Rainer Kulms

# Digital Financial Markets and (Europe's) Private Law – A Case for Regulatory Competition?

**Abstract:** The EU's Digital Finance Strategy assumes that regulations and private laws interact. National private law systems are to demonstrate sufficient evolutionary strength to cope with digital disruption. Regulatory competition is intended to produce adequate private law solutions if EU regulators bring up the right questions. This paper takes a private law perspective to assess the EU's strategy and highlight potential shortcomings. Payment services, outsourcing business models, crowd lending, robo-advice and blockchain applications are identified as test cases where the interface between FinTech regulation and private law is most acutely felt. This translates into a re-interpretation of (digital) contractual duties. Traditional liability rules need to evolve, and incoherent concepts under the EU's digital finance and data protection laws have to be reconciled. Blockchain law is a model case for the far-reaching impact of the interface between FinTech and private law. Member States have to improve the private law status of crypto-assets in order to attract business and address insolvency scenarios. Regulatory sandboxes are addressed as early warning mechanisms, alerting regulators and legislators to risks arising from innovative business models. As innovation intensifies, so will the evolutionary pressure on Member States' private law systems, likely to provoke demands for EU legislative action if Member States underperform.

## Table of Contents



**Rainer Kulms,** Priv.-Doz., Dr. iur., LL.M., Senior Research Fellow, Max Planck Institute for Comparative and International Private Law, Hamburg, Germany.


https://doi.org/10.1515/9783110749472-008

# 1 Digital Disruption and its Fallout

## 1.1 Introduction

FinTech and artificial intelligence have changed the infrastructure of financial markets[1]. Distributed ledger technology stimulates cross-border transactions generated through algorithms, accelerating the privatisation of rule-making[2]. As a corollary, applications of artificial intelligence and machine learning enhance interconnectedness between financial markets and institutions[3]. Networks are emerging which test the viability of private regulation, regulatory intervention and the concept of enforcement of norms in a cross-border scenario[4].

---

**1** *Xavier Vives*, Digital disruption in financial markets – Note, OECD – Directorate for Financial and Enterprise Affairs (Competition Committee), p. 5 et seq. (16 May 2019, DAF/COMP(2019)1) (available at https://one.oecd.org/document/DAF/COMP(2019)1/en/pdf), *José Manuel González-Páramo*, Financial Innovation in the Digital Age: Challenges for Regulation and Supervision, Banco de España, Revista de Estabilidad Financiera, Núm. 32 (May 2017), 11, 15 et seq., Financial Times online 19 November 2020, *Gillian Tett*, Artificial Intelligence is reshaping finance (available at https://www.ft.com/content/c7d9a81c-e6a3–4f37-bbfd-71dcefda3739). Cf. on FinTech business models in Germany: *Gregor Dorfleitner/Lars Hornuf*, FinTech and Data Privacy in Germany – An Empirical Analysis with Policy Recommendations, 2009, p. 85 et seq.

**2** See *Florian Möslein/Sebastian Omlor*, in: *id*. (eds), FinTech-Handbuch – Digitalisierung- Recht – Finanzen, 2nd ed. 2021), p. 4 et seq., on the interface between distributed ledger technology and privatisation of rule-making.

**3** Financial Stability Board (FSB), Artificial intelligence and machine learning in financial services Market developments and financial stability implications (1 November 2017), p. 31 (available at https://www.fsb.org/wp-content/uploads/P011117.pdf).

**4** *Yane Svetiev*, in: *Hans-W. Micklitz/Yane Svetiev* (eds,), A Self-Sufficient European Private Law – A Viable Concept?, European University Institute, Department of Law Working Paper 2012/31) (available at https://works.bepress.com/jan_smits/66/), *Fabrizio Cafaggi*, in: *Kai Purnhagen/Peter Rott* (eds.), Varieties of European Law and Regulation, Liber Amicorum für Hans Micklitz,

FinTech invites regulatory competition on a global scale[5] and among the legal orders of the Member States of the European Union (EU). In some areas, there is evidence that a race to the bottom is conceivable[6]. However, the interface between functioning digital markets and the commodification of financial data leaves regulators and practitioners with a complicated message. Particularly private blockchains operate on a set of rules mutually agreed upon or imposed by the gatekeeper of a permissioned system[7]. Here, legislators might be called upon to supplying private law remedies (with erga-omnes effects) to assure enforceability of the results generated by distributed ledger technology. In 2019, the United Kingdom (UK) Law Tech delivery panel launched a public consultation on the legal status of crypto-assets, distributed ledger technology and smart contracts under English law[8]. It was felt that in spite of the flexibility of English common law the financial community suffered from a lack of certainty about the legal status of these devices[9]. Switzerland has relied on a similar argument: When the Swiss government published the draft for a law on distributed ledger technology, it explained that openness towards innovation needs to be supported by rules on

2014, 259, 262 et seq. See also European Commission, Communication on a Retail Payments Strategy for the EU, sub # III. (Brussels 24 September 2020 (COM(2020) 592 final, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0592&from=EN), on the need to establish full interoperability for cross-border infrastructures for instant payments.

**5** See on the competitiveness of the EU financial as a global standard: Expert Group on Regulatory Obstacles to Financial Innovation (ROFIEG), 30 Recommendations on Regulation, Innovation and Finance, Final Report to the European Commission (December 2019), p. 11 (available at https://ec.europa.eu/info/files/191113-report-expert-group-regulatory-obstacles-financial-innovation_en). From a practical perspective, Switzerland's blockchain law (see infra sub 3.4.) attracts EU banks to offer trading and custody services for digital assets from Switzerland: See Bitcoin.com – News 19 December 2020, Spain's Second Largest Bank BBVA Launches Bitcoin Trading and Custody in Switzerland (available at https://news.bitcoin.com/spains-second-largest-bank-bbva-bitcoin-trading-custody-switzerland/), Frankfurter Allgemeine online 14 December 2020, Kryptowährungen – Bitcoin bei der Bank (available at https://www.faz.net/aktuell/finanzen/digital-bezahlen/bbva-will-2021-in-der-schweiz-bitcoin-handel-anbieten-17102098.html).

**6** See *Luca Enriques*, Welcome to Vilnius: Regulatory Competition in the EU Market for E-Money, Columbia Law School Blog 4 November 2019 (available at https://clsbluesky.law.columbia.edu/2019/11/04/welcome-to-vilnius-regulatory-competition-in-the-eu-market-for-e-money/).

**7** See *Chris Reed/Andrew Murray*, Rethinking the Jurisprudence of Cyberspace, 2018/2020, 112 et seq., 117 et seq., on normative competition in cyberspace through norms emerging from user interaction and technological specificities.

**8** UK Jurisdiction Task Force of the LawTech Delivery Panel, Public Consultation – The status of crypto-assets, distributed ledger technology and smart contracts under English private law (May 2019, available at https://www.lawsociety.org.uk/campaigns/lawtech/news/crypto-assets-dlt-and-smart-contracts-ukjt-consultation).

**9** Ibid., p. 4.

commodification and tradability of financial instruments (i. e. blockchain-based tokens)[10]. Liechtenstein's new blockchain law is also inspired by this legislative approach[11].

Competition authorities emphasise the positive welfare effects of financial disruption through FinTech, arguing for a principle-based approach where technology is faster than law[12]. The Spanish Competition Commission favours market entry under transparency, and disclosure rules with respect to conflicts of interest[13]. From a legislative policy perspective, insistence on transparency reflects a policy choice for informed markets[14]. Less charitably, transparency might also point to legislative unwillingness to interfere with the negative side-effects of (cross-border) digital finance, placing the risk on investors to find out by litigation whether they have to bear the consequences of a fall-out from innovation. The allocative effects this policy approach to innovation[15] have to be absorbed by private actors and their (prescient) ability to design contracts unlikely to fail a reality test[16].

The current regulatory approach towards FinTech has been criticized for an inherent micro-transactional bias which relegates regulators to neglecting macro-level risks for the benefit of private business models[17]. It is posited that a technocratic micro-level focus on FinTech exacerbates self-referential growth

**10** See Schweizerische Eidgenossenschaft, Bundesrat, Press Release 27 November 2019, Bundesrat will Rahmenbedingungen für DLT/Blockchain weiter verbessern (available at https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-77252.html).

**11** Token- und VT-Dienstleister-Gesetz (TVTG), Liechtensteinisches Landesgesetzblatt [Liechtenstein Gazette] 2019, no. 301 of 2 December 2019, *Josef Bergt*, Token als Wertrechte – Token Offerings und dezentrale Handelsplätze, 2nd ed. 2020, p. 67 et seq.

**12** See Competition Bureau Canada, Technology-led Innovation in the Canadian Financial Services Sector – A Market Study, pp. 8, 20 (December 2017, available at https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04322.html)., and the Spanish Comisión Nacional de los Mercados y la Competencia (CNMC), Study on the Impact on Competition of Technological Innovation in the Financial Sector (FinTech) (Madrid 13 September 2018, E/CNMC/001/18),, p. 21 et seq. (available https://www.cnmc.es/sites/default/files/2218346_1.pdf).

**13** CNMC (fn. 12), p. 80.

**14** *Christopher P. Buttigieg et al.*, A Critical Analysis of the Rationale for Financial Regulation Part II: Objectives of Financial Regulation, ECFR 2020, 437, 464 et seq.

**15** See on the allocative effects of the regulatory commitment to promote innovation: *Saule T. Omarova*, Technology v. Technocracy: FinTech as a Regulatory Challenge, 6 J. Fin. Reg. 75, 109 (2020).

**16** See on the interface between financial regulation and private law: *Olha O. Cherednychenko*, Two Sides of the Same Coin: The EU Regulation and Private Law, 22 (1) EBOR 147, 151 et seq. (2021).

**17** *Omarova* (fn. 15), p. 6 J. Fin. Reg. 75, 109 (2020).

and systemic risks, if applied as a normative imperative[18]. Instead, "public accommodation" should provide a framework for "privately created risks and liabilities"[19]. It is difficult to see, however, how the macro-economic effects of a purely transactional approach towards regulation can be ascertained without analysing the private law framework for FinTech transactions[20]. Innovation in finance critically depends on the evolutionary potential of private law[21], as regulators find it difficult to produce standards which demonstrate both understanding and anticipation how machine learning produces (undesired) outcomes[22]. This suggests that EU Financial Regulation might also operate under the tacit assumption that private law will be capable of supplying workable solutions where statutory financial law remains silent[23]. Thus, a polycentric approach is apposite which combines rule-making by governmental actors[24] with efficient rules for private contracts and digital assets.

---

**18** *Omarova* (fn. 15), 6 J. Fin. Reg. 75, 109 et seq. (2020).

**19** *Saule T. Omarova*, New Tech v. New Deal: FinTech as a Systemic Phenomenon, 36 Yale J. Reg. 735, 756 (2019).

**20** See *Randall E. Duran/Paul Griffin*, Smart contracts: will Fintech be the catalyst for the next global financial crisis, 29 (1) J. Fin. Reg. & Compliance 104 – 122 (118) (2021), on devising best practice guidelines mandatory settlement requirements for certain types of smart contracts.

**21** See *Cherednychenko* (fn. 16), p. 147, 163

**22** See Financial Times online 6 August 2019, *Imogen Tew*, Full robo-advice' impossible to regulate' (available at https://www.ftadviser.com/your-industry/2019/08/06/full-robo-advice-impossible-to-regulate/). *Christopher Woolard* (FCA), The future of regulation: AI for consumer good, Speech London 16 July 2019 (available at https://www.fca.org.uk/news/speeches/future-regulation-ai-consumer-good), Financial Times online 16 July 2019, *Imogen Tew*, FCA concerned about firms not tackling tech risk (available at https://www.ftadviser.com/regulation/2019/07/16/fca-concerned-about-firms-not-tackling-tech-risk/). See also regulators' uncertainty due to asymmetric information on digitised processes: FinTech Working Group of the United Nations Secretary-General' Advocate for Inclusive Finance (UNSGSA)/Monetary Authority of Singapore/University of Cambridge, Early Lessons on Regulatory Innovations to Enable Inclusive FinTech: Innovation Offices, Regulatory Sandboxes, and RegTech, p. 23 et seq., on frequent exchanges between the industry and regulators (2019, available at https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2019-summary_earlylessonsregulatoryinnovations.pdf), passim ESMA/EBA/EIOPA, FinTech: Regulatory sandboxes and innovation hubs – Report p. 8 et seq. (JC 2018 74) (available at https://www.esma.europa.eu/sites/default/files/library/jc_2018_74_joint_report_on_regulatory_sandboxes_and_innovation_hubs.pdf), p. 6 et seq. Cf. *Douglas Arner/Janos N. Barberis/Ross P.Buckley*, FinTech, RegTech, and the Reconceptualization of Financial Regulation, 37 (3) Nw. J. Int'l. L. & Bus. 371, 403 et seq., (2017) on the challenges for regulators.

**23** Cf. *Cherednychenko* (fn. 16), p. 147, 163 et seq.

**24** See *Yane Svetiev*, in: Liber Amicorum Micklitz (fn. 4), 153 – 177 (p. 157 et seq)., invoking normative and institutional pluralism and a fragmented legal landscape as arguments supporting a

## 1.2 Outline of the Paper

Financial services are credence goods[25] which depend on consumer confidence[26], trust and the enforceability of public and private law rules[27]. This paper takes a private law perspective on FinTech. It explores the underlying assumption of the EU Commission's digital finance strategy[28] that the law for FinTech and private law rules interact. The – tacit – appeal to Member States to play the evolutionary private law part of FinTech operates to trigger competition between their respective private legal orders[29]. This, however, assumes that the EU's FinTech law 'asks' the right questions. Therefore, prominent FinTech business models will be tested on their capacity to stimulate evolution of national private law orders, but also to aggravate deficiencies from an exclusive reliance on private law solutions.

This paper identifies payment services, outsourcing business models, crowdlending, robo-advice and aspects of blockchain applications as test cases where the interface between the EU's financial market regulation and private law is most acutely felt. Especially in blockchain law, the EU faces competition from non-Member State legal orders. The EU's regulatory approach, as reinforced by

plea for European Regulatory Private Law. See generally on the notion of a European Regulatory Private Law: Guido Comparato/Hans-W. Micklitz/Yane Svetiev (eds.), European Private Regulatory Private Law – Autonomy, Competition and Regulation in European Private Law (European University Law Institute Working Paper LAW 2016/00).

**25** See *Iris H-Y Chiu*, FinRech and Disruptive Business Models in Financial Products, Intermediation and Markets – Policy Implications for Financial Regulators, 21 J. Tech. L. & Pol'y 55 – 112 (74) (2016), cf. *Hillary J. Allen*, Regulatory Sandboxes, 87 (3) Geo. Wash. L. Rev. 579, 587 (2019).

**26** See on (limited) consumer acceptance of automated enforcement through smart contracts: *Danielle D'Onfro*, Smart Contracts and the Illusion of Automated Enforcement, 61 Wash. U. J.L. & Pol'y 173, 183 et seq. (2020).

**27** The debate on the private law effects of conduct of business rules under the Directive 2014/65/EU of 15 May 2014 on markets in financial instruments, O.J. L 173/349 of 12 June 2014 (MiFID II) demonstrates the crucial importance of the interface between supervisory law and private law rules. For a detailed analysis see: *Federico Della Negra*, MiFID II and Private Law – Enforcing EU Conduct of Business Rules, Oxford 2019, p. 27 et seq., and *Marnix W. Wallinga*, EU investor protection regulation and private law (PhD thesis Groningen, 2018), p. 60 et seq. Passim on the interface between supervisory capital market and private laws: *Florian Möslein/Christopher Rennig*, in: *Marco Cian/Claudia Sandei*, *M. Cian/C. Sandei* (eds.), Diritto del FinTech, Milan 2020, p. 471, 472.

**28** See EU Commission, Communication on Digital Finance Strategy for the EU (Brussels 24 September 2020 (COM(2020) 591 final) at # 4.2. (available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0591&from=EN).

**29** See the country studies in: *Cian/ Sandei* (fn. 27), p. 439 et seq.

the digital finance package of September 2020[30], is understood as an incentive to fill – deliberate – gaps by private laws and their evolutionary potential or, private contracting. Shortcomings of this approach will be highlighted which may ultimately trigger the enactment of European regulatory private law instruments. This applies particularly to incoherent liability concepts and the complicated relationship between digital finance and data protection law.

The analysis of current FinTech business models will be supplemented by a survey over regulatory sandboxes. Regulatory sandboxes have been so devised as to test innovative digital business models under the auspices of financial market authorities. Businesses are afforded an opportunity to scrutinize the viability of their digital concepts. Financial market authorities collect empirical data and assess the viability of a principle-based approach to regulatory action. Most sandbox models attempt to avert negative externalities by imposing transparency and insurance requirements. Sandbox models may operate as early-warning mechanisms, indicating where future regulatory action might be necessary. A final section sums up the findings on the state of interaction between financial law and private law.

# 2 FinTech Activities and the Evolving Law of Decentralised Finance

## 2.1 Payment Services – Basics

The amended Payment Services Directive (PSD II)[31] has opened up traditional banking. Peer-to-Peer (P2P) and peer-to-Business (P2B) payments are widely accepted[32], including transactions from mobile wallets[33]. Real-time payment sys-

**30** See EU Commission, Press Release, Digital Finance Package: Commission sets out new, ambitious approach to encourage responsible innovation to benefit consumers and business (Press Release, Brussels 24 September 2020, available at https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1684).

**31** Directive (EU) 2015/2366 of 25 November 2015 on payment services in the internal market amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, O.J. L 337/35 of 23 December 2015.

**32** See Schweizerische Eidgenossenschaft, Eidgenössisches Finanzdepartement, Änderung des Bankengesetzes und der Bankenverordnung (FinTech), Erläuternder Bericht zur Vernehmlassungsvorlage, p. 9 et seq.) (1 February 2017, available at https://www.admin.ch/ch/d/gg/pc/documents/2834/Fintech_Erl.-Bericht_de.pdf).

tems operate on the basis of platforms, frequently surveyed by the ECB or national banks[34]. End-users can observe any delay and disruptions[35], creating reputational risks for the payment services provider[36]. Due to stricter regulatory requirements[37] customer online identification is embracing tokenisation of payment processes, supplemented by artificial intelligence devices to verify customer transactions on the basis of past payment patterns[38]. Once tokenised payments are integrated into distributed ledger technology, such a token may operate as the private key allowing access to value stored on a blockchain[39]. The private law classification of tokens and keys will then determine whether

**33** ING Bank Blog, The impact of real times payments on consumers and their businesses (available at https://www.ingwb.com/insights/articles/the-impact-of-real-time-payments-on-consumers-and-their-businesses); Banking Hub Payments eine Branche im Umbruch – Mit welchen strategischen Veränderungen sind Banken und Zahlungsdienstleister heute und in der Zukunft konfrontiert? (Blog 2 April 2020, available at https://bankinghub.de/innovation-digital/payments).

**34** See European Commission, Communication on a Retail Payments Strategy (fn. 4), sub # III. (Brussels 24 September 2020 (COM(2020) 592 final, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0592&from=EN); European Central Bank, MIP Online, The new TARGET instant payment settlement (TIPSservice (June 2017, available at https://www.ecb.europa.eu/paym/intro/mip-online/2017/html/201706_article_tips.en.html),
*Harsh Sinha*, PayThink The Fed has a key role to play in real-time payments (Blog 18 December 2019, available at https://www.paymentssource.com/opinion/the-fed-has-a-key-role-to-play-in-real-time-payments).

**35** See on near real-time delays prior to the modernisation of the system: *Zhiling Guo et al.*, Near Real-Time Retail Payment and Settlement Systems Mechanism Design, p. 5 et seq. (Swift Institute Working Paper No. 2014 – 004, 8 September 2015) (available at https://www.swiftinstitute.org/wp-content/uploads/2015/11/WP-No-2014-004-1.pdf).

**36** See *González-Páramo*, Revista de Estabilidad Financiera, Núm. 32 (May 2017), 11– 37 (p. 17 et seq.), European Banking Authority (EBA), ℙ 33 Final report on EBA guidelines on outsourcing arrangement (GL/2019/0225, 25 February 2019, available at https://eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7–4855–8ba3–702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf).

**37** See also FINMA's insistence on algorithms designed to scrutinise a client's power to dispose of an external wallet: FINMA; FINMA-Aufsichtsmitteilung 02/2019, Zahlungsverkehr auf der Blockchain (26 August 2019, available at https://www.finma.ch/de/news/2019/08/20190826-mm-kryptogwg/).

**38** *Michael Lynch*, PayThink Real-time payments breaks security 'rules' (Blog 11 December 2019, available at https://www.paymentssource.com/opinion/real-time-payments-breaks-security-rules).

**39** Cf. ibid., p. 170. For a blockchain payment project based on a tokenised fiat currency see Singapore's Project Ubin: Deloitte/Singapore Exchange/Monetary Authority of Singapore, Delivery versus Payment on Distributed Technologies (2018, available at https://www.mas.gov.sg/-/media/MAS/ProjectUbin/Project-Ubin-DvP-on-Distributed-Ledger-Technologies.pdf).

a payment service provider has separated customer accounts properly (with values stored on a blockchain), insolvency-proof from third-party attachment[40]. Ultimately, the success of electronic storage and verifications schemes hinges on their compatibility with data protection law[41].

Digitisation pushes contract law analysis towards exploring specific duties of loyalty and care, once payment services are offered in the context of outsourcing arrangements[42] or distributed networks[43]. Payment service providers delegate the actual transfer of monies to comprehensive algorithms without ever getting hold of the transferred values[44]. Cloud computing supplies an infrastructure for banks and start-ups, allowing for offshore data processing to save cost[45]. It is for the national legal orders to decide whether designing a payment system or a distributed network also means liability for malfunctions[46].

## 2.2 Outsourcing

Under both statutory law and supervisory practice, outsourcing is conditioned on risk management mechanisms[47], assuming that the enforcement threat remains credible. Standard contracts may offer a pragmatic approach to facilitate digital transactions, but it is obvious that the bargaining power of those adhering to a digital network may vary: Banks may lose their autonomy as FinTechs seize some of the added value[48]. A 2013 data protection case from Sweden reveals that data processors may be in a stronger position than the data control-

**40** See infra sub 2.5.1.

**41** Cf. Clifford Chance Talking Tech Blog 18 October 2019, PSD2-innovation and GDPR-protection: a fintech balancing act – Part One (available at https://talkingtech.cliffordchance.com/en/data-cyber/data/psd2-innovation-and-gdpr-protection–a-fintech-balancing-act.html).

**42** See infra sub 2.2.

**43** See Expert Group on Regulatory Obstacles to Financial Innovation (fn. 5), p. 50.

**44** See *Florian Glatz*, in: Möslein/Omlor, FinTech (fn. 2), § 8 ¶ 53. If payment services are outsourced to a blockchain-based intermediary, the latter does not have to issue guaranties for monies 'stored' in the system, because blockchain technology allows for real-time payments: *Glatz*, ibid., § 6 ¶ 56.

**45** See European Commission, Digital Finance Strategy (fn. 28), at # 4.2. and *Xenofon Kontargyris*, IT Laws in the Era of Cloud Computing, 2018, p. 42 et seq., p. 216 et seq.

**46** Expert Group on Regulatory Obstacles to Financial Innovation (fn. 5), p. 48 et seq.

**47** See the analysis in Expert Group on Regulatory Obstacles to Financial Innovation (fn. 5), p. 24 et seq.

**48** *Dorfleitner/Hornuf* (fn. 1), p. 85 et seq.

lers[49]: The Swedish Data Protection Agency criticised that the controller was not afforded sufficient control and insight into the data processing chain for storing information in the cloud[50].

From a consumer perspective, legal uncertainty is magnified once payment service providers operate in a network of interrelated contracts with organizational features[51], sometimes difficult to trace back to a jurisdiction[52]. Moreover, diverging proprietary standards and protocols jeopardise cross-border business[53]. Art. 4 of the Commission's Draft Regulation on digital operational resilience for the financial sector[54] builds on professional standards for financial service providers, their contractors and sub-contractors. Art. 4 of the Draft Regulation prescribes internal governance mechanisms and control frameworks to manage the risks: The financial services provider who plans to outsource remains responsible for the safe storage of personal financial data. Thus, contractual arrangements with third-party providers and potential subcontractors are to

**49** See on the bargaining power of artificial intelligence-equipped platforms in finance: Financial Times online 19 November 2020, G. Tett, Artificial intelligence is reshaping finance (available at https://www.ft.com/content/c7d9a81c-e6a3-4f37-bbfd-71dcefda3739).

**50** *Jenna Lindqvist*, New challenges to personal data processing agreements: is the GDPR fit to deal with contract, accountability and liability in a world of the Internet of Things?, 26 Int'l. J. L. & Techn. 45, 54 (2018).

**51** See Expert Group on Regulatory Obstacles to Financial Innovation (fn. 5), p. 48 et seq. on distributed financial network, *Mark Beer*, in: Marc Schmitz/Patrick Gielen (eds)., Avoirs Dématérialisés et Exécution Forcé, 2019, 153, 159. On nanopayment systems: *Sebastian Omlor*, Nanopayments – Monetisierung des Cyberspace?, MMR 2018, 428 – 433, p. 432.

**52** Cf. on the operational risks if FinTech activities are outsourced to third parties not subject to the existing regulatory framework: European Investment Bank, Blockchain, FinTechs and the relevance for international financial institutions, Economics Working Papers 2019/01, p. 31 (available at https://www.eib.org/attachments/efs/economics_working_paper_2019_01_en.pdf), Basel Committee on Banking Supervision, Sound Practices of FinTech developments for banks and bank supervisors (Bank for International Settlements, February 2018), p. 32 et seq. (available at https://www.bis.org/bcbs/publ/d431.pdf).

**53** European Banking Authority (EBA), Discussion Paper on the EBA's approach to financial technology (FinTech) (4 August 2017), p. 45 et seq. (EBA/DP/2017/02, available at https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1919160/7a1b9cda-10ad-4315-91ce-d798230ebd84/EBA%20Discussion%20Paper%20on%20Fintech%20%28EBA-DP-2017-02%29.pdf?retry=1); Bank of Canada/Bank of England/Monetary Authority of Singapore, Cross-Border Interbank Payments and Settlement – Emerging opportunities for digital transformation (November 2018), p. 10 (available at https://www.mas.gov.sg/-/media/MAS/ProjectUbin/Cross-Border-Interbank-Payments-and-Settlements.pdf).

**54** European Commission, Proposal for a Regulation on digital operational resilience for the financial sector (Brussels 24 September 2020, COM(2020) 595 final (available at https://ec.europa.eu/transparency/regdoc/rep/1/2020/EN/COM-2020–595-F1-EN-MAIN-PART-1.PDF).

replicate the safety standards to be observed by the outsourcing financial entity[55]. However, the Financial Stability Board (FSB) has cautioned against too much optimism that such safeguards will be passed along the chain of contracts with fourth or fifth parties or beyond[56]. Both, the European Banking Authority (EBA)[57] and the Board of the International Organization of Securities Commissions (IOSCO)[58] have promulgated detailed sets of governance rules which seek to reduce the risk that original safeguards will be watered down the line of sub-contracts[59]. The Expert Group on Regulatory Obstacles to Financial Innovation (ROFIEG) envisages a certification or licensing scheme to ensure observance of minimum standards[60].

The Draft Regulation on digital resilience remains silent on liability standards with respect to third-party storage of electronic assets and values[61]. Under art. 10 (1) (a) PSD II safe storage of tokenised funds on permissioned blockchain can be guaranteed only if such tokens are insolvency-proof. Strict observance of art. 20 (2) PSD II would indicate no-fault liability if digital assets stored in networks are misappropriated. Under art. 24 of Directive 2009/65/EU (UCITS), as amended[62], the depositary may escape liability if a loss has arisen due to an external event beyond its reasonable control with unavoidable consequences[63].

**55** Art. 44 of the Draft Regulation provides for administrative sanctions if the statutory professional duties are disregarded.

**56** Financial Stability Board (FSB), Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships – Discussion Paper (9 November 2020), p. 6 et seq. (available at https://www.fsb.org/wp-content/uploads/P091120.pdf).

**57** EBA, Final Report on EBA Guidelines on outsourcing arrangements (25 February 2019), p. 44 et seq. (on the contractual phase) (available at https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf?retry=1)

**58** OICV-IOSCO, Principles on Outsourcing – Consultation Report (May 2020), p. 20 et seq. (CR01/2020, available at https://www.iosco.org/library/pubdocs/pdf/IOSCOPD654.pdf).

**59** On the legal force of these standards see infra 2.4.

**60** Expert Group on Regulatory Obstacles to Financial Innovation (fn. 5), p. 44 et seq.

**61** See the assessment of regulatory policy choices in: European Commission, Commission Staff Working Document, Impact Assessment Report – Proposal for a Regulation on digital operational resilience for the financial sector (Brussels 24 September 2020 (SWD(2020) 198 final, available at https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2020:0198:FIN:EN:PDF), without analysing in detail the interface between digital resilience and data protection requirements.

**62** Consolidated text available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02009L0065–20200107.

**63** See also § 36 (4) of the German Kapitalanlagegesetzbuch (KAGB) on liability in an outsourcing scenario.

Art. 82 (2) of the General Data Protection Regulation[64] allows for an escape from liability if the data controller or processor can establish that they are not responsible for damages sustained by the data subject. As a corollary, a data controller can escape liability if a contractor or sub-contractor dictate the rules of an outsourcing scheme[65]. The Draft Regulation on digital resilience does not decide whether the use of artificial intelligence would be tantamount to imposing no-fault liability on those who stand to benefit from it[66]. Competition between the national private law systems will determine whether joint or vicarious liability is the solution for buttressing digital resilience. On the other hand, the quest for a single digital market may require legislative action on the EU level to eliminate differences between national liability concepts.

## 2.3 Crowdlending

Crowdlending and crowdfunding platforms owe their existence to a shortage of finance for community projects, small businesses and start-ups[67]. Platform-based credit schemes connect project proponents with investors[68]. In Europe, crowdlending essentially takes two forms: In a direct peer-to-peer lending sce-

**64** Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, O.J. L 119/1 of 4 May 2016.

**65** Cf. Christopher Docksey, in: Christopher Kuner/Lee A. Bygrave/Christpher Docksey (eds.), The General Data Protection Regulation (GDPR) – A Commentary, 2020)), p. 566, commenting on a safe-harbour approach in the context of art. 24 GDPR.

**66** For a survey over third-party risks in the context of employing digital technologies for outsourcing financial services: European Commission, Commission Staff Working Document, Impact Assessment Report, Proposal for a Regulation on digital operational resilience for the financial sector, sub ℙ 2.1.4. (Brussels 24 September 2020 (SWD(2020) 198 final, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020SC0198&from=EN).

**67** See the analysis undertaken in this issue by *Eugenia Macchiavello/Antonella Sciarrone Alibrandi*, Marketplace Lending as a New Form of Capital Raising in the Internal Market: True Disintermediation or Re-intermediation, ECFR (2021). For surveys see: OICV-IOSCO, Crowd-funding: An Infant Industry Growing Fast, Staff Working Paper of the IOSCO Research Department, p. 21 et seq. ([SWPP3/2014], available at https://www.iosco.org/research/pdf/swp/Crowd-funding-An-Infant-Industry-Growing-Fast.pdf); *Olha Havrylchyk*, Regulatory Framework for the Loan-Bases Crowdfunding Platforms (OECD Economic Department Working Paper No. 1513, 13 November 2018), p. 10 et seq. (available at http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=ECO/WKP(2018)61&docLanguage=En).

**68** See *Havrylchyk* (fn. 67), p. 11 et seq. For a country-wise survey over the regulatory approaches: OICV-IOSCO, Crowd-funding (fn. 67), p. 52 et seq.

nario, the crowdlending platform acts as the agent of both, the investor-lender and the borrower and establishes a direct loan contract between the parties[69]. Indirect peer-to-peer lending takes place when the platform cooperates with the banks which receives monies from the investor and channels them to the borrower[70]. The new Crowdfunding Regulation of the European Union conditions the establishment of a digital platform on obtaining a license from national authorities[71]. Recital 20 to the Crowdfunding Regulation introduces an analogy with respect to auto-investing: investment decisions triggered by pre-determined algorithms and smart contracts without any direct human intervention will be classified as individualised portfolio management.

From a private contracting perspective, the direct crowdlending model is quite straight forward[72]. The platform provides a digital meeting area where the borrower and the lender-investor conclude a loan contract or an investment contract (in the case of equity-based lending)[73]. The lender acquires the right to use financial information listed on the platform on the basis with an agreement with the platform[74]. The borrower applies to the platform by submitting information on the project to the platform which assesses the quality of the application and eventually lists the project[75]. The platform refrains from making an investment recommendation[76]. However, under the new Crowdfunding Regulation extensive behavioural rules are to be observed, including the risk management and assessment of the of the projects offered to the public via the platform[77].

P2P-lending schemes have suffered from a disconnect between the lender's freedom of contract to conclude a loan agreement and the crucial role of the plat-

**69** *Lea Maria Siering*, in: *Möslein/Omlor*, FinTech, fn. 2, § 24 ¶ 5 et seq.

**70** *Moritz Renner*, in: *Möslein/Omlor*, FinTech, fn. 2, § 23 ¶ 6 et seq.

**71** Regulation (EU) 2020/1503 of 7 October 2020 on European crowdfunding service providers for business, O.J. L 347/1 of 20 October 2020.

**72** See *Mark Cummins et al.*, in: *Theo Lynn/John G. Mooney et al.* (eds.), Disrupting Finance – FinTech and Strategy in the 21st Century, 2019, 15, 17; *Ajay Byanjankar et al.*, Predicting Credit Risk in Peer-to-Peer Lending: A Neural Network Approach, 2015 IEEE Symposium on Computational Intelligence 719 – 725 (p. 720) (available at https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7376683).

**73** See *Manuel Stutz*, Anlegerschutz und FinTech – unter besonderer Berücksichtigung von Zahlungssystemen, Crowdfunding, Tokens und Robo-Advice (Dissertation No. 4923, Universität Sankt Gallen, 2019), p. 192 et seq., see also recitals 10, 11 of Regulation (EU) 2020/1503 of 7 October 2020 on crowdfunding service providers for business, O.J. L 347/1 of 20 October 2020.

**74** See e. g. the Loan Management Service Agreement used by the Landbay P2P Platform (available at https://landbay.co.uk/terms-and-conditions).

**75** *Siering*, in: Möslein/Omlor (fn. 2), § 24 ¶ 1 et seq.

**76** This does not avert problems of adverse selection: *Havrylchyk* (fn. 67), p. 22 et seq.

**77** See art. 3 et seq. of the Crowdfunding Regulation.

form in assessing the creditworthiness of the borrower and the quality of the investment project submitted[78]. P2P-platforms operate digital scoring mechanisms, classifying the borrower and his project within certain risk categories[79]. Art. 5 et seq. of the Crowdfunding Regulation impose rules of sound business administration on the platform managers and addresses conflict of interest. This is intended to stave off situations of asymmetric information between the platform and the investor-lender because the latter bases an investment decision on the information received from the platform, which, in turn, has a business interest in brokering the loan contract. Under the new Regulation financial service providers are under organizational requirements and a duty to disclose the algorithms and smart contracts they are using for obtaining credit-rating scores[80].

As soon as the platform undertakes to manage loans[81], platform services overlap with elements of robo-based asset management. Based on the investor's risk preferences, the platform will re-allocate loans, diversify the portfolio and arrange for collateral[82]. Blockchain technology can be employed to manage client accounts and to match borrowers' requests for finance, based on 'intelligent' smart contracts and algorithms[83]. Art. 11 of the new Crowdfunding Regulation addresses the risk of loss for those investors who place funds with the platform. Platforms shall observe prudential requirements. They must have a minimum capital of 25,000 € and funds to cover operational risks or, alternatively insurance and/or own funds (CET 1). Platform activities may be outsourced but the platform cannot escape liability under the Regulation by way of contractual stipulation with a third-party service provider. Moreover, funds held must be placed with a depositary, unless national law allows for the storage in a separate account administered by the platform.

The new Crowdfunding Regulation has the potential of fleshing out duties which are owed under the contracts normally concluded in the context of plat-

**78** Cf. *Deidre Ahern*, Regulatory Arbitrage in a FinTech world: devising an optimal regulatory response to crowdlending, 2018 J. Bus. L. 193, 196 et seq. See on lender risks in crowdlending settings on the basis of empirical data: *Henri Palomäki*, European Crowdlending Platforms: Evaluating Risks and Comparing Platforms from Investors' Perspective (Oulu Business School 2019) (available at http://jultika.oulu.fi/files/nbnfioulu-201905081654.pdf).

**79** See *Byanjankar* (fn. 72), p. 721 et seq., for a credit scoring model relying on artificial intelligence to classify default and non-default loans.

**80** *Ahern* (fn. 78) p. 198.

**81** See e. g. the Loan Management Service Agreement used by the Landbay P2P Platform (available at https://landbay.co.uk/terms-and-conditions

**82** Ibid.

**83** Eidgenössisches Finanzdepartement (fn. 32), annotation to Art. 7 paras. 1/2 of the Bankenverordnung.

form-engineered contracts. But its success crucially depends on the ability of national contract laws to expand the scope of duties of care and loyalty under a contract which also rests on the observance of organizational duties[84].

## 2.4 Robo-advice

Robo-advisory schemes reinforce the question whether private law systems are capable of balancing the interests of investors against those of financial institutions relying on artificial intelligence. Robo-advisers operate with a variety of business models, depending on the degree of human interaction and intervention when collecting and processing information to generate a recommendation for a specific investment[85]. Fully digitalised robo-advisory systems process market information and restructure customer portfolios. Algorithms invest and rebalance the account in accordance with customer risk preferences[86]. At the outset, robo-advisory services are based on a service contract between the customer and the financial service provider[87], backed up by a contract with the cooperating bank of the financial service provider[88]. Risks under automated financial advice schemes may be magnified if automated services are provided by a network of firms with an unclear allocation of liabilities between the financial institution and an outsource provider[89].

Robo-advice has been observed to be prone to home biases[90], behavioural biases[91] and undisclosed conflicts of interest. Deficient software and design of

**84** Cf. *Florian Möslein/Arne Lordt*, Rechtsfragen des Robo-Advice, ZIP 2017, 293, 702.

**85** U.S. Securities and Exchange Commission, Division of Investment Management – Guidance Update, Robo-Advisers (No. 2017–02, February 2017) (available at https://www.sec.gov/investment/im-guidance-2017-02.pdf). See art. 54 (1) of the Delegated Regulation (EU) 2017/565 (O.J. L 87/1 of 31 March 2017) on the suitability assessment when investment advice is provided through ab automated system.

**86** *Christoph Kumpan*, in: Möslein/Omlor (fn. 2), § 29 ¶ 6 et seq., cf. *Wolf-Georg Ringe/Christopher Ruof*, A Regulatory Sandbox for Robo Advice (European Banking Institute Working Paper No. 26 May 2018, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3188828&download=yes). See also U.S. SEC, Guidance, fn. 85, p. 3.

**87** *Alexis Darányi*, in: Möslein/Omlor (fn. 2), § 30 ¶47.

**88** *Möslein/Lordt* (fn. 84), ZIP 2017, 293, 798.

**89** ESMA/EBA/EIOPA (fn. 22), p. 28 et seq.

**90** Risksave.com News 12 March 2018, Home-country bias in Robo-Advice (available at https://risksave.com/news/2018/3/13/home-country-bias-in-robo-advice).

**91** Cf. on "honesty of the algorithms": *Baker/Dellaert*, 103 Iowa L. Rev. 713, 736 (2018), see also: *Kumpan*, in: Möslein/Omlor (fn. 2), § 29 ¶12.

(matching) algorithms have the potential of translating into customer losses[92]. Regulators have reacted by requiring automated investment services firms to improve the governance and risk management structures, supervise and update algorithms and inform potential customers on the underlying assumptions, limitations and risks of the algorithms[93]. Singapore's Monetary Authority places the responsibility for oversight and governance of client-facing tools with the board and senior management of the robo-advisory firm; EU law takes a similar approach[94]. It remains to be seen whether this combination of oversight and disclosure duties supplements the concept of offering proper investment advice under the service contract[95].

In the US, the scope of duties owed under the service contract has sparked a debate on how robo-advice can be reconciled with statutory duties under investment law, informed by portfolio theory[96]. The US FINRA has noted that financial service providers relying exclusively on robot-generated advice do not meet the

---

**92** Cf. FCA, Automated investment services – our expectations (21 May 2018, available at https://www.fca.org.uk/publications/multi-firm-reviews/automated-investment-services-our-expectations), (Monetary Authority of Singapore, Guidelines on Provision of Digital Advisory Services (Guidelines No. CMG-G02, 8 October 2018), ¶ 28 et seq. (available at https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulations-Guidance-and-Licensing/Securities-Futures-and-Fund-Management/Guidelines-on-Provision-of-Digital-Advisory-Services-CMGG02.pdf), *Möslein/Lordt* (fn. 84), ZIP 2017, 793 – 803 (p. 801 et seq.).

**93** MAS, Guidelines on Digital Advisory Services (fn. 92), ¶ 26 et seq., 31, FCA, Automated Investment Services.

**94** Ibid., ¶ 28 and Art. 54 (1) of the Commission Delegated Regulation (EU) 2017/65 of 25 April 2016 supplementing Directive 2014/65/EU as regards organizational requirements and operating conditions for investment firms and defined terms for the purposes of that Directive, O.J. L 87/1 of 31 March 2017.

**95** See the FCA's concerns about suitability of advice for (vulnerable) customers: FCA Automated Investment Services (fn. 92), Moneymarketing 21 May 2018; *Stephen Little*, Robos under fire over suitability and disclosure failings (available at https://www.moneymarketing.co.uk/news/robos-fire-suitability-disclosure-failings/), cf. *Möslein/Lordt* (fn. 84), ZIP 2017, 793, 801, on the delicate interface between the law of contracts and the financial market regulation during the execution of a service contract for robo-advice.

**96** *Melanie L. Fein*, FINRA's Report on Robo-Advisors: Fiduciary Implications (April 2016) (available at https://pdfs.semanticscholar.org/fd40/34cf0fa3654ce05fd0401c4f97675e27427a.pdf); *Megan Ji*, Are Robots Good Fiduciaries? Regulating Robo-Advisors under the Investment Advisers Act of 1940, 117 Colum. L. Rev. 1543, 1563 et seq. (2017); *Jill E. Fisch/Marion Labouré/John A. Turner*, The Emergence of the Robo-advisor, Wharton Pension Research Council Working Paper No. 10 (1 December 2018, available at https://pensionresearchcouncil.wharton.upenn.edu/wp-content/uploads/2018/12/WP-2018 – 12-Fisch-et-al.pdf), *Demo Clarke*, Robo-Advisors – Market Impact and Fiduciary Duty of Care to Retail Investors (University of Maryland 13 February 2020) (available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3539122&download=yes).

standards of fiduciary care owed when advising clients[97]. As a consequence, financial advisory companies have established hybrid concepts where robot-generated advice is counter-checked by human beings before being applied to customer risk parameters[98]. The Bank of England and the FCA point to specific risk management mechanisms when financial service employ machine learning applications: Prior to execution, machine learning activates an alert mechanism which calls for human approval[99]. In testing robo-advice schemes under its regulatory sandbox scheme, the FCA insists on involving a qualified financial adviser to assess the quality of the underlying algorithms[100]. Algorithms have to be amended in accordance with the advisor's assessment[101]. The US FINRA has proposed a similar approach[102].

In the EU, art. 25 (1) of MiFID II and art. 54 (1) of the MiFID II Delegated Regulation[103] require investment firms to undertake a suitability assessment before giving advice to invest. If investment advice or portfolio management is provided through an automated or semi-automated system, the ultimate responsibility for an appropriate suitability assessment lies nonetheless with the investment firm and shall not be delegated to algorithms[104]. The European Securities and Markets Authority (ESMA) has promulgated organizational standards for investment firms assessing suitability with algorithms[105]: These include *inter alia* policies to review and update algorithms to reflect market changes or legislative developments. Moreover, internal procedures should operate to detect error within the algorithms which might generate inappropriate advice or disregard relevant

**97** Financial Industry Regulatory Authority (FINRA), Report on Digital Investment Advice (March 2016) (available at https://www.finra.org/sites/default/files/digital-investment-advice-report.pdf).

**98** See *passim B. Ferguson* (FCA), Robo Advice: an FCA perspective, Speech London 11 October 2017 (available at https://www.fca.org.uk/news/speeches/robo-advice-fca-perspective).

**99** Bank of England/FCA, Machine learning in UK financial services, p. 27 (October 2019, available at https://www.bankofengland.co.uk/-/media/boe/files/report/2019/machine-learning-in-uk-financial-services.pdf?la=en&hash=F8CA6EE7A5A9E0CB182F5D568E033F0EB2D21246).

**100** FCA, Regulatory sandbox lessons learned report (2017, available at https://www.fca.org.uk/publication/research-and-data/regulatory-sandbox-lessons-learned-report.pdf), at para. 4.40., and infra sub 3.1.

**101** Ibid., at para. 4.41.

**102** FINRA, Report (fn. 97).

**103** Delegated Regulation (EU) 2017/65 (fn. 94).

**104** Art. 54 (2) of the MiFID II Delegated Regulation.

**105** ESMA, Guidelines on certain aspects of the MiFID II suitability requirement, at ⁋82 et seq. (06/11/2018/ESMA, available at https://www.esma.europa.eu/sites/default/files/library/esma35-43-1163_guidelines_on_certain_aspects_of_mifid_ii_suitability_requirements_0.pdf).

law[106]. Although ESMA's guidelines constitute the EU's soft law on finance, they enjoy a high degree of compliance[107]. Standard interpretation techniques will have little difficulty in transforming codes of conduct into specific (algorithm-related) duties of care and loyalty[108] under innovative FinTech contracts[109].While it has been suggested that investment firms should not contract out of their liability under the suitability rule[110], the exact legal implications of art. 25 MiFID and the MiFID II Delegated Regulation for national contracts laws remain unclear. The evolutionary potential of contract law, however, still faces its test when it comes to determining what specific rights parties have when they sue an investment firm for breach of contract[111].

## 2.5 Distributed Ledger Technology – FinTech and Private Law at a Juncture

### 2.5.1 Blockchain Law – The Status Quo

Distributed ledger technology and crypto-assets[112] owe their existence to private contracting. Digital tokens on a ledger stand for the commodification of any bundle of rights and obligations for token holders[113]. The contractual origin of digital tokens has also contributed to one of their major weaknesses: The degree of pro-

**106** Ibid.

**107** *Niamh Moloney*, The Age of ESMA – Governing EU Financial Markets, Oxford 2018, p. 145 et seq.

**108** Cf. *Möslein/Lordt*, ZIP 2017, 793, 702, on ‚algorithmic organization duties'.

**109** For an extensive analysis see *Della Negra* (fn. 27), pp. 84 et seq., 177 et seq. This is also the position of Swiss law: *Rolf H. Weber/Rainer Baisch*, Regulierung von Robo-Advice, AJP/PJA 8/2016, 1065, 1071.

**110** *Della Negra* (fn. 27), p. 86.

**111** See the survey in: *Della Negra* (fn. 27), p. 186 et seq.

**112** According to art. 3 (1) (2) of the Draft Regulation on crypto-assets (Proposal for a Regulation on Markets in Crypto-assets, European Commission (Brussels 24 September 2020 (COM(2020) 593 final, available at https://ec.europa.eu/transparency/regdoc/rep/1/2020/EN/COM-2020-593-F1-EN-MAIN-PART-1.PDF)) "'crypto-asset' means a digital representation of value or rights which may be transferred and stored electronically, suing distributed ledger technology or similar technology…".

**113** See *Javier Wenceslao Ibáñez Jiménez*, Derecho de Blockchain y la tecnología de registros distribuidos, 2018, p. 215 et seq.; *Philipp Hacker/Chris Thomale*, Crypto-Securities Regulation: ICO's, Token Sales and Cryptocurrencies under EU Financial Law, ECFR 2018, 645 – 696 (651). On potential benefits of asset tokenisation: OECD, The Tokenisation of Assets and Potential Implications for Financial Markets (2020), p. 38 et seq.

tection afforded to tokens depends on the willingness of a national legal order to confer property-like status with erga-omnes effects on crypto-assets. Failure to attain this status is to magnify financial risks from investing and trading with crypto-assets. In this, distributed ledger technology and crypto-assets are a model case for demonstrating that the success of a market for FinTech products is conditioned on an efficient interface between the evolutionary potential of private law, FinTech regulation[114] and data protection law[115]. In the following, the evolution of blockchain law will be assessed from its private law beginnings to legislative intervention by national legislators and the European Union.

Legal aspects of distributed ledger technology and tokenisation first reached the courts when cybersecurity was ineffectual and large amounts of bitcoins had disappeared from customer accounts, held with virtual currency exchanges[116]. The owners of bitcoins filed claims for damages, arguing that the loss of bitcoins was caused by a breach of duty the exchange owed to its customers[117]. Although investors in bitcoins entrust value to the operator of an exchange or a currency-platform courts are reluctant to impose a fiduciary duty: Significant control over the platform and customer accounts does not establish a custodianship, triggering a fiduciary duty to protect digital value held[118]. Investors suffering losses of bitcoins have a chance of obtaining a judgment for damages only if the operator of the currency platform or exchange had positive knowledge of the risk of impending hacks, but failed to take protective action or to warn customers[119]. In a recent New Zealand case, the High Court accepted a breach of trust claim after cryptocurrencies had disappeared in a computer hack[120]. In a 2019 Singapore case, the court had to assess the repercussions of a computer malfunction which had occurred in a blockchain-based exchange[121]. The court was receptive to causation analysis, but did not impose a fiduciary duty on the developer of the

**114** See *Philipp Paech*, The Governance of Blockchain Financial Network, 80 (6) M.L.R. 1073, p. 1097 et seq. (2017), on third-party effects of blockchain-held assets, regulation and the interface with private law.

**115** See also in this volume the contributions by *Paolo Giudici/Guido Ferrarini* and *Heikki Marjosola*.

**116** See *Peter Susman*, Virtual money in the virtual bank: legal remedies for loss, (2016) Butterworth's J. Int'l Banking & L. 150 – 152.

**117** See Carmel v. Mizuho Bank, Ltd., 2018 WL 6982840 (C.D. Cal., 2018).

**118** Fabian v. Lemahieu, 2019 WL 4918431 (D. Md., 2019).

**119** Asa v. Verizon Communications, Inc., 20127 WL 5894543 (E.D. Tenn., 2017).

**120** Ruscoe v. Cryptopia Ltd., [2020] NZHC 728, accord: *Ken Moon*. New Zealand: Are Cryptocurrencies Property?, CRi 5/2020, 135, 138.

**121** B2C2 v. Quoine Pte. Ltd., [2019] SGHC (I) 03.

software with respect to those who store digital assets on a blockchain[122]. The Singapore case sheds light on the core problem of FinTech networks where elements of services are frequently outsourced. Uncertainty about the scope of liability in the context of blockchain-based storage of digital value and smart contracts just reflects the current uncertainty on how to accommodate artificial intelligence in traditional concepts of the law of contracts and torts[123]. It is equally uncertain whether courts would go as far as stretching traditional concepts without legislative intervention[124].

The current state of liability rules for assets stored in a blockchain has forced investors to emphasise property aspects of digital value stored on a distributed ledger[125]. Unrestrained by the civil law concept of *numerus-clausus* of property law[126], common law jurisdictions have found it less difficult to integrate digital value into law[127]. In 2019, the UK Jurisdiction Taskforce of the LawTech Delivery Panel recognised crypto-assets as property, inter alia, for the purposes of common law and insolvency law[128]. The panel relied on Lord Wilberforce's test in *National Provinvial Bank v. Ainsworth*[129]*:* To qualify as a property right, it has to be "definable, identifiable by third parties, capable in its nature of assumption by third parties, and have some degree of permanence or stability"[130]. The panel

**122** Ibid. See, however, the plea for placing the responsibility on the firms which develop algorithms: *Kirsten Martin*, Ethical Implications and Accountability of Algorithms, 160 J. Bus. Ethics 835 – 860 (p. 844 et seq.) (2019).

**123** See *Gerhard Wagner*, Verantwortlichkeit im Zeichen digitaler Techniken, VersR 2020, 717, 724 et seq.

**124** See *Raina S. Haque et al.*, Blockchain Development and Fiduciary Duty,2 Stanf. J. Blockchain Law & Pol'y 139, 179 et seq. (2019), arguing against a fiduciary duty owed by the operator of the blockchain.

**125** Cf. *Charles Draper*, Unlocking Value In An Insolvent Estate: An Update on Cryptocurrencies (2020) (available at https://www.restructuring-globalview.com/2020/02/unlocking-value-in-an-insolvent-estate-an-update-on-cryptocurrencies/).

**126** *Kelvin FK Low/Eliza Mik*, Pause the Blockchain Revolution, 69 (1) I.C.L.Q. 136, 149 et seq. (2020).

**127** See the US and Canadian cases on recognising digital assets: Fortified Holistic v. Lucic, 71 N.Y.S. 3d 922 (S. Ct. N.Y., 2017) ('intangible property'); Ajemian v. Yahoo!, Inc., 84 N.E. 3d 766 (768 et seq.) (Mass., 2017); Audet v. Fraser, 332 F.R.D. 53 (65 et seq.) (D. Conn., 2019) (Owners of digital assets also qualify as members of a class for the purposes of class action under securities law.); Copytrack v. Wall, 2018 BCSC 1709; Shair.Com Global Digital Services Ltd., 2018 BCSC 1512.

**128** The LawTech Delivery Panel Legal Statement on crypto-assets and smart contracts (UK Jurisdiction Taskforce) (November 2019) (available at https://35z8e83m1ih83drye280o9d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/11/6.6056_JO_Cryptocurrencies_Statement_FINAL_WEB_111119–1.pdf).

**129** National Provincial Bank v Ainsworth [1965] 1 AC 1175 at 1248.

**130** Legal Statement (fn. 128), sub ¶ 39.

then proceeded to reiterating the criteria enounced in *Fairstar Heavy Transport NV v. Adkins*[131]*:* Property rights are characterised by "certainty, exclusivity, control and assignability"[132]. The panel clarifies the notion of exclusivity with respect to the keys which allow for access to the blockchain: Multiple keys for a cryptoasset indicate shared ownership or separated ownership of different functions of the key[133]. However, a key as such is information, but not property[134]. This reflects the position of English law that pure information does not constitute a proprietary interest[135]. Although the panel's statement is not binding on the courts, it has been treated subsequently as an authoritative statement of English law[136]. In *Ruscoe v. Cryptopia Ltd.*, the New Zealand High Court recognised the property quality of digital assets on a blockchain, based on Lord Wilberforce's criteria[137]. The High Court then analysed the nature of the public and private keys. The private key, the court noted, is "like a PIN", protecting the owner from involuntary transfer of his funds[138], but also provides for the tradability of the digital assets[139]. In Australia, cryptocurrency is accepted as security for costs[140].

With the exception of Italy[141], private keys for access to blockchain-stored digital values present a major obstacle to civil law jurisdictions recognising dig-

**131** [2013] EWCA Civ. 886.

**132** Legal Statement (fn. 128), sub ¶ 39.

**133** Ibid., sub ¶ 43 (b).

**134** Ibid., sub ¶ 85 (e).

**135** *Leigh Sagar*, The Digital Estate.,2018, at ¶4 – 01 et seq.

**136** AA v. Persons Unknown, [2019] EWHC 3556 (Comm). See also the 2018 case Vorotnytseva v. Money-4 Ltd. (t/a Nebeus.com), 2018 WL 09909285 (Ch., 2018). It should be noted, though, that the notion of 'property' in an insolvency context might be broader than in a law-of-contracts scenario: cf. *Sagar* (fn. 135), at ¶ 4 – 03 et seq.

**137** [2020] NZHC 728, sub ¶ 112, for an analysis see *Moon* (fn. 120), CRi 5/2020, 135, 137, and *Paolo Giudici*, Insolvenza di un "custodial marketplace" di valute virtuali e tutela dei clienti, Le Società 5/2020, 588, 591.

**138** See [2020] NZHC 728, sub ¶ 111.

**139** *Paul Babie et al.*, Case Note – Cryptocurrencies as Property: *Ruscoe and Moore v. Cryptopia Ltd. (in Liquidation)* [2020] NZHC 728 (2020) (University of Adelaide Research Paper No. 2020 – 33, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3578264& download=yes).

**140** Hague v. Gardiner (No. 2), [2020] NSWDC 23.

**141** Art. 8-ter of the Italian law no. 12/19 of 11 January 2019 (Gazzetta Ufficiale della Repubblica Italiana of 12 February 2019 (anno 160 – Numero 36) recognises the legal enforceability of time stamps on a distributed ledger by establishing an analogy with time stamps within the meaning of art. 41 of Regulation (EU) no. 910/2014 of 23 July 2014, O.J. L 157/73 of 28 August 2014, see also the judgment of 19 December 2018 (Sent. 18/2019) of the Tribunale di Firenze – Sezione Fallimen-

ital values as property and pledging them as collateral[142]. A key stands for the right to exclude others[143]; the 'possession' of the access code demonstrates control over the crypto-asset[144]. A Tokyo District Court declined to confer property status on bitcoins, since the co-existence of several digital items on a blockchain excluded exclusivity required by Japanese property law[145]. The Japanese legislator has since amended the law[146]. In proposing a rudimentary blockchain law the Swiss government observed that private and public keys as well as multi-signature scenarios exclude that digital assets can constitute an insolvency asset[147]. The Swiss legislator has bypassed this obstacle by conferring property status with erga-omnes effect on tokenised rights once they are registered[148]. Thus, under the amended Swiss insolvency law crypto-assets can now be retrieved from the insolvency estate if the insolvent company administered tokenised assets[149]. Liechtenstein's new blockchain law has chosen a similar approach[150]:

---

tare (available at https://www.coinlex.it/wp-content/uploads/2019/01/Sentenza_Fallimento_Bitgrail.pdf); *Giudici* (fn. 137), Le Società 5/2020, 588, 591.

**142** Cf. *Geoffrey Peck*, Practical Law – Security Interests: Bitcoins and Other Cryptocurrency Assets (24 April 2019, available at https://uk.practicallaw.thomsonreuters.com/w-017–6122?originationContext=knowHow&transitionType=KnowHowItem&contextData=(sc.Default)&firstPage=true).

**143** Under art. 5 (2) of Liechtenstein's new blockchain law (fn. 11), ownership of the key to the blockchain system constitutes a rebuttable presumption that the owner is also entitled to conclude transactions over the token. See also on the 'right to exclude' and the 'right to use' in a blockchain, context: *Philipp Paech*, Securities, Intermediation, and the Blockchain – An Inevitable Choice between Liquidity and Legal Certainty, 21 (4) Uniform L. Rev. 612, 628 (2016).

**144** See commentary on art. 11 of the UNCITRAL Model Law on Electronic Transferable Records, Explanatory Note on the Model Law (13 July 2017). (available at http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2017model.html).

**145** District Court, Tokyo, 5 August 2015, (2014 (Wa) 33320) (Japan), Reference number 25541521 (English translation commissioned by the Digital Assets Project Harris Manchester College, Oxford (available at https://www.law.ox.ac.uk/sites/files/oxlaw/mtgox_judgment_final.pdf).

**146** *Ken Kawai/Takeshi Nagase*, The Virtual Currency Regulation Review – Edition 2: Japan (September 2019), The Law Reviews online: The Law Reviews https://thelawreviews.co.uk/edition/the-virtual-currency-regulation-review-edition-2/1197588/japan.

**147** Schweizerische Eidgenossenschaft, Eidgenössisches Finanzdepartment, Bundesgesetz zur Anpassung des Bundesrechts an Anpassungen an Entwicklungen der Technik verteilter elektronischer Register – Erläuternder Bericht zur Vernehmlassungsvorlage (22 March 2019), at ¶ 3.2.1.2. et seq. (available at https://www.newsd.admin.ch/newsd/message/attachments/56192.pdf).

**148** Ibid., at ¶ 3.2.2.

**149** In June 2021, Germany promulgated a new law (Gesetz zur Einführung von elektronischen Wertpapieren, BGBl. 2021 I 1423 [Federal Gazette]), providing for electronic securities (*Wertpapiere*) to be registered in an electronic register. Crypto securities (*Kryptowertpapiere*) may be stored in a decentralised register. In what looks like an overly cautious attempt to catch up with to-

A token is basically a crypto-value with erga-omnes effects and goes well beyond the limitations of utility or security tokens[151]. Liechtenstein's law also refers to (trustee-like) standards of duty and care for those who administer the tokens and hence, the digital assets stored. Luxembourg law classifies security tokens as intermediated securities[152]. French law confers property status on some securities[153]. The new San Marino *Decreto Delegato* on blockchain technology allows for erga-omnes effects of blockchain-stored investment tokens, but treats utility tokens as mere creatures of contract valid only between the issuer and the holder[154]. Common law countries have legislated for recognising financial tokens as assets[155].

---

kenisation rules under Swiss law, German law will confer property law status on these electronic securities by classifying them as a 'thing' under the Civil Code. It should be noted that this law project does not introduce a general recognition of crypto-assets or digital shares. See Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes zur Einführung von elektronischen Wertpapieren (14 December 2020, available at https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RegE_Einfuehrung_elektr_Wertpapiere.pdf;jsessionid=DE28652CC1EB52BA58814BB62453EBB2.1_cid289?__blob=publicationFile&v=3), and *Elena Dubovitskaya*, Gesetzentwurf zur Einführung von elektronischen Wertpapieren; ein zaghafter Schritt nach vorn, 41 Zeitschrift für Wirtschaftsrecht 2551–2561 (2020), Matthias Casper, in: Möslein/Omlor, fn. 2, § 28.

**150** Cf. *Bergt* (fn. 11), p. 86 et seq.

**151** Ibid., pp. 67, 177 et seq.

**152** Art 18bis of the Loi modifiée du 1er août 2001 concernant la circulation des titres, and the report for the Luxembourg parliament: Luxembourg Chambre de Députés, Session ordinaire 2017–2018, Projet de loi no. 7363 (6 November 2018) (available at https://www.chd.lu/wps/PA_RoleDesAffaires/FTSByteServingServletImpl?path=C9D0C9CB5AC1682F8AD1DC36175252FF26530FBAB20F896BDEC2D74A3FBAB31A3C2CAC62A625123D0A0B697273B03BC6$7517CFC69E1CF4D4FAD36945BC69A3E3)

**153** Cf. Ordonnance n° 2016–520 du 28 avril 2016 relative aux bons de caisse (JORF n°0101 of 29 April 2016, mini-bonds), Ordonnance n° 2017–1674 of 8 December 2017 relative à l'utilisation d'un dispositif d'enregistrement électronique partagé pour la représentation et la transmission de titres financiers (JORF n°0287 of 9 December) 2017 (blockchain-based register for financial instruments)

**154** Artt. 8, 9 of the Decreto Delegato no. 86 of 23 May 2019 of the Repubblica di San Marino (available at https://www.consigliograndeegenerale.sm/on-line/home/archivio-leggi-decreti-e-regolamenti/scheda17163166.html).

**155** See the survey in: The Library of Congress, Regulatory Approaches to Crypto-assets in Selected Jurisdictions (April 2019, available at https://www.loc.gov/law/help/crypto-assets/cryptoasset-regulation.pdf).

### 2.5.2 The EU's Regulatory Strategy

The EU Commission's regulatory strategy towards distributed ledger technology is twofold: The Draft Regulation on a pilot regime for market infrastructures based on distributed ledger technology (DLT) aims at establishing efficient secondary markets for security tokens, as the primary market does not develop significantly[156]. The Draft Regulation on markets in crypto-assets is intended to supply harmonised rules for certain types of crypto-assets and related activities and services[157].

The Draft Regulation on a pilot regime for DLT market infrastructures does not purport to replace existing market infrastructures[158]. Instead, it seeks to open up securities settlement processes and central securities depositories for distributed ledger technology[159]. This will also include crypto-assets which can be classified as financial instruments[160]. Both, multilateral trading facilities and central securities depositories operating a securities settlement system may settle payments by accepting *inter alia* commercial bank money in a token-based form or e-money tokens[161]. In prescribing a catalogue of duties to be observed by operators of distributed ledger technology market infrastructures, art. 6 of the Draft Regulation attempts to flesh out the interface between private law and FinTech regulation. It also highlights where national laws will have to evolve to supply an appropriate framework for cross-border DLT market infrastructures. The Draft Regulation assumes that the participants in digitised market infrastructures can freely stipulate the scope of liabilities of the operator and the applicable law. It remains to be seen whether courts will accept such a choice of law clause when a tort law claim will be litigated. Moreover, art. 6 of the Draft Regulation does not address the private law implications of accepting crypto-assets as tradable securities. Member State law still applies for ascertain-

**156** European Commission, Commission Staff Working Document, Impact Assessment Proposal for a Regulation on a pilot regime for market infrastructures based on distributed ledger technology (Brussels 24 September 2020 SWD(2020) 201final). According to art. 2 (2) of the Draft Regulation a digital ledger technology structure consists of a multilateral trading facility or a securities settlement system.

**157** Recital 5 of the Proposal for a Regulation on Markets in Crypto-assets (fn. 112). See *Dirk A. Zetzsche et al.*, The Markets in Crypto-Assets Regulation (MICA) and the EU Digital Finance Strategy, University of Luxembourg Law Working Paper 2020 – 018 (available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3725395#).

**158** Recital 6 of the Draft Regulation on a pilot regime (fn. 156).

**159** See recital 2 and artt. 2 (2), 5 (1) of the Draft Regulation on pilot regime (fn. 156).

**160** Recital 4 of the Draft Regulation on a pilot regime (fn. 156).

**161** Art. 4 (3) lit. f, 5 (5) of the Draft Regulation (fn. 156).

ing the scope of legal protection afforded to a crypto-asset, thus triggering uncertainty and regulatory arbitrage. Art. 5 (2) lit a. of the Draft Regulation may dispense with the requirement to maintain securities accounts within the meaning of art. 2 (28) of Regulation 909/2014[162]. But this does not solve the problem of whether crypto-assets are insolvency-proof or whether settlements involving crypto-assets generate erga-omnes effects with respect to third parties.

The Draft Regulation on a pilot regime expects operators of a DLT market infrastructure to provide appropriate cyber arrangements and to ensure the safekeeping of clients' funds, collateral and crypto-assets[163]. This emphasises a need to determine liability standards owed under private law. If smart contracts produce undesired results, the operator might be tempted to escape liability by pointing to the developer of the software. Moreover, once artificial intelligence malfunctions dramatically[164], the operator could attempt to exonerate himself by arguing that a knowledgeable businessman should be expected not to benefit from obvious problems of the digitised infrastructure[165]. As an aside, the Draft Regulation on a pilot regime may also call for an amendment of national rules of civil procedure so that electronic evidence of digitised settlement processes can be admitted.

The Draft Regulation on markets in crypto-assets takes a functional approach without interfering with the property law systems of the Member States. It focuses on uniform rules for transparency and disclosure requirements for issuing and trading crypto-assets, the oversight over service providers for crypto-assets and issuers of asset-referenced tokens and electronic money tokens, and for consumer protection[166]. It is specifically designed for assets which have not been covered by existing EU rules on financial instruments, and e-money tokens[167]. The Draft Regulation imposes behavioural duties and governance standards on those who issue and store digital assets. A combination is introduced between data protection principles under the GDPR and traditional principal-agent relationships in private law. Whereas the Draft Regulation on crypto-assets replicates the no-fault liability standard of the Draft Regulation on digital operation-

**162** Regulation (EU) 909/2014 of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories, O.J. L 257/1 of 28.8.2014.

**163** Art. 6 (4), (5) of the Draft Regulation (fn. 112).

**164** See the factual setting in B2C2 v. Quoine Pte. Ltd., [2019] SGHC (I) 03.

**165** See the dissenting opinion of *Lord Mance* in the appellate judgment of the Singapore Court of Appeal: *Quoine Pte Ltd v. B2C2 Ltd*, [2020] SGCA(I) 02.

**166** Art. 1 of the Draft Regulation.

**167** Ibid.

al resilience for outsourcing schemes[168], traditional fault standards remain applicable when selecting third-party providers for administering the reserve of assets for asset-referenced tokens[169]. Similar rules apply if asset-referenced tokens are held in custody by different crypto-asset service providers[170]. Recital 58 and art. 63 (1) of the Draft Regulation refer to the "ownership rights" of clients who have stored crypto-assets with a crypto-service provider, and admonishes service providers to safeguard them in the case of an insolvency scenario. This assumes that 'ownership rights' are creditor-proof in insolvency proceedings[171], relegating owners, service providers and creditors to the respective national order to ascertain the scope of rights enjoyed by the holder of crypto-assets[172].

The viability of DLT business models critically depends on their compatibility with data protection law. The EU's General Data Protection Regulation (GDPR)[173] conditions the lawful, fair and transparent processing of data *inter alia* on the data subject's consent or the data controller's duty to comply with a legal obligation[174]. Art. 17 (1) GDPR confers the 'right to be forgotten' on the data subject unless the establishment, exercise or defence of legal claims is predicated on processing (and storing) of data (art. 17 (3) (e) GDPR). In order to strike a balance between data protection and FinTech's interest in blockchain-based transactions it has been suggested that efficient encryption should qualify as a method of erasing data[175]. However, once crypto-assets attain legal status as

**168** See art. 66 of the Draft Regulation.

**169** See art, 30 (5) of the Draft Regulation.

**170** Art. 41 (1) of the Draft Regulation.

**171** This appears to be in accord with the approach by *Aurelia Gurrea-Martínez/Nydia Remolina León*, in: *Chris Brummer* (ed.), Crypto-assets – Legal, Regulatory, and Monetary Perspectives, 2019, 117, 119 et seq., when they discuss initial coin offerings.

**172** In this respect, crypto-assets are different from intermediated securities where no uncertainty about the legal foundations exists. Legal certainty about the scope of enforceable rights emanating from securities is a blockchain context appears to be tacitly assumed by *Eva Micheler/Luc von der Heyde*, Holding, clearing and settling securities through blockchain/distributed ledger technology: creating an efficient system by empowering investors, (2016) Butterworth's J. Int'l Banking & L. 652–656, and *Eva. Micheler*, Custody Chains and Asset Values: Why Contemplating Crypto-Securities Are Worth Contemplating, 74 (3) Cambridge L.J. 505–533 (p. 528 et seq.) (2015) (on liability for the loss of financial instruments).

**173** Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (Data Protection Regulation), O.J. L 119/1 of 4 May 2016.

**174** Art. 5 (1) (a), 6 (a), (c) GDPR.

**175** Expert Group on Regulatory Obstacles to Financial Innovation (fn. 5), p. 85 (Recommendation 25), Study for the European Parliament, Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law?, p. 76 et seq.

property with erga-omnes effects, it could be argued that the controller of the blockchain is under a duty to protect the integrity of the data storage device[176], and hence, the right to erasure does not apply (including insolvency scenarios). Art. 13 (3) GDPR imposes a duty on the data controller to inform the data subject once the solicited data shall be used for another purpose than originally agreed. Although this does not seem to apply to a mere change in the investment strategies in a robo-advice situation, the duty to inform would be triggered if the data controller plans to outsource data processing to a country with uncertain cybersecurity standards[177]. As a corollary, an information duty would arise if a hybrid robo-advice model is replaced by complete machine-based decision-making processes[178]. Art. 82 (1) GDPR provides for compensation from material or non-material damages if the Regulation has been infringed. The courts will have to flesh out which of the obligations under the Regulation are intended to operate as protective devices for the data subjects[179]. Outsourcing models may affect the allocation of responsibilities: If the processing of data is transferred completely to a third party (e. g. a cloud provider), the latter assumes the status (and liabilities) of a data controller[180]. If not, the parties may act as joint controllers (art. 26 GDPR)[181]. Nonetheless, if banks or financial service providers decide to rely on a given (external) infrastructure with distributed ledger technology, they will be classified as data controllers as they determined the specific purpose for processing data[182]. Art. 5 (4) of the Draft Regulation on a pilot regime for DLT market infrastructures[183] demonstrates that the relationship between data protection law and blockchain may have to be recalibrated: It envisages cyber arrangements which combine the integrity and confidentiality of the data stored with their availability and accessibility. It is for such a scenario that the expert group on

(July 2019, available at https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf).

**176** See *Paul Voigt/Axel v.d. Bussche*, The EU General Data Protection Regulations (GDPR) – A Practical Guide, 2017, p. 113.

**177** Cf. *Lorenz Franck*, in: *Peter Gola* (ed.)., DS-GVO (Datenschutz-Grundverordnung VO (EU) 2016/679 – Kommentar (2nd ed. Munich 2018), Art. 13 ¶ 35.

**178** Cf. *Franck*, in: Gola (fn. 177), Art. 13 ¶ 35.

**179** For a broad interpretation of the concept of damage in the context of the GDPR: *Voigt/Bussche* (fn. 176), p. 205.

**180** Ibid., p. 239. See also the concern of the European Commission, Digital Finance Strategy (fn. 28), at # 4.4., about risks arising from techno-financial conglomerates and groups.

**181** This would require a common plan, allocating responsibilities between the parties: cf. Recital 79 of the GDPR and *Carlo Piltz*, in: Gola (fn. 177), Art. 26 ¶ 3.

**182** European Parliament, Blockchain and the General Data Protection Regulation, p. 49.

**183** Fn. 112.

regulatory obstacles to financial innovation calls for rules facilitating data sharing.[184]

### 2.5.3 Cross-Border Aspects

FinTech regulation and private law systems are jurisdiction-bound. Once digital business transcends national borders (or those of the European Union), diverging regulatory standards and private law differences in accommodating network services and artificial intelligence-based solution cause friction. In *Ruscoe v. Cryptopia Ltd.*, the defendant had operated a cryptocurrency exchange from New Zealand, but stored some of the customers' digital currency online on servers, physically located in Phoenix/Arizona (and perhaps also in the Netherlands)[185]. In recognising a property right under New Zealand law, the High Court appears to have assumed that the place of the register for blockchain-recorded transactions (New Zealand) determined the applicable law. However, as soon as the register is distributed across nodes in various jurisdictions it is unclear on which criteria to base a conflict of laws analysis[186].

From a practical perspective, the International Swaps and Derivatives Association (ISDA) has stepped up its efforts to develop a manageable set of rules for digitising trade in derivatives[187]. ISDA's standards for digitised trading with smart contracts and distributed ledger technology reflect an effort to overcome jurisdictional obstacles by private agreement. Due to the complexity of FinTech transactions it would seem that most distributed ledger systems will be permissioned blockchains where access is conditioned about acceptance of the terms of the platform. Thus, choice-of-law clauses do not appear to present a problem even if the servers are not located at the platform's place of business and mandatory laws are observed[188]. Nonetheless, problems of enforcement through

**184** See Recommendation 28 – Data Sharing (fn. 5).

**185** See Ruscoe v. Cryptopia (fn. 120), at ¶ 22 (c) (ii).

**186** ISDA/Linklaters, Whitepaper – Smart Contracts and Distributed Ledger – A Legal Perspective, p. 9 (August 2017, available at https://www.isda.org/a/6EKDE/smart-contracts-and-distributed-ledger-a-legal-perspective.pdf).

**187** See *Christopher D. Clark/Ciaran McGonagle*, Smart Derivatives Contracts: the ISDA Master Agreement and the automation of payments and deliveries (April 2019) (available at https://arxiv.org/pdf/1904.01461.pdf.)

**188** See the private international law analysis by ISDA et al., Private International Law Aspects of Smart Derivatives Utilizing Distributed Ledger Technology, at pp. 9 et seq., 26 et seq. (January 2020, available at https://www.isda.org/2020/01/13/private-international-law-aspects-of-smart-derivatives-contracts-utilizing-distributed-ledger-technology/).

courts are likely to remain. Moreover, tokenisation is likely to cause considerable problems, especially as civil law jurisdictions may find it difficult to accept the property law reasoning adopted by courts of common law countries. Swiss and Liechtenstein laws seem to assume that the place of the electronic register for tokens is controlling, and hence the respective domestic law would apply. The attractiveness of non-EU jurisdictions and Brexit ensure that private international law problems persist. Nonetheless, the EU Commission should strive for private international law rules within the Union[189].

## 3 Sandboxes – A Regulatory Try and Error Mechanism

In FinTech, regulatory sandboxes are commended as innovative solutions for triggering regulatory learning processes[190], sometimes subject to regulatory capture[191] and an absence of transparency[192]. Current practice appears to confirm the criticism that proponents of regulatory sandboxes are suffering from a micro-transactional bias towards assessing FinTech business models[193]. Closer inspection suggests that sandboxes – however unsystematically they are employed – are likely to offer important insights into the interface between FinTech regulation and private law systems. If properly applied, sandboxes might operate as early warning mechanisms where the balance between financial regulation, the commodification of data and private needs to be recalibrated. The following survey focuses on a typology of regulatory sandboxes[194] to explore potential externalities and private law repercussions[195].

**189** See Recommendation 8 on the commercial law for crypto-assets of the Expert Group on Regulatory Obstacles to Financial Innovation (fn. 5).

**190** Cf. on the positive external effects of regulatory sandboxes: *Dirk A. Zetzsche et al.*, Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation, 23 Fordham J. Corp. & Fin. L. 31–103 (78) (2017), *Ringe/Ruof*, Regulating Fintech in the EU: The Case for a Guided Sandbox, 11 European J, Risk Reg. 604, p. 607 et seq. (2020).

**191** *Christopher P. Buttigieg et al.* (fn. 14), p. 464 et seq.

**192** *Zetzsche et al.* (fn. 190), p. 80.

**193** See *Omarova* (fn. 15), p. 110 et seq.

**194** For a global overview: *Robinson et al.*, 9 (1) Comp. & Risk 10–14 (2020); Baker/McKenzie, International Guide to Regulatory FinTech Sandboxes (2018, available at https://www.bakermckenzie.com/en/-/media/files/insight/publications/2018/12/guide_intlguideregulatorysandboxes_dec2018.pdf).

**195** Some Member States of the European Union (EU) argue for a level playing field in order to escape the negative consequences of regulatory competition in FinTech: See on the competitive

## 3.1 The UK Approach – The FCA's Sandbox[196]

The FCA's regulatory sandbox does not dispense with licensing requirements or authorisation processes to gain access to regulated markets[197]. Rather, it provides for a graduation procedure with admitted cohorts of (innovative) firms on their way to the regulated market[198]. After successful application, cohorts of firms are tested in two six-months-periods per year[199]. The FCA's admission procedure is highly selective[200]. In cohort 4, 40 percent of the participants were testing applications of distributed ledger technology[201] (including crypto-assets, cryptoasset-backed securities, tokenised debt and initial coin offerings)[202]. Cohort 5 included decentralised digital platforms using machine learning identity verification and blockchain-based key management, and facilitating securitisation of debt (by

concerns among Member States of the European Union if diverging approaches to innovation exist: ESMA/EBA/EIOPA (fn. 22).

**196** The FCA studies the establishment of a cross-sector sandbox in order to provide a mechanism for innovative business models which come under the remit of several UK regulators: FCA, Call for Input: Cross-Sector Sandbox (May 2019, available at https://www.fca.org.uk/publication/call-for-input/call-for-input-cross-sector-sandbox.pdf).

**197** FCA, Regulatory Sandbox (November 2015, available at https://www.fca.org.uk/publication/research/regulatory-sandbox.pdf), para.1.1.For a survey of the FCA's practice: *Michael Huertas*, The UK's FCA's regulatory 'sandbox': any lessons for the EU?, 33 (2) B.L.R. 50, 51 (2018).

**198** This applies also to firms which would be subject to dual regulation (i. e. capital market law and prudential law requirements). FCA will consult with prudential authorities to obtain a restriction or a rule waiver so that the innovation can be tested properly: FCA, Sandbox (fn. 197), sub para. 3.2, FCA, Regulatory sandbox lessons learned report, at para. 2.1. (2017, available at https://www.fca.org.uk/publication/research-and-data/regulatory-sandbox-lessons-learned-report.pdf).

**199** To be admitted, the applicant company has to demonstrate that it complies with the FCA's eligibility criteria: "carrying out or supporting financial services business in the UK, ...[a]genuinely innovative [project with] ...identifiable consumer benefit, ... the need for sandbox testing ... [and the readiness] ... to test" (FCA, Regulatory Lessons learned (fn. 100), at para. 5.11). The FCA will look for special FinTech competence and financial viability of the applicant firm in the interest of business integrity and customer protection (FCA, ibid.).

**200** For cohort 5, the FCA selected 29 businesses out of 99 applicants (FCA Update 20 May 2019, Regulatory sandbox – cohort 5 (https://www.fca.org.uk/firms/regulatory-sandbox/cohort-5). For cohort 4, the FCA had admitted 29 businesses out of 69 applications (FCA Update 20 February 2019, Regulatory sandbox cohort 4, (available at https://www.fca.org.uk/firms/regulatory-sandbox/regulatory-sandbox-cohort-4-businesses).

**201** FCA Press Release 3 July 2018, FCA reveals the fourth round of successful firms in its regulatory sandbox (available at https://www.fca.org.uk/news/press-releases/fca-reveals-fourth-round-successful-firms-its-regulatory-sandbox). On earlier cohorts see *Huertas* (fn. 197), 33 (2) B.L.R. 50, p. 53 et seq. (2018).

**202** FCA, cohort 4 (fn. 201).

connecting loan issuance to the underlying financial data with the help of distributed ledger technology and artificial intelligence)[203]. The FCA's first review of sandbox activities noted that some of the start-up firms having successfully passed the sandbox test had entered into partnerships with larger financial institutions (including banks and insurance companies)[204].

The FCA's scrutiny focuses on bilateral relationships, although it acknowledges the specific risks of outsourcing activities to third parties[205]. With respect to negative externalities of sandbox projects, the FCA rejects all-inclusive liability for participating businesses[206]: Admission to the sandbox will not be conditioned on an undertaking that any customer loss will be compensated (including investment losses), and the showing that the applicant business had sufficient funds to finance potential compensation payments. The FCA does not think it appropriate to provide for the same degree of legal protection enjoyed by customers who contract with authorised firms. Instead, the FCA's approach is risk-informed, relying on transparency and disclosure: During the sandbox testing phase firms have to develop arrangements for customer protection while the FCA assesses the suitability of such safeguards in view of disclosure to customers and compensation requirements[207]. The FCA's insistence on compensation arrangements is informed by the insights into the economics of deposit insurance which generate ambiguous welfare effects[208]. Insurance schemes at fair rates will increase competition between financial institutions, but financial institutions may still assume too much risk if they compete for customer money in the face of non-internalised social cost of failure[209]. The FCA's policy aims at cost internalisation[210], but it also acknowledges implicitly that English law does not welcome pre-contractual duties of disclosure or specific warning duties flowing

**203** FCA, cohort 5 (fn. 201).

**204** FCA, Regulatory lessons learned (fn. 198), para. 5.7. et seq.

**205** See FCA, Finalised Guidance (FG 16/5), Guidance for firms outsourcing to the 'cloud' and other third-party IT services, p. 5 et seq. (July 2016 (updated September 2019, available at https://www.fca.org.uk/publication/finalised-guidance/fg16-5.pdf).

**206** See Appendix 4 (Customer protection approaches) to FCA, Sandbox (fn. 197).

**207** Ibid.

**208** See *Xavier Vives*, Competition and Stability Banking – The Role of Regulation and Stability in Banking, 2016, p. 107.

**209** Ibid., p. 127.

**210** See FCA, Regulatory lessons learned (fn. 198), p. 4 et seq., where the FCA notes that sandbox testing may facilitate access to finance for innovators while consumer protection safeguards are implemented.

from a general duty of good faith[211]. Under the sandbox scheme, customers are offered speedy relief. The have to use the Financial Services Compensation Scheme (FSCS)[212].

## 3.2 FinTech Regulatory Sandboxes under the Monetary Authority of Singapore

Singapore's 2016 "FinTech Regulatory Sandbox Guidelines"[213] support a principle-based approach for the benefit of "experimentation of a wide range of financial services"[214]. Once admitted to the sandbox, firms will be subject to a risk-based approach which regards externalities of a project as a trade-off for temporary exemptions from statutory requirements[215]. For admission, the applicant firm has to demonstrate that it plans to apply a different technology, or apply the same technology differently. The applicant has to show due diligence, including an assessment that the proposed financial service is commercially viable in Singapore[216]. The evaluation of a sandbox application is conditioned on welfare

**211** See *Stathis Banakas*, Liability for Contractual Negotiations in English Law: Looking for the Litmus Test, 1 InDret 1–21 (2009); for a comparative approach: *Pierre Legrand*, Pre-Contractual Disclosure and Information: English and French Law Compared, 6 (3) Oxf. J. Leg. Stud. 322–352 (1986). This may have pushed the FCA into enquiring whether a statutory duty of care should be introduced: see FCA, A duty of care and potential alternative approaches: summary of responses and next steps (Feedback Statement FS 19/2 (April 2019, available at https://fca.org.uk/publication/feedback/fs19–02.pdf), *Christopher Woolard* (FCA), Regulation in a changing world, Speech 21 October 2019 (available at https://www.fca.org.uk/news/speeches/regulation-changing-world).

**212** *W.-G. Ringe/C. Ruof*, "Regulating Fintech in the EU: the Case for a Guided Sandbox" 11 European J. Risk Reg. (2020), p. 604; FCA, cohort 5 (fn. 201).

**213** Monetary Authority of Singapore, FinTech Regulatory Sandbox Guidelines (November 2016, available at https://www.mas.gov.sg/-/media/MAS/Smart-Financial-Centre/Sandbox/FinTech-Regulatory-Sandbox-Guidelines-19Feb2018.pdf?la=en&hash=B1D36C055AA641F580058339009448CC19A014F7).

**214** Monetary Authority of Singapore, Response to feedback received – FinTech Regulatory Sandbox Guidelines, at para. 2.4. et seq. (November 2016, available at https://www.mas.gov.sg/-/media/MAS/Smart-Financial-Centre/Sandbox/Response-to-Feedback-Received.pdf?la=en&hash=3F35F4C5F1CF0C7EE85D22E62C4C0B28114BF97E). MAS will move from testing to regulation if the risk of new technology becomes material and regulation is proportionate to the new risk: *Pei Sai Fan*, in: *David Lee Kuo Chen/Robert H. Deng (eds.)*, Handbook of Blockchain, Digital Finance, and Inclusion, Vol. 1, 2018), 347, p. 351.

**215** See MAS, Guidelines (fn. 213), paras. 2.1, 5.1. et seq. and Annex A.

**216** Ibid., para. 6.2.

criteria[217]. The proposed financial service should focus on innovation, measured by an enquiry of whether 'comparable offerings' are available on the Singapore market[218]. If preliminary testing reveals risk, a mitigation proposal has to be submitted[219]. Although the MAS undertakes a cost-benefit analysis with respect to risks for customers and the financial system and potential benefits, the guidelines fall short of providing for compensation arrangements. The Guidelines refrain from prescribing behavioural standards which might translate into specific contractual undertakings for the applicant firms. Instead, the MAS favours information over compensation. The applicant firm, the 'sandbox entity' shall inform customers of the sandbox nature of its financial service and emerging risks. The 'sandbox entity' has to demonstrate that customers are aware of these risks[220]. It is unclear whether a failure to seek customer awareness automatically triggers damages or whether it will terminate 'only' the sandbox experiment.

After nine months, the applicant firm will either 'graduate' or lose its temporary authorisation to do business[221]. Contrary to the FCA, the number of positive 'graduation' cases concluded by the MAS is relatively small, but includes several blockchain projects[222]. In its policy statement, the MAS appears to be at much greater ease in granting ease exemptions from specific legal and regulatory requirements than the FCA: "Possible to Relax" requirements include, inter alia, cash balances, fund solvency and capital adequacy, minimum liquid assets and minimum paid-up capital[223]. MAS has released guidelines for robo-advice[224], but maintains that no exemption from its general sandbox approach is intend-

**217** Cf. *Yaru Chia*, Regulating the algorithms of tomorrow's advice in Singapore, 2020 J.B.L. 40, p. 45.

**218** Consumer and industry research may be adduced to establish the problem-solving nature or the benefits of the new product or service: ibid., at para 6.2 (a), (b).

**219** Ibid., at para 6.2 (f).

**220** Ibid., at para. 8.2 (e). In this context, it is unclear whether the MAS is guided by a notion of sophisticated customer-investors, or whether the MAS also envisages consumer-investors in a contractual relationship with the applicant firm.

**221** For a practical example: Blockchain News 9 November 2019, *Daniel Phillips*, Singapore Sandbox Program Adds Third Blockchain Project) (available at https://beincrypto.com/singapore-sandbox-express-program-adds-second-blockchain-project/).

**222** Ibid.

**223** MAS Guidelines (fn. 213), Annex A ("Examples of Flexibility around Regulatory Requirements and Expectations for the Sandbox").

**224** MAS Guidelines on Provision of Digital Advisory Services (October 2018) (available at https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulations-Guidance-and-Licensing/Securities-Futures-and-Fund-Management/Guidelines-on-Provision-of-Digital-Advisory-Services-CMGG02.pdf).

ed[225]. In 2017 MAS initiated a project for studying the use of distributed ledger technology for interbank payments[226].

## 3.3 Testing FinTech Products in Australia

The Australian Securities and Investments Commission (ASIC) relies on statutory exemptions from licensing requirements and adds flexibility in interpreting statutes[227]. Its sandbox policy focuses on four FinTech business models: digital advice, marketplace lending platforms, payment products and digital currency wallets[228]. A FinTech licensing exemption acknowledges the interface between regulation and potential private law claims raised by customer-consumers. Exemptions are conditioned upon appropriate consumer information[229], and caps on the volume of the total business or a maximum value per individual (consumer) transaction[230]. Systemic risk concerns have led ASIC to introduce a limit on total exposure for testing activities per individual project (including wholesale and sophisticated clients)[231].

In order to "reduce the risk of poor consumer outcomes"[232], FinTech companies must disclose to their clients that they are operating without a licence under the licensing exemption scheme, and that normal protections may not necessarily apply[233]. ASIC requires 'adequate compensation arrangements'[234], but at-

**225** *Chia* (fn. 217), p. 45 et seq.

**226** Deloitte/MAS, The future is here – Project Ubin: SGD on Distributed Ledger (2017, available at https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/financial-services/sg-fsi-project-ubin-report.pdf).

**227** See *N. Selvadurai*, 25 (5) C.T.L.R. 141–148 (2019).

**228** Digital currencies are not regulated by the ASIC. Nor does the licensing exemption apply to certain complex financial products.

**229** Retail clients are to be supplied with basic information on the service provider which is reminiscent of a rudimentary prospectus (RG 257.89).

**230** FinTech companies may only test their business project with respect to a limited number of retail clients. The individual exposure of a retail client may only relate to certain (safer) financial products and may not exceed AUS $ 10,000. With respect to testing services for insurance contracts, the sum insured shall not exceed AUS $ 50,000: See RG 257.83 (a): Deposit products, simple managed investment schemes, securities, government bonds and payment products (ASIC Regulatory Guide 257, Testing fintech products and services without holding an AFS or credit licence (August 2017, available at https://download.asic.gov.au/media/4420907/rg257-published-23-august-2017.pdf).

**231** RG 257.84.

**232** RG 257.79.

**233** RG 257.88.

tempts to strike a balance between innovation without barriers and consumer protection against negative externalities. 'Adequate compensation arrangements' are not intended to introduce all-inclusive insurance or a deposit insurance scheme for the testing phase. ASIC favours a professional indemnity insurance[235], which does not extend to product failures, losses from investment or unsatisfactory returns[236]. Instead, professional indemnity insurance operates to supply coverage for financial losses resulting from poor-quality services and misconduct[237]. Disputes are to be settled in specific resolution procedures[238]. Contrary to Singapore's MAS, ASIC does not determine whether the envisaged innovation will advance Australia's competitiveness or generate consumer benefits. ASIC confines itself to "address[ing] the issues faced by new, innovative businesses"[239]. It would seem that ASIC's scrutiny also addresses the applicant's potential for cyber risk management if services are to be outsourced or cloud-based[240]. The applicant firm and the market will have to decide whether the financial service or product is commercially viable[241].

## 3.4 The Swiss Experience

The Swiss sandbox model favours an institutionalist approach over regulating specific business activities[242]. It does not envisage a graduation mechanism.

**234** See RG 257.96. This reflects compensation requirements under RG 126.6 (ASIC Regulatory Guide 126, Compensation and insurance arrangements for AFS licensees (August 2017, available at https://download.asic.gov.au/media/4425351/rg126-published-29-august-2017.pdf).

**235** See RG 257.97 et seq.

**236** RG 257.99.

**237** ASIC insists on minimum coverage requirements per individual claim, and for aggregated claims, and a ‚run-off cover' for 12 months: RG 257.100 et seq.

**238** See RG 165 (Regulatory Guidance 165, Licensing: Internal and external dispute resolution, (May 2018, available at https://download.asic.gov.au/media/4772056/rg165-published-18-june-2018.pdf).

**239** RG 257.55.

**240** See ASIC, Cyber resilience good practices (last update 30 May 2019, available at https://asic.gov.au/regulatory-resources/digital-transformation/cyber-resilience/cyber-resilience-good-practices/).

**241** See, however, the list of financial services benefitting from the exemption from statutory licensing requirements during the sandbox testing phase.

**242** See Schweizerische Eidgenossenschaft – Eidgenössisches Finanzdepartement, Revision der Bankenverordnung (BankV) "FinTech-Bewilligung" – Erläuterungen, paras. 1.3.3, 3.2.1.1. et seq. (30 November 2016, available at https://www.newsd.admin.ch/newsd/message/attachments/54881.pdf).

The Swiss Financial Market Authority (FINMA) issues FinTech licenses to non-bank institutions[243] soliciting deposits from the general public which may not exceed the total of 100 m Swiss Francs[244]. Non-bank financial services include alternative finance (e. g. crowdfunding), money transfer and storage facilities on the basis of blockchain technology, and (algorithm-based) investment advice and asset management[245]. An application for FINMA's licence has to be supported by documentation on the envisaged business model, governance structures, risks management and compliance mechanisms[246].

The FinTech license scheme supplements private law duties of care with statutory disclosure duties[247]: Under art. 7 (a) of the amended Banking Regulation, the non-bank financial service provider has to inform its customers on its business model, the services to be rendered and the risks potentially arising from the underlying technologies. If the business model implies the holding of customer funds, the non-bank financial service provider must hold them separately and safely[248]. Customers have to be alerted that a deposit insurance scheme does not exist. The information has to be conveyed to the customer timely to allow them to make an informed judgment. Since the introduction of the FinTech licence in 2019 FINMA has noticed an increasing demand for information on the regulators' attitude towards business models with distributed ledger technologies and tokenised securities[249]. From a regulatory perspective, transparency and disclosure duties have to compensate for the fact that FINMA does not assess the merits of the business model submitted by the non-bank financial service provider[250]. Nonetheless, FINMA scrutinises crypto-related risks and insists

**243** See FINMA Press Release 15 March 2019, Fintech licence and sandbox: adjustments to FINMA circular (available at https://www.finma.ch/de/news/2019/03/20190315-mm-fintech/).

**244** Art. 1b of the Swiss Banking Law.

**245** Eidgenössisches Finanzdepartment (fn. 32), para. 1.1.

**246** See the list of criteria for assessing the applicant's business standing: FINMA, Mindestgliederung für den Prüfbericht betreffend das Bewilligungsgesuch für ein um Bewilligung ersuchendes Institut – Berichtsvorlage (April 2019).

**247** Crowdlending now comes within the ambit of the law on consumer credits. See artt. 2 and 4 of the Federal on Consumer Credit (Bundesgesetz über den Konsumkredit).

**248** In this context, the Swiss approach towards non-bank FinTech companies taking in customer monies appears to reiterate legislative choices under the E-Money Directive of the European Union.

**249** FINMA, Jahresbericht 2019 (2020), p. 16 et seq. (available at https://www.finma.ch/de/news/2020/04/20200402-mm-finma-gb-2019/). In 2018, FINMA's advice was frequently sought with respect to initial coin offerings and payment tokens: FINMA, Jahresbericht 2018 (2019), p. 30 et seq. (available at https://www.finma.ch/de/news/2019/04/20190404-mm-jmk2019/).

**250** See the explanations on art. 7 (a) of the Banking Regulation by the Eidgenössisches Finanzdepartement (fn. 147), at para. 2.1 (art. 7a).

on governance structures assuring the safe storage of tokens. This scrutiny includes risks (including cyber risks) resulting from outsourcing transactions to third parties[251]. The courts will have to develop standards for allocating risk in such a scenario, including risk warnings which may allow non-bank financial service providers to contain liability.

## 3.5 More Room for Innovation in the Netherlands

The Dutch capital markets authority (AFM) and country's national bank (DNB) focus on innovation in the sandbox industry without announcing an outright departure from existing law or a rule-based approach[252]. Their regulatory sandbox is primarily an instrument for facilitating the exchange of know-how and accommodating innovative practices within the existing framework of rules. Admission to the sandbox is conditioned on corporate governance processes which the applicant financial service company has implemented to protect, inter alia, customer and stakeholder interests[253]. During the testing phase, a financial product will be assessed on its real-world viability. Innovative projects should be advanced by invoking traditional techniques of continental interpretation of statutes, going beyond the very language and exploring the policy thrust of a specific norm[254]. In approaching blockchains, supervisors should resist a "strict application of the law"[255]. With respect to innovative asset management, AFM/DNB are prepared to relax the traditional scrutiny of the initial intake process, if the investment company is "scrupulously observing its duty of care"[256]. This policy tacitly assumes that interpretation of statutes will be able to accommodate the most sophisticated forms of FinTech where artificial intelligence triggers investment processes which are difficult to trace back to human intervention.

**251** FINMA, Jahresbericht 2019 (fn. 249), p. 18.

**252** See the title of the policy statement: AFM/De Nederlandsche Bank (DNB), More room for innovation in the financial sector (December 2016, available at https://www.dnb.nl/en/binaries/More-room-for-innovation-in-the-financial%20sector_tcm47-361364.pdf?2020070217.

**253** Ibid. Dutch law provides for opt-in authorisation mechanisms into financial supervision where a financial service company receives and holds repayable funds, grants credits or invests monies without qualifying as a bank. In the age of financial disruption, the AFM/DNB feel that such financial service companies should prefer the regulatory sandbox mechanism over opt-in authorisation schemes.

**254** See ibid., p. 7.

**255** Ibid.

**256** Ibid., p. 4.

Financial service companies are eligible to the Dutch sandbox scheme if their innovation project supports an objective of the country's financial supervision laws[257]. This includes companies which are encountering legal barriers although their project conforms to the underlying legislative policy[258]. Sandbox supervisors may impose constraints or requests for modifications which may take the shape of a tailored arrangement, a partial authorisation or an exemption from statutory requirements if the law so allows[259]. Moreover, the applicant company may be restricted to offering its services to professional clients only[260].

# 4 Conclusion

FinTech cannot do without private law and private contracting. The success of the EU's Digital Finance Strategy is conditioned on an efficient interface between financial regulation and the evolutionary potential of private law in the face of a principle-based approach of regulators. It is the intention of the EU to enhance global competitiveness in FinTech while maintaining a high degree of investor protection. In asserting its role as a rule-maker, the EU proceeds on two assumptions with respect to competition. As mandatory rules and soft law codes of conduct are promulgated, they are motivated by the belief that this is sufficient to unleash innovation and frictionless private ordering. Conversely, it is tacitly assumed that externalities flowing from this policy choice will be absorbed by private law. This, in turn, will unleash regulatory competition for the best set of private law rules under the legal system of the Member States. Regulatory sandbox models demonstrate that private contracting frequently is ahead of a formal regulatory framework for FinTech. They also favour ex-ante transparency over ex-post liability for innovation.

This article has assessed both the need and potential for a meaningful interface between financial regulation and private law in prominent fields of FinTech. With respect to payment services, outsourcing models, crowdlending, robo-advice and blockchain applications, the EU proceeds with varying degrees of (legislative) intensity. Nonetheless, national private law systems will have to evolve as the enforceability of claims becomes increasingly important: There is a need for re-interpreting contractual duties of care and loyalty in view of the specificities of soft law codes of conduct, algorithmic business models and the digital

**257** AFM/DNB (fn. 252), p. 4.
**258** Ibid.
**259** Ibid., p. 6 et seq.
**260** Ibid.

division of labour in service chains. Any attempt to establish ground rules for the infrastructure of digital markets is predicated on adequate liability rules. The business models surveyed above are exposed to incoherent degrees of liability under finance law and data protection law (including the intricacies of data sharing). This is partly due to practitioners' and legislators' uncertainty about how to incorporate algorithms and artificial intelligence into established concepts of liability. Moreover, the current practice under regulatory sandbox models to combine transparency for customers with insurance requirements strangely focuses on bilateral business relationships. This ignores a more fundamental liability problem which needs to be resolved especially in the context of long outsourcing chains and digital networks. The courts or perhaps, legislators will have to decide whether those who design the organizational structure of a network should also shoulder liability for its malfunctions. This will also require a re-assessment of current burden-of-proof rules.

The EU's Digital Finance Strategy side-steps the private law classification of crypto-assets. The comparison with non-EU jurisdictions demonstrates that crypto-assets need to be afforded erga-omnes status with respect to third-party interventions. This is especially relevant to service chains for digital payments, outsourcing to clouds, DLT-facilitated settlement processes and insolvency scenarios. The dynamic of FinTech has it that the EU's regulatory instruments and Member State private laws are still in a state of flux. This is not due to deliberate regulatory design or legislative bias. But once private law systems will steadily accommodate the impact of practitioners' creativity and regulators' principle-based approach, shortcomings might be expected to emerge with greater clarity: Where Member State diversity becomes a liability, the EU should move to adopting fine-tuned private law rules for digital finance. Private international law rules for FinTech transactions, and the interface between digital finance law and the GDPR merit priority on a future legislative agenda.