple ways. First, oracle operational risks relate to the risk that the oracle does not transmit the correct information to the off-chain protocol due to operational failure, including latency risk and communication risk. As a result, contracts feeding off data from the failing oracle would produce wrong outcomes which in a world with limited liability power would also mean irreversible. Next, oracle manipulation risk refers to the risk of cyber attack or vulnerability exploitation by an adversary in order to manipulate contracted information like price to her own benefit. In addition, the efficiency of oracle pricing is also subject to market forces. Contracting off-chain implies fees for the service of transmitting information to the contract. Presumably, such data markets are subject to the same forces present in standard digital data markets. The related market failures stemming from anti-competitive

[63] https://www.defisafety.com
[64] https://www.prime.xyz/rating

behavior or investment costs might therefore warrant public stewardship to ensure minimal level playing field and fair access to information feeds.

Note that the development of oracle markets is very much underway and several solutions are being developed. For example, Chainlink[65] introduces Decentralized Oracle Networks (DONs) which allows for protocols to source off-chain information from a set of different oracle nodes and aggregate information through consensus protocols. While this solution addresses some of the risk from single operational failure and manipulation, they introduce two costs. First is the cumulative fee that is associated with needing to contract multiple oracles in order to source the same piece of information. Second is the latency and coordination risk that accompanies sourcing from multiple oracles rather than investing in a single customized feed of information. As a result, we observe potential trade-offs and different information problems might require different solutions.

Ultimately, the nature of the information that needs to be transmitted to the contract should determine the optimal design of oracle service and its related market structure. As such, while sophisticated private solutions might be warranted for costly information or uniquely customized forms of data feeds, generic items of information like standard prices, weather or political elections might benefit from public action in supporting the provisioning of information as well as in ensuring information providers fairly price their services. We discuss these issues more in detail in the next section.

Beyond the role played by oracles, services currently running on off-chain protocols exhibit a series of risks and inefficiencies worth discussing. In particular, credit and derivative services in DeFi require important collateral cost. While volatility plays a role, the main force driving these requirements is the lack of liability and screening of participants' risk profile. While monitoring and screening has been a fundamental part of traditional finance, DeFi accommodates its novel information structure (i.e., pseudonymous requirement) by substituting token requirements for identification requirements. While this solution removes counterparty risk, it does exhibit inefficient pricing and entry barriers. Loan prices in DeFi for instance do not reflect the risk of borrowers or the value of their projects. Also, candidate borrowers poor on legacy tokens are unlikely to obtain funding through current DeFi protocols. These limitations have important welfare implications as they limit the efficient financing of good quality borrowers and projects. Note that in standard settings, imperfect information on the quality of borrowers leads to inefficient credit rationing and market unraveling with large welfare losses (e.g., lemon markets).[66] The long history of success and failure in public actions to support economic growth and credit allocation in presence of such information frictions is therefore relevant when considering public support of DeFi services featuring similar issues.

Another implication of collateralized positions in DeFi is their liquidation risk. That is, once price updates on the value of the posted collateral relative to the funded position triggers a preset threshold, the entire position gets - in principle - automatically liquidated. One major stability concern here is the risk of liquidation cascades and their procyclical effect on prices. As prices drop, the risk of liquidating current positions increases. In case such liquidations are large enough, they would put more downward pressure on prices in turn leading to further potential liquidations down the road. This phenomenon shares several features with standard financial mechanisms such as *fire sales*. Multiple policies have been introduced to address market failures under lack of provisioning for procyclical effects (e.g., macro-prudential policies on countercyclical buffers). Investigating their value for DeFi protocols should therefore be warranted.

---

65 https://chain.link

66 See seminal and Nobel prize awarded work by Stiglitz and Weiss (1981) on credit rationing and Akerlof (1970) on lemon market unraveling.

In addition, a composite fallacy also exists in DeFi borrowing. Such setting features multiple protocols: borrowed token protocol, collateralized token protocol, credit protocol, price oracle protocol, etc. As such, ensuring stability at the macro level requires integrating externalities among the different protocols and their effect on the DeFi ecosystem overall. A particular area of scrutiny is the role played by oracles in feeding prices. Should there be a distortion (resulting from a manipulation or operational mistakes) its effect on triggering large liquidation may become severe. The possibility of *flash loans* with infinite leverage further exacerbates the danger of such shocks.[67]

Finally note that when off-chain protocols interface with other financial systems, it also implies potential spill overs to traditional financial systems and the real economy which may require intervention to prevent systemic risk. A benchmark case here is the potential effect of runs on stable coins. Should an off-chain protocol possess claims on real assets (e.g., dollar reserves), a downturn in DeFi might consequently lead to a run to reserves which in turn might have a sizable reverberation effect into the real economy. This mechanism is in large part similar to the short term funding scheme of money market mutual funds which had a key role in exposing vulnerabilities further during the GFC. Such concern was also at the heart of the discussion regarding the systemic implications of Facebook/Meta's Libra (Cecchetti and Schoenholtz, 2019).

TABLE 6 - List of risk and inefficiency and sources of solution

Taxonomy	Solution	Risk & efficiency
Autarky	Private	– Settlement risk – Congestion risk – Operational risk
	Public	– Rug pull – Maintenance, upgrade – Governance risk
	Private and public	– Key management – Wash trading
Crossing	Private	– Miner risk (MEV) – Exchange design
	Public	– Layering dependencies
	Private and Public	– Complexity – Ratings

Off-chain	Private and Public	– Layering with unverifiable information
		– Stable coin run
		– Collateralisation costs
		– Liquidation risk and cascades
		– Dispute resolution
		– Oracle risk
		  – Operational risk
		  – Price risk
		  – Manipulation and centralisation
		  – Cost of service
		  – Dispute resolution
		  – Systemic risk

[67] For further analysis, modeling and cost estimation for such scenarios see e.g., Gudgeon et al. (2020) and Qin et al. (2021).

6. Opportunities for public policies

As stated by the World Economic Forum: "Regulatory regimes built around intermediaries as regulated processors of transaction information may fit poorly with a disintermediated market structure." (WEF, 2021). As we have observed in Section 5, the shift in information structure between traditional finance and DeFi entails different sources of risk and inefficiency thereby requiring heterogenous forms of solutions. While there can be benefits from past policy experiences, different information structures also imply limits on the applicability and effectiveness of traditional policy frameworks. Whereas the analysis presented sources of market failure which would likely benefit from public action, below, we leverage our information view of DeFi to consider warranted and feasible roles for public authorities. An important criteria for the development and assessment of each approach is that it satisfies the technological constraints imposed by DeFi core features. We articulate these policies around three targets of intervention: entities, protocols and oracles. This section therefore connects with the two previous sections by combining the analysis of information structure and the sources of market failure to obtain candidate policy solutions.[68] Below, we discuss four specific points of entry for public policy in DeFi:

1. Regulating DeFi activity of legal entities falling under current supervisory and regulatory mandates.
2. Offering voluntary compliance opportunities for both entities and protocols.
3. Producing public supervision and issuing public opinions on DeFi activity and protocols.
4. Supervising, regulating and monitoring approaches to oracle markets.

The remainder of this section offers a few preliminary remarks and then elaborates on each proposal. While proposals differ in scope and reach, they also have the capacity to create synergies. For example, a public observatory of DeFi activity could issue opinions which are then included in the process of determining compliance rules for legal entities and voluntary ones. Table 7 summarizes the list of policy proposals and the sources of risk and inefficiency they can help address.

Preliminary remarks

Asymmetry of identification

As already discussed, one of the main disruptions in the information structure of DeFi is the pseudonymous status of participants enabled by public-private key pair generators and signature functions. This system allows participants to verify ownership without revealing their identity. As such, this pseudonymous pairing theoretically prevents any observer from recovering a (legal or physical) identity strictly from public activity on the ledger.

Asymmetric identification has important implications for both supervision and regulation. While it is indeed possible to supervise the activity of legal entities on DeFi protocols by requiring them to disclose their public keys and verify their signatures, the reverse is theoretically not possible. In what follows, we consider that recovering the legal or physical identity behind a public key without consent of the private key holder is technically not feasible. As long as key pairing is impossible to reverse engineer, aspects of traditional regulation and supervision cannot be onboarded in the DeFi ecosystem.[69] According to such a view, policy proposals aimed at regulating activity sourcing strictly from DeFi ledgers are not considered in our scope. Policing DeFi activity starting from a pre-identified set of legal entities is however feasible.

---

[68] An illustration of the sequence from information structure to market failure and policy solution follows from our analysis on the role of oracles in DeFi. First, our analysis on protocol information structures identified protocols which relied on unverifiable information transmitted by oracles (i.e., off-chain protocols). We then discussed the sources of risk and inefficiencies that accompany the presence of oracles in the information structure. In this section, we consider policy initiatives that help address risks and inefficiencies through public action in the market for oracles services.

[69] Should this aspect become possible, the entire foundation of DeFi might collapse since it would allow users to sign in the name of others.

In practice, several initiatives such as the ones led by Chainanalysis have been successful at overcoming pseudonymity and recovering identities from public ledger activities.[70] We note however that pseudonymity is a feature and not a bug of DeFi (see Section 3). In addition, several cases of re-identification successes have relied on information sets outside the ledger (e.g., information revealed by crypto-exchanges or computer hacking). As such we note that on-and-off ramp services which interface between crypto tokens and real assets are key to enabling re-identification processes. They have legitimately captured most of the current attention efforts by anti-crime and anti-money laundering institutions (see e.g., Financial Action Task Force (2021)). While these efforts are timely, they also face context-dependent limits. For instance, assuming that the exchange value of crypto tokens would increase in multiple industries, it is unclear whether on-chain activity would always induce an off-ramping of asset value into traditional currencies.[71] Seeking generalizable principles that would hold in a future with an expanded crypto-economic spectrum, our approach therefore takes the pseudonymous power of participants to its limit. As such, we complement parallel efforts of re-identification by a conceptual upper-bound to the challenges of policing interactions in absence of full identity.

Protocols

Protocols in DeFi are a major shift from traditional finance. Because they allow financial services to operate in absence of legally recognized intermediaries, the traditional approach to policing them becomes ill suited. Below we consider policy approaches that are feasible to the information constraints of DeFi protocols and discuss how they could address market failures identified in the previous section.

Capacity constrained institutions

As will be apparent from the following discussions, the effectiveness of each policy initiative bears a series of challenges. The first major limitation for the success of any policy will be the expertise and capacity building that public institutions can commit to in order to achieve robust policy designs. Talent supply in the world of DeFi is limited. Adding to this the challenge of maintaining interdisciplinary expertise and the large outside options for such experts, calls for sufficient resources on the side of policymakers and supervisors to attract talent and generate credible expertise in the field.

A second important factor in the effectiveness of our proposals will be the actual market demand for some of the policies. In fact, given the permissionless nature of the DeFi ecosystem, policy enforcement bears limitations. Traditional regulatory processes by which rules are mandatorily imposed upon market participants are hard (in cases impossible) to maintain in a permissionless environment. As such, the capacity of public initiatives to be attractive to the DeFi ecosystem and encourage protocols to integrate public policy concerns will be key. For instance, one policy we develop below considers the establishment of a voluntary compliance framework where protocols and users freely choose to adhere to some policy requirements in order to obtain different forms of public support and guarantee such as a stamp of public approval. The fact that a case for such an initiative can be shown to make economic sense, does not guarantee its success as the demand would be relative to the attractive value of - for instance - such a stamp of approval. Further market research will therefore be warranted to evaluate optimal scope of impact and effectiveness for each of the following candidate policies.

---

[70] See for instance “Inside the Bitcoin Bust That Took Down the Web’s Biggest Child Abuse Site” – Wired, April 2022

[71] Considering once more that pseudonymity is a core feature of the original DeFi proposition, this work-around would be akin to the monitoring of cash deposits at bank accounts as a substitute for resolving the anonymity of cash.The value of this latter approach would therefore be directly proportional to the relative importance of cash in the economy at hand.

Proposal 1: Policing the policed

This policy focuses on entities rather than protocols. Given the asymmetric nature of key pairing, legal entities currently supervised or regulated in traditional markets can be identified in the DeFi ecosystem. Should they disclose and verify their public addresses to dedicated institutions, it would allow policymakers to observe their entire DeFi activity and adjust their regulatory framework accordingly. Armed with such information, regulatory requirements aimed at ensuring micro and macro-prudential concerns are effective as regulators can monitor exact exposures from the public ledgers. Furthermore, supervisory activity on legal institutions naturally extends to their DeFi specific activity with direct access to their on-chain positions.

Because of the cost-free generation of public-private key pairs, note that a single legal institution may possess an infinite amount of addresses. Holding multiple identifiers can theoretically be used to achieve opacity but also other forms of deceitful manipulation (e.g., fiscal optimization). Hence there should be a particular effort put into properly incentivising disclosure of the entire list of public addresses associated with a legal entity.

Whether public address disclosure should be made public or be confidential is another aspect to ponder. On the one hand, public disclosure would increase transparency and public view of a legal entity's activity in DeFi. However, such a level of transparency might be excessive and unnecessarily disrupt some trading opportunities.[72] On the other hand, private disclosure of public addresses can be achieved through specific mandates. In this case, the authorized institutions will however need to exert credible efforts to make sure leakages are avoided. The outcome of this situation would be akin to the private-yet-accessible information structure discussed for traditional payment systems in Section 4 (e.g., Figure 1).

Policy institutions have experience in collecting and treating confidential data collection. For example, under the European Market Infrastructure Regulation, institutions such as the European Securities Market Authority and the European Systemic Risk Board are granted access to all derivatives transactions including European counterparties for the purpose of monitoring financial stability and market integrity. Confidential disclosure in DeFi would however bear distinctive features. On the one hand the cost of leakage in DeFi is likely to be more severe than traditional settings: one data point (i.e., public address match with legal identity) would allow one to reconstruct the entire activity history associated with the address from the public ledger. There is therefore a need to develop complementary security expertise with tools specific to the extreme nature of the DeFi information structure.

In addition, the transparency of DeFi public activity also bears favorable outcomes for regulators as it grants them additional means to verify proper reporting. Starting from off-chain cash flows (i.e., transfers into fiat currencies or into another on-the-books statement), supervisors can verify addresses and construct back an entity's entire on-chain activity. As a result, the possibility to publicly audit on-chain activities and match them with reported cash flow statements by legal entities augments a supervisor's credibility and reduces private incentives for deceitful disclosure. A limitation to this outcome would be the previously mentioned case of pure on-chain activities for which it may become harder to acquire information if the legal entity does not disclose it.

In spirit, this proposal extends ongoing initiatives on the regulation of crypto-assets like the European Commission's Regulation on Markets in Crypto-assets (MiCA). It is however important to acknowledge the asymmetry of actions that is specific to DeFi which is a reflection of the underlying DeFi information structure: moving from legal identity to on-chain activity is feasible while the reverse is not.

---

[72] In economics, the famous "Hirshleifer effect" shows that increasing available information too much can sometimes undermine the risk-sharing capacity of a market (Hirshleifer, 1971). See Vives (2010) for a discussion.

A policy granting access to the list of public addresses held by a legal entity is relevant to address several market failures presented in the previous section. In particular, capital requirements specific to DeFi activity and buffering processes to counter procyclical activities would become enforceable onto legal entities. Furthermore, being able to connect crypto-asset exposures with other balance-sheet items would help monitor risk channels in order to prevent externalities in the real economy (e.g., fire sales). Finally, public institutions could also provide last-resort services to the key management of 'to-big-to-lose' addresses.

Proposal 2: Voluntary compliance[73]

In the previous policy, we restricted enforcement to the set of entities that were legally subjected to the authority of standard public institutions. However, the DeFi universe also includes entities that are not or cannot be recognized under the standard legal identity system. In particular, DeFi protocols do not bear means of enforcement from standard policy frameworks.

Once again, the permissionless and pseudonymous nature of DeFi poses a general challenge to a universal enforcement of public actions. On the one hand, the permissionless part allows anyone to either consume or produce DeFi services. On the other hand, the pseudonymous part - owing to the asymmetric identification problem previously discussed - prevents policies to make pseudonymous entities liable for their actions. As a result, policy makers do not theoretically have the power to regulate any given entity or activity out of the DeFi universe.

Limited enforceability does not however imply that DeFi activity should uniquely be undertaken by already regulated entities (cf. policy as set out in the previous section) nor that the residual population of entities and activities bears no reach for policy making. In this section, we consider an open policy framework with attractive benefits to DeFi services that can produce voluntary compliance. In such a setting, entities and protocols voluntarily seek to comply with a given set of policy requirements in order to obtain a public stamp of approval and other potential benefits. On the part of DeFi, public compliance produces public signals of quality and good intentions. On the part of policy institutions, attracting DeFi activity under this framework extends enforceability of rules and guidance.

According to our information framework, a voluntary mechanism is feasible because its implementation is compatible with the information structure of DeFi services: private information can be linked to public activity, while the other way around is not. Technologically, this result could be obtained through the public licensing of non-tradable and non-fungible tokens (e.g., public ID NFT). These tokens would be associated with one or multiple public addresses and serve as legally recognized proof of compliance in the DeFi ecosystem. Similar to the previous policy, the choice of transparency requires careful attention. Note again here that a de-identified public NFT would produce an outcome similar to the private-yet-accessible information that we discussed for payment systems in Section 4.

Voluntary compliance may allow policies to implement traditional regulatory rules such as the detection of illicit activities (e.g., money laundering and ponzi schemes). However it would also require new rules specific to DeFi services and a carefully designed set of incentives to make compliance attractable enough. Below we discuss specific ways in which a voluntary compliance approach would address some of the risks and inefficiencies listed in the previous section.

Commitment problem

As we discussed, lack of commitment and liability in DeFi generate risks and losses of trading opportunities. Importantly, these costs can be borne on both the supply and demand side and for both individuals and protocols. In particular and despite the original core features of DeFi, some protocols might benefit from implementing commitment devices. This would for instance be the

[73] This section extends on a proposal originated by Prof. Hanna Halaburda (NYU Stern) and relates to ongoing research by the author and Prof. Hanna Halaburda.

case for hedging against consumers' fear of rug pulls, as discussed in Section 5. Being subject to a policy framework would therefore give the opportunity for DeFi entities to voluntarily recover commitment because it would provide liability that policymakers can leverage upon in case of wrongdoing. As such, entities could credibly commit their assets and reputation from the real world to the DeFi ecosystem by implementing this legal liability. As mentioned earlier, the fact that protocols are attached to legal liability constraints under a voluntary regulation framework, would signal and demonstrate long term commitment to the governance and maintenance of the protocols. Such public commitment would in turn assure potential users of the developers' good intentions and their vested interest in the long run.

Exogenous and endogenous partitioning of the ecosystem

By offering to voluntarily acquire public stamps of policy compliance, the policy also has the potential to reorganize the DeFi ecosystem both endogenously and exogenously. We consider two possible effects: signalling and type-contingent interactions.

First, while voluntary regulation cannot technically enforce full onboarding of DeFi activity (in contrast to traditional financial systems), its existence can nevertheless serve as a signalling device with positive self selection effects. In fact, publicly entering the policy framework acts as a positive signal to consumers and other DeFi actors. As such, this process potentially imposes a negative stigma for not engaging in the policy framework. Pressure might therefore accrue to marginal entities to proceed with compliance in order to avoid the negative stigma. The same signalling process holds at the protocol level. As such, protocols might compete to obtain public recognition in order to attract a wider set of users wary of the wrong signal sent by those protocols who did not undergo regulatory validation.[74]

Second, providing a public positive recognition of DeFi entities and protocols might in turn benefit the natural rise of services contingent on public compliance. For instance, smart contracts could enforce ring fencing structures by explicitly conditioning for counterparties to be able to prove ownership of a publicly issued registration (e.g., non-tradable public compliance NFT). An alternative would also be that the protocol gives the choice to users to enable transfers strictly between publicly recognised users or protocols.[75] The resulting organization of protocols would also enable a ring-fencing of sets of protocols by allowing them to exclusively interface with regulated protocols. Voluntary regulation would therefore also help address the underlying complexity of crossing protocols and consumers' bounded rationality constraints.

The resulting regulatory ecosystem would endogenously evolve and interact with the rest of the DeFi universe in multiple possible ways. In addition, the policy framework would have room to affect this interface by requiring weak or strict restrictions between regulated and unregulated entities or protocols. It could also include a directionality dimension by allowing for unidirectional or bidirectional interfaces between regulated and unregulated entities or protocols.

Policy enforcement

For entities and protocols which voluntarily engage in the policy frameworks, policymakers recover enforcement power allowing them to address some of the market failures discussed in the previous section. At the entity level, regulators can implement requirements to ensure liability, identification, capital requirements, etc. At the protocol level, regulators would obtain the means to address interdependencies and require actions from protocols when and where needed. The risk and complexity of layering dependency could also be alleviated by enabling

---

[74] Note that the dynamics of protocol competition for public recognition is also affected by the risk of forking. As such, the ease with which protocols can be replicated means that, should there be demand for a regulated version of a given protocol, anyone can fork the original code to voluntarily request a public recognition. This possibility would presumably further incentivize original protocol developers to undertake voluntary compliance themselves.

[75] We thank Julien Prat for this insightful comment.

further oversight on the exact network of interdependencies and ensuring adequate risk management mechanisms be implemented.

A series of requirements can source inspiration from policy experience in traditional financial systems. For instance, regulators could require that counter cyclical mechanisms be embedded into a protocol. Furthermore, leveraging similarities between clearinghouse design and smart contracts with liquidity pooling, historical experience from policies could translate into loss provision frameworks against crash scenarios in smart contracts with liquidity pools. In addition, regulators would consider DeFi specific forms of regulation. For instance, regulators could require that activity restriction be implemented into the protocol's code. An example would be the ring-fencing of some protocols by only allowing access to holders of publicly identified and non-tradable tokens such as the compliance stamp token discussed here to access the protocol's services.

Compliance benefits

A key dimension of this policy proposal is to make the policy framework attractive to both entities and protocol. In principle, issuing a legal reference to users and protocols (e.g., public ID NFT) should already generate demand given the way this could solve commitment problems. However, further benefits might be considered to ensure incentive compatibility and maximum uptake. At the entity level, examples include providing public services like key management or some level of consumer protection. At the protocol level, public guarantees may be implemented similar to the process by which banks in the traditional system obtain privileged access to central bank facilities in exchange for regulatory compliance.

Treatment of unverifiable information

Finally, regulating protocols would also enable policy makers to guarantee proper usage of publicly unverifiable information. First, this would directly concern the issuing of public recognition which constitutes unverifiable information for which the public institution acts as a special form of public oracle. Second, should the public ID NFT be de-identified, the policy institution would have a recourse to obtain private-yet-verifiable information similar to traditional financial systems. Furthermore, this supervision may also include guidance, monitoring and restriction on how off-chain information should be handled by publicly recognised protocols (further on this below).

Proposal 3: Public observatory

Traditional financial supervision includes the monitoring of financial institutions' activity. Such a task is achieved by processing both public and (more importantly) private and sensitive information in order to ensure excessive risk and illegal activities are under control. Warnings, sanctions and other forms of interventions may ensue in case of malpractice. Monitoring processes and their outcomes are usually confidential - though extreme outcomes may become public matters. While it is part of the DeFi design to prevent external arbitrary powers to intervene, the transparency of both protocols and historical activity allows in theory for an adapted form of supervision.[76]

As such while explicit and direct forms of sanctions may be harder or impossible to enforce, public investigation, supervision and statements issued on the riskiness and safety of protocols and public addresses can be achieved without the forms of information costs (e.g., confidentiality) present in traditional financial supervision.

We therefore identify a role for a public observatory of DeFi activity operated by a public authority. Such an institution would deploy public investigations and issue opinions and warnings

[76] This proposal mirrors the concept of 'embedded supervision' from Auer (2019). While the original proposal aims at the possibility of automatizing supervision of traditional finance using blockchain, we are here instead referring to the supervision of DeFi by leveraging the transparency of blockchains.

publicly about specific DeFi protocols, practices and public address activities. Inspiration for such an observatory can for instance be taken from the activity of the MIT Digital Currency Initiative which issues technical opinions and warnings on specific protocols. In 2017, the team publicly posted a warning against the IOTA protocol. The authors identified potential security flaws in the protocol's in-house *hash function* and made them public, forcing IOTA to adjust its security (Heilman et al., 2019).

The observatory may also complement current initiatives that have emerged from within DeFi. In fact, the growing demand for protocol audits to improve efficiency and reduce operational risk of DeFi contracts has proved effective in several cases. However, these initiatives remain private initiatives and they might not have the right incentives to consider externalities to the rest of the economy (DeFi and beyond).[77] Furthermore, when applying our information view of DeFi, we observe that, while auditing of on-chain protocols may be complete and consistent, auditing off-chain protocols might require auditing auxiliaries outside the public reach - in particular oracles, potentially linking back to traditional legal system structures. As such, the observatory could also play a role in assessing oracle services in order to support proper use of unverifiable information in off-chain protocols.

While this proposal does not entail enforcement power - in contrast to the previous case of voluntary regulation - it however covers the entire universe of public protocols. As such the issuance of warnings and opinions can also be used to reduce layering dependencies and complexity. With enough credibility, documented warnings of flash crashes and strong protocol vulnerabilities could be effective in steering market activity away from risky and inefficient segments of the DeFi ecosystem.

Note finally that these opinions and research output could in turn be used to inspire and support activity regulation policy (e.g., Proposal 1). Using the material produced by such an observatory could in fact be a means to apply compliance rules on regulated entities active in those protocols. This could also help limit the level of risk interdependencies between the DeFi world and the financial world.

Proposal 4: Oracles

Oracles constitute the interface between DeFi and the real economy. They are key to the expansion of the information structure - and the contracting space - of DeFi services. By the same token, the future demand for oracle services will grow in sync with the development of smart-contract services in DeFi and, to a larger extent, the digital economy. In light of the sources of risk and inefficiencies that oracles may originate (see Section 5), policymakers should increasingly bring their attention to development of oracle markets.

Despite its importance, the question of the optimal design for oracle markets remains largely under-developed. Hence, a set of concrete policy guidance is hard to obtain at this stage. Below, we consider a series of avenues worth developing in order to support a sustainable and efficient development of oracle services which would in turn help promote growth and stability for the future of the DeFi ecosystem and the real economy.

On the value of oracle services

From an economic perspective, oracles produce information that is not verifiable by the validators of an off-chain DeFi protocol, yet the information can be contracted upon. As such the value of smart contracts written on oracle data is partly determined by the value of the oracle service. In particular, because information is not formally verifiable, trust - the very concept that

[77] While macro-prudential approaches have gained traction and maturity in traditional markets after the 2007-2008 crisis and the global reform, the composite fallacy of micro audits might be stronger in the ever more composable and interoperable world of DeFi

DeFi services attempt to minimize - places an important part in the decision of customers to engage with an off-chain protocol.

Because the value of oracles is determined by the cost of observability and verifiability of the underlying information they seek to transmit to a DeFi protocol, it is likely that different types of information require different design solutions both from a contract and market perspective. As discussed previously: while some services may benefit from decentralized solutions, it is not clear whether such a model is optimal for every type of oracle service. To illustrate this point, let us consider some information dimensions that would affect the optimal design of an oracle contract. We formulate each point as a question related to the nature of the data produced by an oracle. Leveraging this list, we will then consider cases where public attention may be appropriate.

- Is the information verifiable in the real economy? Using standard economic definitions, the information produced by an oracle might be related to verifiable information in the real world. For instance, reporting weather conditions can be verified in the real world. In contrast, reporting an event without witness nor material evidence is not verifiable.
- Is the information public or private? The information transmitted by an oracle may be obtained from the public records (e.g., outcome of an election) but it may also be privately produced (e.g., aggregate statistics on confidential data).
- Is the information hard or soft? The information produced by an oracle may be numerically obtained from a set of objective quantities (e.g., population statistics) but it can also be the result of a subjective process (e.g., forecast).
- Is the information costly to produce? The cost of producing the information collected by an oracle may vary from close-to-zero (e.g., a copy of public digital information) to expensive (e.g., network of smart sensors or expert analysis reports).
- Is the information static or dynamic? Is it low or high frequency? The information produced by an oracle might be dynamic (e.g., prices) or static (e.g., date of an event). If it is dynamic, it might also differ in frequency from low (e.g., quarterly earnings) to high (e.g., tick-level price information).

In addition to these information-specific dimensions, whether the oracle service is integrated to any of the other parties to the contract (i.e., buyer, seller and protocol) also determines the overall efficiency of the service. For instance, the seller of a good might need to provide an oracle to inform the contract on the delivery or quality of the good. In case of high complementarity, a protocol might depend on the existence of a specific oracle which might not yet exist, thereby requiring that the protocol produces the oracle service as well. While disintegrated solutions might intuitively be desirable to avoid conflicts of interests, there exists a well developed literature qualifying settings where disintegrated solutions are sub-optimal due to inefficiencies such as the cost of double marginalization and the risk of inadequate governance.[78]

Trusting oracles

In addition to economic values, the reliability of oracle services also plays a role in determining adoption and stability. Trust in oracles includes at least two dimensions: trust in the production of information by the oracle and trust in the transmission of the information from the oracle to the contract. While the first one may be driven by economic incentives, the second one relates to risks such as operational failure or cyber attacks. These dimensions impose additional challenges to the implementation of oracle services. First, the need to obtain incentive compatibility for oracles typically translates into high fees ensuring that oracles cannot be bribed (Breidenbach,

[78] This strand of the literature includes for instance discussions on the limits of the firm (see e.g. Holmstrom and Tirole (1989)), the organization ownership for incomplete contracts (see e.g. Hart (1995)), and the cost of double marginalization (see e.g. Chap 17 in Belleflamme and Peitz (2015))

2021).[79] Second, the need to ensure proper operational functioning may require coordinated investments in infrastructure or security layers.

Avenues for public action

Despite the early stage of development for oracle services and markets, the above discussion points towards areas where public support might help address some of the risks and welfare losses presented in Section 5. Below, we consider some ways in which public entities could participate to ensure stability, improve growth, welfare and efficiency of both oracle services and DeFi.

Public oracles

Stemming directly from the above list of information dimensions and the costly presence of trust frictions, we observe that some specific combinations of features might be best integrated through a public oracle solution. Consider the case of information that is (i) verifiable in the real economy, (ii) public, (iii) hard, (iv) cheap to obtain and (v) static. One example would be the outcome of a sovereign default. The overall provisioning of such standard information by a public provider has the potential to be a welfare improving alternative to private solutions. The main source of efficiency gain here would be that such a public support should in principle reduce or eliminate the incentive compatibility rent that features private oracle solutions. In fact, theory suggests that parties contracting private oracle services ensure truthful reporting by the oracle through inflated fees which prevent third parties from bribing the oracles. Should parties trust a public oracle for transmitting such cheap, standard and public information, the latter rent would not be needed and the overall price of service would be cheaper (or even free).

Determining general conditions under which public support dominates private solutions for oracle services is complex and requires more research. However, for cases of very low cost of production and high public verifiability, the advantages brought by a public oracle may be straightforward and substantial.

Oracle markets

As any digital market, oracle markets are subject to failures and inefficiencies which public authorities can help fix. The benefits of promoting market integrity, fairness and stability for oracle markets would substantially support the sustainable and efficient growth of DeFi services overall.

In this view, public support for establishing standardized frameworks for specific data production, processes and APIs could promote competition, innovation, adoption and coordination among heterogeneous agents including consumers, protocol designers and oracles. Similar initiatives could be directed to the development of security standards and disclosure guidelines for ensuring conflicts of interest are avoided between oracles and other contracting parties.

Licensed oracles

Compared to DeFi actors, several forms of oracles have a direct presence in the economy. As such, providing a legal framework for them to operate could substantially improve efficiency and trust. First, a legal framework would introduce liability to an oracle's activity. Second, this would pave the way for the possibility to integrate some of the formal financial standards into DeFi services. Licensed oracles could therefore produce reliable information on candidate customers which could then be used by DeFi protocol. For instance, Know-Your-Customer (KYC) non-fungible tokens could be produced by specialized oracles under a public policy framework. These non-tradable tokens would then be recognized and used by the customers to undertake financial activities in DeFi. Similarly, credit-scoring non-fungible tokens could be produced in order to

---

[79] As stated by Gans (2019): "The ability to generate hard evidence is the fundamental smart contract challenge. To the extent that contract obligations rely on evidence to be provided outside of a purely digital realm where evidence may be hard coded, any smart contract needs to create incentives for disclosure of the truth of contract performance."

expand the contracting space of lending protocols. Note that both cases can be achieved while keeping identities private on-chain. That is, ownership of a token would convey information about the user without necessarily revealing the identity of the user.

In general, public support and guidance for such initiatives could boost innovation and growth of DeFi service while leveraging policy experience with traditional requirements and the supervision of third-party agencies in charge of producing such information.[80]

TABLE 7 - Policies and their coverage of risk and inefficiency

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

[80] For instance, in Europe, the European Securities and Market Authority has a mandate to supervise and monitor the activity of credit rating agencies.

8. Conclusion

In spite of the many shortcomings associated with traditional financial systems, substituting automated protocols for financial intermediaries does not solve the fundamental information friction that lies at the heart of financial contracts. Ultimately, the main value proposition offered by DeFi is a shift in the information structure upon which financial services can be deployed. By introducing such a distinction, this report first rationalizes why policy frameworks need to integrate DeFi specific information constraints to be implementable. Next it investigates how the heterogeneous treatment of information under different classes of DeFi protocols presents conditions under which public actions might be warranted. From this analysis, the report finally derives feasible policy approaches that have the potential to generate growth and sustainability for the DeFi ecosystems and its interactions with the real economy.

While the future of DeFi remains open, it is clear that it holds a credible promise for new forms of financial services adapted to a globalized, competitive and digital economy. At the same time, severe threats to consumers, producers and the economy at large accompany this opportunity. This report ultimately aims to support the early stages of a coordinated public effort to promote the growth of DeFi products that are both sustainable and harmonized with general public policy goals such as financial stability, economic inclusion, market integrity and consumer protection.

9. References

Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. Journal of economic Literature, 54(2), 442-92.

Akerlof, G. A. (1970). The Market for" Lemons": Quality Uncertainty and the Market Mechanism. The Quarterly Journal of Economics, 84(3), 488-500.

Allen, F., & Gale, D. (2004). Competition and financial stability. Journal of money, credit and banking, 453-480.

Auer, R. (2019). Embedded supervision: how to build regulation into blockchain finance (No. 811). Bank for International Settlements.

Aymanns, C., Dewatripont, M., & Roukny, T. (2020). Vertically Disintegrated Platforms. Available at SSRN 3507355.

Bakos, Y., & Halaburda, H. (2019). Smart Contracts, IoT Sensors and Efficiency: Automated Execution vs. Better Information. NYU Stern School of Business.

Bakos, Y., Halaburda, H., & Mueller-Bloch, C. (2021). When permissioned blockchains deliver more decentralization than permissionless. Communications of the ACM, 64(2), 20-22.

Battiston, S., Caldarelli, G., May, R. M., Roukny, T., & Stiglitz, J. E. (2016). The price of complexity in financial networks. Proceedings of the National Academy of Sciences, 113(36), 10031-10036.

Belleflamme, P., & Peitz, M. (2015). Industrial organization: markets and strategies. Cambridge University Press.

Belleflamme, P., & Peitz, M. (2021). The Economics of Platforms. Cambridge University Press.

Berger, A. N., & Mester, L. J. (1997). Inside the black box: What explains differences in the efficiencies of financial institutions?. Journal of banking & finance, 21(7), 895-947.

Bhattacharya, S., & Chiesa, G. (1995). Proprietary information, financial intermediation, and research incentives. Journal of financial Intermediation, 4(4), 328-357.

BIS (2021). DeFi risk and the decentralization illusion. BIS Quarterly Review, December 2021.

Bolton, P., Freixas, X., & Shapiro, J. (2012). The credit ratings game. The Journal of Finance, 67(1), 85-111.

Breidenbach, L., Cachin, C., Chan, B., Coventry, A., Ellis, S., Juels, A., ... & Zhang, F. (2021). Chainlink 2.0: Next steps in the evolution of decentralized oracle networks.

Brunnermeier, M., & Oehmke, M. (2009). Complexity in financial markets. Princeton University.

Caballero, R. J., & Simsek, A. (2013). Fire sales in a model of complexity. The Journal of Finance, 68(6), 2549-2587.

Capponi, A., & Jia, R. (2021). The adoption of blockchain-based decentralized exchanges. arXiv preprint arXiv:2103.08842.

Capponi, A., Jia, R., & Wang, Y. (2022). The Evolution of Blockchain: from Lit to Dark. arXiv preprint arXiv:2202.05779.

Catalini, C., & Gans, J. S. (2020). Some simple economics of the blockchain. Communications of the ACM, 63(7), 80-90.

Catalini, C., & Tucker, C. (2019). Antitrust and costless verification: an optimistic and pessimistic view of blockchain technology. Antitrust Law Journal, 82(3), 861-872.

Cecchetti, S., & Schienholtz, K. (2019). Libra: A dramatic call to regulatory action. VOX CEPR Policy Portal.

Chainalysis. (2020). The 2021 geography of cryptocurrency report: analysis of geographic trends in cryptocurrency adoption, usage and regulation. Chainalysis

Chainalysis (2022). The Chainalysis 2022 Crypto Crime Report.

Cong, L. W., Li, X., Tang, K., & Yang, Y. (2021). Crypto Wash Trading. Available at SSRN 3530220.

Daian, P., Goldfeder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., ... & Juels, A. (2020). Flash boys 2.0: Frontrunning in decentralized exchanges, miner extractable value, and consensus instability. In 2020 IEEE Symposium on Security and Privacy (SP) (pp. 910-927). IEEE.

Dell'Ariccia, G. (2001). Asymmetric information and the structure of the banking industry. European Economic Review, 45(10), 1957-1980.

DeMarzo, P. M., Fishman, M. J., & Hagerty, K. M. (2005). Self-regulation and government oversight. The Review of Economic Studies, 72(3), 687-706.

Diamond, D. W. (1984). Financial intermediation and delegated monitoring. The review of economic studies, 51(3), 393-414.

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

Financial Stability Board (2022) Assessment of Risks to Financial Stability from Crypto-assets. Report to the G20.

Freixas, X., & Rochet, J. C. (2008). Microeconomics of banking. MIT press.

Gai, P., Haldane, A., & Kapadia, S. (2011). Complexity, concentration and contagion. Journal of Monetary Economics, 58(5), 453-470.

Gans, J. S. (2019). The fine print in smart contracts (No. w25443). National Bureau of Economic Research.

Grossman, S. J., & Hart, O. D. (1986). The costs and benefits of ownership: A theory of vertical and lateral integration. Journal of political economy, 94(4), 691-719.

Gudgeon, L., Perez, D., Harz, D., Gervais, A., & Livshits, B. (2020). The decentralized financial crisis: Attacking defi. arXiv preprint arXiv:2002.08099.

Hart, O. (1995). Firms, contracts, and financial structure. Clarendon press

Hart, O., & Moore, J. (1990). Property Rights and the Nature of the Firm. Journal of political economy, 98(6), 1119-1158..

Harvey, C. R., Ramachandran, A., & Santoro, J. (2021). DeFi and the Future of Finance. John Wiley & Sons.

Heilman, E., Narula, N., Tanzer, G., Lovejoy, J., Colavita, M., Virza, M., & Dryja, T. (2019). Cryptanalysis of curl-p and other attacks on the iota cryptocurrency. Cryptology ePrint Archive.

Hirshleifer, J. (1971). The Private and Social Value of Information and the Reward to Inventive Activity. American Economic Review, 61(4), 561-574.

Holmstrom, B. R., & Tirole, J. (1989). The theory of the firm. Handbook of industrial organization, 1, 61-133.

IMF (2021). International Monetary Fund’s global financial stability report october 2021: COVID-19, Crypto, and Climate: Navigating Challenging Transitions.

IOSCO (2022). IOSCO Decentralized Finance Report. Report of the Board of IOSCO. OR01/2022

Kwon, Y., Kim, H., Shin, J., & Kim, Y. (2019). Bitcoin vs. Bitcoin cash: Coexistence or downfall of bitcoin cash?. In 2019 IEEE Symposium on Security and Privacy (SP) (pp. 935-951). IEEE.

Lehar, A., & Parlour, C. A. (2021). Decentralized exchanges. Working Paper, University of California, Berkeley.

Lewis, M. (2011). The big short: Inside the doomsday machine. Penguin UK.

Li, B. G., McAndrews, J., & Wang, Z. (2020). Two-sided market, R&D, and payments system evolution. Journal of Monetary Economics, 115, 180-199.

McAfee, A., & Brynjolfsson, E. (2017). Machine, platform, crowd: Harnessing our digital future. WW Norton & Company.

Maia, G., & Vieira dos Santos, J. (2021). MiCA and DeFi ('Proposal for a Regulation on Market in Crypto-Assets' and 'Decentralised Finance'). Forthcoming article in Blockchain and the law: dynamics and dogmatism, current and future.

Moore, J. (1992). Implementation, contracts, and renegotiation in environments with complete information. Advances in economic theory, 1, 182-282.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton University Press.

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

Park, A. (2021). The conceptual flaws of constant product automated market making. Available at SSRN 3805750.

Prat, J., & Walter, B. (2021). An equilibrium model of the market for bitcoin mining. Journal of Political Economy, 129(8), 2415-2452.

Qin, K., Zhou, L., Livshits, B., & Gervais, A. (2021). Attacking the defi ecosystem with flash loans for fun and profit. In International Conference on Financial Cryptography and Data Security (pp. 3-32). Springer, Berlin, Heidelberg.

Rochet, J. C., & Tirole, J. (2003). Platform competition in two-sided markets. Journal of the european economic association, 1(4), 990-1029.

Roukny, T., Battiston, S., & Stiglitz, J. E. (2018). Interconnectedness as a source of uncertainty in systemic risk. Journal of Financial Stability, 35, 93-106.

Rysman, M. (2009). The economics of two-sided markets. Journal of economic perspectives, 23(3), 125-43.

Schär, F. (2021). Decentralized finance: On blockchain-and smart contract-based financial markets. FRB of St. Louis Review.

Stiglitz, J. E., & Weiss, A. (1981). Credit rationing in markets with imperfect information. The American economic review, 71(3), 393-410.

Strahan, P. E. (2013). Too big to fail: Causes, consequences, and policy responses. Annu. Rev. Financ. Econ., 5(1), 43-61.

Tirole, J. (2015). Market failures and public policy. American Economic Review, 105(6), 1665-82.

Vives, X. (2010). Information and learning in markets. Princeton University Press.

Vives, X. (2016). Competition and stability in banking. Princeton University Press.

Wall, L. D. (2016). " Smart Contracts" in a Complex World. Federal Reserve Bank of Atlanta.

World Economic Forum (2021). Decentralized Finance: (DeFi) Policy-Maker Toolkit. WEF.

Yosha, O. (1995). Information disclosure costs and the choice of financing source. Journal of Financial intermediation, 4(1), 3-20.

GETTING IN TOUCH WITH THE EU

In person

All over the European Union, there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: https://europa.eu/european-union/contact/meet-us_en

On the phone or by email

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

- by Freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),

- at the following standard number: +32 2 299 96 96, or

- by email via: https://europa.eu/european-union/contact_en

FINDING INFORMATION ABOUT THE EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: https://europa.eu/european-union/index_en

EU publications

You can download or order free and priced EU publications from:

https://publications.europa.eu/en/publications.

Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see https://europa.eu/european-union/contact/meet-us_en).

EU law and related documents

For access to legal information from the EU, including all EU law since 1952 in all the official language versions, go to EUR-Lex at: http://eur-lex.europa.eu

Open data from the EU

The EU Open Data Portal (http://data.europa.eu/euodp/en) provides access to datasets from the EU. Data can be downloaded and reused for free, for both commercial and non-commercial purposes.

EV-07-22-933-EN-N

doi: 10.2874/444494

ISBN 978-92-76-56387-7