

Decentralized Finance

Dirk A. Zetzsche[†], Douglas W. Arner^{*}, and Ross P. Buckley^{**}

ABSTRACT

DeFi ('decentralized finance') has joined FinTech ('financial technology'), RegTech ('regulatory technology'), cryptocurrencies, and digital assets as one of the most discussed emerging technological evolutions in global finance. Yet little is really understood about its meaning, legal implications, and policy consequences. In this article we introduce DeFi, put DeFi in the context of the traditional financial economy, connect DeFi to open banking, and end with some policy considerations. We suggest that decentralization has the potential to undermine traditional forms of accountability and erode the effectiveness of traditional financial regulation and enforcement. At the same time, we find that where parts of the financial services value chain are decentralized, there will be a reconcentration in a different (but possibly less regulated, less visible, and less transparent) part of the value chain. DeFi regulation could, and should, focus on this reconcentrated portion of the value chain to ensure effective oversight and risk control. Rather than eliminating the need for regulation, in fact DeFi requires regulation in order to achieve its core objective of decentralization. Furthermore, DeFi potentially offers an opportunity for the development of an entirely new way to design regulation: the idea of 'embedded regulation'. Regulatory approaches could be built into the design of DeFi, thus potentially decentralizing both finance and its regulation, in the ultimate expression of RegTech.

KEYWORDS: decentralized finance; FinTech; RegTech; financial regulation; blockchain; distributed ledger technology

[†] Dirk A Zetzsche is Professor of Law, ADA Chair in Financial Law (Inclusive Finance), Faculty of Law, Economics and Finance, University of Luxembourg; Director, Center for Business and Corporate Law, Heinrich-Heine-University. Dirk can be contacted at Dirk.Zetzsche@uni.li

^{*} Douglas W Arner is Kerry Holdings Professor in Law and Director, Asian Institute of International Financial Law, University of Hong Kong; Board Member, Centre for Finance, Technology & Entrepreneurship. Douglas can be contacted at douglas.arner@hku.hk

^{**} Ross P Buckley is KPMG Law and King & Wood Mallesons Professor of Disruptive Innovation, Australian Research Council Laureate Fellow, and Scientia Professor, UNSW Sydney. This article benefited from presentation at the Georgetown University / Barbados Financial Services Commission Seminar on Sustainable De-Fi and Financial Inclusion and from the helpful discussions, comments, and questions from Chris Brummer and other event participants: Linn Anker-Sørensen, Raphael Auer, Luca Enriques, Jon Frost, and Dirk Schoenmaker. The authors thank the Georgetown University's Institute of International Economic Law, the Hong Kong Research Grants Council Research Impact Fund, the Qatar National Research Fund National Priorities Programme, and the Australian Research Council Laureate Fellowship, for financial support, and Mia Trzcinski and Jessie Xiao for their expert research assistance. All responsibility is the authors'. Ross can be contacted at ross.buckley@unsw.edu.au

I. INTRODUCTION

'Decentralized Finance' (DeFi) is neither a legal nor a technical term. It is nonetheless increasingly used in the context of discussions about the future evolution of finance and its regulation. Common usage incorporates one or more elements of: (i) decentralization; (ii) distributed ledger technology and blockchain; (iii) smart contracts; (iv) disintermediation; and (v) open banking.¹ While decentralized systems such as Bitcoin rely on distributed ledger technology (DLT) and blockchain to underpin token-based ecosystems, the combination of DLT and blockchain is not the only way to achieve decentralization. Further, many distributed ledgers (and most distributed ledgers operated by large financial intermediaries) operate today with a hierarchical, centralized governance model, limiting access to permissioned participants only. In turn, decentralized does not necessarily mean distributed.² In a similar way, disintermediation is not a prerequisite for decentralization; rather, disintermediation may be one (side) effect of decentralization, given that the establishment costs of centralized infrastructure will be difficult to recoup in a world where services can be provided on a distributed or decentralized basis. Hence, in this article we understand DeFi to comprise, at its core, what its simple name suggests: the *decentralized* provision of financial services³ through a mix of infrastructure, markets, technology, methods, and

- 1 See Fabian Schär, 'Decentralized Finance: On Blockchain- and Smart Contract-based Financial Markets' (2020) <<https://ssrn.com/abstract=3571335>> accessed 20 August 2020 ('Decentralized Finance (DeFi) ... generally refers to open financial infrastructures built upon public smart contract platforms, such as the Ethereum blockchain. . . . In contrast to the traditional financial sector, DeFi does not rely on intermediaries and centralized institutions. Instead, it is based on open protocols and decentralized applications (DApps)'); Yan Chen and Cristiano Bellavitis, 'Decentralized Finance: Blockchain Technology and the Quest for an Open Financial System' (2020) 13 *Journal of Business Venturing Insights* (forthcoming 2019) ('Blockchain technology reduces transaction costs, creating a new paradigm for decentralized business models, which has led to the emergence of decentralized finance'); Robert Leonhard, 'Decentralized Finance on the Ethereum Blockchain' (2019) <<https://ssrn.com/abstract=3359732>> accessed 20 August 2020 ('This essay proposes an alternative form of financial planning that circumvents dysfunctional governments and insolvent banks. This alternative is referenced in online parlance as "decentralized finance." The decentralized aspect derives from its use of the 6 blockchain protocol, which powers cryptocurrencies'). This view is confirmed by technologically oriented websites, see BitKom, 'Decentralized Finance (DeFi)—A New Fintech Revolution? The Blockchain Trend explained' (2020) <https://www.bitkom.org/sites/default/files/2020-07/200729_whitepaper_decentralized-finance.pdf> accessed 20 August 2020 at 4 ('DeFi refers to an ecosystem of financial applications that are built on top of a blockchain. Its common goal is to develop and operate in a decentralized way—without intermediaries such as banks, payment service providers or investment funds—all types of financial services on top of a transparent and trustless blockchain network'); EthHub, *Decentralized Finance* <<https://docs.ethhub.io/built-on-ethereum/open-finance/what-is-open-finance>> accessed 20 August 2020 ('Decentralized Finance (a.k.a. "DeFi" or "Open Finance") refers to a number of decentralized protocols building open financial infrastructure. These protocols are valuable because they're creating the necessary plumbing to enable anyone in the world with an internet connection to access self-sovereign, censorship resistant financial services').
- 2 See for cryptoassets, specifically, Angela Walch, 'Deconstructing "Decentralization": Exploring the Core Claim of Crypto Systems' in Chris Brummer (ed), *Crypto Assets: Legal and Monetary Perspectives* (Oxford University Press 2019) 39, 49.
- 3 Decentralization with a focus on financial regulation has been, to our knowledge, not previously discussed from a legal perspective. Similar concerns were raised, however, in the context of blockchain-based crypto assets. See, for instance, Walch (n 2) 47–51 (starting with the statement that 'no one knows what decentralization means', describing a number of features of decentralization, and concluding (at 67) that the fuzziness of the term 'decentralized' has significant implications for law making as it furthers unsubstantiated conclusions.) We share Angela Walch's concern, yet see merit in analysing decentralization as a real-world phenomenon

applications. Decentralized provision of financial services means, in turn, provision by multiple participants, intermediaries, and end-users spread over multiple jurisdictions, with interactions facilitated, and often in fact enabled in the first place, by technology.

We analyse the roots and tools of this decentralization of financial services and focus on how financial regulation will need to respond to it. In particular, we place DeFi in the context of the traditional financial economy, connect DeFi to open banking and RegTech ('regulatory technology'), and end with some policy considerations.

Many find the promise of decentralization and its potential to displace the regulatory state with technology as a seductive ideal. We take a different approach here: rather than arguing the potential benefits of DeFi, we seek to identify what is actually taking place and the sorts of regulatory implications this may have. We analyse DeFi, not as a desired goal, but as a real-world phenomenon, and seek to understand the growing challenges this trend poses for financial regulation. Challenges to traditional modes of governance and regulation are one aspect.

We suggest that decentralization has the potential to undermine traditional forms of accountability and erode the effectiveness of traditional financial regulation and enforcement. We also predict some surprising effects: where parts of the financial services value chain are decentralized, we expect reconcentration in a different (but possibly less regulated, less visible, and less transparent) part of the value chain.

In short, DeFi requires careful regulatory attention. In situations where DeFi produces new forms of technological reliance, regulation needs to focus on the reconcentrated portion of the value chain to ensure effective oversight and risk control: in this framework, regulation is necessary in order to support decentralization, in much the same way that regulation is at the core of securities markets and other financial services. In other situations, regulation will be necessary to protect markets and participants from predation by non-decentralized system, for instance when a participant in one market seeks to take advantage of technology for regulatory arbitrage.

In more visionary ways of thinking, regulation may insist that compliance requirements and real-time supervisory access be embedded in the very technology that allows for decentralization, thereby potentially decentralizing both finance and its regulation in the ultimate expression of RegTech: not only 'embedded supervision' as suggested by Auer but in fact 'embedded regulation.'⁴

The article is structured as follows. [Section II](#) seeks to place DeFi in the context of traditional finance and its regulation. [Section III](#) (far from claiming completeness)

in finance (as we do in this article), in contrast to using it as a descriptive term for a certain technology or application (as many do for cryptoassets). See also Wulf A Kaal, 'Decentralization—Past, Present, and Future' (2019) University of St Thomas (Minnesota) Legal Studies Research Paper No 19–23 <<https://ssrn.com/abstract=3411897>> accessed 20 August 2020 (engaging in a general analysis of the impact of decentralization on commerce and society and arguing that 'no two minds will agree on a common definition or scope and scale of decentralization' before stating that 'decentralization is not synonymous with partnership, delegation, de-concentration, disassortative, devolution, circulation', and that '[d]ecentralization is not the addition of hierarchical levels in a centralized organization' nor 'just the redistribution of centrally organized authority or redistribution of centrally collected revenue' nor 'the delegation of centralized authority to managers on all levels of an organization').

4 Raphael Auer, 'Embedded supervision: how to build regulation into blockchain finance' BIS Working Paper 811 (2019) <<https://www.bis.org/publ/work811.htm>> accessed 20 August 2020.

seeks to highlight the central elements from a technical perspective of DeFi. Sections IV and V address financial regulation and supervision, analysing first the challenges for financial supervision and enforcement before turning to the options available to regulators and law makers across the globe. Section VI considers the connection between decentralization and open banking, arguing that decentralization requires sovereign intervention from several different standpoints: from the standpoint of mandating open and enforcing open access to data; from the standpoint of supervising or even operating the core underlying technological infrastructure; and from the standpoint of requiring the embedding of regulation directly into DeFi systems. Section VII concludes.

II. DEFI VS TRADITIONAL FINANCE

While most recent treatments approach DeFi from a technical perspective,⁵ it is instructive to first highlight the structure of traditional finance before turning to discussion of how DeFi may contrast to this.

1. Traditional finance

At the heart of market-based finance is a series of intermediaries that bring together disparate participants. The paradigmatic intermediaries are financial institutions such as banks, and market providers such as securities exchanges. These intermediaries bring together a range of financial market participants, in particular those with finance resources (for example savers, lenders, and investors) and those seeking financial resources (for example borrowers, entrepreneurs etc). We often think of the intermediary as the central point when separating market-based financial systems into their traditional sectors of money, payments, banking, securities, and insurance.

Traditional finance is thus characterized by major intermediaries, which centralize functions and financial resources. This results in the hub-and-spoke conceptualization of finance and centres of finance. Technology and globalization together characterize traditional finance today.

2. Centralization for scale

When clients have local access to services such as payments, ATMs, savings, investments, and insurance, these services are not provided at the point of access. Rather, financial markets and activities traditionally cluster in local, regional, and super-regional/global access points ('hubs').⁶ These services are in substance provided from a financial centre where sufficient concentration of transaction volumes and numbers in a given sector(s) or service(s) allow the development of expertise and resources.⁷ Depending on the sector(s) / service(s), the required volume and numbers may be developed locally, regionally, or globally.

5 See for instance Schär (n 1) (detailing tokenized applications); Chen and Bellavitis (n 1) (relying on specific examples), Leonhard (n 1) (analysing opportunities to decentralize on the Ethereum blockchain).

6 Douglas W Arner, 'The Competition of International Financial Centres and the Rule of Law' in K Meesen (ed), *Economic Law as an Economic Good* (Sellier 2009) 203.

7 Arner (n 6).

Take the example of a rarely traded currency issued by a developing country's central bank. The currency tends to be illiquid as there is limited demand, often aggravated by underdeveloped market infrastructure and barriers to access. In order to bring together sufficient supply and demand, and for transactions to take place at all, it may be necessary to look beyond the domestic market to regional or global markets. Similarly, certain investment and insurance services require global diversification to function well. In contrast, the domestic or regional level typically provides sufficient scale for the efficient provision of basic financial services such as cash business (ATMs), savings, and loans.

Following this economic logic, financial centres have evolved, with local, regional, and global roles and significance. For instance, New York, London, and Hong Kong provide investment banking services around the globe—or at least throughout their region/timezone. London (at least prior to Brexit) served as a centre of the global derivatives and foreign exchange markets; Luxembourg served as the global investment fund hub; Switzerland and Singapore served as global private banking centres; and the Bahamas served as a global insurance hub. Centres are constantly evolving and competing, with competition in FinTech ('financial technology') in particular now focusing on Singapore and London.⁸ As a competitive factor, these hubs usually provide tailor-made sets of financial regulation and enforcement of these rules, in an effort to protect the parties transacting through the hub.

3. Regulation and traditional finance

These financial centres fundamentally depend on trust and confidence in order to function.⁹ Trust and confidence, along with the basic functioning of financial systems, is underpinned by law: rules, institutions, regulation, and courts.¹⁰ While many of these systems originally evolved as forms of private ordering or self-regulatory frameworks, over time the state has taken an increasing role as a result of failures of private ordering and self-regulation that have come to the surface periodically, often in the context of financial crises. This can be seen in the context of money as a sovereign function, as well as the role of government regulation in almost all aspects of finance, in particular in the aftermath of the 2008 financial crisis.

Market-based financial systems thus are often seen as fundamentally unstable, with instability and other forms of market failures being addressed by regulation, albeit never entirely successfully.¹¹

8 See Deloitte, *FSIReview: Driving FinTech Innovation in Financial Services* Issue 13 (November 2016) 2 <www2.deloitte.com/content/dam/Deloitte/sg/Documents/financial-services/sg-fsi-fsireview-issue13-fintech.pdf> accessed 20 August 2020; ICAEW, 'Fintech Innovation: Perspectives from Singapore and London' (2018) 3 <<https://charteredaccountantsworldwide.com/wp-content/uploads/2018/12/isca-icaew-fintech-innovation-perspectives-from-singapore-and-london-final.pdf>> accessed 20 August 2020.

9 DW Arner, *Financial Stability, Economic Growth and the Role of Law* (Cambridge University Press 2007).

10 See K Pistor, *The Code of Capital* (Princeton University Press 2019).

11 RP Buckley and DW Arner, *From Crisis to Crisis: The Global Financial System and Regulatory Failure* (Kluwer Law International 2011).

It is this weakness that underlies the ideal of DeFi and its techno-utopian vision of finance without the dominance of concentrated intermediaries—and the too-big-to-fail risks that they embody—and without reliance on the weaknesses of states, governments, and regulators. DeFi presents a vision of a world in which technology replaces frail humans and their institutions. It is at its heart a utopian vision but one with attractions for many. However, over time, it has moved from a utopian vision to a simpler idea in which technology can potentially eliminate the risks inherent in the concentrated systems central to traditional finance.

4. DeFi: a response and challenge for traditional modes and conceptions of finance?

In the past, hubs were necessary since services were provided locally and booked on a single balance sheet, with the provider of that balance sheet usually headquartered in a hub. This hub would usually be protected by high regulatory and supervisory standards, reflecting the large quantity of risks from pooling and balance sheet concentration at the hub.

DeFi challenges this hub logic. Where scale can be created by technology rather than by bundling business in a hub, hubs make little sense, because a hub comes with downsides for clients: they need to adjust in terms of language and law, subscribe to the high compliance standards reflecting the concentration of risks, accept information costs (for instance, for legal counsel), and may be subject to penalties for non-compliance with laws implemented at the hub level, but not (yet) at the local level. As many developing countries lack equivalent regulation and supervision, hub access becomes problematic. Clients from countries with weaker institutional environments need to rely on costly workarounds, sometimes through several jurisdictions functioning as regional hubs (in particular as often seen in the Gulf). This means that firms from developing countries can often only access services provided in global financial centres indirectly (albeit at cheaper costs than by accessing them directly). In the example used for emerging market currencies, for instance, services could be tokenized and provided to the token holder regardless of places of origin of provider and recipient, with Bitcoin a prominent example: Bitcoin holders are linked through common technology rather than a massive balance sheet in a highly regulated payment hub.

Finally, hub structures create dependencies which may be unattractive from the political standpoint—for instance, if RMB or EUR are settled in London or New York, the English and US regulators acquire influence over the currency, which may be used in the political context.

As a result of technological evolution, the future of finance may look different. This justifies a closer look at the underlying technologies, systems and infrastructure that underpin decentralization and decentralized finance—the focus of [section III](#). However, as we argue in the remainder of this article, we suspect that the future may not look so different after all—we consider it more likely that traditional finance will assimilate DeFi and in particular its core technologies rather than vice versa.

III. DEFI AND ITS TECHNOLOGICAL FOUNDATIONS

Underlying the utopian ideal of DeFi—an ideal in which technology allows the elimination of the traditional centralized governance structures seen with traditional finance and financial centres—as well as its more pragmatic practical evolution, is a series of technologies. As a result of long-term technological evolutionary processes, the technological potential to underpin entire systems without any one necessarily being in charge exists, as demonstrated—if nothing else—by Bitcoin.

1. DeFi and the patterns of technological evolution

DeFi emerges from three important patterns in technological evolution: Moore's law, Kryder's law, and another pattern for which there is, to our knowledge, no term yet established. Moore's law refers to the assumption that the amount of data processing power grows exponentially.¹² Kryder's law posits the same for data storage capacity.¹³ The combination of ever-increasing processing power and ever-increasing data storage capacity leads to ever-lower costs for both. The third factor making DeFi possible is the tremendous growth we have seen in communications bandwidth combined with decreasing costs—a phenomenon which has been discussed since the late 1990s,¹⁴ if not earlier. The underlying assumption of bandwidth growth at decreasing costs is supported by increasing network efficiencies, which lead to more bandwidth per dollar invested. This may arise, inter alia, from lower production costs of network components, denser and faster ports, higher utilization, and integrated photonics,¹⁵ or the use of higher frequency microwaves requiring smaller cells using multiple frequency bands (with 5G as an example).

These three evolutionary patterns enable hardware virtualization: software is hosted, updated, and run at decentralized servers rather than on each workstation. Only data that needs to be processed locally (under conditions of instant online connection and abundant bandwidth) tends to remain processed locally. Hardware virtualization allows for the creation and set-up of service-oriented architecture ('software as a service') which is at the heart of DeFi. Interestingly, at the same time Moore's law, Kryder's law, and bandwidth growth at decreasing costs all continue to apply, providing the potential for ever greater development of machine learning and other forms of artificial

12 According to the prediction by Intel's founder, Gordon Moore, in 1965 (referred to as Moore's law), the number of transistors that could be fixed per square inch on integrated circuits doubles every two years, while the costs are halved. Moore's law predicted an enormous increase in data processing capacity. See Gordon E Moore, 'Cramming More Components onto Integrated Circuits' (1965) 38(8) *Electronics* 114.

13 Mark Kryder was Seagate Corp's senior vice president of research and chief technology officer who focused on information storage throughout his life. Former CNN journalist Chip Walter honoured Mark Kryder's lifetime achievement in an article highlighting the rising hard-disk capacity against the background of rising processor capacity (referred to as Moore's law: see n 12). See Chip Walter, 'Kryder's Law' (2005) 239(2) *Scientific American* 32.

14 See CA Eldering, ML Sylla and JA Eisenach, 'Is there a Moore's law for bandwidth?' (1999) 37 *IEEE Communications Magazine* 117; KG Coffman and AM Odlyzko, 'Internet growth: Is there a "Moore's Law" for data traffic?' in James Abello, Panos M Pardalos and Mauricio GC Resende (eds), *Handbook of Massive Data Sets* (Springer 2002).

15 See, for these technical preconditions, Scott Kipp, 'Exponential Bandwidth Growth and Cost Declines' *Network World* (10 April 2012) <www.networkworld.com/article/2187538/exponential-bandwidth-growth-and-cost-declines.html> accessed 20 August 2020.

intelligence (AI)¹⁶ as well as ‘edge’ based systems, where significant amounts of independent processing takes place in the context of individual devices (for instance in the context of the Internet of Things (IoT) accessing virtual as well as local data and processing power). These trends in technology and in the intellectual processes which allow their combination and use in ever more ways are transforming finance and most everything else as well.

2. ABCD: the roots of DeFi

At the core of DeFi stand a number of new technologies best summarized with the acronym ‘ABCD’, representing the four technologies at the heart of FinTech and RegTech: **AI**, **Blockchain** (including distributed ledgers and smart contracts), **Cloud**, and **Data** (big and small); or, in another iteration, **AI**, **Big Data**, **Cloud**, and **DLT** (including blockchain and smart contracts).

Although many will be familiar with these concepts, we will give a brief account of the underlying technologies to underpin our analysis of DeFi’s policy implications.

a. Artificial intelligence

The idea underlying AI is to develop software that mimics human cognitive functions, such as ‘learning’ and ‘problem solving’.¹⁷ AI puts data to use by drawing conclusions as to the probability of an event from prior knowledge of conditions related to the event; the greater the volume of data, the more insightful and accurate the inferences drawn from the data.¹⁸ Machine learning is a subset of AI that uses statistical, data-based methods to progressively improve the performance of computers on a given task, without humans reprogramming the computer system to achieve enhanced performance.¹⁹ In practice, the learning is achieved through extensive ‘practice’ with multiple feedback rounds through which the machine is told whether it has passed or failed a task.

b. Blockchain, distributed ledger technology, and smart contracts

A distributed ledger is ‘a database that is consensually shared and synchronized across networks spread across multiple sites, institutions or geographies, allowing a transaction to have [multiple private or] public “witnesses”’.²⁰ The sharing of data results in a database distributed across a network of servers, all of which together function as a

16 See Dirk A Zetzsche and others, ‘Artificial Intelligence in Finance: Putting the Human in the Loop’ CFTE Academic Paper Series 1/2020 <<https://ssrn.com/abstract=3531711>> accessed 20 August 2020.

17 See Stuart J Russel and Peter Norvig, *Artificial Intelligence: A Modern Approach* (3rd edn, Pearson 2016) (defining AI as devices that perceive their environment and take actions that maximize their chances of successfully achieving their task and describing the origin of the term AI in the Turing Test where ‘a computer passes the test if a human interrogator, after posing some written questions, cannot tell whether the written responses come from a person or from a computer’, and defining six core capabilities that together compose most of AI, including natural language processing, knowledge representation, automated reasoning, machine learning, computer vision, and robotics). The seminal work on AI is of course Alan M Turing, ‘Computer Machinery and Intelligence’ (1950) 49 *Mind* 433.

18 Russel and Norvig (n 17) 495–99.

19 Russel and Norvig (n 17) 693–859 (describing the training methods).

20 World Economic Forum, ‘Innovation-Driven Cyber-Risk to Customer Data in Financial Services’ White Paper 5 (2017) 6 (Figure 2) <www3.weforum.org/docs/WEF_Cyber_Risk_to_Customer_Data.pdf> accessed 20 August 2020.

ledger.²¹ Distributed ledgers are characterized by an absence of, or minimal, central administration and no centralized data storage. They are, hence, ‘distributed’, in the sense that the authorization for the recording of a given piece of information results from the software-driven interaction of multiple participants. Coupled with cryptographic solutions, such features (decentralization and distribution across a network of computers) curtail the risk of data manipulation,²² thereby solving the problem of having to trust third parties, specifically data storage service providers, as this is the point where the data is stored and can most easily be manipulated.²³

The modus operandi of distributed ledgers is best understood by looking at their counterpart, the concentrated ledger. Let us assume that a centralized register administered by a single entity contains all relevant data, and let us further assume that, contrary to present practice, the centralized register is not secured and thus ‘semi-distributed’ through a myriad of back-ups stored on multiple servers. That arrangement entails a number of risks. First, if the hardware where the register is ‘located’ is destroyed, the information content, as well as the authority to ascertain that it is correct, is lost. Second, disloyal employees of the database administrator or an unfaithful administrator may manipulate the information content of the register. Third, a cyber-attack may result in manipulations and data losses.²⁴

Distributed ledgers address these problems by raising the barrier for manipulation. The underlying technology requires consensus of many data storage points (‘nodes’). If there are n nodes (instead of one concentrated ledger) and e describes the effort necessary to break into any single server, all other conditions being equal (safety per server etc), the effort necessary to manipulate all the linked servers will be $n \times e$ rather than $1 \times e$.

Distributed ledgers are usually paired with a blockchain protocol. Blockchain refers to the storage of data in data bundles (the ‘blocks’) in a strict time-related series with each block linked to the previous and subsequent blocks through a time stamp as well as a number of protocols providing evidence of a user’s authority to amend the data stored.²⁵ The blockchain renders data corruption even harder, because a successful cyberattack would have to simultaneously corrupt not just one set of data

21 See David Mills and others, ‘Distributed Ledger Technology in Payments, Clearing, and Settlement’ Washington: Board of Governors of the Federal Reserve System, Finance and Economics Discussion Series 2016-095 (2016) 10–11 <<https://doi.org/10.17016/FEDS.2016.095>> accessed 20 August 2020.

22 We do not claim that distribution of ledgers is the sole instrument available to curtail data manipulation. For instance, lack of data manipulation can easily be proven in a centralized system using cryptographic techniques.

23 See Sinclair Davidson, Primavera De Filippi and Jason Potts, ‘Blockchains and the Economic Institutions of Capitalism’ (2018) 14 Journal of Institutional Economics 639 (arguing that blockchain technology is a new governance institution that competes with other economic institutions of capitalism, namely firms, markets, networks, and even governments); Primavera De Filippi and Aaron Wright, *Blockchain and the Law: The Rule of Code* (Harvard University Press 2018) 55, 136–40 (arguing that widespread deployment of blockchain will lead to tech-based business practices that could prompt a decline in importance of centralized authorities, such as governments, and urging a more active regulatory approach).

24 Any server can be manipulated with sufficient computing power and time (even if no other weakness in an encryption system is known to the attackers). See generally Jean-Philippe Aumasson, *Serious Cryptography: A Practical Introduction to Modern Encryption* (No Starch Press 2017) 10–18, 40–48.

25 These protocols seek to address the risk that the timestamp may be unreliable, or open to easy manipulation.

but all subsequent data sets (ie the whole blockchain) as well as the time stamps simultaneously.

Distributed ledgers have provided fertile ground for the application of another innovation that seeks to address the problem of trust in human interactions (in particular relating to compliance with and enforcement of contracts) while at the same enhancing efficiency: smart contracts.²⁶ While neither smart, nor contracts in a legal sense, they are self-executing software protocols that reflect some of the terms of an agreement between two parties.²⁷ The conditions of the agreement are directly written into lines of code. Smart contracts permit the execution of transactions between disparate, anonymous parties without the need for an external enforcement mechanism (such as a court, an arbitrator, or a central clearing facility). They render transactions traceable, transparent, and irreversible. Processes driven by smart contracts may take place via and be recorded on distributed ledgers secured via blockchain. This particular combination is at the core of most discussions relating to DeFi.²⁸

c. Cloud services

DeFi, with regard to cloud computing,²⁹ refers to the decentralization of server capacity. Rather than using one server at one server centre, datasets can be distributed over many server centres accessible through the internet by many users located around the globe, more or less simultaneously.

Cloud computing refers to on-demand availability of data storage and processing power without the users owning or controlling the servers providing these services. Cloud computing relies on data centres operated by commercial providers; these providers rent capacity to customers, who access the capacity over the internet.

In order to provide for cloud stability in light of volatile demand and energy supply, to diversify against demand peaks, and ensure economic operations where energy costs fluctuate through the day, cloud service providers typically link server centres across different time zones, countries, and economic regions, and channel excess demand to servers where data processing capacity is cheaper, due to lower demand and energy costs.

d. Data

Data are at the core of all of these innovations, resulting from the digitization of an ever-increasing range of processes: the idea of the 'digitization of everything' that underlies theories of the Fourth Industrial Revolution.³⁰ The ever-greater volume

26 See Kevin Werbach and Nicolas Cornell, 'Contracts Ex Machina' (2017) 67 Duke Law Journal 313.

27 Smart contracts can implement and execute contractual conditions and, in this sense, certainly have legal effect, as identified by the UK LawTech Delivery Panel, *Legal Statement on Cryptoassets and Smart Contracts* (2019), at 8, but smart contracts cannot yet typically in practice embody all the terms of an enforceable legal contract purely in code.

28 See n 1 and accompanying text.

29 For an overview of cloud computing in the *regulated* financial sector see Hal S Scott, John Gulliver and Hillel Nadler, 'Cloud Computing in the Financial Sector: A Global Perspective' Program on International Financial Systems 2019 (July 2019).

30 See Klaus Schwab, *Fourth Industrial Revolution* (World Economic Forum 2016) 9–14 (predicting profound and systemic change due to physical, digital, and biological megatrends driving the renewal of industrial production).

of data supports both traditional data analytics and ‘Big Data’ approaches. Big Data analytics refers to the collection and processing of data sets that are too large or too complex for traditional data processing applications.³¹ Big Data applications look at massive numbers of data points and apply advanced data analytics methods to detect unexpected correlations, test expected correlations for causation, or determine the probability of a predefined pattern.³²

3. The interrelations between DeFi and ABCD

These four rapidly evolving technologies are each typically central to, because they are applied in the pursuit of, the decentralization of finance. Many decentralized financial functions utilize (i) the powerful efficiencies and cost-savings offered by AI; (ii) the superior record-keeping and efficiencies of smart contracts embedded on distributed ledgers secured via blockchain; (iii) the potentially decisive power of the algorithmic analysis of data; and (iv) cloud systems to host virtually all decentralized financial functions.³³ Each of these four technologies benefit from the ‘laws’ of technology discussed earlier, since each of these technologies individually becomes less expensive and more convenient and efficient to use—thus enabling cooperation among the multiple participants that together provide the financial services in a decentralized manner.

4. Libra as DeFi?

An example of how DeFi might manifest may prove helpful. Probably the most successful example so far is Bitcoin—in terms of its decentralization if not its financial utility. Perhaps the most significant proposal so far is the first generation of Facebook’s Libra proposal, Libra 1.0.³⁴ While Libra 1.0 was to start as a centralized permissioned system, it intended eventually to become a decentralized permissionless system.³⁵ In the Libra 1.0 structure, the consortium participants (a number of multinational firms and organizations) would function as nodes linking a myriad of Libra exchanges and wallet providers (attached to the Libra distributed ledger) to Libra holders. Libra 1.0

31 See Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (John Murray 2013) 12–14 (predicting that big data will transform societies).

32 Mayer-Schönberger and Cukier (n 31) 6 (stating that the volume of information has outpaced IT engineers’ manual data handling capacity so that they need to reinvent data analysis tools; the latter will result in new forms of value creation that will affect markets, organizations, and other institutions).

33 Data stored ‘in the cloud’ are data stored on servers accessible from various points across the world that can be accessed and stored by many users distributed across the globe.

34 See Dirk Zetsche, Ross Buckley and Douglas Arner, ‘Regulating Libra’ *Oxford Journal of Legal Studies* (forthcoming 2020); Libra Association, ‘White Paper v2.0’ (April 2020) <<https://libra.org/en-US/white-paper/>> accessed 20 August 2020.

35 Libra 2.0 is no longer planning to move to a permissionless system. The Libra 2.0 white paper states:

In the first Libra white paper, we sought to achieve this goal by announcing our intention to eventually transition the network to a permissionless system. However, in the months since, a key concern expressed by regulators in a number of jurisdictions, including the Swiss Financial Market Supervisory Authority (FINMA), is that it would be challenging for the Association to guarantee that the compliance provisions of the network would be maintained if it were to transition to a permissionless network where, for example, no due diligence is performed on validators.

Rather, Libra’s intention now is to forego ‘the future transition to a permissionless system while maintaining its key economic properties’. See Libra Association (n 34).

has been replaced by Libra 2.0, which has a similar structure, albeit in the context of a permanently permissioned network; hence it will not form an example of DeFi in its purest form but instead risks resulting in exactly the sort of centralization of power and control against which DeFi rebels.

Libra 1.0 demonstrated how in some cases it would be possible for DeFi not necessarily to mean all parts of the system must be decentralized. The structure of Libra 1.0's node function was to be, at least initially, only partially distributed, with the blockchain operating as a private, rather than public, system. The potential liability of the large players that would function as nodes of the Libra blockchain provides an important incentive for this approach: their large balance sheets and clear localization mean they would be held liable in case of default, malfunction, and misconduct, while the many individuals relying on Libra would probably not face these risks.³⁶ At the same time of course, this structure would allow the early consortia members to benefit directly from their investment. For these and other reasons, by far the largest number of DLT applications in finance are structured as permissioned as opposed to permissionless systems. This, of course, now includes Libra 2.0 as well.

While the transformative potential of permissionless systems excites, the economic and legal realities in most cases—with the conspicuous exception of Bitcoin—have prevented full decentralization to date. However, efforts in this respect are at the heart of the DeFi ideal, if not its actual evolution.

Despite technological limitations of the Bitcoin design, particularly in terms of speed and scalability, DeFi enthusiasts argue that the cryptoanarchist vision which was part of the motivation for Bitcoin is now attainable: the democratization of finance.

5. 'Democratization' of finance

DeFi enthusiasts go beyond technical decentralization. For them, DeFi offers governance structures they perceive as the 'democratization' of finance, while incumbents might well view such structures as 'anarchy'.

At the core of this claim lies a positive connotation of disintermediation (understood as disrupting incumbent financial institutions, particularly those that are very large: the 'too-big-to-fail' problem at the heart of the 2008 financial crisis) and of decreasing state influence and control of the financial system. Tech proponents frame the vision as follows:

Imagine a global, open alternative to every financial service you use today—savings, loans, trading, insurance and more—accessible to anyone in the world with a smartphone and internet connection.³⁷

36 On liability of nodes in DLTs, see Dirk Zetsche, Ross Buckley and Douglas Arner, 'The Distributed Liability of Distributed Ledgers' [2018] *University of Illinois Law Review* 1361, 1383–86. See also Philipp Hacker, 'Corporate Governance for Complex Cryptocurrencies? A Framework for Stability and Decision Making in Blockchain-Based Organizations' in Philipp Hacker and others (eds), *Regulating Blockchain: Techno-Social and Legal Challenges* (Oxford University Press 2019).

37 See Sid Coelho-Prabhu, 'A Beginner's Guide to Decentralized Finance (DeFi)' *CoinBase* (6 January 2020) <<https://blog.coinbase.com/a-beginners-guide-to-decentralized-finance-defi-574c68ff43c4>> accessed 20 August 2020.

At a first look, such an idea seems to be very attractive, not least from the standpoint of financial inclusion, an area where we likewise argue that digital finance has transformative potential³⁸ which comes from the decentralization of finance enabling the embedding of local compliance standards and customs which tend to reduce costs of access to financial services. The DeFi vision however is more than this: the objective is to develop systems which use technology to eliminate borders, jurisdiction, and the necessity of centralized control including governments. However, further analysis reveals that much larger challenges are likely to arise (discussed in [sections IV and V](#)), which leads us to challenge whether DeFi, certainly in its purest form, is in fact desirable, without even addressing the limited likelihood of it coming to pass.

These ideas also relate to one of the other major themes emerging in finance: the idea of ‘open banking’ or ‘open finance’, to which we return in [section VI](#).

IV. DEFI VS THE STATE

Despite the excitement over its potential, DeFi comes with many challenges. From a legal perspective, DeFi may arguably undermine the rule of law, at least as we normally think about this from the standpoint of the Westphalian nation-state, and may also bring tech risks previously unknown and on a scale never before seen.

1. Undermining the rule of law?

In terms of the rule of law, DeFi poses a direct challenge to state-based systems, in that in its strong form (as fully decentralized finance) it seeks to eliminate the role of the state as rule-maker and enforcer. In its purest expression, DeFi thus serves as the ultimate form of ‘code is law’, with technology replacing state-based legal systems.³⁹ But beyond the obvious challenge of the strong form of DeFi, weaker forms of DeFi (in which some control remains with system operators) nonetheless pose major challenges for traditional geographically based, nation-state legal systems.

2. The challenges of jurisdiction, enforcement, and data protection and privacy

Three examples highlight how DeFi may be seen to undermine the rule of law: legal jurisdiction and applicable law, enforcement, and data protection and privacy.

a. Jurisdiction and applicable law

In a DeFi world of whatever form—anywhere along the spectrum from fully centralized to fully decentralized—determining the jurisdiction of courts and applicable law becomes increasingly difficult. Take, for instance, an unincorporated distributed ledger system, such as those used for Bitcoin or Ether. Private international law and

38 See Douglas W Arner, Ross P Buckley and Dirk A Zetzsche, ‘Fintech for Financial Inclusion: A Framework for Digital Financial Transformation’ UNSW Law Research Paper No 18–87 (2018) 13, 18 <<https://ssrn.com/abstract=3245287>> accessed 20 August 2020.

39 See John Flood and Lachlan Robb, ‘Trust, Anarcho-Capitalism, Blockchain and Initial Coin Offerings’ Griffith Law School Research Paper No 17–23 (2017), 19 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3074263> accessed 20 August 2020; Lawrence Lessig, *Code Version 2.0* (Basic Books 2006) ch 1 ‘Code is Law’ <<http://codev2.cc/download+remix/Lessig-Codev2.pdf>> accessed 20 August 2020.

civil procedural law look at the substantive claim to determine a court's jurisdiction and the applicable law. The substantive claim regarding distributed ledgers may be based on entirely different legal concepts in different jurisdictions, including but not limited to contracts, torts, joint venture and partnership law, antitrust law, and in some jurisdictions blockchain-specific legislation.⁴⁰ Decentralization results in uncertainty as to which courts and laws apply—if any.⁴¹

The same concern—determining jurisdiction—also extends to matters of financial regulation. While we think of finance as global, as is logical given the hub structure outlined at [section II.1](#), the reality is a world of individual legal jurisdictions and regulators, coordinated through a range of soft-law systems. Established approaches tend to look at the entity that provides the service, the client to whom the product is sold or services provided, or the market in which it is traded. Each of these is problematic in the age of DeFi: in a network economy multiple entities provide parts of a service and clients are similarly spread around the globe, and markets and individual providers lose importance as supervisory access and control points.

Further, technology allowing decentralization may render entity-based approaches generally less effective.⁴² The often-discussed alternative—a focus on functions—may be less than convincing where the services are performed by a set of algorithms in a permissionless system, for two reasons: first, where decentralization is advanced it would require the supervision of a myriad of small contributors to the services, many of which lack the size and financial resources to pay supervision fees and many of which contribute only gradually and partially to the overall service; and, second, machine learning technologies may permanently change the nature of these functions.⁴³ DeFi may force us to look beyond the entities involved and concentrate supervisory efforts on the underlying technological infrastructure that ties all contributors together. In fact, more and more of the risks in DeFi projects will come from the technology connecting all relevant entities rather than simply the entities formally connected to the project.

Take the example of BlackRock's risk management platform, Aladdin.⁴⁴ Beyond BlackRock's own US\$6 trillion in assets under management, Aladdin provides risk data, and measures and controls risk for more than US\$20 trillion in assets, which is around 10 per cent of the world's financial assets—a figure equal to four times the value of all

40 See Zetzsche, Buckley and Arner (n 36) 1391–402.

41 See Matthias Lehmann, 'Who Owns Bitcoin? Private Law Facing the Blockchain' European Banking Institute Working Paper Series 2019/42 <<https://ssrn.com/abstract=3402678>> accessed 20 August 2020.

42 Karen Yeung, 'Regulation by Blockchain: The Emerging Battle for Supremacy Between the Code of Law and Code as Law' (2019) 82 *The Modern Law Review* 207, where she writes: 'The decentralized, distributed nature of public blockchains means that there is no single, centrally controlled and integrated entity which conventional legal systems can readily identify as potential bearers of legal rights and/or duties. This may generate difficulties for conventional law-makers.'

43 See Dirk A Zetzsche, Douglas W Arner, Ross P Buckley and Brian Tang, 'Artificial Intelligence: Putting the Human in the Loop' CFTE Working Paper (2020) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3531711> accessed 28 September 2020.

44 See Dirk A Zetzsche and others, 'Digital Finance Platforms: Towards a New Regulatory Paradigm' *University of Pennsylvania Journal of Business Law* (forthcoming 2021) <www.ssrn.com/abstract=3532975> accessed 21 August 2020.

cash in the world,⁴⁵ the annual GDP of the United States, or total US stock market capitalization.⁴⁶ About 25,000 investment professionals globally—13,000 from BlackRock and 12,000 from BlackRock's clients—rely on Aladdin. More than 1,000 internal and external developers work continuously on the ongoing development of the platform.⁴⁷ Overall, Aladdin hosts the portfolios of 210 institutions worldwide, including some of the largest asset owners (for example, California State Teachers' Retirement System (CalSTRS)) and competitors including Schroders and Vanguard.⁴⁸ Yet, Aladdin as such has neither entity status, nor licence nor headquarters, and thus is not directly subject to financial regulation and supervision. Aladdin is a mere set of algorithms with a server and lots of data available to be processed.⁴⁹ Aladdin is connected globally, yet owned by the asset management giant BlackRock. Technically decentralized by connecting hundreds of entities, Aladdin is economically and technologically centralized. This ensures BlackRock's control over the strategic development of, and accountability for all of, Aladdin's functions.⁵⁰

Imagine now a DeFi Aladdin *not* controlled by BlackRock: an independent data framework on which market participants could operate—developing their own applications and frameworks without any dominance of a single firm in investment and maintenance. For instance, we can envisage an open risk management platform whose code and functions are written by multiple individual programmers (instructed by multiple risk managers) developing multiple new platform functions and efficiencies.⁵¹ This would have the advantage of generating a variety of niche risk management models for the risk managers' choice—in addition to the standard ones Aladdin will, in any event, offer—thereby potentially reducing the systemic dimensions of model risk.⁵²

In case of need, regulators currently have jurisdiction over Aladdin indirectly, through the regulated entity BlackRock, as well through as the asset managers employing Aladdin. A fully decentralized, self-directing Aladdin, however, would have serious legal consequences when it came to determining which regulator and

45 See Will Dunn, 'Meet Aladdin, The Computer "More Powerful Than Traditional Politics"' *The New Statesman* (6 April 2018) <www.newstatesman.com/spotlight/2018/04/meet-aladdin-computer-more-powerful-traditional-politics> accessed 20 August 2020.

46 See Daniel Haberly and others, 'Asset Management as a Digital Platform Industry: A Global Network Perspective' (2019) 106 *Geoforum* 167, 168–170.

47 See Aladdin® platform overview, available on www.BlackRock.com (2020) <www.blackrock.com/aladdin/offerings/aladdin-overview> accessed 20 August 2020.

48 See Amy Whyte, 'Can Anyone Bury BlackRock?' *Institutional Investor* (1 October 2018) <www.institutionalinvestor.com/article/b1b672fxttfl/Can-Anyone-Bury-BlackRock> accessed 20 August 2020.

49 On Aladdin, see Zetzsche and others (n 42) 14–18.

50 We have outlined elsewhere that this control may itself pose problems, Zetzsche and others (n 42) 30–58.

51 Readers may doubt whether such a decentralized giant could develop scale *and* work and operate efficiently. Yet, the global applications of some open domain software challenge this doubt, with Linux's usage in most web servers and supercomputers worldwide and LibreOffice, as two notable examples.

52 Model risk refers to the risk that a model does not reflect reality and potentially leads to misallocation of funds and losses if the parts of reality not reflected in the model become manifest. If all risk managers use the same model, model risk increases and can undermine financial stability. We do not claim that the open platform model erases model risk; the niche models may have their own problems, and BlackRock's expertise and reputation may function as gatekeeper against poor modelling, but a diversity of models should at least work to reduce the *systemic* dimension of model risk.

supervisory authority would be in charge. A fully DeFi Aladdin would, most likely, be located everywhere and nowhere—which would make it very difficult to ascertain jurisdiction, assign responsibility and liability rules, and penalize misconduct. Even if we rely on indirect regulation and supervision, the regulated entities will have little means to comply with the regulators' demands: if it is a truly independent system, they might not be able to influence its operation. Supervisory requirements in relation to, for example, organization, governance, legal structure, and management are impossible if there are no staff. Where, for instance, are the headquarters of the BTC blockchain? Does BTC mining take place where the nodes are, even though each block of BTC will probably be mined in a different location? And where are the BTC wallets or the BTC beneficial owners located? Each of these criteria result potentially in different supervisory jurisdictions. The important point is there is no 'traditional' firm, entity, or headquarters to which financial regulation will apply; without this our regulatory agencies are likely to struggle to exert control and the salient, risk-reducing effect of law and regulation will thus be much diminished.

It has frequently been argued that DLT is not subject to law anywhere; we have made the counterargument that the likely result is that it is subject to law *everywhere*, with every major participant and developer potentially at risk of liability.⁵³ It is this dichotomy between liability and economic benefit which makes it so difficult to develop true DeFi frameworks.

b. Enforcement

Enforcement becomes problematic in the context of DeFi. For instance, financial regulation on outsourcing and delegation, as a general principle, seeks to ensure that one entity is in charge and liable for compliance with all laws and regulations applicable to that entity even where that entity relies on external service providers, and regulation generally requires entities to manage legal, concentration, and reputation risks relating to outsourcing.⁵⁴ In short, these rules create a hierarchy of liability and accountability, based on contractual rather than technical or financial relationships, where the supervised entity needs to ensure compliance from all service providers connected to it. How, in the world of DeFi, could a supervised entity enforce its oversight requirements vis-a-vis multiple, dispersed network participants that are spread around the world and subject to entirely different rules, ethics, and reputational concerns?

The core concern is not that the network participants reside in different countries, but that they are dispersed and decentralized. Non-compliance with rules in a network setting is best understood if considered as a risk of defection. The service-integrating entity internalizes all risks from services further down in the financial services value chain. As the entity most likely to be sanctioned and held liable, and in the absence of under-capitalization, it has a general interest in compliance to avoid sanctions and liability. The interests of the providers of the services that are integrated are not necessarily

53 Zetsche, Buckley and Arner (n 36).

54 See Board of Governors of the Federal Reserve System, Division of Banking Supervision and Regulation Division of Consumer and Community Affairs, 'Guidance on Managing Outsourcing Risk' (2013) <www.federalreserve.gov/supervisionreg/srletters/sr1319a1.pdf> accessed 20 August 2020.

the same: to the extent that the provider is too financially insignificant to be sanctioned and be held liable, they fear neither sanctions nor liability. In a DeFi setting, many different providers contribute to the end product, and in the absence of collusion among the network participants, issues of causation may well erect insurmountable hurdles to liability and sanctions since the burden is on the claimant or sanctioning entity to show that the specific non-compliance of a minor contributor caused the problems at issue. For this reason, where compliance is costly the many small contributors each have a strong incentive to defect—that is, to deviate from the integrator's general interest in complying with law, regulations, and contractual provisions. The risk of defection increases with the number of parties involved and decreases with the benefits generated by compliance for each party.

In the cross-border world of DeFi, this incentive structure creates additional difficulties. The costs of complying only with one's own rules are lower than complying with those rules plus the rules of one or more foreign jurisdictions, due to information costs and the necessity of duplicative processes internally and externally. Regardless of how expensive or inexpensive one's own rules and regulation, where the delegate complies with both its own and the outsourcing entity's rules, the compliance costs of the outsourcing entity are always lower than the compliance costs of the delegate.⁵⁵

Assume two parties, X and Y, located in two different countries, with X, from a legal perspective, being the integrator and Y the contributor. While X has only its home jurisdiction costs, Y has at least the costs of X's jurisdiction, plus its own, since compliance costs are never zero.⁵⁶ Whether Y complies then depends on Y's benefits from Y's function as a delegate. In a world of centralized finance, the benefits would be concentrated in X as the entity that has client access, and these benefits would be shared with Y, thus Y is compensated for compliance with X's laws, reducing X's benefit.⁵⁷

The problem of DeFi is that we are not talking about two entities (X;Y), but potentially dozens if not hundreds (with N referring to these multiple entities).⁵⁸ In turn, X must compensate the many entities (N) for compliance with foreign laws in order to make their compliance profitable, while we see no reason why X's benefits would increase from doing so. In turn, either X stops cooperating with others (in which case there is no decentralized finance) or X's profitability decreases (rendering X more likely to defect to save costs) or the many entities (N) receive less for their compliance with foreign laws, so their likelihood of defection increases.⁵⁹ In both DeFi scenarios we will see less compliance by either X or the many entities (N), that is, existing

55 Note that the delegate's *other* costs are most likely lower than the outsourcing entity's costs otherwise outsourcing would not happen.

56 This holds true at least in the absence of substituted compliance—which we rarely see today.

57 Assume that $B(X;Y)$ describes the shares of X and Y in the benefits, and $C(X;Y)$ the costs of compliance of each party with the rules of their respective home jurisdiction. The fact that Y is compensated for compliance with X's laws, reducing X's benefit, could then be written as: $B - B(Y) = B(X_Y)$.

58 Assume that N refers to the multiple entities: if $B - B(N) = B(X_N)$ and $B(Y) < B(N)$, then the result is $B(X_Y) > B(X_N)$.

59 Note that this is independent of large penalties threatened by X's regulator against either X or Y to N, since the threat of penalties will be factored in and make it more costly to comply, at least in theory—if X is hit by them, X will want to have a greater share leaving less for Y to N, while a threat being imposed on Y to N increases the benefits Y to N will want to have from X (and reduces X's share).

rules will be enforced less stringently than in a world of a centralized financial services value chain.

One may wonder whether scale effects in compliance offset the non-compliance effect of decentralization. If a service provider serves clients primarily from one jurisdiction with one set of financial regulation applicable, we would expect that provider to adjust its own organization to that regulatory environment of its clients. Yet, this is not the DeFi world: DeFi means cooperation *on a cross-border basis*; for small firms cross-border regulatory harmonization is even less likely than for large financial institutions, further reducing scale effects in compliance.⁶⁰

On top of this comes a problem incurred by the different valuation models of the old and new economy:⁶¹ existing financial institutions have few ways to ensure compliance and honest conduct from very large technology firms. This is due to the size, scope, scale, power, different culture, and current valuation of BigTech firms when compared to BigFinance institutions. Customers cannot credibly put a firm under pressure if that firm's market value is many times larger than their own⁶² and if they depend on the firm's services, given very high switching costs, strong information asymmetries as to the underlying technology and service quality, and few alternatives due to high market concentration.⁶³ In such a dynamic, the outsourcing relationship is inverted and the tail wags the dog.

This becomes obviously even more problematic if there is no tech firm in charge of the DeFi infrastructure at all, in those—so far very rare—instances in which technological systems become self-operating, whether intelligently (in the context of AI and its ultimate expression, the singularity) or through complete automation (arguably at the heart of the DeFi ideal).

c. Data protection and privacy

Decentralization in the datafied world means that data are accessible at many points rather than one.⁶⁴ Given the cloud and DLT operate on arrays of servers rather than

60 Take the example of the US: small financial firms are often subject to state rather than federal regulation, resulting in 50 different legal environments. The same is true for other large markets, notably the EU, where due to proportionality as a regulatory maxim small financial firms are often exempted from the single European rulebook. For instance, small fund managers are exempted from European harmonized rules for alternative investment funds, pursuant to article 3 of the Directive 2011/61/EU of the European Parliament and of the Council of 8 June 2011 on Alternative Investment Fund Managers [2011] OJ L174/1 (AIFMD).

61 See Mark Fenwick, Joseph A McCahery and Erik PM Vermeulen, 'The End of "Corporate" Governance: Hello "Platform" Governance' (2019) 20(2) European Business Organization Law Review 171 (arguing that the most successful firms today operate as an intermediating platform, and that the platform model drives up valuations).

62 For instance, Amazon—the largest cloud provider in the world—has a market valuation of US\$1 trillion while Goldman Sachs, the largest US financial institution, hardly reaches US\$80 billion (as of August 2020). The former could easily purchase the latter, if their relations become an issue.

63 Of course, reputation may play a role, yet given that in addition to the BigTech's reputation the reputation of the financial services firm is also at risk if issues materialize, both parties have an incentive to settle quietly, reducing the impact of reputation as a discipline-enhancing incentive.

64 See Financial Stability Board (FSB), 'Decentralised Financial Technologies: Report on Financial Stability, Regulatory and Governance Implications' (June 2019) 3–4 <www.fsb.org/wp-content/uploads/P060619.pdf> accessed 20 August 2020.

individual single servers, saving data in the cloud or on a DLT means spreading data over multiple servers. Data protection and privacy violations are potentially very costly to institutions relying on DeFi.⁶⁵ The argument that arises is that regardless of what data protection principles apply, any data generated will be ‘decentralized’ this way, rendering concepts of ‘data ownership’ or, more precisely, ‘effective data control’, merely theoretical. Even if there was legal standing to sue for data protection or privacy violations and data deletion, some data particles would remain—in this sense, the internet does not forget.

At the same time, in reality today, as a result of jurisdictional data requirements and data localization rules such as the EU’s General Data Protection Regulation (GDPR), we observe jurisdictional (re-)concentration of data.⁶⁶ The major cloud service providers (Amazon, Microsoft, IBM, Alibaba, Google, Apple) increasingly locate data in data centres located in an ever-increasing range of individual jurisdictions.⁶⁷ Any of these data centres ‘contains’ the data of a given client, such as a large financial institution or tech company. The end result of this interaction of technology, law, and economic incentives is not as envisaged by DeFi proponents: centralization is often at the heart of decentralization as a result of this interaction.

DeFi in both the ideal and also the reality is thus a challenge to the traditional legal role of the state, either from the standpoint of intention in the DeFi ideal or the reality of technological evolution.

3. Increasing tech risk

In addition, the very centrality of technology as the foundation of DeFi brings entirely new risks: DeFi in whatever form increases technological security risks due to tech dependency and connectivity.⁶⁸ This is the case regardless of whether one considers ‘strong form’ DeFi or ‘weak’ DeFi, or even DeFi built on centralization (eg cloud).

a. Tech dependency

The risks from the rapid growth of financial technology continue to rise while international FinTech governance lags behind. Another risk stems from the increasing mix of national security and financial stability factors in financial regulation, leading to potentially sub-optimal regulation. Finally, the ongoing concentration in crucial financial

65 See Zetzsche, Buckley and Arner (n 36) 1375–79.

66 ‘Regulation (EU) 2016/679 (General Data Protection Regulation)’ (2016) OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018. For an overview of the GDPR’s approach and provisions, see Chris Jay Hoofnagle, Bart van der Sloot and Frederik Zuiderveen Borgesius, ‘The European Union General Data Protection Regulation: What It Is and What It Means’ (2019) 28 Information & Communications Technology Law 65. For an instructive overview of how to square blockchain-based decentralization with the GDPR’s requirements see Michelle Finck, *Blockchain Regulation and Governance in Europe* (Oxford University Press 2018) 88–116; M Finck, *Blockchain and the General Data Protection Regulation*, Study on behalf of the European Parliament, 24-07-2019, <[https://www.europarl.europa.eu/thinktank/de/document.html?reference=EPRS_STU\(2019\)634445](https://www.europarl.europa.eu/thinktank/de/document.html?reference=EPRS_STU(2019)634445)> accessed 20 August 2020.

67 David Vaile and others, ‘Data Sovereignty and the Cloud: A Board and Executive Officer’s Guide’ Cyberspace Law and Policy Centre Version 1.0 (2013) 16 <www.bakercyberlawcentre.org/data_sovereignty/CLOUD_DataSovReport_Full.pdf> accessed 20 August 2020.

68 For a discussion of the risks of decentralized financial technologies for financial stability, see FSB (n 48) 6–7. See also Ross P Buckley and others, ‘TechRisk’ [2020] Singapore Journal of Legal Studies 35, defining ‘tech risk’ to include security, data protection and privacy, and concentration.

market infrastructure and the underlying tech industry furthers a tech-monoculture which facilitates cyberattacks: a weakness detected and used for a cyberattack on one network may be used to force entry into another network.⁶⁹ If one adds the interdependence due to decentralization of finance, the outcome becomes potentially very dangerous.⁷⁰

b. Connectivity

DeFi connects many servers around the globe, and these servers are owned, operated, updated and otherwise influenced by many different entities. While the network structure can reduce the risk of manipulation, as with distributed ledgers, it also enhances two other types of cyber risks. First, the number of access points to the network have multiplied. Each access point provides a cyber risk that needs to be managed. Second, many servers are connected, and new risks may come from this connectivity.

At the end of the day, any extensive DeFi system provides a huge potential vulnerability: imagine a world in which a highly successful, fully decentralized Libra provides the monetary instrument and payment system for a very large portion of the world. What if it is hacked? Or should we ask ‘when’ rather than ‘if’ it is hacked?

c. Lack of support points

If a tech operation providing material financial infrastructure experiences difficulties, it is much more difficult to organize meaningful support for a decentralized network than for a concentrated system, where technical or financial support⁷¹ for one entity will mean that the entity providing the infrastructure has the technical or financial means to address the operational difficulties until a long-term solution can be worked out. Such technical or financial support can be through, for instance, emergency liquidity assistance, ‘lender of last resort’ facilities, deposit guarantee schemes, or, indirectly, bankruptcy protection by way of a special resolution schemes.⁷²

This is particularly important in crises where systems and rescue schemes are stressed. Imagine that a network function depends on a myriad of small entities cooperating across the globe and all relying on crucial spare parts—in times where travel is severely impaired it is easier to channel spare parts to a handful of firms than to dispersed network partners.

These issues suggest that the state will not be yielding to the challenge of the DeFi ideal any time soon.

V. ASSIMILATING DEFI: THE EMPIRE STRIKES BACK

As we have laid out, DeFi in its ideal form clearly brings with it a range of challenges, particularly from the standpoint of state sovereignty but also from its technological

69 See Buckley and others (n 68).

70 Buckley and others (n 68) 16–19.

71 See for an overview of privileges granted to the ‘incumbent’ payment system, and the risks to clients and financial stability resulting from their lack with regard to new variants of payment systems, Dan Awrey and Kerstin van Zwieten, ‘The Shadow Payment System’ (2018) 43 *Journal of Corporation Law* 776, 794–95 and 796–808.

72 Awrey and Zwieten (n 71).

dependence. While these are likely to mean that the ideal does not become the reality, the foundational technologies are nonetheless transforming finance. At the same time, certain aspects of the ideal have real value from the standpoint of improving traditional finance. The result is that the DeFi is increasingly being assimilated into traditional finance rather than disrupting it.

The question is how to balance the challenges with the opportunities in the context of policy and regulation.

1. Balancing investor protection and technological development

The greatest amount of regulatory attention to DeFi so far has focused on the traditional concerns of money laundering, financial crime, market integrity, and investor and customer protection, particularly in the context of crowdfunding, cryptocurrencies, and Initial Coin Offerings (ICOs). We have previously argued for a functional approach in the context of addressing regulatory concerns around digital assets.⁷³ Facebook's Libra proposal has also dramatically increased the relevance of considerations of systemic risk as well as of challenges to state sovereignty in monetary affairs. In each case, traditional regulatory approaches are being extended as necessary in order to address new innovations.

There are a number of aspects of DeFi regulation, however, that are proving challenging.

From a conceptual framework, one problem is developing appropriate approaches to regulation for a truly decentralized system that is, at least in the beginning, centralized in the hands of its developers. In the US, a proposal from Hester Pierce of the US Securities and Exchange Commission (SEC) highlights the challenges in this respect:

Many crypto entrepreneurs are seeking to build decentralized networks in which a token serves as a means of exchange on, or provides access to a function of the network. In the course of building out the network, they need to get the tokens into the hands of other people. But these efforts can be stymied by concerns that such efforts may fall within the ambit of federal securities laws. The fear of running afoul of the securities laws is real. Given the SEC's enforcement activity in this area, these fears are not unfounded.⁷⁴

Commissioner Pierce suggests a viable potential approach, built on a 'safe harbour' for centralized, yet DeFi-to-be platforms which can be secured through a series of steps designed to balance investor protection with the needs of innovation in seeking to build decentralized systems, including for finance. While Commissioner Pierce's proposals are seemingly yet to attract majority support within the SEC, they highlight the difficulties in striking a balance between innovation and protecting passive, potentially vulnerable constituencies.

73 See Dirk A Zetzsche and others, 'The ICO Gold Rush: It's a Scam, It's Bubble, It's a Super Challenge for Regulators' (2019) 60 Harvard International Law Journal 301; Douglas W Arner and others, 'Cryptocurrencies, Blockchain and ICOs: Policy and Regulatory Challenges of Distributed Ledger Technology and Digital Assets in Asia' in Christopher Brummer (ed), *Cryptoassets: Legal and Economic Perspectives* (Oxford University Press 2019).

74 Hester M Pierce, 'Running on Empty: A Proposal to Fill the Gap between Regulation and Centralization' (Chicago, 6 February 2020) <www.sec.gov/news/speech/peirce-remarks-blockress-2020-02-06> accessed 20 August 2020.

2. Enhancing regulatory cooperation

The challenges are even greater in the cross-border context. Since determining jurisdiction is far from easy, DeFi projects tend to fall under many different state, federal/national, and regional licensing and supervision regimes. Each potentially involved regulator will impose additional conditions reflecting its own perspective, mandate, and powers.⁷⁵ This will result in a mixed and potentially fragmented regulatory framework which will both limit some of DeFi's advantages and at the same time make it difficult to address its risks. A highly fragmented regulatory landscape is also likely to lead to inefficient regulation that is in some respects very strict and in others too lax, increasing risks of regulatory arbitrage and gaps.

The better alternative is substituted compliance,⁷⁶ or in European law terms, equivalence.⁷⁷ Once a DeFi project is licensed in one jurisdiction, other jurisdictions could recognize its supervision in the home jurisdiction and reduce their own requirements, for instance on capital reserves, risk management, and IT infrastructure (this is on the basis that the financial legislation and supervision in the home country has substantially the same effects as the legislation and supervision in the host country). While simple in theory, substituted compliance/equivalence has proven difficult to achieve in practice, outside the specific context of the EU's passporting regime. The most significant developments have occurred in the context of over-the-counter (OTC) derivatives (in response to problems observed in conflicts resulting from differential implementation of internationally agreed approaches to issues which arose in the 2008 financial crisis). Conflicts between OTC derivatives regulations are a major concern of discussions at the G20 and FSB level about fragmentation.⁷⁸ At the same time, the EU's move towards rule-based access for financial institutions from third countries has been stalled by Brexit.

In the context of banks and financial market infrastructure, however, regulators since the 2008 global financial crisis and the 2010 Eurozone debt crisis have largely abandoned the home regulator approach; even the EU has moved in the form of the European Supervisory Authorities (ESAs) European Securities and Markets Authority (ESMA), European Banking Authority (EBA), and European Insurance and Occupational Pensions Authority (EIOPA), and in the Eurozone with the European Central Bank, towards a regional supervisor as opposed to the pre-crisis structures of lead home regulators. This is another of the fundamental issues that arises in international discussions of fragmentation.

Given that substituted compliance comes with a loss of sovereignty of the respective regulator and supervisory authority, in the current crisis of multilateralism it would be overly optimistic to expect any sudden change to the unilateral approach. It is increasingly difficult to compromise on basic questions relating to substituted

75 Again, perhaps the best example of this in practice is occurring with Facebook's Libra proposal.

76 See Howell E Jackson, 'Substituted Compliance: The Emergence, Challenges, and Evolution of a New Regulatory Paradigm' (2015) 1 *Journal of Financial Regulation* 169.

77 See on equivalence Dirk A Zetzsche, 'Competitiveness of Financial Centres in Light of Financial and Tax Law Equivalence Requirements' in Ross P Buckley, Emiliós Avgouleas and Douglas W Arner (eds), *Reconceptualizing Global Finance and Its Regulation* (Cambridge University Press 2016) 393–406.

78 See FSB, 'FSB Report on Market Fragmentation' (4 June 2019) <<https://www.fsb.org/2019/06/fsb-report-on-market-fragmentation-2/>> 21.

compliance, for instance which supervisory authority is in charge and the scope of the substitution: while the EU has expanded the equivalence principle into the field of data protection, with GDPR allowing data transfer into countries that have equivalent data protection regulations and enforcement as the EU,⁷⁹ strong data protection regulations are largely absent in the US and China,⁸⁰ to name but two important jurisdictions. Even jurisdictions friendly to substituted compliance hesitate to rely on this concept for providers that service retail clients.

At the same time, cooperation based on Memoranda of Understanding (such as those brokered by IOSCO⁸¹) does not result in the same level of cost reductions for the supervised entities and come with high costs for smaller authorities needing to maintain multiple memoranda with multiple authorities over multiple sectors and activities worldwide.

Notwithstanding the former, regulators are encouraged to intensify cooperation on DeFi matters. This should include working groups or supervisory colleges on global DeFi projects, to counter the collective intelligence of DeFi users with the authorities' collective insights. In fact, global DeFi systems could warrant the adoption of a specific global cooperation framework among regulators, as is under discussion for global stablecoins⁸² and for global payment systems.⁸³

A specific global approach for addressing global DeFi systems may be appropriate and in fact necessary from both the DeFi and regulatory standpoint. Such an approach could be based on IOSCO's Multilateral Memorandum of Understanding, laying out common minimum approaches as a precondition for joining, perhaps combined with supervisory college structures for systems involving multiple operators across multiple jurisdictions, of which Libra is probably the most significant potential example so far. For instance, the Libra 2.0 white paper offers explicitly such a 'supervisory college': a committee of regulators from the jurisdictions across which it will operate, chaired by its home regulator (in this case proposed to be the Swiss Financial Market Supervisory Authority (FINMA)).

3. Tech risk management

In addressing tech risks it will be crucial to expand the breadth of cyber incident scenarios internationally that are likely to arise from decentralization. This will ask a

79 Pursuant to article 45 of the GDPR, a transfer of personal data to a third country outside the EU may take place if the European Commission has decided that the third country ensures an adequate level of protection.

80 See, for an overview of the approaches of China, the US, and the EU, Emmanuel Pernet-Leplay, 'China's Approach on Data Privacy Law: A Third Way Between the U.S. and the EU?' (2020) 8(1) Penn State Journal of Law and International Affairs 1.

81 International Organization of Securities Commissions (IOSCO), 'Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and the Exchange of Information (MMoU)' IOSCO (2020) <<https://www.iosco.org/about/?subsection=mmou>> accessed 20 August 2020.

82 FSB, 'Addressing the regulatory, supervisory and oversight challenges raised by "global stablecoin" arrangements: Consultative document' (14 April 2020) <<https://www.fsb.org/2020/04/addressing-the-regulatory-supervisory-and-oversight-challenges-raised-by-global-stablecoin-arrangements-consultative-document>> accessed 20 August 2020.

83 Bank for International Settlements, Committee on Payments and Market Infrastructures, *Enhancing cross-border payments: building blocks of a global roadmap—Stage 2 report to the G20* (July 2020) <<https://www.bis.org/cpmi/publ/d193.html>> accessed 20 August 2020.

variety of financial and tech firms not only to assess system weaknesses and costs by way of stress tests, but also to clarify liability assignment, which may be instrumental to reducing uncertainty in cases of cyber-caused crises. In a geographically decentralized context, such stress tests have to be designed and conducted as collaborative efforts among a number of regulators.

Cooperation among mature tech and financial institutions and regulators may further the understanding of the nature and scale of risks, given that the most effective way to advance effective cyber risk and data assessments is through networks of cyber risk and data specialists exchanging best practices.⁸⁴ Regulators in this setting can be instrumental by (i) demanding cooperation, and (ii) creating the atmosphere for cooperation and exchanges of lessons learned by potentially granting leniency to institutions in case of failure if institutions have seriously and constantly contributed to cyber and data working groups prior to the failure.

4. Data, reserve, and tech localization

Regulators may respond to the new dimension of enforcement difficulties by requiring data and reserve localization.

Data localization requirements were originally developed in data protection laws to ensure a national regulator's sovereignty over its citizens.⁸⁵ In recent years, however, financial supervisory authorities have increasingly imposed similar requirements: when a group of companies is in trouble, the data necessary to maintain crucial services in the respective country must be stored, and remain accessible, even in times of crisis and if the financial services conglomerate become insolvent. The challenge of data localization requests is to determine which data are crucial to perform the service, and where such data should be localized if many countries are involved? Take the example of Big Data applications—localization will help little if it means hiving off a small section of a big data pool that can cover only a minor part of real-world correlations.⁸⁶ These issues have been pushed forward dramatically in the context of the COVID-19 pandemic, where data collection by governments and BigTech firms is increasingly central to management of the crisis.

Banking regulators practice reserve localization in order to ensure sufficient funds for an institution's risk coverage relating to its exposure in the regulator's jurisdiction: this is the core of requirements for separately capitalized subsidiaries combined with TLAC (Total Loss Absorbency Capital⁸⁷). The additional stability generated by reserve localization, however, comes with the downside of potential under-diversification of global exposures. This can render impossible certain DeFi business models.

84 See Buckley and others (n 68) 15–16, 19.

85 Anupam Chander and Uyên P Lê, 'Data Nationalism' (2015) 64 Emory Law Journal 677.

86 See Nigel Cory, 'Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?' *Information Technology and Innovation Foundation* (May 2017) 7 <www2.itif.org/2017-cross-border-data-flows.pdf> accessed 20 August 2020. For a discussion of the costs of data localization, see Matthias Bauer and others, 'The Costs of Data Localisation: Friendly Fire on Economic Recovery' (2014) Ecipe Occasional Paper No 3/2014 <www.aicasia.org/wp-content/uploads/2017/06/OCC32014__1.pdf> accessed 20 August 2020.

87 TLAC refers to an international standard endorsed by the FSB, intended to ensure that global systemically important banks have enough capital and bail-in debt to minimize the risk of a government bailout.

Take the example of the Libra Reserve. Under the Libra 1.0 white paper the Libra Reserve would hold A+-rated assets from a multitude of jurisdictions. This requires rebalancing of exposures over time, resulting in an incredibly challenging risk management process if billions of Libra holders use Libra as their main means of payment. If this risk management fails, US Libra holders may find themselves exposed to currency risks—the very risk the Libra project promised to curtail. This may explain why in the Libra 2.0 white paper, the proposed structure is individual stablecoins tied to the major currencies—USD Libra, EU Libra, Yen Libra—with a synthetic combination available. This is a much different—and economically less decentralized—proposition than Libra 1.0.⁸⁸ Libra 1.0 showed what is *technically possible*, but the changes reflected in Libra 2.0 were required by the attitudes of powerful regulators. The potential size of Libra/Facebook forced regulators to take action. However, many other examples of DeFi, most notably Bitcoin and, for a time, ICOs, could operate and grow without an immediate regulatory response. This is unsurprising given that regulation is costly, both in terms of money and reputation, and these costs are often only worth incurring, especially on a large scale, if the case in favour of regulation is clear. Thus *some* successful DeFi applications have slipped through the regulatory net and gained significant size unimpeded by financial regulation—and this likely to happen again in the future.

In addition to the incumbent methods of data and reserve localization, we propose adding a third measure: tech localization. For crisis continuity management, as for sustainability reasons, regulators could require infrastructure providers to keep crucial spare parts and tech support for the network available within the territory to secure network operations within their territory. If all regulators apply similar requirements, the network will be based on more localized tech supply and be more stable in crises which interfere with global supply chains.

Each of these examples highlights that although there are indeed challenges in addressing DeFi, there are viable regulatory approaches available, which would allow the state to assimilate DeFi, rather than face disruption.

At the same time, we suggest that exercise of centralized sovereign authority may in fact be necessary to achieving DeFi's central objective of decentralization.

VI. Decentralization and concentration: the centrality of the state

Central to DeFi is a reaction to risks of concentration and dominance. Can DeFi render regulators superfluous? This is part of the DeFi vision but is not easy to attain. While DeFi proponents hope it can be done, we doubt this will happen in the foreseeable future.⁸⁹ While the Pierce proposal highlighted in [section V](#) can be seen as a step in that direction, a second look reveals that the Pierce proposal follows traditional patterns of risk-based supervision: under that proposal, regulators define the minimum

⁸⁸ Libra Association (n 34).

⁸⁹ See, for the same argument in the context of Corporate Technologies, Luca Enriques and Dirk Zetsche, 'Corporate Technologies' *Hastings Law Journal* (forthcoming 2020) <www.ssrn.com/abstract=3392321> accessed 20 August 2020.

decentralization parameters that developers of decentralized systems must address as part of the evolution from initial creation to full decentralization. Only rules addressing risks associated with the centralized function of an ‘issuer’ cease to apply with sufficient decentralization achieved. Other rules such as those on Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) and minimum disclosure continue to apply and remain to be supervised. The application of the Pierce proposal does not render regulators superfluous.

While evolving from different sources, the objectives of DeFi and ‘open banking’/‘open finance’ overlap. Could this be a way to address concentration and dominance in finance?

1. Open finance as antitrust

Essentially, ‘open finance’ is based on decentralized rather than centralized control of data, in particular the data relating to individuals and its potential for use in finance.

Open finance, as a policy goal, is justified on pro-competition and other regulatory grounds, as it addresses market efficiency and antitrust concerns stemming from economies of scale and networks effects in the data economy, where the size of the data pool determines competitive strength⁹⁰ and where technology firms like Amazon, Google, Alibaba, and others have foregone profits for years to build platforms with overwhelmingly dominant market share. At the core of all this are network effects plus economies of scope and scale, which combine to give rise to the potential for industry concentration and dominance. Data-driven industries often naturally gravitate towards ‘winner takes all outcomes’, with the potential for significant benefits followed by significant negative externalities. American tech and data markets have tended towards oligopoly or monopoly over time,⁹¹ a process which seems to have occurred in China as well. Both jurisdictions have allowed commercial enterprises to acquire control of large consumer and other data pools. The core assets of those platforms are the pools of data relating to shoppers and merchants. Once these data pools are assembled they can be used for targeting advertising, undercutting prices, offering new tailored services more quickly to more clients, or data analysis in all markets where superior information benefits profits.

Legal competition and antitrust scholars argue that where investors reward growth over profit, predatory pricing becomes highly rational and, even when costly, is a worthwhile strategy since it ensures monopoly rents due to control over the essential infrastructure on which their rivals depend: ‘This dual role also enables a platform to exploit information collected on companies using its services to undermine them

90 See European Parliament, Directorate General for Internal Policies, ‘Competition Issues in the Area of Financial Technology (Fintech)’ PE 631.061 (July 2018) 103–04 <[www.europarl.europa.eu/RegData/etudes/IDAN/2019/631061/IPOL_IDA\(2019\)631061_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/IDAN/2019/631061/IPOL_IDA(2019)631061_EN.pdf)> accessed 20 August 2020.

91 See Tim Wu, *The Master Switch: The Rise and Fall of Information Empires* (Vintage 2011) (arguing that American information industries tend to press towards monopolies). See also, on the promise and perils of technology-driven competition, Ariel Ezrachi and Maurice E Stucke, *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy* (Harvard University Press 2016).

as competitors.⁹² This has prompted the policy demand to treat data as a product, since information and data, although different from traditional goods and services, pose problems familiar to antitrust law, such as monopolistic behaviour and collusion.⁹³ Treating data as a product becomes a particular consideration in avoiding potential reductions in innovation and therefore in long-term growth and development.

These debates are increasingly strong in the EU, the US, and across the world, even in China.⁹⁴ To our knowledge, only the EU, the UK, and Australia have so far adopted open banking (with the EU's revised Payment Services Directive (PSD2) for payment services the first closely related initiative) but many countries around the world are working towards implementing such strategies or at least analysing them closely.⁹⁵

What role does open banking/open finance play in DeFi—and the converse—what role will DeFi play in open banking/open finance? In essence, open banking facilitates greatly increased levels of democratization of finance by enabling participants to simply, swiftly, and safely provide their raw financial data to competitors of their current financial services provider.⁹⁶ This should support the growth of many new competitors in financial services. Most financial ecosystems are dominated by a relatively small number of very large banks or, in the case of China, very large tech companies providing financial services. Open banking should result in a far greater range of product offerings and ecosystem participants. These new participants will not be burdened with legacy systems and many will utilize more cost-efficient decentralized systems. As part of DeFi, DLT in particular could be used to decentralize and democratize access to data, thereby reducing concentration and control of the data both by the state and by BigTech / BigFinance. Open data and DLT aim for much the same things and DLT-based open data infrastructure will form the tech core of DeFi.

92 See Lina M Khan, 'Amazon's Antitrust Paradox' (2017) 126 Yale Law Journal 710, 803; K Sabeel Rahman and Lina Khan, 'Restoring Competition in the U.S. Economy' in Nell Abernathy, Mike Konczal and Kathy Milani (eds), *Untamed: How to Check Corporate, Financial, and Monopoly Power* (Roosevelt Institute 2016) (arguing that the harms from dominant platforms include lower income, rates of new business creation and local ownership, and outsized political and economic control in the hands of a few); see also ACCC, 'Digital Platforms Inquiry: Preliminary Report' (December 2018) <www.accc.gov.au/system/files/ACCC%20Digital%20Platforms%20Inquiry%20-%20Preliminary%20Report.pdf> accessed 20 August 2020.

93 See Mark R Patterson, *Antitrust Law in the New Economy: Google, Yelp, LIBOR and the Control of Information* (Harvard University Press 2017) (arguing in favour of conceptualizing information and user and use data as a product, since information and data although different from traditional goods and services, pose problems familiar to antitrust law, such as monopoly and collusion).

94 See Dirk A Zetsche and others, 'The Evolution and Future of Data-Driven Finance in the EU' (2020) 57 Common Market Law Review 331.

95 A coalition of central banks have committed to work together to assess Central Bank Digital Currency (CBDC) use cases and design choices. These comprise the Bank of Canada, Bank of England, Bank of Japan, European Central Bank, Sveriges Riksbank, and Swiss National Bank. The People's Bank of China is not a member, although its work is more progressed than that of any other central bank. Other central banks that have announced they are researching or testing use cases for CBDC include: Ukraine, France, Thailand, South Korea, Uruguay, Turkey, The Bahamas, South Africa, Eastern Caribbean Currency Union, Saudi Arabia, Marshall Islands, UAE, Brazil, Israel, Norway, Cambodia, Denmark, Ecuador, and Iceland. See Davis Polk, 'The Federal Reserve and Central Bank Digital Currencies' (20 August 2020) <<https://alerts.davispolk.com/10/5131/uploads/the-federal-reserve-and-central-bank-digital-currencies.pdf?sid=281566df-9de6-477a-9d7e-834d74e82e20>> accessed 20 August 2020.

96 See Christopher C Nicholls, 'Open Banking and the Rise of FinTech: Innovative Finance and Functional Regulation' (2019) 35 Banking & Finance Law Review 121, 123.

2. Countering pro-concentration effects

DeFi relies, to a large extent, on data, processing, and storage power distributed across the globe over many servers and re-concentrated for purposes such as bundling liquidity and Big Data applications. Promoting DeFi as such may thus be too simple an approach—rather we need to ask *which parts* of the financial services chain should be decentralized and which parts (re)concentrated.

Three data-related factors together may lead to friction in the market for financial services, preventing private ordering from leading to socially optimal outcomes in the sense that market forces ensure competition among services providers. These factors are traditional economies of scale, data-driven economics of scale, and network effects.⁹⁷ The argument is that DeFi is different because it is decentralized, with core infrastructure neither owned nor controlled by any participant.

In this regard, open data (or open finance) is a two-edged sword. While the EU (with GDPR and PSD2) has required the financial industry to develop appropriate systems for data management and limited the use the industry can make of pooled data (thereby reducing the advantages of traditional financial institutions through their data pools), it has also driven the standardization of data processes outside of finance—potentially making for a larger data pool and enabling new entrants to potentially access more data of their individual customers. In other words, data are now more freely accessible and transferable than ever before. Large technology companies know well how to make use of the new rights to data transfer—much more so than do new entrants, with access to customers limited by budgets and resources. This could prompt utterly unexpected results. While PSD2 and GDPR were originally designed to curtail the power of data behemoths, the eventual outcome of these two groundbreaking initiatives may well be less competition due to the greater concentration of data in the hands of the few.⁹⁸ As a result, it may be necessary for regulators to impose open data requirements only on firms with a potentially dominant position, regardless of whether they are financial institutions or tech firms.

Nonetheless, requirements for open data/open finance fit well with the DeFi objectives of democratization and decentralization, albeit on the basis of state regulation. At the opposite extreme, DeFi infrastructure could be provided directly as a sovereign function—an idea that is being increasingly advanced in discussions of central bank digital currencies.⁹⁹

97 See Zetsche and others (n 34) 33–39.

98 See Zetsche and others (n 42).

99 See on CBDCs, Bank for International Settlements, Committee on Payments and Market Infrastructures, *Central Bank Digital Currencies* (March 2018) <<https://www.bis.org/cpmi/publ/d174.pdf>> accessed 20 August 2020; Bank for International Settlements, *Annual Economic Report 2020*, Ch III ('Central banks and payments in the digital era'); Saule T Omarova, 'Technology v Technocracy: Fintech as a Regulatory Challenge' (2020) 6(1) *Journal of Financial Regulation* 75, 122–23; DW Arner and others, 'After Libra, Digital Yuan and COVID-19: Central Bank Digital Currencies and the New World of Money and Payment Systems' European Banking Institute Working Paper Series 65/2020 <<https://ssrn.com/abstract=3622311>> last accessed 20 August 2020, all with further references.

3. Nationalization of core infrastructure

Government development, provision, control, or even nationalization of core DeFi infrastructure may be necessary, as radical a step as the latter may initially sound. If this happens, the claims of decentralization will be utterly upended as DeFi will have had the opposite effect of its professed mission to reduce government control.

First, nationalization leads to informational advantages as to what data and financial streams are processed via the network. Second, the public stakeholder can force upon the network the cybersecurity measures that it deems necessary. Third, setting and enforcing data and reserve localization by legal means and supervisory tools become less important—the public stakeholder could simply (re-)arrange the systems architecture to meet its localization requirements. Finally, the public stakeholder could apply all tools available to address pro-concentration effects, given that public stakeholders are less driven by the need to make profits.

Naturally, nationalization can take various forms, ranging from taking a stake, co-management, and public coordination by a regulator or central bank to full ownership of a decentralized system or network. The range of potential structures ranges from something like SWIFT to domestic real-time gross settlement (RTGS) systems, faster payment systems, property registries, and central bank digital currencies. For DeFi the first variant—a public-private partnership where a public authority assumes a node function¹⁰⁰—is probably most advisable in many cases, given that full ownership would require reconcentration and create a new single point of failure, thereby removing key benefits of decentralization.

While national operation or control of crucial financial market infrastructure sounds radical, it is, in fact, far from it. For example, the US Federal Reserve currently functions as operator of the National Settlement Service (NSS), the Fedwire® Funds Service, and—together with the Electronic Payments Network (EPN)—the Automated Clearing House (ACH) system, through which depository institutions send each other batches of electronic credit and debit transfers.¹⁰¹ Further, the US Federal Reserve has committed to develop and operate the FedNow Service, a real-time payment and settlement service expected to start operations in 2023.¹⁰² Other examples include the European Central Bank's payment-vs-delivery system Target-2-Securities, which ensures that the transfer of securities and derivatives can occur among local and global custodians and central securities depositaries,¹⁰³ as well as the Bank of England's CHAPS system.¹⁰⁴

100 See for a sample infrastructure Auer (n 4).

101 See Federal Reserve Board, 'Automated Clearinghouse Services' (6 January 2020) <www.federalreserve.gov/paymentsystems/fedach_about.htm> accessed 20 August 2020.

102 See Federal Reserve Board, 'Press Release: Federal Reserve Announces Plan to Develop a New Round-the-Clock Real-Time Payment and Settlement Service to Support Faster Payments' (5 August 2019) <www.federalreserve.gov/newsevents/pressreleases/other20190805a.htm> accessed 20 August 2020.

103 See Deloitte, 'TARGET 2 Securities: Time to Settle' *Inside Magazine* Issue 12 (June 2016) <www2.deloitte.com/content/dam/Deloitte/lu/Documents/financial-services/lu_target-2-securities.pdf> accessed 20 August 2020.

104 See, for an overview of CHAPS, Bank of England, 'A Brief Introduction to RTGS and CHAPS' (July 2019) <www.bankofengland.co.uk/-/media/boe/files/payments/rtps-chaps-brief-intro.pdf> accessed 20 August 2020.

In the DeFi space, a number of initiatives that are nationalizations in function, if not in name, can be found. For example, the Unified Payments Interface (UPI) that introduced real-time settlement in inter-bank payments in India was developed by the National Payments Corporation of India and regulated by the Reserve Bank of India. Designed to support direct payments on a mobile platform, it has reached more than 800 million transactions per month and is now developing cross-border linkages.¹⁰⁵ India's UPI has become the role model for networked mobile finance,¹⁰⁶ leading to similar initiatives around the world. With the UPI, the Indian central bank has acquired control over the technological link between all payment providers and its clients; any new institution can link itself to the network by using the UPI, thereby breaking the control of incumbent financial institutions and enabling innovation.

Another example is provided by the People Bank of China's plan to introduce a new 'Digital Yuan'—the Digital Currency/Electronic Payment (DCEP) project at least partially in response to initiatives such as Facebook's Libra.¹⁰⁷ Finally, we are seeing an increasing range of DLT-based corporate, securities, secured transactions, and other forms of property registries, providing the decentralized infrastructure for a wide range of financial and economic activity but under the overall supervision of governments, public actors, or public-private partnerships.

Thus, despite the anti-government ideal, it may well be that the government is in fact necessary to achieve democratization and decentralization.

4. RegTech and embedded regulation

Finally, in looking at regulation and DeFi, a real opportunity may come in the form of RegTech—the use of technology for regulatory compliance, monitoring, and supervision (sometimes called 'supervisory technology'¹⁰⁸), and infrastructure and system design.¹⁰⁹

In order to strengthen supervision and enforcement in the context of decentralization, competent authorities should design *technology-based* regulatory systems and systems of supervision. Regulatory requirements could be embedded *technically* into DeFi systems in order to use the same framework to embed systems to achieve regulatory objectives as part of the authorization requirements inherent in DeFi development.

105 Andy Mukherjee, 'India Going Cashless Could Be a Model for the World' *Washington Post* (7 June 2019) <www.washingtonpost.com/business/india-going-cashless-could-be-a-model-for-the-world/2019/06/05/d8fec830-87ee-11e9-9d73-e2ba6bbf1b9b_story.html> accessed 20 August 2020.

106 See Advait Rao Palepu, 'Can India's UPI Become a Global Model? Google Thinks So' *Bloomberg Quint* (14 December 2019) <www.bloombergquint.com/business/can-indias-upi-become-a-global-model-google-thinks-so> accessed 20 August 2020.

107 See Paul Vigna, 'UBS-Led Group to Launch Blockchain-Based Trade-Settlement Platform' *Wall Street Journal* (3 June 2019) <www.wsj.com/articles/ubs-led-group-to-launch-blockchain-based-trade-settlement-platform-11559554201> accessed 20 August 2020.

108 See Luca Enriques, 'Financial Supervisors and Regtech: Four Roles and Four Challenges', *Revue Trimestrielle de Droit Financier* 53 (2017) <<https://ssrn.com/abstract=3087292>> accessed 20 August 2020 (discussing this very role of technology for supervisors under the term 'oversightTech').

109 See Janos N Barberis, Douglas W Arner and Ross P Buckley (eds), *The RegTech Book: The Financial Technology Handbook for Investors, Entrepreneurs and Visionaries in Regulation* (Wiley 2019); Douglas W Arner, Janos N Barberis and Ross P Buckley, 'FinTech, RegTech and the Reconceptualization of Financial Regulation' (2017) 37 *Northwestern Journal of International Law and Business* 371.

This could take the form, for instance, of ‘*embedded supervision*’, that is, ‘a regulatory framework that provides for compliance in tokenized markets to be automatically monitored by reading the market’s ledger, thus reducing the need for firms to actively collect, verify and deliver data.’¹¹⁰ Embedded supervision can thus be seen as an automated form of compliance, monitoring, and supervision, using the system itself to implement, monitor, and enforce compliance requirements.

For DeFi, we suggest an expansion of this idea: ‘*embedded regulation*’.¹¹¹ Under an ‘*embedded regulation*’ approach the key regulatory objectives of market integrity, market conduct, and financial stability are included as part of the design of any DeFi system; supervision is but one part of an effort to achieve the former. Beyond the service as such, any system’s architecture should include systems of transparency, disclosure, compliance, etc. In other words, a properly designed DeFi system should implement such features as part of its own automated structures, requiring input of certain data, assurances of quality, and other traditional forms of gatekeeping necessary for proper market functioning. This comes, naturally, with limited ability to override the systems’ limitation. For instance, we could envisage that certain types of conduct and certain combinations of conduct are not possible at all, while others are possible only with the supervisors’ consent, which in the DeFi world means the consent of many supervisors—a high barrier. At the same time, certain risk factors may be modified by supervisors while the system is running—basically a live systemic risk control.

Embedded regulation could also serve as the basis for addressing a range of cross-border collaboration issues: if data spread over many nodes of a given DLT are accumulated, sorted, and pooled by several supervisory authorities across several countries, re-concentration on the side of supervisors, collaborating in an embedded regulation platform, could offset some of the disadvantages with regard to determining jurisdiction and enforcing financial and data regulations.

The end result, however, may be that the objective of decentralization in fact requires an external guarantor—the platform where the regulation is embedded and that facilitates supervisory cooperation.

VII. LOOKING FORWARD

Looking forward, a number of initial conclusions are possible.

Increasing processing, storage and bandwidth capacity are enabling the potential for the decentralization of finance, while AI, blockchain, cloud and data provide the technological enabling environment for DeFi.

At the same time, by connecting multiple small actors decentralization may facilitate the creation of efficient scale with regard to data and liquidity pools that in the past has justified the regional or global clustering of services in financial centres and the pooling of both through large balance sheets. Decentralization may thus undermine some of the bundling activity performed by intermediaries. This trend is likely to be at most partial. In other words, decentralization will probably see more diverse and competitive

110 See Auer (n 4) (arguing that embedded supervision would reduce compliance costs both on the side of supervisors and supervised entities).

111 This is an argument we have previously made in the context of ICOs, see Zetzsche and others (n 73).

financial services ecosystems, and reduce the centrality of the role of financial hubs, which will be to the good, but it will not remove the considerable data advantages enjoyed by the largest tech platforms such as Aladdin's Blackrock in the US or Ant Financial in China.

Yet, DeFi, in its purest form, cannot meaningfully exist within a properly regulated setting, given that decentralization is no panacea—quite the opposite. The problem of pure DeFi is 'the tragedy of the commons'.¹¹² As Aristotle said about children, and Milton Friedman adapted for the overall economy, 'when everybody owns something, nobody owns it, and nobody has a direct interest in maintaining or improving its condition'.¹¹³ Wherever technical and economic decentralization is taking place, incentives to invest in the sustainable development of a technology or business model potentially vanish: this is one of the core focuses of the economics discipline which is increasingly developing around theories of design of such systems.

DeFi also raises accountability and enforcement issues around issues of both public and private ordering. Most notably, difficulties of establishing standing to sue and of determining the applicable law and jurisdiction of regulators, supervisory authorities, and courts, and the difficulties of establishing how many clients or counterparties are located in a given jurisdiction, all undermine the rule of law in financial services. But then again, to some extent that is one of the major objectives of DeFi.

In reality, it is highly likely that both economic and legal factors explain why *efficient* DeFi can never be total, but at best partial: where parts of the financial services value chain are decentralized there will be a reconcentration of a different (but possibly less regulated, less visible and less transparent) part of the value chain, with cloud computing and BigData pools providing a vivid example. In this sense, real-world DeFi potentially increases concentration effects somewhere else in the financial system and introduces further dimensions of cyber risk from tech dependency and interconnectivity.

Law thus faces real challenges from DeFi. If DeFi is to work in its ultimate expression, the rules governing it will need to be embedded in the system. This is the ultimate opportunity for RegTech and possibly for building better markets through technology. Beyond this, law must adapt to the challenges of DeFi. Tools include those designed to enhance cooperation of competent authorities, enhance tech risk management, require data and reserve localization, require RegTech to strengthen financial supervision and enforcement, and mandate open data and open access to services where data economies lead naturally, as in other forms of core infrastructure, to reconcentration. These tools may well require a central role for government in monitoring and potentially controlling the central underlying systems: ironically, realization of the DeFi dream may well require government intervention. Given that DeFi will come with reconcentration *somewhere* in the value chain, this reconcentration *enables, justifies, and requires* control over the DeFi systems, with DeFi supervision to focus on these new point(s) of failure.

112 See, on the original concept, William Forster Lloyd, *Two Lectures on the Checks to Population* (Oxford University 1833). The concept became widely known after it was used by Garrette Hardin (see Garrette Hardin, 'The Tragedy of the Commons' (1968) 162 *Science* 1243).

113 See M Friedman and R Friedman, *Free to Choose—A Personal Statement* (Mariner Books 1990) 24.