NUS National University of Singapore | Centre for Banking & Finance Law
Faculty of Law

Banking, Finance and Technology Conference

NUS Faculty of Law
18th – 19th May 2023

Collection of Selected Presentation Summaries

Compiled by:

Rachel Phang
Research Associate
CBFL, NUS Law

Alessio Azzutti
Research Associate
CBFL, NUS Law

[CBFL-Rep-2301]
July 2023

This collection is based on the proceedings of the Banking, Finance and Technology Conference organised by the Centre for Banking & Finance Law, and held on 18th – 19th May 2023. The views expressed in this report reflect the authors' personal opinions and do not necessarily reflect the policies or views of the Centre for Banking & Finance Law.

Centre for Banking & Finance Law
Faculty of Law
National University of Singapore
Eu Tong Sen Building
469G Bukit Timah Road
Singapore 259776
Tel: (65) 6601 3878
Fax: (65) 6779 0979
Email: cbfl@nus.edu.sg

http://law.nus.edu.sg/cbfl/

The Centre for Banking & Finance Law (CBFL) at the Faculty of Law, National University of Singapore, focuses broadly on legal and regulatory issues relating to banking and financial services. It aims to produce research and host events of scholarly value to academics as well as of policy relevance to the banking and financial services community. In particular, CBFL seeks to engage local and international bankers, lawyers, regulators and academics in regular exchanges of ideas and knowledge so as to contribute towards the development of law and regulation in this area, as well as to promote a robust and stable financial sector in Singapore, the region and globally.

Table of Contents

I. **The Nature of Property in Cryptoassets**

Mr Timothy Chan (National University of Singapore)....4

II. **The Regulation of Crypto-Lending**

Dr Alexandros Seretakis (Trinity College Dublin)....9

III. **Insolvency of Crypto-Asset Service Providers: Legal Problems and Regulatory Responses**

Mr Ilya Kokorin (Leiden University)....12

IV. **A Framework for the Interoperability of CBDCs**

Dr Kosmas Kaprinis (Binance/IE University)....16

V. **Regulating DeFi and On-Chain CeFi: Centralisation Points as Regulatory Hooks**

Dr Ann Sofie Cloots (University of Cambridge)....20

VI. **A Multi-Layered Framework of AI Governance in China's Finance Sector**

Ms Jinghe Fan (University of Oxford) and Dr Xin Zhang (University of International Business and Economics)....25

VII. **Financial Regulation and the Advent of Digital Reporting: The End of Rule-Use as We Know It?**

Dr Andromachi Georgosouli (Queen Mary University of London)....31

VIII. **Challenges Posed by the Second Generation of Digital Technologies to Financial Regulatory Strategies**

Dr Teresa Rodríguez de las Heras Ballell (Universidad Carlos III de Madrid)....35

IX. **AI in Credit Lending and Enforcement Decision-Making by Banks: Accuracy, Risk, Data and Consumer Protection**

Dr Jeannie Marie Paterson (University of Melbourne)....42

X. **At the Crossroads Where Robo-advisers Stand**

Mr Selwyn Lim (Syfe)....48

XI. **Payment Fraud and Consumer Protection**

Dr Sandra Booysen (National University of Singapore)....53

I. The Nature of Property in Cryptoassets[1]

Mr Timothy Chan
(National University of Singapore)

Most courts[2] and commentators[3] agree that cryptoassets are property. However, in order to develop that conclusion further, two important questions must be answered. First, why should cryptoassets be regarded as property? And second, how do property rules operate when it comes to cryptoassets? This presentation explores how we should approach the second question. As it proceeds on the basis that cryptoassets are property, it will not explore *why* they should be regarded as property.[4] It focuses on the mechanics rather than the justification of property in cryptoassets, which are important for various private law aspects of property in cryptoassets in both the contexts of two-party and three-party disputes.

It may be helpful to begin with a brief recap of how blockchain transactions are executed.[5] The blockchain is a decentralised ledger maintained by nodes which keep track of user balances and validate transactions for crypto rewards ('mining'). To send 1 BTC to B, for example, A sends an instruction to the network. The first node to receive the instruction verifies that (i) A's balance is sufficient; and A's signature is valid. The transaction then enters a pool of pending transactions where it awaits inclusion within a new 'block'. Once done, the answer forms part of the blockchain and the transaction is 'confirmed'. Importantly, nodes do not undertake an obligation to validate any particular transactions—mining is a self-interested process designed to earn Bitcoin rewards and the process is fundamentally extra-contractual.

What is the 'thing' or '*res*' that is the subject-matter of property rights in cryptoassets, considering that neither a physical 'thing' nor a contractual counterparty can be identified? One option, proposed by David Fox[6] and the Law Commission,[7] conceives of the *res* as a 'data string' or 'data structure', which should be treated as an exception to the rule that information

[1] This summary is based on a forthcoming paper, which may be cited as Timothy Chan 'The Nature of Property in Cryptoassets' (2023) *Legal Studies* (forthcoming), https://doi.org/10.1017/lst.2022.53.

[2] *See, e.g.*, *CLM v CLN* [2022] 5 SLR 273; *Janesh s/o Rajkumar v Unknown Person ("CHEFPIERRE")* [2022] SGHC 264; *Piroozzadeh v Persons Unknown and ors* [2023] EWHC 1024 (Ch); *Re Gatecoin Limited* [2023] HKCFI 91.

[3] *See, e.g.*, Michael Bridge et al. (eds) *The Law of Personal Property* (London: Sweet and Maxwell, 3rd edn, 2022), para 8-050; D Fox 'Cryptocurrencies in the common law of property' in D Fox and S Green (eds) *Cryptocurrencies in Public and Private Law* (Oxford: Oxford University Press, 2019); Kelvin FK Low and Ernie GS Teo 'Bitcoins and other cryptocurrencies as property?' (2017) 9(2) Law, Innovation and Technology 235.

[4] For some comments, see Timothy Chan and Kelvin FK Low 'DeFi Common Sense: Crypto-backed Lending in *Janesh s/o Rajkumar v Unknown Person ("CHEFPIERRE")*' (2023) *Modern Law Review* (forthcoming), 5–9, https://doi.org/10.1111/1468-2230.12804.

[5] *See* Chan (n 1) 3–5 and the references cited there.

[6] David Fox 'Digital assets as transactional power' (2022) 1 Journal of International Banking and Financial Law 3.

[7] Law Commission Consultation Paper on Digital Assets Law Com No 256, 28 July 2022, ch 10.

is not property,[8] insofar as it has the particular functionality of allowing the user to effect transactions on a blockchain network. But some difficulties should be noted.[9] First, it is not clear how such 'data' can be identified in different accounting systems (while it might be possible in unspent transaction output (UTXO)-based systems such as Bitcoin, it seems difficult in account-based systems, such as Ethereum). More importantly, framing data as the *res* seems inconsistent with the idea of proprietary exclusion, since the data has to be publicly available on the blockchain. And third, it is hard to explain why, after a cryptoasset is 'spent', it ceases to be property. On another view, proposed by Kelvin Low and Ernie Teo, the *res* is a legal right of cryptoasset holders to have their cryptoassets 'locked to their chosen public bitcoin address on the blockchain'.[10] But what is the legal basis for this right? As there is no contractual or statutory basis, it must be a claim that the courts *should* recognise a *new* right, as they did with common law copyright in the 18th century.[11] Even then, the corresponding duty must be a duty of non-interference, which seems better analysed as an incident of property rather than an item of property itself.[12]

Perhaps the better approach is to return to first principles. Most Commonwealth property scholars agree that property is about some combination of exclusionary control and a power of alienation.[13] What is the 'thing' that cryptoasset users seek to exclude others from by protecting their private keys, and 'transfer' through blockchain transactions? I suggest that it is a factual 'transactional ability'—an ability to effect a blockchain transaction (with the specific assets held at that public address) that will be recognised as valid under the relevant consensus algorithm.[14] It may seem unusual to regard an essentially factual ability as an item of property. But there is in fact precedent for this: goodwill, defined as the 'benefit and advantage of the good name, reputation, and connection of a business',[15] is recognised as a type of property,[16] albeit an unusual one. A state of reputation is essentially a state of factual recognition (or consensus), and the proposed 'transactional ability' is precisely an ability to change a state of consensus on the blockchain network. This conception accommodates various

[8] *Your Response v Datateam* [2014] EWCA Civ 281.

[9] *See* Chan (n 1) 9–10.

[10] *See* Low and Teo (n 3).

[11] In *Millar v Taylor* (1769) 4 Burr 2301. *See* Kelvin FK Low, 'Cryptoassets and the Renaissance of the *Tertium Quid*?' in *Chris Bevan (ed), Edward Elgar Handbook on Property Law and Theory* (forthcoming), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4382599.

[12] *See* Chan (n 1) at 11–12.

[13] *See, e.g.*, Bridge et al. (n 3) para 1-006.

[14] *See* Chan (n 1) 6–9.

[15] *Commissioners of Inland Revenue v Muller and Co's Margarine Ltd* [1901] AC 217 at 223–224.

[16] *See, e.g.*, *Harrods Ltd v Harrovian School Ltd* [1996] RPC 697 at 711 per Millett LJ; *Spalding (AG) and Bros v AW Gamage Ltd* (1915) 32 RPC 273 (HL) at 284 per Lord Parker; *Star Industrial v Yap Kwee Kor* [1976] FSR 256 (PC) at 269 per Lord Diplock.

types of cryptoassets, both first- and second-layer, and explains various practical aspects of property in cryptoassets, such as what happens when a private key is irretrievably lost.[17]

Another key issue is the characterisation of blockchain transactions: do such transactions amount to true legal 'transfers', or are they events by which the original asset (conceptualised as a transactional ability or otherwise) is extinguished, and a new asset created (which we may call a '*res*-creating' event)? If the latter, which is generally thought to be the case with bank transfers,[18] then traditional rules of title transfer such as *nemo dat* probably would not apply.[19] This led the UK Jurisdiction Taskforce to the unpalatable conclusion that where cryptoassets are stolen, *nemo dat* would not apply.[20] Factually, at least, whether an event is '*res*-transferring' or '*res*-creating' depends on the 'thing' being transferred. On Fox's 'data centric' view and the present view that the *res* is a transactional ability, the relevant 'function' or 'ability' is rendered 'spent' and extinguished upon each blockchain transaction. On Low's view that the *res* is a 'right to a registry entry', no such issues arise—the right is a legal construct, so whether it is 'transferred' need not take reference from the factual mechanism of the transaction. I argue, however, that whether a true 'transfer' has occurred should be treated as a normative rather than a factual question.[21] The best analogy is with chattels which go through a process of manufacture, where the suggested test is whether the raw materials and the product are economically identical.[22] This 'economic identity' test is suitable for the context of intangibles because they cannot be physically enjoyed; importantly, it also explains why bank transfers are new items of property, since each bank account is governed by different sets of terms and conditions with the counterparty bank. In the crypto context, there is no counterparty and each transactional ability is economically identical. I suggest this provides a strong basis to regard blockchain transactions as true 'transfers', rather than '*res*-creating' events.

I argue that the foregoing analysis provides principled grounds for extending to cryptoassets existing rules of title transfer which presently apply to chattels. There are two important similarities between the two. First, and most importantly, blockchain transactions as true 'transfers' are different from bank transfers, where *nemo dat* does not apply. Second, control of cryptoassets via a private key is programmed to be both rivalrous and transferable.

[17] *See* Chan (n 1) 8.

[18] *R v Preddy* [1996] AC 815.

[19] Cf *Trustee of the Property of FC Jones and Sons v Jones* [1997] Ch 159; Ben McFarlane and Robert Stevens 'The nature of equitable property' (2010) 4 Journal of Equity 1 at 22; Lionel Smith 'Simplifying claims to traceable proceeds' (2009) 125 LQR 338 at 347.

[20] UK Jurisdictional Taskforce Legal Statement on Cryptoassets and Smart Contracts, November 2019, para 47.

[21] *See* Chan (n 1) 12–17.

[22] Duncan Webb 'Title and transformation: who owns manufactured goods?' (2000) Journal of Business Law 513 at 523.

As Fox has pointed out,[23] this makes such control functionally similar to the possession of tangible assets. A transfer of legal title to cryptoassets therefore probably requires both an intention to transfer and some proxy to delivery (a transfer of the private key itself or, more commonly, a blockchain transaction).[24] Further, where a party purports to transfer a cryptoasset to which he does not have legal title, *nemo dat* (which is a rule of general application to all legal transfers) should apply.[25]

These rules provide a starting point for resolving proprietary disputes over cryptoassets. For example, in *Jones v Persons Unknown*,[26] the claimant sent around 89.6 BTC to fraudsters' accounts which was subsequently traced to Huobi wallets. On the claimant's application for summary judgment, the court held Huobi a constructive trustee of that BTC. However, it was far from clear how the court reached that conclusion, and in particular why Huobi was said to have obtained legal title to the BTC. In fact, Clause 5(i) of Huobi's 'Platform User Agreement' stated that 'title to the Digital Assets shall remain with you [the customer] and not transfer to us.'[27] What then was Huobi holding on trust? Perhaps the better analysis was that legal title remained with the fraudsters, but was subject to a constructive trust in favour of Jones, who could then enforce the fraudsters' rights against Huobi under the *Vandepitte* procedure.[28] Another recent example is provided by the interlocutory proprietary injunction granted in the *Chefpierre* case, which involved a DeFi arrangement for a loan of 45 ETH granted subject to some sort of quasi-security over a Bored Ape Yacht Club NFT. [29] In such cases, the question of title is inextricably tied up with the characterisation of the security arrangement. Here, the courts 'take account of the language used by the parties in order to decide what rights and obligations are created by the agreement, so long as the agreement is internally consistent, and there is no evidence of a sham'.[30] The focus remains, therefore, on the intentions of the parties, although the subsequent question of characterising the arrangement presents particular difficulties in the DeFi context.[31]

[23] *See* Fox (n 3).

[24] *See* Chan (n 1) 17; *see also* Fox(n 3) para 6.49; Hin Liu, 'Transferring legal title to a digital asset' (2023) 5 JIBFL 317.

[25] See Chan (n 1) 18; *see also* Fox (n 3) para 6.48.

[26] [2022] EWHC 2543 (Comm).

[27] Terms dated 22 February 2021 and last updated on 22 June 2022, https://www.huobi.com/support/en-us/detail/360000298561.

[28] *See* Timothy Chan and Kelvin FK Low 'Post-Scam Crypto Recovery: Final Clarity or Deceptive Simplicity?' (2023) LQR (forthcoming), SSRN preprint, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4394820.

[29] *Janesh s/o Rajkumar v Unknown Person ("CHEFPIERRE")* [2022] SGHC 264.

[30] Louise Gullifer, *Goode and Gullifer on Legal Problems of Credit and Security* (Sweet & Maxwell, 6th ed, 2017), para 1-36.

[31] For further discussion, see Timothy Chan and Kelvin FK Low 'DeFi Common Sense: Crypto-backed Lending in *Janesh s/o Rajkumar v Unknown Person ("CHEFPIERRE")*' (2023) *Modern Law Review* (forthcoming), https://doi.org/10.1111/1468-2230.12804.

To properly resolve proprietary disputes over cryptoassets, we must figure out what title rules apply, and why they apply. My core argument here is that there is good reason for traditional rules to be applied by analogy, and I have sought to demonstrate the relevance of these rules to practical decisions. This space continues to develop rapidly and remains one to watch.

II. The Regulation of Crypto-Lending

Dr Alexandros Seretakis[1]
(Trinity College Dublin)

Summary of the Presentation Delivered at the CBFL Banking, Finance and Technology Conference, 18-19 May 2023, NUS Law. The Presentation is based on the paper "How Should Crypto-Lending Be Regulated under EU Law?" jointly authored with Professor Emilios Avgouleas, University of Edinburgh.

The last few years have seen the exponential growth of crypto lending, with lenders such as Celsius and BlockFi, and DeFi protocols such as MakerDAO and Compound dominating the space.[2] Nonetheless, the failures of Celsius Network and Voyager have alarmed policymakers, alerting them to the importance of crypto lenders for crypto markets and the fragility of their business model. Moreover, the spectacular collapse of FTX created contagion across the industry and had a spillover effect on crypto lenders, with major firms such as Genesis and BlockFi suspending withdrawals of customer funds and filing for bankruptcy.[3]

Crypto lenders, such as Celsius and Voyager, sought to provide a solution to two distinct problems facing crypto holders: lack of liquidity and market purchasing power.[4] Crypto holders face a liquidity problem, since crypto is not widely accepted as a medium of exchange. As a result, holders of crypto who want to monetise their holdings must convert them into fiat currency.[5] Moreover, the opportunities to earn handsome returns on crypto holdings, such as staking, are only available to the holders of big portfolios.[6] Crypto lenders engage in secured lending by allowing holders to deposit their assets and borrow fiat currency or other digital assets using their crypto holdings as collateral. Moreover, users can also earn rewards on these assets at rates that are more favourable than those offered by traditional intermediaries or other

[1] Assistant Professor of Law in Capital Markets and Financial Services and Fellow (elected 2023) Trinity College Dublin.

[2] Leeor Shimron, 'Exploding Past $10 Billion, Interest Income and Lending are Bitcoin's First Killer Apps' *Forbe*s (26 May 2020), https://www.forbes.com/sites/leeorshimron/2020/05/26/exploding-past-10b-interest-income-and-lending-are-bitcoins-first-killer-apps/.

[3] Laurence Fletcher and Joshua Oliver, 'Hedge Funds Left With Billions Stranded on FTX' *The Financial Times* (22 November 2022), https://www.ft.com/content/125630d9-a967-439f-bc23-efec0b4cdeca; Stephanie Findlay et al., 'Crypto Broker Genesis Puts Lending Unit Into Chapter 11 Bankruptcy' *The Financial Times* (20 January 2023), https://www.ft.com/content/c040bc6c-08be-48dd-8af9-3b11b8b67c99. More than $900 million in customer funds remain frozen in Genesis's bankruptcy. *See* Ken Sweet, 'Crypto Firms Acted Like Banks, then Collapsed Like Dominoes' *Associated Press* (23 January 2023), https://apnews.com/article/cryptocurrency-technology-financial-services-bankruptcy-bitcoin-f7d97ff9cc12afc1fd845648b5f13ea7.

[4] In re CELSIUS NETWORK LLC, et al., Declaration of Alex Mashinsky, Chief Executive Officer of Celsius Network LLC, In Support of Chapter 11 Petitions and First Day Motions, p. 2.

[5] *Ibid*.

[6] *Ibid*.

crypto platforms. Crypto lenders are in essence performing credit intermediation outside the regular banking system. As a result, they form part of the so-called shadow banking system.

The key financial stability threat of crypto lending comes from the excessive volatility of crypto currency markets and the fact that lots of crypto assets like NFTs—non fungible tokens[7]—are very complex and very difficult to value, making it is very difficult to obtain sufficient collateral to secure the loan.[8] So, leverage within the system remains uncontrolled. It makes lenders vulnerable to suspicions of bankruptcy, thus triggering market panic (depositor runs), which may result in lenders facing the risk of illiquidity.

The activities of crypto lenders, which involve the taking of deposits in crypto-assets and the granting of crypto loans, resemble the activities of credit institutions. As a result, prudential regulation should be extended to crypto lenders. Crypto lenders are currently not captured by banking regulation. In the US, numerous state regulators and the Securities and Exchange Commission (SEC) have taken the view that the interest-bearing accounts offered by crypto lenders are unregistered securities. For instance, in February 2022, the SEC charged BlockFi, a major crypto lender, with failing to register the offers and sales of its retail crypto lending product.[9] US regulators seek to regulate crypto lenders and protect the public against their risks via securities law. Nevertheless, securities regulation is not suitable for tackling the risks posed by crypto lending. Instead, it may exaggerate financial instability. Securities regulation is based on disclosure.[10] In the event of a market panic, market players do not act to rationally and it is unlikely that they will stop "running" in the face of more information.

Even though crypto lending is a form of narrow banking and the usual rationales for prudential regulation, namely, fractional reserve and depositor protection, may not apply, the risks created by the crypto lending industry are important enough to justify the full panoply of prudential regulation. As the Celsius and Voyager debacles demonstrated, crypto lenders face the risk of investor runs, which can lead to their demise triggering a cascade of failures in crypto markets. Moreover, taking a functional approach, regulation should not distinguish

[7] According to Makavor and Schoar, NFTs are "a unique piece of data stored on a blockchain. The data can be associated with a particular digital or physical asset or a license to use the asset for a specified purpose." *See* Igor Makavo and Antoinette Schoar, 'Cryptocurrencies and Decentralized Finance (DeFi)' (April 2022) NBER Working Paper 30006, 26.

[8] Collateral made up of crypto assets can be very volatile and can quickly lose value. For instance, Sam Bankman-Fried in a letter to staff argued that the value of collateral held by FTX fell from $60 billion to $8 billion. Nikhilesh De, 'Bankman-Fried Apologizes to FTX Employees, Details Amount of Leverage in Internal Letter' (*CoinDesk*, 23 November 2022), https://www.coindesk.com/business/2022/11/22/bankman-fried-apologizes-to-ftx-employees-details-amount-of-leverage-in-internal-letter/.

[9] In the Matter of BlockFi Lending LLC, SEC Order, https://www.sec.gov/litigation/admin/2022/33-11029.pdf.

[10] John C Coffee Jr, 'Market Failure and the Economic Case for a Mandatory Disclosure System' (1984) 70(4) Virginia Law Review 717; Paul G Mahoney, 'Mandatory Disclosure as a Solution to Agency Problems' (1995) 62 University of Chicago Law Review 1047; Paul Mahoney, 'The Economics of Securities Regulation: A Survey' (2021) Virginia Law and Economics Research Paper No. 2021-14.

between the two types of intermediaries, namely the mainstream lending institutions and crypto lenders. Cranston, Avgouleas et al. define prudential regulation as the thick and complex web of rules employed to (a) keep financial institutions safe and a going concern, and failing that, (b) to assist their resolution and/or restructuring, and (c) to augment the resilience of financial systems to withstand shocks.[11] Prudential regulatory tools include capital requirements, liquidity requirements,[12] corporate governance and remuneration rules, lender of last resort facilities and deposit insurance.

The application of prudential rules—excluding lender of last resort and deposit insurance arrangements in order not to heighten moral hazard—would have averted the recent collapses of Voyager and Celsius. Adequate capital reserves would ensure the stability of the crypto lending operators and reduce the risk of bankruptcy. The balance sheet hole would have been covered. Prudential regulation would have also prevented concentration of balance sheets on a single asset class. Moreover, liquidity requirements would have required crypto lenders to hold some of their assets in liquid form ensuring thus that they had enough funds to repay users and avert the run. Corporate governance standards and remuneration rules would have guaranteed effective risk management and prevented excessive risk-taking. For instance, Celsius's collapse can be in part attributed to the losses suffered from erroneous and risky asset deployment decisions, such as investments in long-term and illiquid assets. To avoid giving false assurances to crypto lending users, crypto lenders should not benefit from deposit insurance schemes or lender of last resort facilities. The application of deposit insurance and lender of last resort facilities to crypto lenders would create moral hazard and extend implicit government guarantees to crypto lenders.[13] Crypto lenders would thus become another category of too-big-to fail institutions.

[11] Ross Cranston et al., *Principles of Banking Law* (Oxford University Press 2018) 31.

[12] Liquidity requirements are composed of the Liquidity Coverage Ratio and the Net Stable Funding Ratio. The Liquidity Coverage Ratio seeks to ensure that institutions have enough liquid assets to withstand a 30-day stress period. The Net Stable Funding Ratio forces institutions to finance long-term assets with long-term liabilities. *See* Clemens Bonner and Paul Hilbers, 'Global Liquidity Regulation – Why Did It Take So Long?' (2015) 455 DNB Working Paper January 2015, https://www.dnb.nl/media/wkjpo4kj/working-paper-455.pdf.

[13] On how deposit insurance creates moral hazard, *see* Charles W Calomiris, 'Is Deposit Insurance Necessary? A Historical Perspective' (1990) 50(2) The Journal of Economic History 283; Stanley Fischer, 'On the Need for an International Lender of Last Resort' (1999) 13(4) Journal of Economic Perspectives 85.

III. Insolvency of Crypto-Asset Service Providers: Legal Problems and Regulatory Responses

Mr Ilya Kokorin[1]
(Leiden University)

Insolvencies of crypto-asset service providers (CASPs or crypto firms) are not new. Perhaps the most well-known example is the collapse of the Japanese crypto exchange Mt.Gox in 2014. While customers of Mt.Gox are still waiting to get compensation, crypto markets have experienced a major downturn since the spring of 2022—the so called "crypto winter". By some estimates, from May 2022, over US$1.8 trillion of crypto value dissolved.[2] Last year, we witnessed collapses of some major market players, including Three Arrows Capital, Voyager, Celsius, FTX, Alameda and BlockFi. Crypto failures continued in 2023 (e.g., Genesis, Bittrex Inc). These domino-like crashes highlight the interconnectedness of market participants (e.g., crypto lenders, crypto hedge funds, crypto exchanges), integrated nature of many crypto enterprises, multi-layered group structures behind a recognised brand name, and frequent disregard of corporate formalities. Ultimately, insolvencies of CASPs emphasise the importance of both private and public law for the protection of stakeholders, especially consumers and crypto investors.

Insolvency is the ultimate litmus test that may reveal the (in)adequacy of regulation and test the application of various rules and doctrines from different areas of law, including property, contract, insolvency and financial law. It brings to light complex legal problems and exposes the vulnerabilities of the existing business models. In this presentation, I examine the most common legal problems that arise in crypto bankruptcies and explore regulatory responses to them.

The first part of the presentation outlines some general observations concerning the current wave of crypto failures. It highlights the major role of intermediaries in crypto markets and summarises the main causes of CASPs' insolvencies. Interestingly, despite the promises of disintermediation, famously proclaimed in the Bitcoin White Paper,[3] the present-day reality is that a significant share of crypto-assets remains in the hands of centralised entities. This creates single points of failure. Such failure could be caused by a variety of non-exclusive and frequently overlapping events and reasons, including hacks (Mt.Gox, Gatecoin, Cryptopia), unsustainable business models resulting in negative net interest margin (Celsius), overreliance or overinvestment in a particular asset like a stablecoin (Three Arrows Capital), large exposure

[1] PhD candidate at the Department of Financial Law, Leiden University, the Netherlands.
[2] Giulio Cornelli et al., 'Crypto shocks and retail losses', BIS Bulletin, No. 69 (20 February 2023), https://www.bis.org/publ/bisbull69.pdf.
[3] Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System', https://bitcoin.org/bitcoin.pdf.

and industry contagion (Voyager, BlockFi, Genesis), as well as regulatory issues and/or likely mismanagement or even fraud (Bittrex Inc, FTX/Alameda).

Insolvency means that there are insufficient assets to fully satisfy creditors' claims. This is why "who should get what in insolvency" becomes a crucial and heavily-litigated question. An answer to this question in many cases depends on whether customers of a failed CASP are general unsecured creditors or whether they can exercise *in rem* (property rights) over deposited crypto-assets. As demonstrated by a line of cases from civil and common law jurisdictions, the existence of such *in rem* rights depends on individual facts of the case and on applicable (property) law—and specifically whether this law recognises the concept of trusts or otherwise permits preservation of property rights over commingled fungible assets.[4] In some of the most recent cases, courts in common law jurisdiction paid particular attention to the Terms & Conditions or Terms of Use of crypto platforms.[5] In one of them, the court even concluded that the "issue of ownership of the assets in [accounts] is a contract law issue."[6] Be it as it may, even if a contract with a CASP explicitly states that "Title to your Digital Assets shall at all times remain with you and shall not transfer to CASP", this does not guarantee full protection of customers' assets and rights. For instance, if a CASP (in violation of a contractual undertaking) disposes of (or re-uses) customers' crypto-assets—as was likely the case with FTX[7]—the return of such assets may be difficult, if not impossible.

In order to promote legal certainty, protect consumers and crypto investors, ensure market integrity, and preserve financial stability, while at the same time supporting innovation and the development of new technologies—regulation is necessary. But what type of regulation? The second part of this presentation summary is devoted to the issue of regulation. One can regulate the relations around crypto-assets through private law instruments (e.g., Article 12 of the Uniform Commercial Code, UNIDROIT Digital Assets and Private Law Principles) or via rules of a public (administrative) law nature (e.g., EU Markets in Crypto-assets Regulation or MiCA, EU Transfer of Funds Regulation, Japanese Payment Services Act, Swiss "Blockchain Act"). Public law aims to establish the rules of the game for market participants and for crypto markets. In this paper, I look at one example of such law—MiCA.

[4] *See In re MtGox*, Tokyo District Court, 5 August 2015, Reference No. 25541521; *In re Bitgrail*, Court of Florence, 21 January 2019, Bankruptcy Docket Nos. 178/2018 and 205/2018, Decision No. 17/2019; *Ruscoe & Moore v. Cryptopia Limited (in liquidation)* [2020] NZHC 728.

[5] *See In re Celsius Network LLC et al.*, Case No. 22-10964 (MG) (Bankr. S.D.N.Y. 4 January 2023); *Re Gatecoin Ltd (in liquidation)* [2023] HKCFI 914; HCCW 18/2019 (31 March 2023).

[6] *See In re Celsius Network LLC et al.*, Case No. 22-10964 (MG) (Bankr. S.D.N.Y. 4 January 2023).

[7] *See CFTC v. Samuel Bankman-Fried et al.*, Amended Complaint for Injunctive and Other Equitable Relief, Case No. 1:22-cv-10503-PKC, 21 December 2022; *SEC v. Samuel Bankman-Fried*, Complaint, Civil Action No. 22-cv-10501, 13 December 2022.

On 24 September 2020, the European Commission adopted a Digital Finance Package with the goal of boosting Europe's competitiveness and innovation in the financial sector, and making the European Union (EU) a global standard-setter.[8] The Digital Finance Package contained a number of legislative proposals, including the Proposal for a Regulation on Markets in Crypto-assets.[9] MiCA is truly ambitious, both in length (with more than 140 articles) and scope. It constitutes the largest piece of supranational legislation targeting crypto-assets, which seeks to integrate them into the modern financial system.

MiCA was approved by the European Parliament on 20 April 2023 and will be applicable in 2024.[10] It will apply to crypto-assets, which are defined as "digital representation of a value or of a right that is able to be transferred and stored electronically using distributed ledger technology or similar technology."[11] Thus, it will cover all major types of crypto-assets (i.e. cryptocurrencies, stablecoins, utility tokens). However, it excludes tokens that qualify as securities (e.g., tokenised shares or bonds). These "blockchain-wrapped" financial instruments and services around them fall within the scope of the long-standing financial regulation, including instruments like MiFID II[12] and the Prospectus Regulation.[13] MiCA also does not extend to unique non-fungible tokens (NFTs), central bank digital currencies (CBDCs), and lending and borrowing of crypto-assets.

MiCA introduces detailed rules on issuance, offering to the public, admission to trading of crypto-assets and provision of certain services like exchange and custody of crypto-assets.[14] For example, it stipulates that CASPs that hold crypto-assets belonging to clients should ensure that those crypto-assets are not used for their own account.[15] In theory, this should prevent an FTX-like scenario involving a re-use of customers' crypto-assets. In addition, MiCA obliges CASPs to "make adequate arrangements to safeguard the ownership rights of clients",[16] and provides for different types of segregation arrangements which must be employed by CASPs

[8] European Commission, 'Digital finance package', https://finance.ec.europa.eu/publications/digital-finance-package_en.
[9] Proposal for a Regulation on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, COM(2020) 593 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0593. Other instruments from the Digital Finance Package include the Digital Operational Resilience Act (DORA) and the DLT Pilot Regime Regulation.
[10] MiCA, text adopted by the European Parliament, https://www.europarl.europa.eu/doceo/document/TA-9-2023-0117_EN.html.
[11] MiCA, Article 3(1)(5).
[12] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments.
[13] Regulation (EU) 2017/1129 of the European Parliament and of the Council of 14 June 2017 on the prospectus to be published when securities are offered to the public or admitted to trading on a regulated market.
[14] For a concise overview of MiCA, see Patrick Hansen, 'The EU's new MiCA framework for crypto-assets – the one regulation to rule them all' (20 April 2023), https://paddihansen.substack.com/p/the-eus-mica-framework?utm_source=direct&utm_campaign=post&utm_medium=web.
[15] MiCA, Recital 83.
[16] MiCA, Article 70(1).

offering custody services.[17] To the extent that segregation helps to identify customers' crypto-assets and ensure that these assets are not commingled with the assets of a CASP (and, therefore, are less likely to be re-used), they promote protection of clients' (property) rights.

To conclude, the recent wave of crypto bankruptcies exposed a plethora of risks characterising the activities of crypto-asset service providers. Failures of large crypto firms like Celsius and FTX also emphasised the urgency of regulation. Such regulation is necessary to protect consumers and investors, but also to help crypto businesses, as they often struggle with legal uncertainty. MiCA—a new ground-breaking law harmonising the regulation of crypto firms and crypto-asset services in the European Union—can prevent or at least reduce the damaging effects of crypto insolvencies. That said, given the global nature of crypto-assets and services provided by CASPs registered all over the world, a global response may be required.[18]

[17] MiCA, Article 75.

[18] *See* FSB, Regulation, 'Supervision and Oversight of Crypto-Asset Activities and Markets: Consultative document' (11 October 2022), https://www.fsb.org/wp-content/uploads/P111022-3.pdf; IOSCO, 'Policy Recommendations for Crypto and Digital Asset Markets: Consultation Report' (May 2023), https://www.iosco.org/library/pubdocs/pdf/IOSCOPD734.pdf.

IV. A Framework for the Interoperability of CBDCs

Dr Kosmas Kaprinis
(Binance/IE University)

The exploration of central bank digital currencies (CBDCs) has accelerated rapidly in recent years. While each central bank has different motivations for exploring CBDC systems at the domestic front, the potential for improved cross-border payments through CBDC arrangements is perceived as a common goal across jurisdictions. In the context of CBDCs, interoperability refers to the ability of different CBDC systems to interact with each other, allowing financial institutions and retail customers to transfer money between different CBDC networks. The interoperability of CBDCs has raised several legal issues that need to be addressed before practical cross-border arrangements are established.

As a brief overview, CBDC is defined as central bank money in a digital format, denominated in the national unit of account, and is a direct liability of the central bank. Retail CBDCs are designed for individuals and businesses to hold and utilise in their everyday transactions. Wholesale CBDCs are held by eligible financial institutions and used for the settlement of interbank payments. There are a number of well-recognised policy choices faced by CBDCs at the domestic level. These include: whether the CBDC should be architected on an ‘account’ or ‘token’ model; whether the CBDC should be accessible to retail users or restricted to wholesale users; and whether the central bank should pay interest on CBDC holdings. It is projected that the CBDC ecosystem would comprise similar elements and functions as traditional payment systems. In this respect, financial service providers will likely maintain their intermediary role in CBDC distribution, compliance, and CBDC wallet provision.

In the sciences, interoperability refers to the technical and business compatibility that enables a system to be used in conjunction with other systems. In CBDCs, interoperability enables financial institutions from various CBDC systems to conduct cross-system payments without the need to engage in multiple systems simultaneously. The concept of interoperability is interpreted from a different angle for each financial market participant: for retail users (or wholesale) users, interoperability is perceived as a state of seamlessness, where transactions between platforms occur with minimal costs; for financial service providers, it is perceived as a business environment that would diminish hurdles to entry in new markets; for regulators, interoperability would reduce operational risks of operators and promote the efficiency of the financial sector. In this regard, an international CBDC system will need to “compete” with other payment schemes on user experience and regulatory efficiency if it is to be widely adopted.

In the CBDC pilots that have been conducted internationally, three broad models have emerged in terms of interoperability:

- The compatible model—refers to individual/domestic CBDC systems that use common standards to communicate, reducing the operational burden on financial institutions while participating in multiple systems. For example, if a national CBDC system allows for direct access, a foreign bank could directly access the system to facilitate a cross-border payment using the domestic CBDC of that jurisdiction. In this regard, the compatible model does not link different CBDC systems, though it has the potential to improve efficiency of payment processing.
- The interlinked model—refers to the process of connecting different CBDC systems using standardised technical protocols, which not only enable foreign banks to process payments but also assist in ensuring compliance, facilitating foreign currency provision, and settling transactions. As in the first case, these common arrangements would allow participants in the interlinked CBDC systems to transact with each other without the need to become a direct participant in each of them.
- The single system model—refers to CBDC systems that use a single common technical infrastructure. This model is not about connecting separate systems, but rather establishing a common platform to achieve interoperability between CBDCs.

There is no universal model that can be applied to all cases when it comes to accessing and ensuring interoperability among different CBDC systems. For example, while compatibility might be the least costly form of interoperability, it may not achieve similar efficiency benefits to interlinking or a single system. The majority of the pilots for multi-CBDC interoperability have adopted option 3 of a single, shared settlement system.

According to the Bank for International Settlements (BIS), approximately 28% of the central banks surveyed are considering the possibility of creating multi-CBDC arrangements to achieve interoperability among different CBDC systems. Singapore has been at the forefront of research and testing in the field of CBDC interoperability. Indicatively, in November 2018, the Monetary Authority of Singapore (MAS), the Bank of Canada (BoC), and the Bank of England (BoE) released an early report evaluating different approaches to improve cross-border payments and settlements. Following this, MAS and BoC connected their experimental domestic payment networks, known as Project Jasper and Project Ubin, and in May 2019, they announced a successful trial of cross-border and cross-currency payments using CBDCs. Presently, Singapore, along with South Africa and Australia, is participating in cross-border CBDC testing.

From a policy perspective, we identify three important policy priorities for policy makers: (i) international governance arrangements on CBDC design and infrastructure, (ii) interoperability of CBDCs that is robust to operational risks, and (iii) maximising the potential of CBDC arrangements for enhancing inclusive growth globally. Our hypothesis is that the divergent (and not sufficiently harmonised) legal domestic frameworks can pose challenges to the above goals. This is attributed to the fact that interoperability is not viewed as a technical process, but part of a wider strategy of sovereign states to exert influence over global finance.

From a legal perspective, the primary legal concern is the issue of jurisdiction. Specifically, the transaction processing, settlement, and clearing of CBDCs involve the transfer of assets across borders. National regulators have the responsibility of overseeing the operations of a domestic CBDC, but cross-border operations involve multiple jurisdictions, each with its own set of regulations. Currently, such transfers adhere to conditions specified by cross-border payment systems such as SWIFT and TARGET2, with established international standards and arbitration procedures. Similarly, for CBDC systems to be interoperable, they must ensure that their transactions are legally enforceable across different jurisdictions. Secondly, interoperability requires establishing effective know your customer (KYC) and anti-money laundering (AML) procedures across different CBDC systems. Ensuring that all participants in the interconnected CBDC networks comply with KYC and AML requirements is vital to prevent money laundering, terrorist financing, and other illicit activities. Interoperability increases the attack surface for cyber threats and fraud attempts. Implementing robust cybersecurity measures, including encryption, authentication protocols, and fraud detection systems, is necessary to mitigate compliance risks related to cybersecurity and fraud prevention. Additionally, ensuring consumer protection in an interoperable CBDC environment is crucial. Clear rules and mechanisms should be in place to address issues such as unauthorised transactions, disputes, refunds, and customer support across different CBDC systems. Finally, the legal consequences of interoperability also encompass matters of privacy and data protection. When different CBDC systems interact with each other, they must exchange transaction data, personal information, and other sensitive data, which can raise concerns regarding data privacy.

It is widely agreed that CBDCs could play an important role in addressing long-standing challenges in the cross-border payments market It is crucial to avoid creating fragmented systems that hinder interoperability and resemble isolated entities. Instead, CBDCs should serve as inclusive platforms supporting global financial inclusion and fostering innovation in the financial markets. In this respect, the interoperability of CBDCs poses several real legal implications that need to be worked out for the above goals to be achieved.

Broader international coordination on domestic designs would be beneficial to lower barriers to cross-border compatibility and could serve as a launching pad for interoperability. International organisations such as the BIS, International Monetary Fund, and the Financial Action Task Force should play a critical role in developing common understanding and approaches for cross-border CBDCs. Even jurisdictions not planning to issue a CBDC ought to be involved in this work as they will still be part of this new regime. Finally, given the constant changes in the payments market, a cross-border CBDC system should also be flexible enough to interoperate with future payment services arrangements.

Bibliography

"Proceeding with Caution — A Survey on Central Bank Digital Currency," Bank for International Settlements, January 2020. Source: www.bis.org/publ/othp33.pdf

"Central Bank Digital Currency: The Quest for Minimally Invasive Technology," Raphael Auer and Rainer Boehme, BIS Working Papers, June 2021. Source: www.bis.org/publ/work948.htm

"Project Jasper and Project Ubin: Cross-border Interoperability Prototype for Payments and Settlements Using Central Bank Digital Currency," Bank of Canada, Monetary Authority of Singapore, 2019. Source: www.bankofcanada.ca/wp-content/uploads/2019/05/Project-Jasper-and-Project-Ubin-Cross-border-Interoperability-Prototype-for-Payments-and-Settlements-using-Central-Bank-Digital-Currency.pdf

"Central Bank Digital Currencies: Foundational Principles and Core Features," International Monetary Fund, October 2020. Source: www.imf.org/en/Publications/Policy-Papers/Issues/2020/10/13/Central-Bank-Digital-Currencies-49843

"Central Bank Digital Currencies: The Quest for Legitimacy and Efficiency in the Digital Age," European Central Bank, February 2020. Source: www.ecb.europa.eu/pub/pdf/other/ecb.cbdcquestforlegitimacyandefficiency202002~f2e7a67016.en.pdf

"Report on the Cross-border Retail Payments," Committee on Payments and Market Infrastructures and the World Bank Group, January 2021. Source: www.bis.org/cpmi/publ/d200.pdf

"Cross-border Retail Payments," Financial Action Task Force, June 2020. Source: www.fatf-gafi.org/media/fatf/documents/reports/Cross-Border-Retail-Payments.pdf

V. Regulating DeFi and On-Chain CeFi: Centralisation Points as Regulatory Hooks

Dr Ann Sofie Cloots
(University of Cambridge)

1. Introduction

Decentralised Finance (DeFi) has raised concerns among regulators, lawmakers and policymakers. Whereas regulation of centralised finance (CeFi) to a large extent relies on centralised intermediaries as legal hooks, DeFi is designed to reduce or bypass the reliance on such centralised intermediaries. The fear is that this undermines the ability to regulate decentralised financial infrastructure and the actors involved. This presentation summary shows why that fear is at least partially misplaced.

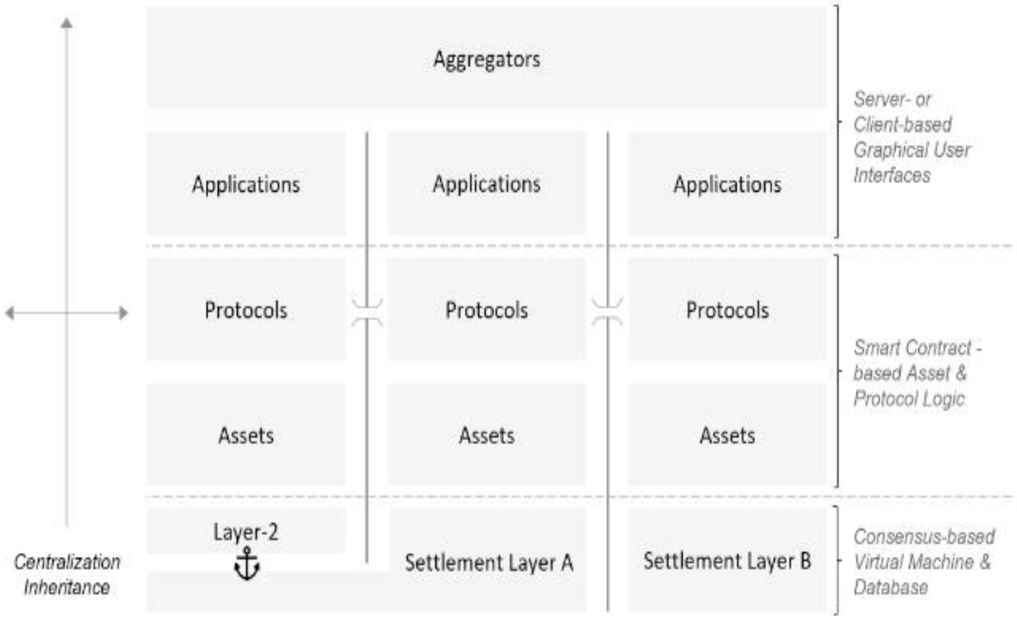
In a recent paper,[1] we propose a framework to assess the factual decentralisation of DeFi. A systematic analysis of DeFi's architecture shows various potential centralised 'hooks' on the different layers of DeFi's technology stack. These 'hooks', or centralisation vectors, can, and very likely will, be relied upon by lawmakers and regulators considering a legal framework for DeFi.

The proposed systematic analysis of DeFi requires sufficient understanding of the technological architecture of DeFi, from the blockchain (settlement) layer to the application layer.

Within this technology stack, various endogenous centralisation vectors can be identified at each layer. Moreover, a higher layer inherits centralisation concerns of a lower layer. For example, if a permissionless blockchain has centralised elements, this centralisation will be inherited by any protocol or application built on top of it.

In addition to centralisation vectors that are endogenous to one layer of the DeFi stack or are inherited from a lower layer, other centralisation vectors arise from interactions between the blockchain and the off-chain world.

[1] Katrin Schuler, Ann Sofie Cloots, and Fabian Schär, 'On Defi and On-Chain CeFi: How (Not) to Regulate Decentralized Finance' (2023) SSRN preprint, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4422473.


Aggregators
Applications
Applications
Applications
Server- or Client-based Graphical User Interfaces
Protocols
Protocols
Protocols
Smart Contract - based Asset & Protocol Logic
Assets
Assets
Assets
Layer-2
Settlement Layer A
Settlement Layer B
Consensus-based Virtual Machine & Database
Centralization Inheritance

For a legal analysis of DeFi, the first step is to locate a particular project in the DeFi stack. The second step is to scrutinise the project for endogenous centralisation vectors and the third step is to assess centralisation inheritance from a lower layer. Finally, centralisation vectors from a lateral layer or interaction with off-chain centralised entities need to be assessed. The aim is to identify centralisation vectors that distinguish genuine DeFi from on-chain CeFi when considering an adequate legal response.

Below we briefly assess the centralisation vectors at the three layers of the DeFi stack: (1) the settlement (blockchain) layer, (2) the asset and protocol layer and (3) the application and aggregator layer.

2. Settlement Layer (Blockchain Layer)

We analyse the capacity of users to directly join the network and exchange data with other network participants. Restrictions or special privileges can be used to exclude certain participants or transactions from the network, creating centralisation vectors that suggest one is dealing with on-chain CeFi rather than genuine DeFi.

Second, we assess the ability of participants to mathematically verify the authenticity and integrity of a transaction. Decentralisation in this respect may help achieve the regulatory goals of reducing information asymmetry in financial markets. Transparency of on-chain transaction data and execution logic could reduce the need for statutory disclosure obligations at the settlement layer. However, there may be various types of restrictions to this ability, which can be either explicit (off-chain computations by a third party) or implicit (the verification is prohibitively expensive for most average users).

The last and arguably most complex design aspect for a blockchain is reaching consensus over the current state. We assess different consensus models and their trade-offs, including the risks of frontrunning-like behaviour through MEV.[2] From a legal perspective, it is important to note that consensus models are designed to reach an agreement on the current state and discourage nodes from including invalid transactions. They are not designed to exclude unlawful transactions. Compliance with sanctions law (or other rules) can be enforced through on- and off-ramps or other centralised entities rather than through consensus-relevant nodes (such as miners or consensus-relevant nodes).

For regulators assessing whether and how to regulate this settlement layer, there are three important points to consider. First, if such legal obligations impose a degree of centralisation on the settlement layer (which is highly likely), in practice, this will undermine the possibility of DeFi, as DeFi requires a decentralised and independent settlement layer. Second, the settlement layer is not only used for DeFi but also for a variety of other applications. Regulating the settlement layer as a way to regulate DeFi will also affect all non-financial transactions on that layer. Third, there are other means to indirectly regulate, namely by regulating on- and off-ramps or scrutinising upper layers in the DeFi stack.

3. Asset and Protocol Layer

The asset and protocol layers are arguably the core element of the DeFi ecosystem where most of the 'action' happens. Both are smart contract-based and therefore have similar centralisation vectors and legal considerations.

Assets (or tokens) use standardised smart contract interfaces to keep track of balances and allow the transfer of funds. Protocols use smart contracts to recreate a wide array of financial market infrastructure, such as exchanges, lending markets, derivatives, and asset management services.

From a legal perspective, there have been proposals to regulate asset issuers as well as identify persons who control the asset's or protocol's smart contracts to place legal hooks. This assumes a level of centralisation at the asset or protocol layer or even, as one OECD report suggests, a need to recentralise DeFi to get "some comfort from a regulatory and supervisory standpoint, without necessarily completely undermining decentralisation".[3] It is difficult to see

[2] Maximum Extractable Value.

[3] OECD, 'Why Decentralised Finance (DeFi) Matters and the Policy Implications' (19 January 2022), https://www.oecd.org/daf/fin/financial-markets/Why-Decentralised-Finance-DeFi-Matters-and-the-Policy-Implications.pdf.

how this can be achieved, however, as it is technically impossible to introduce centralisation vectors ex post into a genuinely decentralised protocol. Moreover, this may not be desirable, as it undermines the potential benefits of genuine decentralisation.

Smart contract upgradeability: opt-in versus opt-out

To distinguish genuine DeFi from on-chain CeFi, we assess different types of centralisation vectors depending on the type of smart contract set-up (static, parametric or proxy contracts). A rough analogy is to see static contracts as 'opt-in' for users, while parametric and proxy contracts are 'opt-out'.

Smart contracts are functions that contain a condition that will be verified when someone 'calls' (relies on) this function. These conditions can introduce centralisation vectors, for example by imposing blacklists used for sanctions compliance) or whitelists.[4] In such cases, the functions are restricted: there is a gatekeeper that can exercise centralised control over who can interact with or change the smart contracts.

Some of these restricted functions may allow their controllers to effectively expropriate users. A straightforward example is when the functions allow the controller to unilaterally adjust user balances on an asset or protocol level without the holder's private keys. A further concern in terms of decentralisation is any emergency stop functions.

Governance: account-based versus token-based

We explore the governance and control structures behind these restricted functions.

First, we analyse account-based governance: setups in which the right to execute a restricted function is given to one or multiple account-holders. The holders of these so-called admin keys can exclusively call (execute) restricted functions.

Second, we assess token-based governance: a setup in which voting rights are tied to governance tokens.

Finally, we explore lateral centralisation that undermines genuine DeFi, through 'oracles' and 'bridges'.

[4] Sanctions law compliance has led several crypto companies to resort to blacklisting sanctioned addresses. Compliance with sanctions imposed against *individuals* requires KYC, which can be enforced through crypto-fiat on- and off-ramps. However, when sanctions target a blockchain *address* rather than the individual who controls it, the address can be blacklisted by centralised exchanges and protocols with blacklist functions.

4. Application and Aggregation Layer

Next, we assess the off-chain layers of DeFi. They provide graphical user interfaces (a website or app through which people interact with the underlying smart contracts, also called 'front-ends'). The applications are non-custodial.[5]

From a legal perspective, a DeFi project's activities on the front-end layer could be subjected to rules such as those on misleading advertisement or financial promotions. Other obligations that have been considered include audit requirements and governance standards.[6]

From a competition law viewpoint, the open technical interface to the on-chain DeFi infrastructure holds promise. Meanwhile, the potential abuse of dominant position by applications that garner substantial user traction raise centralisation concerns (for example, by bundling a popular wallet app with other services). Apps may also accept kick-backs from protocols.

5. Conclusion

Most of what is commonly referred to as DeFi today has severe centralisation vectors.

Centralised financial services that run on a blockchain should not be referred to as DeFi. Instead, we propose the term *on-chain CeFi* and argue that these centralised service providers can and should be regulated in line with their non-blockchain-based counter-parts. The two categories have different risk profiles and require distinct regulatory approaches.

While there is a certain grey area today, we argue that there will be a diversion toward the two extremes: projects will either become fully decentralised (genuine DeFi), acting as neutral infrastructure with no regulatory hooks, or they retain centralised elements (on-chain CeFi) and the corresponding hooks, through which they can and will be regulated.

[5] Otherwise they are purely centralised finance and outside of the scope of the analysis.

[6] HM Treasury, 'Future Financial Services Regulatory Regime for Cryptoassets. Consultation and Call for Evidence' (February 2023), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1133404/TR_Privacy_edits_Future_financial_services_regulatory_regime_for_cryptoassets_vP.pdf.

VI. A Multi-Layered Framework of AI Governance in China's Finance Sector

Ms Jinghe Fan (University of Oxford) and Dr Xin Zhang (University of International Business and Economics)

Artificial intelligence (AI) plays a central role in changing financial services around the globe.[1] In recent decades, AI has not only created new business models, like upgrading programme trading and developing robo-advisers, but also transformed the methods of fulfilling compliance duties and assisting risks assessment in credit lending, etc.[2]

In 2017, China released the *Next Generation Artificial Intelligence Development Plan* ('AIDP') which outlines China's overarching policy objectives of AI development strategy. As a highly incentivised 'wish list',[3] the AIDP indicates the importance of developing AI as one of the driving forces for multiple sectors which entail finances. The People's Bank of China has also called for applying AI steadily and properly promoting 'the deep integration of artificial intelligence technology with the financial business' in the *FinTech Development Plan (2019-2021)*. Against this backdrop, the market size of AI-powered financial products has been anticipated to constantly expanding.[4]

Despite the potential of facilitating transactions, enhancing market efficiency, and improving customer experience,[5] the expanding application of AI in financial services could also bring about a myriad of risks. These risks could be basically classified into three categories based on the underlying reasons. The first type of risk—*endogenous risks from AI technologies*—is predominantly affected by the technical features of developing and using AI.[6] A straightforward example would be that the use of non-traditional data and novel models (e.g., Machine Learning) could exacerbate the opacity of AI systems and further create challenges of explainability. Also, the multiple stages of developing AI may increase the number of actors involved in the supply chain and obscure the responsibility allocation.[7] The second category of

[1] Florian Ostmann and Cosmina Dorobantu, 'AI in Financial Services' (The Alan Turing Institute 2021) 5 https://www.turing.ac.uk/news/publications/ai-financial-services.

[2] Richard Hay and Sophia Le Vesconte, 'Financial Regulation', *Artificial Intelligence Law and Regulation* (2022) 292.

[3] Huw Roberts et al., 'The Chinese Approach to Artificial Intelligence: An Analysis of Policy, Ethics, and Regulation' (2021) 36 AI & Society 59, 61.

[4] *See* iResearch, 'Research Report on the Development of AI+ Finance Industry in China in 2022' (2022), https://www.iresearch.com.cn/Detail/report?id=4101&isfree=0. The market size of AI-powered financial services is anticipated to reach 66 billion CNY for core products and 1562 billion CNY for related industries in 2026. The core products refer to products that include technologies such as computer vision, speech recognition machine learning, knowledge graph, natural language processing, and other core technologies of AI. Related industries refer to the procurement of relevant software and hardware products that are associated with achieving the objective of AI application.

[5] OECD, *OECD Business and Finance Outlook 2021: AI in Business and Finance* (OECD 2021) https://www.oecd-ilibrary.org/finance-and-investment/oecd-business-and-finance-outlook-2021_ba682899-en.

[6] Xin Zhang and Qi Gao, 'Types of Risks and Regulatory Measures Pertaining to the Application of Artificial Intelligence in Finance' (2022) 6 China Banking 67, 67.

[7] Ostmann and Dorobantu (n 1) 21.

risks arises from societies even without the innovation of AI technology. These risks could be named *inherent risks from societies*.[8] The complexities of AI systems could further entrench the risks that are not restricted to specific industries, such as fairness, privacy, freedom of expression, competition, etc. The final category entails those *risks from specific domains*, which are unique to one sector in which AI is applied. For instance, the usage of similar AI strategies could arguably exacerbate the risks of procyclicality.[9] Responsible AI in the financial sector also pays attention to consumer protection, aiming to prevent financial losses caused by the mismatch between products and customer needs.[10]

These categories are neither exhaustive nor fully delineated. Some challenges brought about by AI could fall into multiple categories. Nevertheless, this classification could provide a lens through which we could zoom in on how legislative developments respond to AI-related challenges and explore the promises and uncertainties that are involved.[11]

1. Legislative Trends in AI in China's Financial Sector

To address these risks, China is dedicated to a three-step development of AI governance framework according to the AIDP.[12] The *FinTech Development Plan (2019-2022)* also set up the objective of stipulating clear and comprehensive regulations including both universal standards and targeted requirements. Since then, a burgeoning field of regulations at various levels has arisen within both the technology and financial sectors.

This work intends to provide an overview of the expanding field of legislation since 2017. It could be observed that the year 2021 may possibly mark the beginning of the expansion of the AI governance landscape. Before 2021, AI in financial services is predominantly regulated under the existing legislative framework of finances. A few domain-specific rules

[8] Zhang and Gao (n 6) 67–68.

[9] Ekaterina Svetlova, 'AI Ethics and Systemic Risks in Finance' (2022) 2 AI and Ethics 713.

[10] Ostmann and Dorobantu (n 1) 38.

[11] It is worth noting that it is beyond the scope of this short summary to completely examine the enforcement in AI-powered financial services. This work will primarily focus on responses to AI challenges in the financial sector from legislations.

[12] As per the AIDP, initial ethical norms, policies and regulations should have been created in some areas of AI by 2020. By 2025, China expects to initially establish laws, regulations, ethical norms, and policy systems related to AI. Further upgrades and a comprehensive system of these levels of regulations are intended to be completed by 2030.

clarified the requirements of using AI in specific financial services, such as robo-adviser and online loaning by commercial banks.[13]

Since 2021, multiple landmark legislations have been promulgated as part of the efforts to strengthen general AI governance. Having regard to the *infrastructure level* which provides the foundational elements of developing AI, China's data governance regime has gradually come into shape.[14]

On the level of *AI technologies and application*, a series of horizontal legislations (or drafts) which applies to all sectors has been gradually promulgated since 2021, in accordance with several core areas of AI technologies, such as algorithmic recommendations services,[15] deep synthesis services,[16] and generative AI services (for public consultation).[17] These departmental rules are designed to substantiate service providers' accountability over algorithms. For example, the *Internet Information Services Algorithmic Recommendation Management Provisions* ('IISARMP') confirms that algorithmic recommendation service providers shall fulfil their primary responsibility of ensuring algorithmic security, technology ethics review, information security, and lawfulness by regularly examining and verifying algorithmic mechanisms, models, data, and applications.[18] Individual rights and special protection for specific groups are also reiterated.[19] In soft law, it is worth noting that ethical

[13] In light of robo-advisers, for instance, as per the 2018 *Guiding Opinions on Regulating the Asset Management Business of Financial Institutions* ('*Guiding Opinions on Asset Management*'), Paragraph 23 connects to the general duties of asset management, including the suitability obligations and information disclosure, while also calling for more stringent requirements of transparency, internal monitoring, and accountability due to the deployment of AI. The *Interim Measures for the Administration of Internet Loans of Commercial Banks* (2020) Article 22 also mandates commercial banks to integrate human intervention into the automatic approval of risk models that are used for loaning.

[14] Both the *Personal Information Protection Law* and the *Data Security Law* have been enacted in 2021. Regulatory systems of data protection and utilisation that are neutral and specific to finances have both been initially formulated through both hard and soft law. For example, within the financial sector, the Banking and Insurance Regulatory Commission issued *Guidelines on Data Governance for Banking Financial Institutions* (hard law) in 2018 and the People's Bank of China issued the *Personal Financial Information Protection Technical Specification* (soft law) in 2020.

[15] *Internet Information Service Algorithmic Recommendation Management Provisions* (promulgated on 16 November 2021, took effect from 1 March 2022)

[16] *Provisions on the Administration of Deep Synthesis of Internet-based Information Services* (promulgated on 3 November 2022, took effect from 10 January 2023).

[17] *Public Comments Requested on Administrative Measures for Generative AI Services* (released on 11 April 2023).

[18] According to the IISARMP Article 2, the use of algorithmic recommendation technology as mentioned in the previous Paragraph refers to the use of generative or synthetic type, personalised recommendation type, ranking and selection type, search filter type, dispatching and decision-making type, and other such algorithmic technologies to provide information to users. The scope of application is relatively broad and may cover some AI-powered financial services that are related to information recommendation.

[19] In the IISARM, individuals who might be affected by the algorithm recommendation services have the right to be informed (Art 16), right to opt-out of customisation based on individual characteristics (Art 17), right to delete personal characteristics in recommendation (Art 17), access to portal for complaints (Art 22). Specific groups include minors, elders, workers, and consumers.

principles of AI governance have been elaborated.[20] Arguably, due to the broad scope of application, general AI regulations in China may have the potential to provide certain safeguards against AI-related risks in financial services if the AI technologies fall within the scope of respective legislations.

In the financial sector, soft law measures, such as industry standards, have been particularly developed. Some glimmers are shown in the *Evaluation Specification of Artificial Intelligence Algorithm in Financial Application* (JR/T 0221-2021) which provides for a unified framework of pre-emptive measures to integrate four core aspects of responsible AI—safety, explainability, accuracy, and performance (robustness) into the whole lifecycle of preparing, building, and applying AI models.

2. Legislative Responses to Certain AI-Related Risks and Areas of Concern

As illustrated above, this work intends to examine how the current multi-level regulatory framework responds to three types of AI-related risks by using examples of risks in each category.

Among the endogenous risks from AI technologies, extended AI supply chains could exacerbate the complexities of governance. The development of AI systems may rely on off-the-shelf tools, pre-existing models, or software that were developed externally and not specifically for the purpose of financial services.[21] However, the present regulations in the financial sector (e.g., the *Guiding Opinions of Asset Management* paragraph 23) concentrate on financial institutions, who usually play the role of deployers of AI when there are third-party developers.[22] This may not necessarily give clear guidance on how multiple players in the AI supply chain could detect and mitigate risks proactively and pre-emptively. The excessive reliance on deployers is also reflected in the general AI rules, like the IISARMP.[23] In this regard, it remains to be seen how the *Evaluation Specification of Artificial Intelligence Algorithm in Financial Application* could be implemented to give clearer instructions for

[20] *See* the *Opinions on Strengthening Governance over Ethics in Science and Technology* (2022) and the *Ethical Norms for New Generation Artificial Intelligence* (2021). Some principles include advancing human welfare, promoting fairness and justice, protecting of privacy and security, assuring controllability and worthiness, and strengthening accountability.

[21] Ostmann and Dorobantu (n 1) 23.

[22] For example, regarding issues of robo-advisers, financial institutions can either develop robo-adviser software themselves or purchase such from third-party technology companies. In general, they play the role of deploying AI systems in financial services.

[23] IISARMP Article 2 states that the regulation applies to those who use algorithm recommendation technology to provide internet information services.

promoting responsible AI at different stages, combining concrete and unique requirements from different financial services.[24]

Moving to inherent risks from societies, bias, in reality, may creep into each domain of AI application. AI in insurance and credit lending may make worries of inequality more prominent if an individual's risks profile cannot be precisely established.[25] Though the principle of fairness has been stressed in the multi-layered legislative framework of AI governance,[26] there may still be some uncertainties during implementation that are worth further addressing. From the outset, the provisions related to non-discrimination are too general without providing clearer definitions of discrimination and legal standards for direct or indirect discrimination.[27] The absence of comprehensive non-discrimination rules would further impede the promotion of fairness in AI-powered financial services. Moreover, as a principle, fairness could have been listed as a dimension distinguished from security, robustness, and privacy, and fully elaborated in industry standards such as the *Evaluation Specification of Artificial Intelligence Algorithm in Financial Application*. Both aspects need to be facilitated by legislators, regulators, the industry, and public participation.

Domain-specific risks in the financial sector would be another source of AI-related challenges. Supervision over AI needs to strike a balance between redressing macro-prudential supervision and financial consumer protection.[28] Taking the provisions of transparency related to AI as an example, it remains unclear whether this balance has been successfully struck. When providing services like robo-advisers, financial institutions are mandated to report the main parameters of AI models and the main logic of asset allocation to the regulators in order to strengthen supervision.[29] However, the main logic of asset allocation need not be demonstrated to consumers. The inherent weaknesses of AI algorithms and the risks of using AI in financial services, which should be mandatorily disclosed, are not further explained. The

[24] Insights could also be borrowed from *the Provisions on the Administration of Deep Synthesis of Internet-Based Information Services* and the *Administrative Measures for Generative AI services (Draft)* which incorporate entities who develop or provide technical support to AI services within the scope of application.

[25] Lin Lin and Christopher C Chen, 'The Promise and Perils of InsurTech' (2020) Singapore Journal of Legal Studies 115, 125.

[26] In the context of AI governance, the principle of fairness has been cited non-exhaustively in the Personal Information Protection Law Article 24, IISARMP Article 21, *Ethical Norms for New Generation Artificial Intelligence* Article 13, etc. Discrimination has also been prohibited according to *Law on the Protection of Women's Rights and Interests*, the *Law on Protection of Disabled Persons*, the *Labour Law*, the *Employment Promotion Law*, etc.

[27] Bin Wang, 'China's Anti-Discrimination Law Legislation: Difficulties and Future' in Xiaonan Liu and Liwan Wang (eds), *Equality and Anti-Discrimination* (Brill 2021) 88 https://brill.com/view/book/edcoll/9789004421011/BP000004.xml.

[28] *See* Hui Huang 'The Logics and Path of China's Financial Regulatory Structure Reform: International Experiences and Local Choice' The Jurist (2019) 124. It is suggested that if AI algorithms start following similar strategies in lending for banks or in robo-advisers for consumers, markets may be overheated in the upturn and undervalued in the downturn and face more risks of instability.

[29] *See* the *Guiding Opinions on Asset Management* Paragraph 23.

gap between the information reported to regulators and to the public also exists in general AI rules. As per the IISARMP Article 24, a service provider[30] with public opinion properties and social mobilisation capacity shall report to regulators a wide range of information through the Internet Information Services Algorithm Filing System,[31] while the information demonstrated to the public through the filing system is relatively restricted.[32] How precisely these types of information should be disclosed is completely subject to the discretion of algorithm service providers. It should be noted that reducing information asymmetry between deployers of AI and consumers, and between regulators and consumers, could have paramount implications for individuals, and also be beneficial in promoting polycentric governance by enhancing public oversight and leveraging the efficiency of supervision.

3. Conclusion

AI governance in China’s financial sector has gradually transformed from legislative plans to multi-layered concrete rules in both hard and soft law, general AI regulations, and specific provisions in the financial sector that could complement each other. The current legislative framework represents a clear step forward to the objective set up by the AIDP to initially establish a legal system of AI by 2025. It is, however, also a point of departure for us to devote more efforts to examining how distinct AI-related risks and challenges arise and could be redressed, in order to ultimately formulate a coherent, efficient, and holistic regulatory framework in the AI-powered financial sector, which is envisioned to be established by 2030.

[30] If providers of AI-related financial services use the information recommendation technologies that fall within the scope of IISARMP, they will also be subject to the IISARMP.

[31] According to the *User Manual for Internet Information Service Algorithm Filing System* (2022), the information that needs to be disclosed to the system includes but is not restricted to (1) basic properties of algorithms: categories, name, algorithm security self-assessment report; (2) detailed properties of algorithms: data that is used; intended purposes; methods of demonstration; (3) algorithm data: including biometric characteristics or not; including personal identification or not; (4) algorithm models: sources of training data; description of open-source training datasets; self-made datasets and sources. *See* Cyberspace Administration of China, ‘Internet Information Service Algorithm Filing System’, https://beian.cac.gov.cn/#/index.

[32] According to the IISARM Article 16, individuals could be informed about the basic principles, the purpose and intention, and the main operation mechanisms, etc. of their algorithmic recommendation services.

VII. Financial Regulation and the Advent of Digital Reporting: The End of Rule-Use as We Know It?

Dr Andromachi Georgosouli
(Queen Mary University of London)

The UK and other countries around the world are shifting to a new digital economy. This shift is powered by big data, advanced analytics and artificial intelligence (AI) and goes hand-in-hand with fundamental changes in the design of the legal framework that supports the regulation of economic activity. As technology penetrates the sphere of regulation, it transforms how regulators gather information, how they monitor compliance, and how they impose sanctions. Furthermore, it gradually changes how regulators draft rules and how they use them in their interaction with the regulated industry. The impact of technology on the use of rules as instruments of social organisation and control has received growing attention in recent legal scholarship. [1] The intersection of artificial intelligence, technology and the law in financial markets has also been researched extensively.[2] The implications of re-writing reporting requirements into code to enable machine-readability and machine-executability and, in particular, the merits of a system of data-driven financial governance with little or no reliance on human interpretation has escaped systematic examination. This presentation summary seeks to address this gap in the literature making special reference to the digitalisation of reporting requirements that is currently in progress around the globe. It provides a more balanced assessment of what digital regulatory reporting can actually do for us and of the minimum requirements for its effectiveness.

Regulatory technology (Regtech) has a huge potential but also comes with risks, which we do not fully understand at present. To be sure, the future ahead of us need not be dystopian. However, we need to refrain from the naïve view of a problem-free data-driven future in which machines will take care of everything. The digitalisation of reporting requirements in the field of financial regulation is an exemplary case in point. The chief purpose of reporting requirements is to increase transparency, promote market discipline and help financial regulators detect and respond to emerging risks. However, the existing reporting processes are

[1] *See notably* Aaron Wright and Primavera De Filippi, 'Decentralized Blockchain Technology and the Rise of *Lex Cryptographia'* (2015) SSRN preprint, https://ssrn.com/abstract=2580664; Anthony J Casey and Anthony Niblett, 'The Death of Rules and Standards' (2017) 92(4) Indiana Law Journal 1401.

[2] The scholarship focuses primarily on Financial Technology (FinTech), technology governance, and competition law issues associated with sandboxes for FinTech experimentation. *See* Eva Micheler and Anna Whaley, 'Regulatory Technology: Replacing law with computer code' (2020) 21(2) European Business Organisation Law Review 349; Saule T Omarova, 'Technology v. Technocracy: Fintech as a Regulatory Challenge' (2020) 6 Journal of Financial Regulation 75; Rory Van Loo, 'Making Innovation More Competitive: The Case of Fintech' (2018) 65 UCLA Law Review 232; in parallel to this literature, a more theoretical discourse examines the advent of algorithmic regulation, and the impact of technology on legal concepts and doctrines. *See* Roger Brownsword, Eloise Scotford and Karen Yeung (eds), *The Oxford Handbook of Law, Regulation and Technology* (OUP 2017); Martin Lodge and Karen Yeung (eds), *Algorithmic Regulation* (OUP 2019); and Mireille Hildebrandt, 'Law as information in the era of data-driven agency' (2016) 79(1) MLR 1.

complex, time consuming and expensive for the financial industry. At the same time, delays in reporting and data of poor quality often compromises the effectiveness of financial regulators and their overall responsiveness to risks in the delivery of their mandate. These concerns have become powerful drivers of a series of Digital Regulatory Reporting ('DRR') initiatives. From the side of the financial industry, the International Swaps and Derivatives Association (ISDA) is a leading champion of digitalisation and is currently running an industry-wide DRR initiative for the trade reporting requirements under the European Market Infrastructure Regulation (EMIR) as well as the reporting requirements of the US Commodity Futures Trading Commission (CFTC). Financial regulators around the world have also launched a series of DRR initiatives. For example, in the UK, there are pilots and projects run by the Financial Conduct Authority (FCA) and the Bank of England in collaboration with leading members of the industry. In the EU, there are similar initiatives run by the European Commission and by the European Supervisory Authorities (ESAs). There is also a variety of international projects. Notable examples include, the G-20 TechSprint initiative and the Bank for International Settlements (BIS) Innovation Hub's Project Ellipse.

DRR is a machine-readable and machine-executable system of automatic reporting, and it is a conspicuous case of innovation in the field of Regtech. If fully developed and successfully implemented, it will enable the industry to interpret and implement reporting rules consistently via a common machine-readable code thanks to -inter alia- a standardized data model. The DRR will cut the time and cost of data reporting and processing, and will reduce mistakes, ambiguities and inconsistencies. At the same time, DRR is set to improve the monitoring and oversight capabilities of financial regulators. Specifically, it is anticipated that, thanks to digitalisation and further technological advancements, financial regulators will be able to access a larger pool of data and, as a result, to make more accurate predictions. They will be better able to detect emerging risks and intervene earlier and in a more targeted fashion. Financial regulators will also be able to pull data themselves instead of requiring members of the industry to submit data, hence, obviating the need for extra oversight.[3]

Despite the fact that the digitalisation of reporting requirements is currently at the stage of experimentation, there are plans to expand digitalisation beyond reporting. DRR enthusiasts claim that the digitalisation project will revolutionise how we use rules, with some of them going as far as to argue for a future of rule-use without humans, as everything—from the engineering of code-based micro-directives to the execution of those micro-directives for compliance purposes—will be machine-driven. There is no doubt that there are benefits to be

[3] On the distinction between the "push" and the "pull" model of reporting, see Bank of England, 'Transforming Data Collection from the UK Financial Sector' (Discussion Paper, January 2020) 42–5, www.bankofengland.co.uk/-/media/boe/files/paper/2020/transforming-data-collection-from-the-uk-financial-sector.pdf?la=en&hash=6E6132B4F7AF681CCB425B0171B4CF43D82E7779.

gained from digitalisation; however, the view that DRR will dramatically change how we use rules as we know it is not entirely persuasive.

I provide three arguments to support my thesis.[4] The first draws attention to the limited translatability of regulatory content into code. To make rules machine-executable, one must make them machine-readable. Machines deal in black and white. As a result, it is necessary to use unambiguous language to facilitate machine-readability and machine-executability, but here lies a problem: While coding is possible, there is an increased risk of loss of meaning. Most probably, it is not too difficult to turn highly technical standards into their digital equivalent compared to vague regulatory stipulations (e.g., the requirement to treat customers fairly). However, even technical standards come with a marginal degree of ambiguity. Furthermore, they need to be read in conjunction with more open-ended rules in order to apply correctly. The second argument concerns the limited capabilities of machines in making determinations (e.g., with regard to what sort of data needs to be reported) given the existing and foreseeable development of the relevant technology. Machines can retrieve factual information, match past legal facts, enlist similarities and differences, rank data in terms of relevance, and use statistical modelling to output compliance scores in impressive speed. However, machines cannot engage in normative reasoning equally well especially when compared to humans. This is due to their constrained capacity to root their determinations on principled-judgments according to public criteria that are open to intelligible scrutiny and contestation. Finally, the third argument refers to an indispensable aspect of rule-use, namely, that of human interpretation, which is deliberative in nature and crucial for the legitimacy of financial regulation. Contrary to received wisdom, regulatory law is not there just for the sole purpose of communicating to regulatees what they may or may not do a predictable fashion. Over and above communicating stipulations, prescriptions and the regulators' expectations, regulatory law embeds interpretive processes of constructive deliberation whose function is to legitimise the regulator's highly consequential decisions. Undoubtedly, interpretation is a burdensome task. It is also true that humans err and that they often exhibit predictable and irrational behaviour. However, they remain moral agents capable of self-reflection, of holding each other accountable, and of taking responsibility for their acts and omissions.

To conclude, the digitalisation of reporting requirements will be beneficial if carefully designed, but it will not dramatically change how we use rules. Even though any projection about the future is bound to be an imprecise science, there are reasons to believe that digital reporting will most likely become an extension of the existing regulatory practice.[5] From this,

[4] For a more detailed discussion see Andromachi Georgosouli, 'Metarules, judgment and the algorithmic future of financial regulation in the UK' (winter 2023) *Oxford Journal of Legal Studies* (forthcoming).

[5] Martin Lodge and Andrea Mennicken, 'Reflecting on Public Service Regulation by Algorithm' in Martin Lodge and Karen Yeung (eds), *Algorithmic Regulation* (OUP 2019) 178, 180.

it follows that the real challenge is not how to move to a system of data-driven governance with little or no reliance on human interpretation—but how to design rulebooks which will help their human users take advantage of their own general intelligence, and of the specialist intelligence of machines.[6]

[6] On the distinction between "specialist" and "general" intelligence see Margaret Boden, *Artificial Intelligence, A Very Short Introduction* (OUP 2018) 18.

VIII. Challenges Posed by the Second Generation of Digital Technologies to Financial Regulatory Strategies

Dr Teresa Rodríguez de las Heras Ballell
(Universidad Carlos III de Madrid)

1. Introduction: The Context

The financial sector, traditionally receptive and permeable to technological advances, is not oblivious to the extraordinary opportunities provided by the second generation of digital technologies (AI, platforms, DLT, big data, augmented and immersive reality, IoT). There is increasing penetration of digital technologies in financial markets, in adoption rates[1] among users, expanding presence of fintech firms,[2] and the growing use of fintech solutions[3] by incumbents.[4] The increasingly popular term "Fintech" captures the accelerated transformation of contemporary financial markets driven and enabled by technology, and encapsulates its multifarious potential impact on services, market structures, and business models.[5]

[1] *See* EY, 'EY Fintech Adoption Index 2017, The Rapid Emergence of Fintech' (2017) 5-7 and 12, https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/banking-and-capital-markets/ey-fintech-adoption-index-2017.pdf, showing a global fintech adoption of 33 percent compared to the 16 percent rate in 2015; the adoption increases up to 46 percent across five emerging markets (Brazil, China, India, Mexico and South Africa), whereas the adoption rates are disparate in European countries. Among the twenty countries studied, the highest percentage in a European country corresponds to the United Kingdom with 42 percent, followed by Spain with 37 percent. Other European countries surveyed, except Germany, are at or below the threshold of 30 percent. The report pivots on a definition of fintech that includes not only early-stage start-ups and new entrants, but also scale-ups, maturing firms and even non-financial services firms).

[22] *See* A Fraile Carmona et al., *Competition issues in the Area of Financial Technology (FinTech)* (2018) Policy Dep't for Econ., Sci. and Quality of Life Policies, European Parliament, 32, https://www.europarl.europa.eu/RegData/etudes/IDAN/2019/631061/IPOL_IDA(2019)631061_EN.pdf, illustrating the size of the fintech market in number of fintech-labelled technologies, according to the Crunchbase database that provides 4,359 companies in 2018 classified as fintech. The authors refine the overall number of fintech-labelled companies, adjusting the figure to 3,852. Upon the adjustment, the report identifies that the European Union contributes to the global fintech sector with 1,020 fintech companies.

[3] Fintech is not only describing an ecosystem of innovative startups invading the financial markets with groundbreaking technological solutions to revolutionise the delivery of financial services; it also comprises incumbent firms that adopt advanced technological strategies to effectively compete and innovate. Bernardo Nicoletti, *The Future of Fintech: Integrating Finance and Technology in Financial Services* (Springer 2017) 13.

[4] Traditional commercial banks indicated increasing adoption of machine learning techniques to increase efficiency. Institute of International Finance, 'Machine Learning in Credit Risk', August 2019, 2nd Edition Summary Report, 2, https://www.iif.com/Portals/0/Files/content/Research/iif_mlcr_2nd_8_15_19.pdf. That strategy would provide signs that incumbents are reacting to fintech challenges by the implementation of technology-driven solutions. *Ibid.* In addition, PwC's 2018 Digital Banking Consumer Survey does also stress the need for traditional banks to reconsider how they sell and provide their services and how they interact with their customers. *See* PwC Financial Services, PwC's 2018 Digital Banking Consumer Survey: Mobile users set the agenda (2018), https://www.pwc.com/il/he/bankim/assets/2018/PwC%202018%20Digital%20Banking%20Consumer%20Survey.pdf. The incorporation of digital technologies—namely, as highlighted by the report, mobile-based services and products—is crucial.

[5] *See generally* Capgemini et al., 'World FinTech Report 2018' (2018), https://www.capgemini.com/wp-content/uploads/2018/02/world-fintech-report-wftr-2018.pdf (spotting and describing the potential impact of emerging technologies in the provision of customer-oriented financial services—artificial intelligences, data analytics, robotics, distributed ledger technologies, biometrics, platforms, internet of things and sensors, augmented reality, chatbots, etc.).

Fintech is not, indeed, a single, global phenomenon. It comprises a vast complexity of multifaceted, evolving groups of solutions, applications, and uses based on technology-intensive strategies. Consequently, the expansive use of digital technologies crosscuts the entire financial market and impacts the structure of the market, the market actors, the provision of services, the type of products, and the relationships with the clients and the supervising authorities. Such a transversality of fintech effects reveals the severity and the extent of the impact on financial regulatory strategies and supervision models.

To assess the adequacy of regulation and devise a fit-for-purpose regulatory response, a multi-layered regulatory strategy is proposed in this presentation summary (at Part 2). Financial digital innovation (fintech) is stratified in three layers: the structural layer, the material layer, and the personal layer—each of which identifies and analyses the impact of digital innovation on a financial-market dimension. Thus, this paper devises and develops a multi-layered regulatory response to face fintech challenges.

2. The Layers of Financial Digital Innovation Theory

The "layers of digital financial innovation" theory is based on the idea that the impact of digital technology on financial markets penetrates all of its layers and thus, produces specific effects and poses singular challenges at each layer. Dismembering or disassembling the digital impact in different layers provides a better structured framework to classify new models, new products or services, and new operators, identify and assess the resultant risks, where they arise, and detect which traditional components of the regulatory and supervisory schemes could more likely be affected.

Structural layer: architecture, structures and models

The first visible impact of digital technology is on financial market architecture: particularly, market structure and business models. The architecture of financial markets is being reshaped under new structures. It is therefore described as the structural layer of the fintech challenge.

Digital innovation has contributed to the development of two structural models in the market, which interestingly reflect two diametrically opposed architectures: platforms and distributed ledgers. On one hand, as the digital economy has transformed into a platform economy, platform-based models have populated the financial sector.[6] The expansion of

[6] The continuous growth of crowdfunding platforms and other alternative finance platforms illustrates this statement. *See e.g.*, The Cambridge Centre for Alternative Finance, 'Shifting Paradigms: The 4th European Alternative Finance Benchmarking Report' (2019), https://www.crowdfundinsider.com/wp-content/uploads/2019/04/CCAF-4th-european-alternative-finance-benchmarking-industry-report-shifting-paradigms-April-2019.pdf. According to this report, in 2017, the alternative finance volume from across Europe grew by 36 percent, while the Asia-Pacific region and the Americas experienced a 4-year average annual growth rate of 145 percent

crowdfunding, aggregators, multilateral trading systems, and other sharing-inspired financial models—including social trading and copy trading—has been substantially facilitated and accelerated by platform models.[7] Platforms offer self-regulated, multilateral, centralised, and trustworthy models for the provision of financial services.[8] On the other hand, platforms concurrently coexist and compete with decentralised schemes operating on distributed ledger technologies (DLT). Unlike platforms, the use of DLT relies on decentralised schemes, distributed trust, and peer-to-peer (P2P) operations.[9]

The structural layer has a two-fold impact on regulatory strategies and practices.

First, it dilutes the classical distinction between markets and financial service providers, insofar as the use (primarily) of platforms to provide financial services assimilates its structure and operation to genuine markets.[10] As the boundaries among markets (exchanges and exchange-like models), traditional financial intermediaries, and new services providers are blurring, the classical regulatory and supervisory schemes seem unsuited, or at least too simplified, to embrace hybrid models. The emergence and flourishing of Multilateral Trading Facilities represents an illustrative example of how these firm-market figures require a hybrid regulatory approach.[11] Despite the value of this suitable precedent, the contemporary

and 89 percent respectively. *Ibid* 22–23. In numbers of operating crowdfunding platforms, as per the data provided by Massolution, in 2014 the threshold of 1,250 platforms active in the world had been reached. Massolution, 'The Crowdfunding Industry Report' (2015) 2015CF 82, https://www.smv.gob.pe/Biblioteca/temp/catalogacion/C8789.pdf. Without specifying which fintech are based on platforms, Deloitte also reports growing data in fintech. *See* Deloitte, 'Fintech by the Numbers: Incumbents, Startups, Investors Adapt to Maturing Ecosystem' (2017) 7, https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-dcfs-fintech-by-the-numbers-web.pdf.

[7] *See generally* Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Online Platforms and the Digital Single Market Opportunities and Challenges for Europe (25 May 2016) COM (2016) 288 final, 2, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1590005545023&uri=CELEX:52016DC0288.

[8] Teresa Rodríguez de las Heras Ballell, *The Legal Anatomy of Electronic Platforms: A Prior Study to Assess the Need of a Law of Platforms in the EU*, 3 ITALIAN L.J. 149 (2017); *see generally* Teresa Rodríguez de las Heras Ballell, *El régimen jurídico de los Mercados Electrónicos Cerrados (e-marketplaces)* [The Juridical Regime of the Closed Electronic Markets (E-Marketplaces)] (2006) 56–58, 210–29, describing platforms as closed, self-regulated environments and explaining the functions and role of platform operators as regulators, supervisors, and trust-generators.

[9] Distinctive features of DLT-based schemes are based on the structural and operational characteristics of distributed ledger technologies as explained by scholars and experts Aaron Wright and Primavera De Filippi in *Decentralized Blockchain Technology and the Rise of Lex Cryptographia* (2015), SSRN preprint, https://ssrn.com/abstract=2580664.

[10] Ruben Lee, *What is an Exchange? The Automation, Management, and Regulation of Financial Markets* (Oxford University Press 1998) 117–39, defining and describing trading platforms as alternative trading systems to traditional exchanges.

[11] Jan De Bel, 'Automated Trading Systems and the Concept of an "Exchange" in an International Context. Proprietary Systems: A Regulatory Headache!' (1993) 14 U. PA. J. INT'L BUS. L. 169, 208; Jonathan R Macey and Maureen O'Hara, Regulating Exchanges and Alternative Trading Systems: A Law and Economics Perspective (1999) 28 J. LEGAL STUD. 17.

multiplication of hybrid models[12] and their proliferation in the fintech sector invite dynamic solutions to deal with architectural transformation on a large scale. In the context of a digital economy that has evolved into a platform economy, market-like models compete with traditional exchanges,[13] platform operators act as new intermediaries, and platforms serve as support for the provision of new services and the running of innovative business activities (e.g., aggregators, social trading, copy trading, and trading platforms).

Second, these new structures do not fit into the current regulatory framework, as they relocate the regulation/supervision focus. Under platform models, new players come to the financial fore: platform operators. As platform operators are not—in some business models—direct providers of financial services, but mere enablers for platform users to interact and carry out financial-like activities, it is reasonable to wonder how the financial market regulations should address platform operators. Are platform operators new financial intermediaries or instead, simply intermediary service providers (digital intermediaries) facilitating the delivery of financial services? The regulatory response to crowdfunding platforms, for instance, illustrates a genuine financial-operator-based regulatory strategy. However, other platforms (such as social trading, aggregators, and copy trading) have not attracted the same regulatory attention and might not deserve an equivalent response.

Contrarily, DLT-based models pose a completely different challenge to regulators. These models operate on a decentralised and disintermediated basis. In the absence of an identifiable central operator, the traditional operator-based regulatory strategy does not work. Although the ecosystem of DLT-based models comprises a variety of variants—from permissioned to permissionless—the regulator faces the question of how to regulate a decentralised structure

Material layer: services, products and instruments

The second angle of digital impact is on the nature and attributes of financial products and services and, therefore, on the perimeters of financial activity. The activity layer represents the second layer of the fintech challenge.

Technology applications to products and services can transform the characteristics of financial activities and enable the configuration of new products and services. Accordingly, the applicable legal regime might need to be reconsidered to some extent.

Several examples may serve as illustrations:

[12] Thomas W Malone, 'Modeling Coordination in Organizations and Markets' (1987) 33 MGMT. SCI. 1317; Thomas W Malone et al., 'Electronic Mkt. and Electronic Hierarchies' (1987) 30 COMM. OF THE ACM 484.

[13] *See generally* Martin Bichler, *The Future of e-Markets. Multidimensional Market Mechanisms* (Cambridge University Press 2001).

First, the application of artificial intelligence (AI) throughout the value chain (front-office, middle-office, and back-office)[14] and along the entire array of financial services. Among them, robo-advisers provide customised, low-cost, highly efficient algorithm-driven financial advice. Considering their level of automation, can robo-advisers be legally treated as human financial advisers? Can liability rules and regulatory requirements be applied to robo-advice, or exclusively to the development of the software and the establishment of the pre-conditions of the programme? Thus, robo-advisers represent another expression of fintech that might require regulatory attention. On one hand, the advent of robo-advisers entails the emergence of new actors in the financial markets. Robo-advising solutions can be provided by fintech start-ups, technological companies, or traditional financial institutions. In the two former cases, it implies the irruption of new actors competing with incumbents (fintech companies and bigtech firms). On the other hand, the automation of financial advice also poses a conceptual challenge. The existing rules for human-centric financial advice have to be applied to an algorithm-driven system. To a certain extent, that implies a shift of the regulatory focus from a human activity to an automated process. In fact, the spotlight changes from behavioural aspects of human conduct to the design and the operation of an algorithm-driven system.

Second, P2P payments enable the completion of payments between users. The decentralised network enables users to complete payments. Should payment services rules be applied there? And if so, to whom?

Third, if insurance companies incorporate big data to foresee the likelihood of the covered risks, and adjust the insurance fees accordingly ("dynamic insurance"), would the duty to notify a change in risk be relevant?

Finally, as a result of a burgeoning trend towards the tokenisation of assets, values, and services, the market is receiving digital assets and customised tokens with an uncertain and intricate legal characterisation. In conjunction with DLT, tokenisation unleashes opportunities for asset management, fund raising, investing, and other financial services.

These examples reveal that the technological impact on the activity layer may affect four groups of attributes of products, services, and activities in the financial markets. Insofar as algorithm-driven solutions enable highly automated tasks and processes and increasingly autonomous decision-making, technology impacts the procedural attributes of the activity, infusing celerity, automation, and autonomy. The facilitation of P2P schemes for the provision of financial—or quasi-financial—services represents the impact on structural attributes. A

[14] Chatbots, virtual assistants, credit scoring, KYC/AML applications or smart contracts exemplify varied possibilities for the use of AI in all financial sectors. Ana Fernández, *Inteligencia Artificial en los Servicios Financieros* (29 March 2019) Boletín Económico 2/2019, 3–4. These prospective applications show today different levels of maturity in the market. *Ibid*, *Diagram* 1, 3.

widespread use of big data along the successive stages of the activity process affects the attributes related to the magnitude, scale, and scope of the activity.[15] Interestingly, such a scale shift is not a mere incremental change, but a radical transformation likely to redefine the information asymmetries and reshape the traditional schemes to allocate duties and liabilities.

Finally, the possibilities and the extent of tokenisation touch the very core of the legal categorisation of financial instruments by challenging the current demarcation for financial supervision and regulation.

Personal layer: From disintermediation to reintermediation

Digital technology has not only reconfigured the profile of incumbents, but has also triggered the emergence of new players competing with incumbents. Fintech has then put in motion a cycle of disintermediation and reintermediation.[16] The entry of crowdfunding platforms in the credit market, the emergence of aggregators and comparators in the insurance and the banking sector, or the increasing competition of bigtech companies providing techfin solutions in payments are some examples of the transformation of the financial intermediation arena. These examples reveal a circular process of removing intermediaries in certain areas, followed by the emergence of new intermediaries in others.

New market players have become protagonists with the proliferation of platform models. Platform operators are not necessarily financial intermediaries or financial service providers, who can indeed become platform users. In particular, sharing-based platform models have raised concerns about the genuine role of platform operators and consequently, the applicable legal regime. The recent Court of Justice decisions on the Uber Spain Case[17] in 2017, the Uber France Case[18] in 2018, and, lately, the Airbnb Ireland Case[19] in 2019 have contributed with a case study to the debate.[20] Likewise, burgeoning fintech models give rise to new players: aggregators, comparators, robo-advisers, and recommenders.

[15] According to the European Commission Communication, the term "big data" refers to "large amounts of different types of data produced with high velocity from a high number of various types of sources," whose processing requires new tools and methods, such as powerful processors, software and algorithms. Hence, the disruptive character of big data pivots on three "Vs": velocity, volume, and variety. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Towards a Thriving Data-Driven Economy* (2 July 2014) COM (2014) 442 final, 4, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1590006916232&uri=CELEX:52014DC0442.

[16] *See* Shaun French and Andrew Leyshon, 'The New, New Financial System? Towards a Conceptualization of Financial Reintermediation' (2004) 11(2) Rev. of Int'l Political Econ. 263.

[17] *See generally* Case C-434/15, Asociación Profesional Elite Taxi v. Uber Systems Spain SL, 2017 E.C.R. 981.

[18] Case C-320/16, Uber France SAS v. Nalib Bensalem, 2018 E.C.R. 221.

[19] Case C-390/18, Airbnb Ireland, 2019 E.C.R. 1112.

[20] In the three cases described above, the European Court of Justice has been asked about the role of platform operators—Airbnb and Uber—in the rental industry and the urban transport sector, respectively. The Court held that Uber is not a mere digital intermediary-information society services provider. Rather, Uber operates as a genuine transport service provider, insofar as it exercises certain control over the quality of the service, the drivers,

Thus, the “layers of digital financial innovation” theory has been formulated in an attempt to understand the true impact of this disruption on financial regulation and to dissect its implications. In accordance with this original theory, this paper explains how challenges are located on three layers of financial markets: structures and architectures; market players; and products, services and activities.

The observation of each layer reveals diverse consequences of the fintech impact and announces different challenges. The “layers of digital financial innovation” theory aspires to serve as a theoretical and analytical framework to understand prospective technological advances and to ensure that regulation is well-equipped to face future challenges.

and the cars. The Court also held that by determining the maximum fare, Uber exerts decisive influence over the conditions under which drivers provide their services. Accordingly, Uber is not subjected to the legal regime applicable to intermediary service providers, but instead, to the regime applicable to transport service providers. However, the Court held under the same analysis that Airbnb has neither control nor decisive influence on the rental transactions conducted between the users within its platform. Consequently, Airbnb is not treated as a real estate agent, but as a mere digital intermediary instead. The diverse legal treatment entails different legal obligations as well as liability regimes.

IX. AI in Credit Lending and Enforcement Decision-Making by Banks: Accuracy, Risk, Data and Consumer Protection

Dr Jeannie Marie Paterson
(University of Melbourne)

1. Overview

Artificial intelligence (AI) offers opportunities for improving efficiency, cost and inclusion in consumer credit, including in informing the credit scores and credit assessments that influence a lenders' decision to lend. Equally, standards for ethical, responsible, and trustworthy AI have a particularly important role to play in consumer credit transactions, which are characterised by an inequality of bargaining power and information asymmetries.[1] This presentation summary agrees with recommendations for greater transparency and accountability in the use of AI generally, and particularly in lending decisions. The paper also argues that the design of policy and regulation to address concerns about the risks of harm to consumers from the use of AI in making lending decisions should recognise the complexities of practice, technology and existing law in this field. Concerns about bias and financial inclusion in AI credit rating and assessment should be addressed with clarity in objectives and precision in proposed interventions. Moreover, the value of responsible lending, that is, lending in ways that do not cause undue financial hardship, should be recognised. This approach does not stifle innovation but rather, by promoting genuinely responsible AI, supports the trustworthiness of AI in consumer credit decision making.[2]

2. AI in Lending

Fintech and open banking initiatives

The growing capacity of the cluster of data-driven technologies commonly grouped under the title of AI, such as machine learning, neural networks, and natural language processing, is transforming established financial services. AI is being used in fraud detection, cybersecurity, marketing, and onboarding new clients.[3] New consumer-facing AI-informed services are also being made available, such as through chatbots for seamless consumer-lender interfaces, robo-advisers,[4] and personalised budgeting tools.[5] Governments have supported

[1] Jeannie Ma Paterson and Yvette Maker, 'Artificial Intelligence and Consumer Protection' in Ernest Lim and Phillip Morgan (eds), *The Cambridge Handbook of Private Law and Artificial Intelligence* (Cambridge University Press, 2023), http://dx.doi.org/10.2139/ssrn.3973179.

[2] See AI Singapore, https://aisingapore.org/.

[3] Bank of England and Financial Conduct Authority, 'Machine Learning in UK Financial Services' (Report, October 2019) 8.

[4] Jeannie M Paterson, 'Making robo-advisers careful? Duties of care in providing automated financial advice to consumers' (2023) Law and Financial Markets Review 1-18, doi:10.1080/17521440.2023.2196027.

[5] Jeannie M Paterson, Tim Miller, and Henrietta Lyons, 'Demystifying Consumer-Facing Fintech: Accountability for Automated Advice Tools' (April 11, 2023). Zofia Bednarz and Monika Zalnieriute (eds), *Money, Power and*

developments in financial AI to improve market competition and consumer wellbeing, including through open banking initiatives[6] and regulatory sandboxes.[7]

Big data and AI in lending to consumers

Accompanying these developments has been considerable interest in using the combination of big data and AI for lending decisions. AI in lending decisions, supported by open banking, is touted for its potential to provide more consistent, efficient and fine-grained assessments [8] and make credit available to a wider number of borrowers.[9] Concerns have also been raised about the risk of AI in credit scoring and assessments to give rise to inaccuracy and bias. These concerns have prompted statutory and soft law interventions. Notably, the proposed EU AI Act places the use of AI for making decisions about lending in the high-risk category of uses, which would be subject to robust requirements of transparency, testing and monitoring.[10] Other jurisdictions stress the need for AI used in decision-making for access to public and private goods to meet the demands of codes of AI ethics or responsible AI frameworks.[11] In the US, the Equal Credit Opportunity Act (regulation B) prohibits lenders from discriminating against borrowers on the basis of protected attributes, such as age, colour, religion, national origin, sex, marital status, or age, including in decisions made by algorithms.[12]

AI: From Automated Banks to Automated States (Cambridge University Press, 2023), https://ssrn.com/abstract=4414789.

[6] Douglas W Arner, Ross P Buckley, and Dirk A Zetzsche, 'Open Banking, Open Data and Open Finance: Lessons from the European Union' in Linda Jeng (ed), *Open Banking* (Oxford University Press 2021), Chapter 8, UNSW Law Research Paper No. 21-69, University of Hong Kong Faculty of Law Research Paper No. 2021/49, https://ssrn.com/abstract=3961235; Christoph Frei, 'Open Banking: Opportunities and Risks' (January 3, 2023) in Thomas Walker, Elaheh Nikbakht, and Maher Kooli (eds), *The Fintech Disruption: How Financial Innovation Is Transforming the Banking Industry* (Palgrave Macmillan 2023) 167–190, https://ssrn.com/abstract=4316760 or http://dx.doi.org/10.2139/ssrn.4316760

[7] Douglas W Arner et al., 'Sustainability, FinTech and Financial Inclusion' (2020) 21 European Business Organization Law Review 27, http://dx.doi.org/10.1007/s40804-020-00183-y

[8] Ross P Buckley and Natalia Jevglevskaja, 'Australia's Consumer Data-Sharing Regime: A World-Leading Reform' (January 1, 2022) University of New South Wales Law Journal, forthcoming, UNSW Law Research Paper No. 22-2, https://ssrn.com/abstract=4042404.

[9] *See e.g.*, Dirk Zetzsche et al., 'From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance' (2017) 14 European Banking Institute Working Paper Series 2017 – no. 6.

[10] Gerald Spindler, 'Algorithms, Credit Scoring, and the New Proposals of the EU for an AI Act and on a Consumer Credit Directive' in Martin Ebers and Susana Navas (eds), *Law and Financial Markets Review* (Cambridge University Press 2023).

[11] *See e.g.*, soft-law instruments established in Singapore (https://aisingapore.org/); in the US (https://www.nist.gov/artificial-intelligence); and at the supranational level (https://www.oecd.org/digital/artifici al-intelligence/).

[12] Consumer Financial Protection Bureau, '§ 1002.1 Authority, Scope, and Purpose', https://www.consumerfinance.gov/rules-policy/regulations/1002/1/.

3. AI and Data in Consumer Credit

AI in credit assessments and credit scores

The decision about whether to lend to a consumer is usually described as credit assessment or credit under-writing. Credit assessments are influenced by a number of considerations, including prudential requirements, the lender's risk profile, financial modelling, regulatory requirements and the borrower's credit score/report. Credit scoring, usually performed by a third-party ratings agency, involves calculating a score about the way in which a consumer has previously managed credit on the basis of data gathered from lenders, and in some jurisdictions, sources such as utilities.[13]

Lenders have long used statistical credit risk modelling to determine who gets a loan, and many of these credit assessment processes have been automated using computer software. Lenders may also use insights from AI to refine lending decisions.[14] These techniques may allow new insights from the data available about borrowers that is not captured in existing financial modelling.

Data in lending decisions

The use of AI in decision-making about lending is primarily fuelled by the increased availability of consumer data, was well as improved computer processing power. One of the most significant initiatives is open banking, with market-led adoption in Singapore, supported by the Monetary Authority of Singapore,[15] and mandatory schemes in Australia[16] and the UK.[17] Before open banking, lenders might look at borrowers' data, but would do this via the practice of screen scraping.[18] Open banking enables consumers to direct the transfer of this data without giving access to their accounts to prospective lenders.

4. Risks of AI in Consumer Credit Assessments

AI inaccuracy and opacity

[13] Nydia Remolina, 'The Role of Financial Regulators in the Governance of Algorithmic Credit Scoring' (15 March 2022) SMU Centre for AI & Data Governance Research Paper No. 2/2022, 7.

[14] Matthew Bruckner, 'Preventing Predation & Encouraging Innovation in Fintech Lending', 72 Consumer Fin. L. Q. Rep. 370, 371 (2019), who gives the examples of Lenddo and Zest.

[15] Joe Jelinek, 'The state of Open Banking in APAC today' *The Payers* (20 January 2023), https://thepaypers.com/expert-opinion/the-state-of-open-banking-in-apac-today--1259954/. *See also* Leong, Emma and Jodi Gardner, 'Open Banking in the UK and Singapore: Open Possibilities for Enhancing Financial Inclusion' (2021) 5 Journal of Business Law.

[16] Australian Banking Association, 'What is Open Banking?', https://www.ausbanking.org.au/priorities/open-banking/.

[17] Open Banking, https://www.openbanking.org.uk/.

[18] Natalia Jevglevskaja and Ross P Buckley, 'Screen Scraping of Bank Customer Data: A Lamentable Practice' (2023) UNSW Law Research Paper No. 23-3, https://ssrn.com/abstract=4382528 .

Where the use of AI in credit scoring or assessment relies on large data sets and complex neural networks, the accuracy of and reasons for decisions become particularly hard to ascertain.[19] Responsible AI principles and some regulatory regimes require lenders to give explanations of why borrowers are denied credit,[20] so called explainable AI.[21] It is unclear how effective these processes are in the face of complex machine learning algorithms and low borrower financial literacy.[22]

AI bias and discrimination

A key concern about the use of AI in lending decisions is bias in training data leading to discrimination in outcomes.[23] The risk arises because any data-driven decision may replicate and amplify previous bias in lending.[24] Typically, and in some places in compliance with the law, a lender automating a lending decision or using the insights would not directly include protected attributes. The concern about bias nonetheless remains. Machine learning algorithms may find the proxies in the data for protected attributes to replicate and amplify that bias.[25] Discrimination in credit rating or assessments can be difficult to identify, especially where the decision is based on very large data and uses complex machine learning algorithms or neural networks. Accordingly, most of the proposed regulatory responses to responsible or ethical AI require robust systems for monitoring the inputs and design of AI systems and oversight and review for the outputs.[26]

Thin data and financial exclusion

Greater financial inclusion is another commonly cited aim of AI in credit rankings and assessment, as well as in open banking. Certainly, improving the credit assessment process should reduce the cost of lending to many consumers, thus making credit more readily

[19] Matthew Bruckner, 'Regulating Fintech Lending' (2018) 37 Banking & Fin. Services Pol'y Rep. 1,3; Mikella Hurley and Julius Adebayo, 'Credit Scoring in the Era of Big Data' (2016) 18(1) Yale Journal of Law and Technology 148, 153.

[20] *See e.g.*, US Equal Credit Opportunity Act Regulation B; *see also* Consumer Financial Protection Bureau, 'Consumer Financial Protection Circular 2022-03, https://www.consumerfinance.gov/compliance/circulars/circular-2022-03-adverse-action-notification-requirements-in-connection-with-credit-decisions-based-on-complex-algorithms/.

[21] Tim Miller, 'Explainable AI is Dead, Long Live Explainable AI! Hypothesis-driven Decision Support using Evaluative AI*'* (2023) FAccT 2023, https://arxiv.org/abs/2302.12389.

[22] Jeannie M Paterson, 'Misleading AI: Regulatory Strategies for Transparency in Information Intermediary Tools for Consumer Decision-Making' (2023) Loyola Consumer Law Review, https://ssrn.com/abstract=4422456.

[23] Matthew Bruckner, 'Preventing Predation & Encouraging Innovation in Fintech Lending' (2019) 72 Consumer Fin. L. Q. Rep. 370, 378 (2019); Holli Sargeant, 'Algorithmic Decision-making in Financial Services: Economic and Normative Outcomes in Consumer Credit' (2022) AI Ethics, https://doi.org/10.1007/s43681-022-00236-7.

[24] *See* Sargeant (n 23).

[25] *See* Matthew Bruckner, 'The Promise and Perils of Algorithmic Lenders' Use of Big Data' (2018) 93 Chi. Kent L. Rev. 3, 25-27.

[26] *See e.g.*, the approach taken by the US Federal Trade Commission, https://www.ftc.gov/business-guidance/blog/2020/04/using-artificial-intelligence-and-algorithms.

available. But some prospective borrowers may miss out on these gains by being found less credit worthy. Others will not benefit from the advances because they were not benefiting from mainstream or even fringe lending in the first place.[27] Indeed, data scientists speak about 'noise' arising from these kinds of 'thin' data sets, which means the outcomes simply do not reflect the creditworthiness of the excluded individuals because there is not enough data to form an accurate prediction about them.[28] Measures to remove bias based on protected attributes, or proxies for them, in the loan decision will therefore not address financial exclusion.

5. AI Responsible Lending

Responsible lending

Not all differential treatment is discrimination—it is legitimate for lenders to refuse to lend to borrowers who are unable to be likely to repay the loan. In some jurisdictions, lenders have a legal obligation to consider the ability of the borrower to repay without undue hardship,[29] and lending in the face of indicators of overcommitment may amount to unconscionable or unfair dealing.[30] People who cannot get access to credit may struggle with full participation in society, with limited access to items like transport, consumer goods and housing. However, consumers who are overcommitted in borrowing risk the profound social and economic devastation of financial hardship or bankruptcy.[31] AI models used in credit scoring and assessment should be tested not only for discriminatory bias, but also the sustainability of loans made. Moreover, the benefits of AI in lending, if verified, might usefully be extended to the other field that affects consumers, namely, enforcement decisions. Much like its use in financial fraud detection, AI might be used to identify the key indicators and patterns of default and provide more fine-grained basis for enforcing a loan, or even early proactive intervention.

Predatory lending

A related unaddressed concern about the use of AI in credit scoring or credit assessment is the potential for it to facilitate predatory lending by unscrupulous lenders. These concerns

[27] Mikella Hurley and Julius Adebayo, 'Credit Scoring in the Era of Big Data' (2016) 18(1) Yale Journal of Law and Technology 148, 156.

[28] Laura Blattner and Scott Nelson, 'How Costly is Noise? Data and Disparities in Consumer Credit' (2021) https://doi.org/10.48550/arXiv.2105.07554; Bruckner, Matthew, 'The Promise and Perils of Algorithmic Lenders' (2018) Use of Big Data, 93 Chi. Kent L. Rev. 3, 18-19.

[29] *See* Jeannie M Paterson and Nicola Howell, 'Everyday Consumer Credit Overview of Australian Law Regulating Consumer Home Loans, Credit Cards and Car Loans: Background Paper 4' (2018) The Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry, Australia.

[30] *See e.g.*, *Stubbings v Jams 2* [2022] HCA 6.

[31] *See also* Emma Leong, 'Regulating Borrower Hardship in Australia, Singapore, and Hong Kong: Payment Holidays During COVID-19 and Beyond' (2022) *Journal of Consumer Policy.*

mean that the accountability mechanisms for AI decision-making in lending should require lenders to review and monitor lending outcomes not only for bias in the loans refused, but also overcommitment in the loans that are made.

6. Take Away Points

1. AI and big data may be used in credit scoring and credit assessment, and potentially enforcement decisions;
2. The use of AI in making lending decisions has the potential to improve outcomes for lenders and borrowers;
3. The kinds of data used in AI decision-making about credit, and in particular the use of data that is not directly related financial factors (i.e. social media), should be reviewed;
4. Systems for accountability for AI are imperative in guarding against inaccuracy, discrimination and overcommitment in AI-informed credit scoring or assessments;
5. Improving financial inclusion through the combination of AI and big data requires deliberate intervention;
6. It may be possible to use AI for predatory lending and this risk requires regulatory vigilance;
7. Best practice guidelines for the use of AI in credit should be developed;
8. Responsible AI should include a commitment to responsible lending.

X. At the Crossroads Where Robo-advisers Stand

Mr Selwyn Lim
(Syfe)

1. Introduction

Robo-advisers set out to empower the individual retail investor and to provide investment options beyond conventional bank deposits, insurance policies, and self-selected stocks. The business thesis was that unlike human advisers, robo-advisers:

- are always available;
- help the investor avoid decision paralysis;
- are transparent and without conflict; and
- can scale at close to zero marginal cost.

To that end, the hundreds of thousands of users in Singapore who today use the services of a robo-adviser to help them to save and invest better are testament to the gap that existed in the market previously.

Robo-advisers do not exist in a vacuum. They arose to serve a perceived need of the retail investor for empowered investing, and so the state and regulation of the industry must continually evolve to keep pace with the context in which it exists. This presentation summary explores the development of the robo-advisory industry hitherto, the regulatory regime that governs the industry, the crossroads where it now stands in the face of stagnant regulation in the context of the above trends, and posits the future of the industry having regard to the twelve or so robo-advisers in the Singapore market today and their plans for the future. How should regulation respond?

2. Regulation of Robo-Advisers

From a regulatory standpoint, the Monetary Authority of Singapore (‘MAS’) ought to be lauded for encouraging the development in Singapore of this most recent wave of growth in the fintech industry that started in the mid-2010s, and continues to develop now with electronic payments and decentralised finance. By determining quickly that regulation is technology-neutral and that the new fintech business models could be regulated under existing laws—the MAS issued the Guidelines on Provision of Digital Advisory Services (‘Guidelines’) that provided clarity on how prevailing rules operate to apply to digital advisers—the robo-advisory industry was able to rapidly take off and carve out a new segment in the investment intermediary space dominated hitherto by traditional brokerages, banks, insurers, mutual fund asset managers and independent (human) financial advisers.

There were three aspects of regulation that were unique in driving this development:

- First, the MAS typically required that retail fund management companies need a five-year track record of managing funds for retail investors, and manage total assets of at least S$1 billion, before they would be granted a licence to operate in Singapore. The Guidelines offered a concession—the MAS would licence robo-advisers to operate if they limit portfolios offered to retail clients to comprise only collective investment schemes ('CIS') that are in substance excluded investment products (i.e. simple products such as shares and deposits).
- Second, a robo-adviser should only operate client-facing tools that are fully automated, to avoid undue influence on the advisory and portfolio construction process or the client's investment decision.
- Third, the MAS required governance and supervision arrangements to be put in place to oversee algorithms used by the robo-adviser. There was to be no fault or bias in the algorithms that could lead to clients suffering a detriment when using the robo-adviser's platform to select investments.

Collectively, the above regulatory policies allowed the existing laws governing financial intermediary supervision under the Securities and Futures Act 2001 ('SFA') and the Financial Advisers Act 2001 ('FAA') to remain intact in regulating the robo-advisory industry, with the touch of overlay regulation arising under the Guidelines.

This means that in practice, robo-advisers who construct portfolios in which their clients may invest (and handle clients' moneys in relation to the portfolio management) will be licensed to carry on fund management activity under the SFA, because they are regarded as managing a portfolio of securities for their clients. The robo-adviser retains discretion as to the portfolio composition and its ongoing management. This is referred to as a discretionary portfolio management service. At the same time, there is an expectation that the robo-adviser is providing financial advice because its client is reasonably expected to rely on the robo-adviser when making an investment decision. For this reason, a robo-adviser also holds an exempt financial adviser status under the FAA.

3. Growth of Robo-Advisers

The robo-advisory industry has grown rapidly in the five years since the MAS issued the Guidelines. It is estimated that there is now over S$4 billion in assets under management held by investors in Singapore, much of it for the benefit of the retail investor.

Much of this growth for robo-advisers was catalysed by two trends. First, a significant pick-up of interest in investing driven by the Covid-19 pandemic, when people fortunate enough to remain employed found themselves with more time and money during lockdown. Second, the growth of financial commentary in social media, which served to educate the retail public on investing in ways that were relatable and accessible.

But the industry is at a crossroad. The investing boom during the Covid-19 years has wilted in a rising interest rate environment which has had the effect of depressing asset prices. The retail investor has also grown increasingly sophisticated with the barrage of financial commentary and information that is now easily accessible—they may now prefer investing without advice, human or digital. Cryptocurrencies and other asset classes (such as private markets) also offer competition for the investing dollar.

These are not necessarily negative trends for the robo-advisory industry. They bring about opportunities that could be tapped upon too—but this author submits that the regulatory framework may need to be refined to allow the industry to continue to flourish.

4. How Should Regulation Respond?

Looking back at the three aspects of regulation examined above, it is submitted that robo-advisers and the retail investor have both matured over the last decade, and it is time to bring regulation for robo-advisers into greater parity with the rest of the financial industry.

(a) Expanding regulation

The premise for much of the consumer protection purpose of regulation examined above—thereby requiring robo-advisers to only construct portfolios of simple products and to minimise human interaction with the user—may no longer hold true. It would be a more level playing field for robo-advisers to compete with traditional capital markets intermediaries, provided that they are able to meet the requirements of existing regulation. Given that regulation is meant to be technology-neutral, it follows also that robo-advisers ought not to be denied the benefits of utilising human advisers as a complement to a digital service. Robo-advisers should also be allowed to construct portfolios which provide investors with more options, rather than being limited to portfolios comprising CIS that constitute excluded investment products.

(b) Clarify statutory duty for robo-advisers

It is generally accepted that a robo-adviser which is dual-regulated as a fund manager and a financial adviser is likely subject to a duty under section 36(1) of the FAA to have a reasonable basis for making an investment recommendation to a client. In other words, the robo-adviser is required to ensure that its investment recommendation is suitable for the client, having due consideration to the client’s investment objectives, financial situation and particular needs.

Section 36 of the FAA sets out the basis for statutory liability for a financial adviser recommending unsuitable products. It requires that for a client to make out a claim for damages where a recommendation was made without a reasonable basis, the client must show reliance on the recommendation, and that it is reasonable, having regard to the recommendation and all other relevant circumstances, for that client to have purchased the investment *in reliance on the recommendation.*

Section 36 was enacted at a time when robo-advisers did not exist. The MAS has itself, in the Investigation Report on the Sale and Marketing of Structured Notes Linked to Lehman Brothers, noted that "(i) whether an investor bringing an action against a financial adviser can prove that there was reliance; (ii) whether such reliance was reasonable; and (iii) to what extent, if any, the recommendation could be shown to have affected the investor's actual decision to invest is a matter that would need to be established by each investor based on the specific facts and circumstances at the time of purchase. Establishing such a case in law would depend, among other things, on the oral and documentary evidence as to what transpired between the client and the representative of his [financial adviser] and what documents the client signed as part of the transaction process".

In this regard, it is submitted that it is particularly difficult to establish the reliance element in the context of a robo-advisory service. In a fully automated digital process where there is no human interaction between a robo-adviser and its client, and where clients may be told (via a digital prompt) that an investment is unsuitable for them but they choose to nevertheless to proceed with the investment, it can be difficult for a robo-adviser to accept that a client has solely relied on its recommendation when making a losing investment, or for a client to admit that he had in fact self-selected the losing investment on the platform without any real intention to rely on the advice dispensed on the platform. The line between whether a platform is providing full, partial, product-only or execution-only advice, and whether an investor's insistence to proceed even in the face of a risk warning on the platform amounts to non-reliance and acceptance of the risk, therefore becomes blurred.

There is also the technical point as to whether the reference to "investment product" in section 36 includes a discretionary portfolio managed by a fund manager. ("Investment product" as defined in the FAA technically would not capture such a discretionary portfolio.)

Accordingly, existing regulation on the duty of financial advisers to recommend suitable products presents an ambiguity in its application to robo-advisers. It is submitted that it would be more ideal for both robo-advisers and their clients to understand at the outset what their respective duties are when interacting with each other through a digital platform. The law can find a balance between the principles of caveat emptor and caveat venditor in determining the extent to which financial regulation should intervene to protect the interests of an investor transacting via a digital platform, if the platform and algorithms were otherwise properly designed.

Notably, some of the difficulty here could be resolved if robo-advisers start complementing their services with human advisers. In such event, the element of human interaction and possible undue influence that comes with it could perhaps justify a presumption of reliance by an investor as to ground a claim under section 36.

XI. Payment Fraud and Consumer Protection

Dr Sandra Booysen
(National University of Singapore)

Payment fraud (or payment scams) can take different forms, including forgery of the drawer's signature on a cheque, the unauthorised use of a payment card (most commonly in 'card not present' transactions), and by tricking an account holder into making a payment from his/her bank account through a fraudulent misrepresentation. Cases from the last category are mostly examples of 'authorised push payment' (APP) scams.[1] They are considered 'authorised' payments because the payment instruction emanates from the bank account holder who is entitled to make payments from the account, and they are 'push' payments because the payment instruction is received by the paying bank before it enters the relevant payment system.[2]

APP scams have become a significant category of payment fraud in many jurisdictions, for which reason they are receiving growing attention from governments, regulators, and consumer welfare groups. They are also giving rise to a notable number of disputes that are being litigated in the courts. It seems clear that the worrying rise in APP scams is closely aligned with the increase in electronic or digital methods of payment. In other words, as payment preferences have evolved and moved away from cheques to online and mobile payments, the tactics of fraudsters have similarly evolved. Electronic payments are harder to forge than paper-based payments, thus prompting fraudsters into soliciting payments by deceit instead. Because of the attention that APP fraud is currently receiving, the focus here is on APP fraud.

A forged signature is no signature, both at common law and under the Bills of Exchange Act, section 24. A bank that pays on a forged signature does so without the customer's authority which means that there is a breach of mandate and the bank is not entitled to debit its customers account with the payment. This position is subject to qualification, for example the customer may be estopped from denying his/her signature.[3] The position may also be modified by legislation, such as the Payment Services Regulations 2017 in the UK; by soft law codes, such as the MAS E-payments User Protection Guidelines; and by contract terms which shift the risk of forgery onto the customer, an example of which is the verification and conclusive evidence clause.[4]

[1] *See, e.g.*, *Tidal Energy Ltd v Bank of Scotland plc* [2014] EWCA Civ 1107, discussed in Sandra Booysen 'Trade Practices, Contract Doctrine and Consumer Protection' (2021) LMCLQ 316.

[2] By contrast, cheque and card payments are 'pull' payments because the paying bank receives the payment instruction only after it has been routed through the relevant payment system.

[3] *See, e.g.*, *Greenwood v Martins Bank* [1933] AC 5.

[4] *See Major Shipping & Trading Inc v Standard Chartered Bank (Singapore) Ltd* [2018] SGHC 4. *See also* Sandra Booysen 'Consumer Protection and the Court's Role in Shaping the Bank-Customer Contract' (2019) 135 LQR 437.

The distinguishing feature about authorised scam payments is that the paying bank has prima facie authority to make the payment, and ordinarily a bank must process payment instructions promptly. For this reason, the risk of APP scams falls on the customer. It is well-established, however, that banks owe their customers an implied duty of care in rendering their services. A similar duty may also be owed in tort. In some jurisdictions (e.g., the UK and Hong Kong), there is a statutory duty on service providers to render their services with care. As regards its scope, the bank's duty of care has been recognised as applying where the bank executes payment instructions. In this context, the duty goes by the label of the *Quincecare* duty.[5] The duty ordinarily requires a bank not to pay and make inquiries when it suspects, or should reasonably suspect, that the customer is being defrauded. The standard expected is that of the reasonable bank.[6] Two relatively recent cases have highlighted the difficulty that a bank may face should it need to make inquiries. In *Singularis*,[7] company monies were misappropriated by the controlling shareholder who was also dominant in running the company. In *JP Morgan Chase v Nigeria*,[8] the payment instruction was given by a senior figure in the government of Nigeria at the time. The claim was brought by a successor government which alleged that the payment instruction was given fraudulently and therefore it triggered the bank's *Quincecare* duty. Both scenarios highlight the difficulties banks may face once their suspicions have been aroused by a payment instruction. Unlike cases such as *Lipkin Gorman*, there is no obviously independent person whom the bank can reliably contact to confirm or dispel their concerns.

Although the recognition of the *Quincecare* duty has been challenged as unwarranted and inconsistent with the bank's duty to execute mandates promptly,[9] it has been confirmed in the UK by the Court of Appeal,[10] and more recently in the Supreme Court.[11] It has also been recognised by the Singapore Court of Appeal.[12] The existence of the duty is backed by considerable precedent. These cases, however, involved examples of an agent abusing his/her authority (internal fraud).[13] The scope of the *Quincecare* duty in the context of APP scams, which involves fraud by a third party (external fraud), was until recently, untested.

[5] [1992] 4 All ER 363. *See also Lipkin Gorman v Karpnale & Co* [1989] 1 WLR 1340, issue not raised on appeal, [1991] 2 AC 548.
[6] *Hsu Ann Mei Amy v OCBC* [2011] 2 SLR 178, [24].
[7] *Singularis Holdings Ltd (in Official Liquidation) v Daiwa Capital Markets Europe Ltd* [2020] AC 1189.
[8] [2019] EWHC 347 (Comm); on appeal, [2019] EWCA 1641. For the subsequent factual findings on fraud see, *The Federal Republic of Nigeria v JPMorgan Chase Bank, NA* [2022] EWHC 1447 (Comm).
[9] See, e.g., Peter Watts, 'The Quincecare Duty: Misconceived and Misdelivered' (2020) JBL 402; Peter Watts, 'Playing the Quincecare Card' (2022) 138 LQR 530.
[10] *Lipkin Gorman* (n 5).
[11] *Singularis* (n 7).
[12] *Hsu Ann Mei Amy* (n 6); *Yogambikai Nagarajah v Indian Overseas Bank* [1996] 2 SLR(R) 774.
[13] For a recent case from Hong Kong raising interesting issues in the context of internal fraud, see *PT Asuransi Tugu Pratama Indonesia TBK v Citibank NA* [2023] HKCFA 3.

The question recently came before the English courts in *Philipp v Barclays Bank Ltd*.[14] The Philipps fell victim to an APP scam which saw them transfer £700,000 to accounts in the UAE. They sued their bank for not taking a number of steps to protect them from the scam (before, during and after they made the payments), based on the *Quincecare* duty. The High Court gave summary judgment to the bank on the basis that the *Quincecare* duty does not apply where the payment instruction emanates from the customer as a result of a third party's fraud (i.e. external fraud). It is limited to cases where an agent of the customer abuses his/her authority and misappropriates monies from the customer's account (internal fraud). The court's reasoning reflects a concern about the difficult position that banks are in with conflicting duties, on the one hand to pay promptly, and on the other hand, not to pay where fraud should reasonably be suspected. The Court of Appeal unanimously overturned the summary judgment against the customer. It pointed out that the articulation of the duty in the salient cases (e.g., *Quincecare* and *Lipkin Gorman*) did not restrict the duty to cases of internal fraud,[15] although the facts in those cases did involve internal fraud. The court was also sceptical of claims that the duty was unworkable in the modern payment environment. The court rightly reasoned that the duty was calibrated to take account of the general duty to process payment instructions promptly. The everyday push payments made by customers will ordinarily not trigger the duty.

The recognition of the *Quincecare* duty in the APP scam context is supported. It is only in a limited range of circumstances that the *Quincecare* duty will be triggered. It is well-established that banks do not have to be detectives or be overly suspicious. But they should not be entitled to turn a blind eye if transactions are objectively suspicious. An additional reason in support of recognising the duty in this context is policy. APP scams are growing at an alarming rate, and are a menace to society. Customers do not have the bargaining power to insert terms in their account contracts to require banks to reduce the risk. There are many measures which banks can take to warn, detect, and intervene to reduce the risk to customers. Indeed, they already take a variety of measures, and are expected to do so by regulatory and soft law measures.[16] The common law should also respond to the problem, by recognising the duty in external fraud cases. *Philipp* and the scope of the *Quincecare* duty is now before the Supreme Court. The questions of law which have been raised are (1) whether *Quincecare* is limited to cases of internal fraud, and if so, (2) whether it should be extended to external fraud

[14] [2022] EWCA Civ 318. *See also* Sandra Booysen 'Authorised Payment Scams and the Bank's Duty of Care' (2022) LMCLQ 349.

[15] Cf *Singularis* (n 7) para 55, although this decision must be seen in context. The bank's duty of care was not in issue, and the articulation of the duty sufficed for the facts of the case.

[16] *See, e.g.*, MAS E-Payments User Protection Guidelines (Singapore); Contingent Reimbursement Model Code for Authorised Push Payment Scams (UK). *See also* Sandra Booysen 'Tackling Payment Scams: A Comparative Review' (2019) ABLU 1.

or whether an analogous duty should be recognised in such cases. The Supreme Court's answer to these important questions is eagerly anticipated.

The bank's duty of care to non-customers has also been considered by the courts recently. Such a duty can arise in tort if the elements of a duty of care are satisfied.[17] In this context, the duty would typically be based on an assumption of responsibility. However, the common law is generally cautious of imposing a duty of care for pure economic loss outside of a contractual relationship. This point is illustrated by *Customs & Excise v Barclays Bank Ltd*, where a bank overlooked a freezing order in favour of a customer's creditor, and paid most of the monies away. The House of Lords considered that the bank did not owe a duty of care to the creditor as there was no voluntary assumption of responsibility; nor did policy considerations favour the recognition of such a duty. The recent case of *Royal Bank of Scotland v JP SPC 4*,[18] is consistent with this approach. An investment fund sued RBS after fund monies, held in an account with RBS, were misappropriated by the account holder. The Privy Council held that a duty of care in tort would be owed if the bank had a 'special level of control over the source of danger' or if it assumed responsibility to protect the fund from the danger of misappropriation by the account holder.[19] On the facts, the Privy Council advised that RBS did not owe the investors a duty of care in tort.

[17] Famously recognised in *Hedley Byrne & Co Ltd v Heller & Partners Ltd* [1964] 1 AC 465.

[18] *Royal Bank of Scotland International Ltd v JP SPC 4* (Isle of Man) [2022] UKPC 18.

[19] *Ibid*, 83.