decade.[4] The concrete demands that evolving consumer/investor expectations translate into in the financial services field include real-time access to financial information, the faster, more convenient consumption of affordable, user-friendly financial services, the instant processing of basic financial transactions, crucial to the satisfaction of everyday consumer needs (such as low-value, point-of-sale or remote payments), and, more generally, the simplification of personal finance.[5]

The global digitisation and digitalisation trend and the steady rise in consumer demand for innovation in the field of financial services offer new opportunities for consumers, financial service providers and financial regulators alike but, also, pose novel challenges, including legal ones. By way of introduction to this study, the author briefly considers, in the remainder of this chapter, the core promises of digital financial innovation, or 'FinTech', the counter-veiling challenges they come with, and some of FinTech's most probable areas of application in the field of financial services.

§1.01 FINTECH AND ITS PROMISES

As further explained in this study, FinTech's core promise is to reduce or to altogether eliminate some of the inefficiencies surrounding the process of creating/registering, recording and transferring financial assets, including cash and transferable, book-entry securities, paving the way for faster, cheaper and more resilient payments, securities transactions and other, day-to-day exchanges of value.[6] These promises have in recent years attracted considerable attention from leading financial institutions, including the European Central Bank (ECB), the World Bank, the Organisation for Economic Co-operation and Development (OECD), the International Organization of Securities Commissions (IOSCO) and several of the Bank for International Settlements (BIS)-hosted Committees,[7] as well as from several of the world's leading central banks. The

4. *See* indicatively, AT Kearney/Efma, *Going Digital: The Banking Transformation Roadmap*, 2016; PwC, *The New Digital Tipping Point*, 2016; Ernst & Young GCC, *Where Your Customers Want You to Be*, 2015; Deloitte/Visa, Digital Transaction Banking, *Opportunities & Challenges*, 2014.
5. What prompted the creation of the world's first (and, to this date, dominant) virtual currency was the desire to facilitate payments linked to E-commerce, pointing to a clear nexus between prominent aspects of digital financial innovation and the rise in E-commerce (*see* S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, November 2008 (Nakamoto 2008)).
6. For an account of the efficiency improvements of distributed ledger technologies for derivatives post-trading, including swap data reporting, documentation, portfolio reconciliation and portfolio compression, *see* J.E. Cieplak and M. Gill, *How Distributed Ledgers Impact Post-Trade in a Dodd-Frank World*, Coindesk, 9 July 2016.
7. *See*, for instance, CPMI, *Distributed Ledger Technology in Payment, Clearing and Settlement – An Analytical Framework*, February 2017; IOSCO, *Research Report on Financial Technologies (Fintech)*, February 2017 (IOSCO, 2017); ESMA, *The Distributed Ledger Technology Applied to Securities Markets*, Report, February 2017 (ESMA, 2017); A. Pinna and W. Ruttenberg, *Distributed Ledger Technologies in Securities Post-trading: Revolution or Evolution?*, ECB Occasional Paper Series, No. 172, April 2016 (Pinna and Ruttenberg, 2016); D. He, K. Habermeier, R. Leckow, V. Haksar, Y. Almeida, M. Kashima, N. Kyriakos-Saad, H. Oura, S.T. Sedik, N. Stetsenko and C. Verdugo-Yepes, *Virtual Currencies and Beyond: Initial Considerations*, IMF Staff Discussion Note, SDN/16/03, January 2016 (He et al., 2016); ECB, *Virtual Currency Schemes – A Further Analysis*, February 2015; CPMI/BIS, *Digital Currencies*, November 2015 (CPMI, 2015); A. Robleh, J. Barrdear, R. Clews and J. Southgate, *Innovations in Payment Technologies and the Emergence of Digital Currencies*, 54 (3) Bank of England Quarterly Bulletin (2014) (Robleh et al., 2014); CPMI, *Non-banks in Retail Payments*, September 2014; The World Bank, *Innovations in Retail Payment Worldwide*, October 2012; CPSS, *Innovations in Retail Payments*, May 2012 (CPSS, 2012); and S.A. Lumpkin, *Regulatory Issues Related to Financial Innovation*, (2) OECD Financial Market Trends (2009).
8. To take the example of payments, both start-ups and major E-commerce retailers, including *Apple*, *Google*, *PayPal* and *Alibaba*, were, at the time of writing, active in the provision of payment products and services to their customers.
9. Cashaa is one recent example of a distributed ledger technology-powered peer-to-peer cash transfer and exchange (remittances) platform powered by blockchain (*see* https://cashaa.com/).
10. In this regard *see*, generally, G.W. Peters and E. Panayi, 'Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money', in P. Tasca, T. Aste, L. Pelizzon and N. Perony (eds), *Banking Beyond Banks and Money – A Guide to Banking Services in the Twenty-First Century* (Springer, 2016) (Peters and Panayi, 2016), 258-260.

author briefly examines, below, FinTech's core promises for consumers, financial service providers as well as for financial regulators and supervisors.

[A] The Consumer Perspective

The rising public interest in FinTech is largely a byproduct of the promises it holds for retail consumers. From a retail consumer's perspective, FinTech promises to facilitate access to lower-cost, 'disintermediated' financial services, while at the same time encouraging competition, both among 'incumbents' (i.e., established financial service providers) and between incumbents and 'disruptors' (i.e., new entrants).[8] Other perceived retail consumer benefits of financial innovation include *transactional simplicity* and *convenience*: FinTech could facilitate the purchase of goods and services online, the remote transfer of funds and the sending of remittances,[9] consumer access to financial data, 365/24/7, through Internet-enabled smartphones or other portable devices, and the receipt of targeted financial and investment advice, also outside business hours. While none of the above is impossible using the currently available digital technologies and centralised relational databases, the use of cryptographically enabled distributed databases to verify transactions, and to maintain consensus in respect of the existence of certain financial assets and their proprietary status could promote auditability, transparency and accountability and, depending on their design, also compress end-user costs and increase the speed of execution of financial transactions.

[B] The Financial Institutions' and Service Providers' Perspective

FinTech could throw open new opportunities for financial institutions and other established service providers willing to leverage modern technology and mobile connectivity so as to expand their product range and customer base and to reduce their operating costs.[10]

At the time of writing, financial institutions and service providers were still struggling with the financial, reputational and regulatory fallout of the global financial

and economic crisis of 2008-2009, the deepest and longest-lasting economic downturn since the Great Depression of 1929.[11] As of writing, the triple objectives of regaining public trust – severely tarnished on account of the financial and economic crisis – recovering profitability – despite the onerous legacy of asset impairments and write-downs – and keeping pace with the more exacting regulatory environment borne out of the financial crisis still dominated the agendas of many financial service providers and, in particular, banks, across the Western World. The judicious use of FinTech could help banks edge closer to achieving the above objectives. Applied to the provision of financial services, Blockchain,[12] high-speed computing and innovations in machine learning[13] hold the promise of compressing the operating and collateral-management costs of banks and other financial service providers, either by facilitating the automation and optimisation of some of their systems and processes (especially repetitive, low-risk transactions, such as recurring low-value payments but, also, data validation and reconciliation processes) or by helping to streamline their regulatory compliance and reporting procedures. By revolutionising the way in which banks offer payment and other services to their clients, digital innovation has the potential to bring about substantial changes in the traditional, bricks-and-mortar banking services delivery model.[14] No less importantly, FinTech promises to help banks and other financial service providers preserve their customer base and attract new custom, either by offering new, technology-driven financial products (such as personal finance tools[15] and E-wallets[16]) or by enabling customers to access, through mobile connectivity and interactive bank applications, existing financial products and services, including

11. The predicament of banks has aptly been described by a commentator, who has expressed the view that, 'the greatest long-lasting victim of the global financial crisis could be the bank itself' (J. Authers, *Role of Banks Recedes in Wake of Crisis*, Financial Times, 22 June 2014).
12. On Blockchain, *see* the discussion in Chapter 2.
13. Machine learning refers to the use, by computers, of algorithms to dissect large amounts of data and to make real-world predictions, without explicit software pre-programming. Machine learning is one of the paths to artificial intelligence, examples of which include retail purchase prediction engines (such as those operated by on-line retailers), music and film recommendation services (such as those offered by *Netflix*), the fraud detection engines operated by several commercial banks, and, closer to the time of publication of this study, self-driving (or 'smart') cars.
14. While the size of the global banking sector assets has declined since the start of the financial crisis, the drop in the number of bank branches and their employees has not been commensurate (*see* PwC, *That Shrinking Feeling: Tracing the Changing Shape of the European Banking Industry*, February 2015).
15. The reference is to 'money-management' software, through which users can keep track of their account balances and expenses, so as to, *inter alia*, adjust their saving/spending habits, create a budget, monitor compliance with it, and centralise bill-payment. At the time of writing, HSBC and the Bank of America were amongst the first banks to offer this type of personal finance service, with start-ups dominating the field.
16. One of several E-wallet schemes in existence at the time of writing was Barclays Bank's *Pingit*, a mobile app linking the user's mobile telephone number with her current account, to facilitate the making and receipt of payments. To make transfers, users need not know the recipient's account number or sort code, nor do they need to use passwords. At the time of publication, over 2 million customers had reputedly downloaded the *Pingit* app.

savings accounts and term deposits.[17] The straight-through processing of simple banking transactions, the increase in financial service providers' connectivity with customers through mobile functionalities (such as readily accessible mobile banking apps) and the offer of practical customer legitimation and real-time payment solutions (whatever the settlement medium) are only *some* examples of the efficiency gains and operational cost savings that FinTech could facilitate, of the improvements in customer access that it could foster, and of the product, networks and infrastructure innovations that digital technology could usher-in, increasing customer demand for financial and accessory services and, with it, the engagement of financial service providers with digital innovation.

There is, inevitably, something of a paradox in financial intermediaries, including banks, central securities depositories (CSDs) and central clearing counterparties (CCPs), seeking to harvest the benefits of technologies, which, as explained later in this study, have the potential to profoundly affect their business model or to render those very intermediaries obsolete. Two observations are apposite here. The first is that the prospect of the large-scale adoption of FinTech (and, by necessary implication, of the eventual substitution and displacement of established market intermediaries) is, in this author's view, not imminent.[18] Concerns with scalability and legal certainty are bound to delay the pace of the adoption of digital financial innovation, pushing it further into the future, and offering policymakers the margin that is necessary for a thorough assessment of the risks and challenges of FinTech.[19] The second observation is that, vested interest and self-serving considerations aside, there may be compelling public policy reasons for banks and other financial sector entities *not* to yield, too early, to the hype surrounding FinTech: established financial service providers will have to balance the benefits of occupying the digital financial innovation space sooner rather than later against the risks of too premature an adoption of technological financial innovations, before their robustness and practical utility have been established, and before it is clear that there is no material risk, in their context, of applying intrinsically good technologies to bad uses with, as yet, unforeseeable consequences.

17. The challenge for banks will be to go beyond making established banking products or services available in virtual form (a mere technological 'twist' to their existing product range and business models), and to genuinely innovate, emulating E-commerce retailers and technology sector start-ups.
18. At the time of writing, a technology research firm predicted that it would take between 5 and 10 years until the mainstream adoption of FinTech (*see* Gartner Inc., *Hype Cycle for Emerging Technologies*, 2016). In a 2016 joint report, Oliver Wyman and JP Morgan estimated that the widespread use of distributed ledger technologies in capital markets infrastructure was unlikely to occur before 2020-2030 (Oliver Wyman/JP Morgan, *Unlocking Economic Advantage with Blockchain, A Guide for Asset Managers*, 2016). Closer to the time of publication of this study, commentators had expressed the view that, '[T]rue blockchain-led transformation of business and government … is still many years away' (M. Iansiti and K.R. Lakhani, *The Truth About Blockchain*, Harvard Business Review (2017), 119).
19. The latency of Fintech's application to the financial sector, due to concerns with scalability or legal certainty, could, arguably, encourage apathy on the side of traditional financial intermediaries vis-à-vis digital financial innovation, delaying the pace (or, even, negating the prospect) of its eventual large-scale adoption.

[C] The Regulators' and Supervisors' Perspective

FinTech could turn into an unexpected blessing for regulators and supervisors, whose mission includes not only *reining-in* but, also, *promoting* innovation and competition between incumbents and new entrants for the sake of greater market efficiency and broader consumer choice. A few words are apposite on the regulatory interest in FinTech.

The global financial and economic crisis has brought with it a surge in regulation[20] and in the attendant compliance burden (and costs)[21] for financial service providers. FinTech could serve as a potent tool in the hands of regulators and regulated entities alike, helping with the management of heavier regulatory compliance and reporting burdens, post-crisis. Considering that supervision is a data-driven activity, and that, as explained later in this study, digital innovations could facilitate data-recording and sharing, FinTech holds the promise of simplifying the process of the *collection* of supervisory data and of its subsequent *processing* and *verification*; no less importantly, digital innovation could enable financial firms to provide supervisors with real-time access to their books, so that the latter can monitor, at all times, the risks to which financial firms are exposed, facilitating the prompt detection and combating of sources of financial or systemic vulnerability.[22] To the extent that it can facilitate supervisory data collection, promote transparency vis-à-vis supervisors and foster a more 'collaborative' approach to supervision,[23] FinTech could have an invaluable contribution to make, even if only indirectly, to counterparty credit risk transparency and, through it, to the achievement of financial stability.[24]

20. The reference is, in particular, to the European Market Infrastructure Regulation (in the EU), the Dodd-Frank Wall Street Reform and Consumer Protection Act (in the US), and the similarly-inspired legislative reforms introduced in other leading economies, including Canada, Australia, Singapore, Hong Kong and Japan. For an illustrative account of the added regulatory compliance costs brought about by Dodd-Frank, *see* P.J. Wallison, *Is the Dodd-Frank Act Responsible for the Economy's Slow Recovery from the Financial Crisis and the Ensuing Recession?*, Paper prepared for the Ninth Hillsdale College Free Market Forum, 16 October 2015.
21. According to estimates, the anti-money laundering/counter-terrorist financing and know-your-customer compliance costs alone incurred by major financial and capital market participants exceeded $12 billion per annum (Oliver Wyman, *The Capital Markets Industry: The Times They Are-A-Changin*, 2015).
22. 'A nascent idea is that the regulator acts as another node of the network, so it has real-time access to the ledger, either in read-only mode or with more attributions' (J.S. Cermeño, *Blockchain in Financial Services: Regulatory Landscape and Future Challenges for Its Commercial Application*, BBVA Research, Working Paper No 16/20, December 2016 (Cermeño, 2016), 9). On the idea that regulators could participate as one of the nodes in a distributed ledger environment, *see* IOSCO, 2017, 64.
23. It is telling of the interest in the potential of digital innovation to assist supervisors in their work, that a May 2016 Report of the European Parliament's ECON recommended that, 'government agencies and competent authorities that are tasked with analysing large quantities of data' explore the use of real-time distributed ledger technology-driven supervision and reporting tools as part of a RegTech agenda in the financial sector (European Parliament, ECON, *Report on Virtual Currencies*, 2016/2007(INI), 26 May 2016 (European Parliament, 2016), point 13).
24. It has aptly been observed that, 'the financial crisis in 2008 happened due to the lack of transparency surrounding traded positions that impacted trading activity and liquidity', and that 'Distributed ledger technology will bring absolute transparency and more certainty' (*see* German Banking Industry Committee, response to the ESMA Discussion Paper on the Distributed Ledger Technology applied to Securities Markets, June-September 2016 (https://www.esma.europa.eu/press-news/consultations/consultation-distributed-ledger-technology-applied-securities-markets) (ESMA, 2016), response to Q.11). On the financial stability implications of FinTech *see*, generally, FSB, *Financial Stability Implications from FinTech – Supervisory and Regulatory Issues that Merit Authorities' Attention*, 27 June 2017 (FSB, 2017). The conclusion reached by the FSB in its report is that, 'there are currently no compelling financial stability risks from FinTech innovations. The analysis identifies, however, 10 issues that merit authorities' attention, of which three are seen as priorities for international collaboration. Addressing these priority areas is seen as important to promoting financial stability, fostering responsible innovation and preventing any derailment of authorities' efforts to achieve a more inclusive financial system' (FSB, 2017, 1).

§1.02 FINTECH: RISKS AND CHALLENGES

The foregoing discussion suggests that FinTech throws up new possibilities for financial market stakeholders and participants alike, in the form of greater transparency and auditability, procedural simplification and, possibly, cost savings. But, inevitably, as with most forms of untested innovation, there are also countervailing risks to FinTech and unexplored facets to its many promises. Indeed, for all their promises and their transformative potential, technological, financial innovations entail risks and pose challenges for financial service consumers, investors, service providers and supervisors alike, many of which are of a legal nature.[25] These challenges inevitably double as barriers to be overcome before the widespread adoption of digital innovation in the highly regulated financial sector context. To avoid pre-empting the analysis, later in this study, of those very risks, what follows is only a summary account of the broad contours of FinTech's headline challenges and some high-level illustrations thereof.

[A] Headline Consumer and Investor Risks

From a consumer/investor perspective, the flipside to end-user convenience and cost gains generated by FinTech-driven disintermediation[26] comes in the form of concerns with consumer/investor protection, compounded by risks to privacy and data security.

While established financial service providers are regulated and supervised to uphold the financial interests of consumers and public trust in the financial system, the same need not be true of (all) innovators (disruptors), some of whom operate on the fringes of the contemporary legal and supervisory frameworks, either because they are anonymous or harder to pin-down compared to conventional operators (as in the case of distributed ledger technology (DLT) network validators) or because their activities

25. According to the FCA Business Plan for 2016/17, 'Blockchain technology represents an alternative approach to the safe storage of information of value such as trade execution, clearing and settlement and custody. It can provide for secure, transparent and immediate confirmation of information that can then be distributed to all interested parties without the need for a central record-keeping authority. While this new alternative approach has many advantages, it also presents new challenges related to data privacy, defect corrections, and trust in decentralised financial servicing.'
26. The growth of E-commerce looks set to diminish the importance of traditional intermediaries, while the rise of Blockchain, virtual currencies and digital innovation have the potential to foster disintermediation.

do not neatly fit into any of the regulatory perimeter's established categories (as in the case of so-called virtual currency exchanges or digital innovation-driven 'decentralized autonomous organisations' or DAOs).[27] Legal and regular taxonomy considerations aside, the application of digital innovation in the field of financial services is bound to raise a number of consumer protection-related concerns, some more warranted than others, including the lack of depositor protection for the benefit of the holders of virtual currencies,[28] the absence of statutory protections similar to those applicable to the users of mainstream payment instruments, such as credit cards, uncertainty in terms of the precise legal basis of so-called distributed ledgers (*see infra*, Chapter 2), the finality attributes of transactions settled in a distributed ledger environment, and the *locus* of securities 'accounts' in the case of decentralised securities trading platforms (*see infra*, Chapter 6), and concerns with the legal (and, broader, jurisprudential) difficulties raised by the prospect of human agents entering into enforceable consumer 'smart contracts' with computers as counterparties (*see infra*, Chapter 5). Finally, given the fallibility of its underlying technology and the open-source logic of many of its manifestations, digital innovation is bound to give rise to *cyber-security* and privacy/data confidentiality concerns.

[B] Headline Risks for Financial Institutions and Service Providers

Digitisation and modern technology pose a litany of challenges for financial service providers, the severity and near-existential significance of which can hardly be ignored or downplayed.[29]

27. The position of disruptors and the issues to which their activities may give rise are not without parallels to shadow banking and the non-bank entities active in it, which, while engaging in financial intermediation, similarly to banks, are not supervised in the same way as banks, and may have no (direct) access to public sources of liquidity. The shadow-banking sector attracted considerable attention in the wake of the global financial and economic crises, as FinTech has, the run up to the publication of this study. For expressions of the public interest in shadow banking, which could be instructive for the debate on the regulatory approach to FinTech, *see* FSB, *Global Shadow Banking Monitoring Report*, 12 November 2015; Association of German Banks, *Regulation of Shadow Banking*, January 2014; L.E. Kodres, *What Is Shadow Banking?*, 50 (2) IMF Finance & Development (2013); and Z. Pozsar, T. Adrian, A. Ashcraft and H. Boesky, *Shadow Banking*, 19 (2) *Federal Reserve Bank of New York Economic Policy Review* (2013).
28. One may query whether such protection is necessary in the first place, considering that *first*, deposit guarantees are features of *fractional reserve systems*, typical of *fiat* (but not virtual) currencies; *second*, transactions in virtual currencies are to be fully funded upfront (lenders cannot create new funds through accounting/monetary expansion), and *third*, (linked to the preceding points) virtual currencies are not susceptible to bank runs, the avoidance of which is the raison d'être of deposit guarantee schemes.
29. The weight of those challenges should not be exaggerated: established financial institutions enjoy several advantages over the competition, including a relationship of trust with their customers (in an ideal scenario), their large customer base, and the substantial amount of information they have on their customers' spending habits and transactions, which they can capitalise on (for instance, by helping customers decide *what* to purchase, instead of merely helping them pay for it). The emergence of on-line booking sites did not bring about the disappearance of travel agencies, any more than the emergence of on-line real estate rental agencies resulted in the downfall of real estate agents.

Reaping the benefits of FinTech would entail substantial pecuniary outlays[30] for those of the incumbents who choose to move away from legacy systems and invest in digital innovation,[31] as well as added regulatory compliance costs, as financial service providers seek to ensure that their transition to new technologies does not expose them to regulatory non-compliance risks, including in terms anti-money laundering/counter-terrorist financing (AML/CTF), know-your-customer (KYC) rules and regulations, and tax law. Concerns with *regulatory compliance* are bound to exercise the minds of financial institutions and service providers as they position themselves to benefit from the FinTech (r)evolution. By way of example, payment service providers (PSPs) that are keen on digital innovation will need to reflect on how the provision of innovative payment products and services may bring them within the remit of the Second Payment Services Directive (PSD2),[32] the Second Electronic Money Directive (EMD2),[33] and the Fourth Anti-money Laundering Directive (AMLD4)[34] (in the EU), or render them subject to US state laws, such as the Uniform Money Services Act (UMSA),[35] laying down licensing and compliance standards for money transmitters, or the US Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) Money Services Business regulations, and how the operation of digitalised crowdfunding platforms may be appraised from an investment and securities law perspectives.

Financial and legal considerations aside, the proliferation of digital innovation in finance is likely to signal fundamental cultural changes for established financial service providers, as they shift from defending their existing range of products, services, processes and customer relationships, to adjust to constantly evolving customer demands. Changes in the traditional business model of incumbents appear inevitable,

30. For instance, investments in FinTech only in the Asia-Pacific region were thought to have increased from around $880 million in 2014 to nearly $3.5 billion in the first nine months of 2015 (*see* Accenture, *Fintech Investment in Asia-Pacific Set to at Least Quadruple in 2015*).
31. A commentator has incisively observed that, '[B]anks are technology businesses. They exist for two reasons. First, to provide payment services. Secondly, as distribution channels for capital. Both of these are problems which can be solved by technology. Technology is expensive, however' (C. Kerrigan, *The Interpretation of Contracts Relating to Financial Transactions: Postscript*, 11 Butterworths Journal of International Banking and Financial Law (2014) (Kerrigan, 2014), 724). Given the challenging economic environment, one is tempted to argue that, from the perspective of established financial service providers, the digital revolution could hardly have come at a less opportune moment.
32. Directive (EU) 2015/2366 of the European Parliament and of the Council 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, OJ L 337, 23.12.2015.
33. Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC OJ L 267, 10.10.2009.
34. Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, OJ L 141, 5.6.2015.
35. *See* UMSA, sections 201-502.

at a time when financial service providers in general, and banks in particular, are still settling into the post-financial and economic crisis environment, rationalising their operations and trimming-down their business activities.[36] However, with no let-up in the pace of technological change, and with record-low (or, in many jurisdictions, negative) interest rates compressing their profit margins, established financial service providers may have no choice but to engage with FinTech in the hope of automating some of their data-collection and other business processes, sharing information with their peers, creating innovative products, building new customer relations and exploring novel ways through which to manage their regulatory compliance burden. The risk for banks is that new entrants who can exploit novel technologies to deliver innovative services or a superior customer experience will consign banks to the limited role of providing only basic banking services. Considering the pivotal role that banks play in financial intermediation, in the operation of the payment system, and in the transmission of monetary policy, a scenario in which banks would lose their preponderant role in value transfers – if it should ever materialise – would inevitably have far-reaching implications for the very structure and operation of the global financial system, for financial regulation, as well as for the implementation of monetary policy, the magnitude of which can only be the object of speculation at the time of writing.[37] FinTech's potential to change not only the technological underpinnings of contemporary financial markets but, also, their very *architecture* has aptly been hailed as one of the most important implications of its eventual large-scale deployment.[38]

[C] Regulatory Challenges: Highlights

As it will have become apparent from the foregoing, FinTech is also bound to have an impact on regulators and their work, posing a number of regulatory challenges.

36. It is telling of the scale of the challenge for established financial institutions that mergers were under discussion, in 2016, to help banks weather the fallout of the crisis. For instance, reports were rife of a possible merger between Germany's biggest lenders, *Deutsche Bank* and *Commerzbank* (*see* A. Kirchfeld and J.H. Foerster, *Deutsche Bank and Commerzbank Said to Have Held Merger Talks*, Bloomberg, 31 August 2016).
37. Regulatory changes in response to technology-driven market shifts, with an impact on the position of credit institutions, were already occurring at the time of writing. To take the example of retail payments, PSD2, which was due to enter into force in 2018, sought to enable bank customers to use the services of third party providers (referred to, in the Directive, as 'Account Information Service Providers' and 'Payment Initiation Service Providers'). By compelling banks to grant third party providers access to customer accounts through open application programme interfaces, PSD2 could encourage customers to use *Facebook* or *Google* to pay for bills, make other fund transfers, or keep track of their spending, while still maintaining their accounts with a bank. Besides, by allowing third party providers to build their services on top of banks' data and infrastructure, PSD2 could pave the way for them to compete with banks as 'alternatives' for the provision of traditional banking services, depriving banks of some of their business and revenue.
38. *See* D. Mills, K. Wang, B. Malone, A. Ravi, J. Marquardt, C. Chen, A. Badev, T. Brezinski, L. Fahy, K. Liao, V. Kargenian, M. Ellithorpe, W. Ng and M. Baird, *Distributed Ledger Technology in Payments, Clearing and Settlement*, Finance and Economics Discussion Series 2016-095, Board of Governors of the Federal Reserve System (Mills et al., 2016), 4 and 10.

There is hardly a shortage of recent examples drawn from the field of financial services where various forms of 'innovation', from collateralised debt obligations and credit-default swaps to private-label mortgage securities, have caused harm both to the financial system and to the real economy.[39] Data protection and confidentiality, cyber-security, interoperability and settlement finality are only some of the areas of regulatory concern relevant to FinTech. Indeed, the regulatory issues that policymakers would have to grapple with are legion, not least on account of the great diversity of the players active in the FinTech space, the mismatch between the current regulatory framework and the business activities that disruptors look set to engage in, and the sheer pace of technological innovation, which tends to evolve at a faster pace compared to the regulatory responses to it.[40] Regulatory challenges are only accentuated by the potential of digital technology to transform financial services in ways that, as suggested above, are not yet sufficiently well understood by the unavoidable vulnerabilities of the largely untested technologies that underlie some of its potential financial sector-specific applications and by the global reach of digital innovation, which inevitably puts a strain on attempts at efficient regulatory control. What the above also suggests is that the regulatory issues at stake may be hard to tackle nationally, without global coordination and multilateral cooperation.[41]

The preservation of market integrity and public trust in the operation of payment systems, securities settlement systems (SSSs) and financial markets at large are bound to represent regulatory policy priorities, as policymakers seek to make sense of and navigate through FinTech's constantly shifting landscape. The challenge for policymakers and regulators will be to temper the less benevolent aspects of FinTech with targeted, risk-focused regulation, so as to promote innovation and preserve FinTech's potential benefits for financial markets and their participants alike.

§1.03 HEADLINE USE CASES OF FINTECH: AN INTRODUCTION

New, technology-enabled digital innovations promise to radically change the processing and settlement of retail payments, the issuance, clearing and settlement of

39. These and other 'financial innovations' allowed banks (and other lenders) to finance their credit-provision activities through excessive leverage and risk-taking, and paved the way for the financial crisis. The resulting deficit of trust within the interbank market set the scene for the sovereign debt stage of the financial crisis, which destabilised the Euroarea, and which continued to torment its periphery nearly a decade after the outbreak of the European sovereign debt crisis.
40. One of the areas where the gap between FinTech and its regulation is particularly acute is cyber-security. On the impact of concerns with cyber-security on the regulatory debate surrounding FinTech, *see* Chapter 2.
41. Despite the transiting of digital data through several different jurisdictions, and the sheer volume of digital data travelling through cyberspace, there is no coherent body of 'international cyberspace law', and no operationalised mechanism, which regulators and law enforcement authorities could rely on to prevent, detect and punish illegal or otherwise harmful private or state-sanctioned activities in cyberspace. The UN, G7 and the G20 have, in recent years, taken an interest in building a consensus around a workable international cyberspace law regime, which, however, deals more with the state liability aspects of cyberattacks rather than with private activities targeting private interests in foreign jurisdictions.

transferable book-entry securities, and, more generally, the process of storing and validating financial data, transforming the ways in which financial services are delivered, their actual content and the very identity of financial service providers.[42] Building on the foregoing, high-level discussion of FinTech's benefits, this author provides, below, a brief introductory account of some of FinTech's financial sector-specific use cases.[43] Whilst any such account is bound to be speculative, an effort to conceptualise and classify concrete use cases is essential at the present juncture: without clarity on some, at least, of the headline use cases of digital financial innovations, it can be difficult to determine the legal and regulatory issues that their use could give rise to, whether and how to regulate them, and what the appropriate moment may be for their subjection to regulatory scrutiny.

[A] Clearing and Settlement of Payments

The clearing and settlement of payments (whether domestic or international) are amongst FinTech's most promising areas of future application.[44] The cross-border payments system, which consists of an intricate web of (correspondent) bank and non-bank intermediaries involved in the clearing and settlement of international payment transactions, is notoriously 'slow, inconvenient, [and] costly',[45] mostly out of choice than on account of technological constraints, with the latency of the settlement cycle between the issuance, by a payor, of a payment instruction and the final crediting of funds to the payee's account giving rise to counterparty, liquidity and credit risks. The rationale underlying the operation of *decentralised* networks for the transfer of virtual currencies, one of the better-known applications of technological financial innovations, could, if applied to retail (and, possibly, also wholesale, large-value) payment systems, speed up the execution of payments (on account of the involvement, in their processing, of fewer intermediaries), dispense with 'central points of failure' (thanks to its decentralised nature), promote payment network resilience and compress costs.

42. It is trite that the introduction of new technologies may bring about changes in market practices and structures. A financial sector-specific example is that of the introduction of advanced communication and data technologies, which both changed the processes associated with the clearing and settlement of physical stock certificates and paved the way for the dematerialisation and immobilisation of securities.
43. For a more detailed account, *see* J.P. Dwyer and P. Hines, *Beyond the Buzz – Exploring Distributed Ledger Technology Use Cases in Capital Markets and Corporate Banking*, CELENT, August 2016.
44. It is stated, in a 2016 Opinion of the ECB (CON/2016/49, available on the website of the ECB) that, '[T]he ECB recognises that the technological advances relating to the distributed ledger technology underlying alternative means of payment, such as virtual currencies, may have the potential to increase the efficiency, reach and choice of payment and transfer methods. The Union legislative bodies should, however, take care not to appear to promote the use of privately established digital currencies, as such alternative means of payment are neither legally established as currencies, nor do they constitute legal tender issued by central banks and other public authorities' (para. 1.1.2).
45. Federal Reserve System, *Strategies for Improving the U.S. Payment System*, Report, 2015 (Federal Reserve System, 2015), 25, fn. 35. In this regard, *see also* CPMI, *Correspondent Banking*, July 2016.

At the time of writing, a number of FinTech-driven initiatives had been announced to address existing frictions in cross-border payments by, *inter alia*, simplifying and automating international payment processes.[46] Others will no doubt follow making of payments a genuine 'proving ground' for the practical application of digital innovation in a financial sector context. The legal implications of the application of FinTech to the execution of payments (in particular, retail payments) are explored in Chapters 3 and 4, below.

[B] Securities Issuance, Trading and Post-trading

Securities issuance, trading and post-trading could provide another, fertile ground for the application of FinTech. Securities markets can only serve as genuine investment alternatives if they can ensure the safe, swift, uncomplicated and cost-efficient transfer of the financial instruments issued and held in CSDs and SSSs, as well as their pledging, as collateral, for lending operations. Both the cross-border clearing and settlement of transactions over securities, and their pledging, leave much to be expected in terms of efficiency since, 'to settle a transaction in a particular security, both counterparties must have access to [settlement] systems where it is possible to deliver and receive that security'.[47] Without shared access to a common ledger, the parties to a securities transaction cannot ascertain whether the transferor owns the relevant securities so as to legally transfer them. The costs and complications arising from the need to rely on third-party intermediaries for the purpose of facilitating securities transfers are apt to discourage cross-border securities trading or the pledging of securities as collateral. FinTech holds the dual promise of providing the technological underpinning of innovative platforms for securities issuance while, at the same time, improving the efficiency of securities post-trading by, *inter alia*, eliminating the need for trade reconciliation,[48] and facilitating counterparty access to the same digital record of securities transactions and ownership, and to a single, verifiable version of the 'truth', accessible, real-time, without recourse to intermediaries.

The extent to which 'securities' issued on FinTech-driven platforms may be recognised as national law securities, whether or not digital representations of real-world securities can be treated as proof of ownership over them, and the degree and conditions subject to which FinTech can facilitate the simultaneous execution and Delivery versus Payment (DvP) settlement of transactions over securities are examined in detail in Chapter 6.

46. For instance, in June 2016, Santander UK joined forces with *Ripple* to become the first bank in the UK to introduce Blockchain technology for international payments (*see* http://www.santander.com/csgs/Satellite?appID=santander.wc.CFWCSancomQP01&c=GSNoticia&canal=CSCORP&cid=1278712674240&empr=CFWCSancomQP01&leng=en_GB&pagename=CFWCSancomQP01%2FGSNoticia%2FCFQP01_GSNoticiaDetalleMultimedia_PT18).
47. The Giovannini Group, *Cross-Border Clearing and Settlement Arrangements in the European Union*, November 2001, Economic Papers, European Commission, Directorate-General for Economic and Financial Affairs (Giovannini Group, 2001), 8.
48. What renders trade reconciliation indispensable under the current set-up is the lack of other alternatives through which multiple market participants can agree on the status of important transactional data.

contract would be 'written' on a distributed ledger in accordance with a defined protocol (such as Blockchain) its validation and execution would also follow a pattern similar to that of asset transfers performed by the Blockchain protocol. As explained in this chapter, instead of making use of DLTs as a means through which to create an indelible, disintermediated record of *past* transactions (as in the case of the *Bitcoin* Blockchain),[432] smart contracts rely on DLTs to schedule, execute and record transactions based on the occurrence of *future* events. It is their 'forward-looking' and 'customisable' dimension that makes smart contracts stand out in terms of their instrumentalisation of DLTs and Blockchain for the programming of business logic and for the facilitation of contractual-type agreements.

The second remark concerns instant payments. What should be made clear from the outset is that the road to their achievement does not necessarily pass through DLTs. Instant payments are, technologically, already possible, even if the most widely used payment option, across retail payment systems, is the 'slow', low-cost payment option, requiring payment system participants to submit their payment instructions to the system operator for clearing, netting and, finally, for settlement *in batches*.[433] Besides, faster retail payments could be achieved through improvements in the capacity of existing market infrastructures, without the need to resort to technological innovation.[434] Whilst instant payments are not, *stricto sensu*, an example of the application of digital innovation to the delivery of financial services, DLTs, Blockchain and smart contracts, whether or not in conjunction with innovative means of payment (such as virtual currencies), have the potential to dramatically increase the speed of settlement

432. In truth, *bitcoin* transactions are smart contracts and *bitcoin* itself is a programmable money. Indeed, it is conceivable that *bitcoin* could register not only transfers of value but also additional terms and conditions written into the *bitcoin* protocol, becoming part of the value transfer. A commentator has proposed placing *bitcoin* into, and releasing it from, escrow accounts depending on the fulfilment of certain pre-agreed conditions (Kerrigan, 2014, 724), demonstrating that virtual currencies in general, and *bitcoin* in particular, could have contract terms 'added' to them, in line with the wishes of the parties to transactions involving an exchange of virtual currency units.

433. Most payment systems will qualify either as 'net' or as 'gross-settlement' payment systems. Net settlement payment systems (technically known as 'Designated-Time Net Settlement' or 'DTNS' systems) are those where the final settlement of funds occurs on a net basis, at a designated time of the day (typically, end-of-day). The net position of each participating bank corresponds to the value of all the fund-transfers it has received up to the designated, cut-off point in time minus the value of all fund transfers it has sent. Gross-settlement systems are those where the settlement of funds occurs on a gross basis (meaning that payment instructions are processed on a one-by-one basis, without netting), and where final settlement is made on a real-time basis during the day (rather than in batches), to guarantee immediate finality of payments. Retail payment systems tend to be net-settlement systems, whereas large-value payment systems are, increasingly, gross-settlement systems. By achieving finality *earlier*, Real Time Gross Settlement payment systems are deemed to be superior to DTNS systems in terms of settlement risk, despite being typically more costly for users.

434. In particular, instant cashless retail payment solutions could rely on established payment instruments (such as payment cards, credit transfers, direct debits and e-money) denominated in *fiat* money, or on established payment rails (the centralised payment system, such as TARGET2, the coverage of which could be expanded to include retail payments, or individual retail payment systems, such as those operated by banks, card-schemes or single operators, such as PayPal, with the possible addition of a liquidity buffer feature, to cater for the credit risk between the posting of funds and the actual deferred net settlement of payment transactions).

of retail payments, while at the same time reducing their cost, by removing intermediaries, and the delays that their involvement in the payment-processing cycle entails.[435] This is what accounts for the interest, in the latter part of this chapter, in the convergence between DLTs, smart contracts and retail payments and on the legal challenges that DLT-driven faster payments are apt to give rise to.

§5.01 'SMART CONTRACTS': WORKING DEFINITION, LINK TO DLTs AND PRACTICAL EXAMPLES

As a prelude to the examination of the benefits of smart contracts and of the legal issues to which their use would *a priori* give rise, this section considers their *definition* and chart their core financial sector-specific use cases.

[A] Smart Contracts: Working Definition

It is very often the case that the debate on DLTs and their potential applications to financial services involves *some* mention of 'smart contracts'. What this debate lacks is a commonly accepted understanding of the underlying concept: indeed, there are as many definitions of smart contracts as there are commentators, with the differences amongst the proposed definitions pointing to subtle but, often, legally significant differences of perception with regard to the smart contracts phenomenon.[436]

435. It is telling that, while traditional payment rails (such as wire or credit card transfers) can take several hours or days to clear, the median confirmation time for a *Bitcoin* transaction did not exceed 10 minutes in August 2016 (*see* https://blockchain.info/charts).

436. Szabo, who is credited with devising the concept of smart contracts, has defined them as 'a computerized transaction protocol that executes the terms of a contract', adding that '[T]he general objectives of smart contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries' (*see* N. Szabo, *The Idea of Smart Contracts*, 1997 (Szabo 1997)). Pinna and Ruttenberg have defined smart contracts as 'a way of transposing the contractual obligations imposed on users into the digital distributed ledger' (Pinna and Ruttenberg, 2016, 18). Mills et al. have perceived 'smart contracts' as the transposition, in a DLT environment, of conditional contractual obligations, to ensure the automatic execution and recording, within a shared ledger, of predefined actions as soon as a pre-agreed event or events have occurred (Mills et al., 2016, 14). More recently, Lauslahti et al. defined smart contracts as 'digital programs based on a Blockchain consensus architecture that automatically implement their internal logic as certain preconditions are met, and which are also able to prevent unauthorised changes of their internal logic …' (K. Lauslahti, J. Mattila and T. Seppälä, *Smart Contracts – How will Blockchain Technology Affect Contractual Practices?*, ETLA Reports No 68, 9 January 2017 (Lauslahti et al., 2017)), while Koulu has defined smart contracts as 'programmable contractual tools, … contracts embedded in software code' (R. Koulu, *Blockchains and Online Dispute Resolution: Smart Contracts as an Alternative to Enforcement*, 13 (1) *SCRIPTed* (2016) (Koulu, 2016), 53). IOSCO has, for its part, defined smart contracts as '… computer programs written on the distributed ledger. These computer programs are pre-written logic stored in, and executed by the nodes in the DLT. Upon the execution and verification of the actions triggered by the smart contract, the latest state (outcome) associated with the business activities will be recorded and stored in the block' (IOSCO, 2017, 51-52).

Given the lack of a settled, commonly accepted definition and taking into account that smart contracts will typically operate on the basis of conditional statements ('if X then Y, otherwise Z'), which computer code (software) can process and action 'autonomously', i.e., without human intervention, censorship or any other form of third-party interference, it is proposed to define smart contracts as 'contractual-type' arrangements embedded in software, which the latter can validate, execute and record *automatically*, on a DLT platform, as soon as certain pre-programmed conditions, agreed upon by human agents, have been met, based on information fed into the distributed ledger itself or received from a predefined (mostly external) source. From a functional standpoint, what distinguishes a conventional from a smart contract is the potential of the latter, derived from the software in which it is embedded, to automate pre-agreed responses, conditional on the occurrence of specific events, determined *ex ante* by the contractual parties and to update records accordingly, once those events have materialised. The definition, above, is without prejudice to whether smart contracts will necessarily amount to *legally binding* arrangements, a question to be addressed later in this chapter.

The 'canonical real-life example' and 'primitive ancestor' of a smart contract is the 'humble vending machine',[437] which automates the execution of *irrevocable* transactions by dispensing items in return for money. Vending machines only dispense items once the pre-agreed conditions have been fulfilled (once, in other words, a sufficient amount of money has been tendered). Anyone who, wishing to purchase an item, tenders the necessary amount of money can enter into a contract with the machine, with the latter acting as 'contract bearer'. Since both the items for sale and the money received in return for them are securely retained within the vending machine, the latter can effectively protect both against external 'attacks'.

[B] Modus Operandi and Financial Sector-Specific Use Cases of Smart Contracts

In their modern conception, smart contracts will depend, for their operation, on technology similar to the one that underpins *bitcoin* and the Bitcoin network, i.e., a Blockchain or other DLT-based distributed ledger. Smart contracts hosted on a distributed ledger will typically operate on the basis of conditional statements ('if X then Y, otherwise Z'), which computer code (software) can process and action 'autonomously', i.e., without human intervention, censorship or any other form of third party interference, to execute prior agreements, whether in whole or in part.

Financial sector-specific applications of smart contracts could include, by way of example, the processing of electronic payments,[438] the matching of buy-and-sell orders within a securities trading platform and the facilitation of aspects of the clearing and settlement of securities transactions, the automatic execution of obligations built into derivative contracts (e.g., the obligation of a party to make a top-up payment if the

437. Szabo, 1997.
438. Payment transactions the triggering of which turns on an ascertainable event could be pre-programmed and automated through recourse to smart contracts.

value of a reference asset should drop below a certain level), the automatic issuance of margin calls (in the context of repurchase agreements), the facilitation of collateral management,[439] the setting up of escrow arrangements,[440] the automatic substitution of collateral under a lending agreement, the automatic execution of corporate actions (including the payment of dividends, coupons or interest to a shareholder, bondholder or lender, respectively, on a predetermined date),[441] the prioritisation of repayments under a structured note, the trading and settlement of syndicated and other, large collateralised loans within groups of financial institutions, the processing of claims under insurance contracts, the management of loan agreements and the automation of payment functions in fulfilment of a contractual payment obligation.[442] It is also conceivable that smart contracts could find applications in the field of central banking, with an impact on the conduct of monetary policy.[443]

To illustrate, more concretely, the use of smart contracts in a financial sector context, the exercise of stock options is taken as an example. The contracting parties will enter the agreed terms (including the strike price and the option expiration date) into the DLT platform where the smart contract is to be hosted, executed and recorded. The software in which the smart contract is embedded would each time validate whether the option is 'in the money' (i.e., whether it is worth exercising from the option holder's perspective) and, depending on the outcome of the validation process, it will either exercise the option (by debiting the option holder's account with the agreed strike price) or allow it to expire. The value of the underlying stock would typically be derived from an external source, agreed upon by the contracting parties, and fed into the smart contract's software, to enable it to conduct the validation necessary for the exercise (or otherwise) of the option.

439. The reference is, for instance, to the exchange of ownership interests over collateral upon the default of a party to a collateralised financial arrangement.
440. The reference is, for instance, to the release of funds from a dedicated account once the contractually agreed conditions have been fulfilled.
441. The debt-issuing company would specify the parameters of the contract, such as its par value, tenor and coupon payment structure. Once assigned to an owner, the smart contract would automatically make the required coupon payments until the bond reaches maturity.
442. If stored as smart contracts in a Blockchain or another DLT-operated platform, mortgage loans could be managed so that if the borrower were to default on a payment, the smart contract could automatically revoke his access to, and use of, the mortgaged property.
443. Milton Friedman famously argued that, 'we could replace the Federal Reserve System by a computer, and have a computer calculate month by month how much currency has to be printed in order to achieve a steady rate of growth in the quantity of high powered money over time' (M. Friedman, *Do We Need Central Banks?* in *Monetary Management in Hong Kong*, Proceedings of the Seminar on Monetary Management organised by the Hong Kong Monetary Authority on 18-19 October 1993). One could, therefore, imagine a scenario where all economic data on the basis of which a central bank determines inflation, would be stored and processed in a ledger; smart contracts could, then, be written into the ledger's software, to ensure that, depending on the economic aggregates, interest rates can be adjusted, automatically, upwards or downwards, with liquidity being simultaneously provided to counterparties or absorbed from the market, depending on the shift in interest rates. While arguably far-fetched, the above demonstrates some of the transformative potential of smart contracts executed in a DLT environment, and the ability of ledgers, in combination with smart contracts, to facilitate a certain measure of automation in the definition and implementation of monetary policy.

The connecting thread that runs through the above-mentioned examples of the use of smart contracts in transactions over financial assets is that they all involve a *programmable movement of value* (money or money's worth) from the account of one contracting party to the account of another: transfers of value triggered by ascertainable events are, by nature, pre-programmable and capable of automation. Subject to the limitations of artificial intelligence,[444] smart contracts could, with time, see their use cases expand to other, more complex financial transactions, with smart contracts running on DLT platforms being used to implement a broad range of transactions, and to record changes in ownership, which the parties have agreed as being the legal consequence of the fulfilment of a predetermined condition, from the very simple (for instance, the execution of a payment and/or the delivery of goods, the payment of insurance policy monies to their beneficiaries or the crediting of dividend/coupon payments to the holders of shares or bonds) to the more complex.

The creation and administration of DAOs is yet another, more complex, application of the use of smart contracts in combination with DLTs. DAOs can be defined as innovative, software-controlled unincorporated associations, akin to partnerships or joint ventures (but, crucially, devoid of legal personality), the aim of which is to pool their investor-members' financial resources (in the form of *Ether*)[445] towards the achievement of a common business objective. Sets of rules encoded as DLT-embedded smart contracts and executed upon fulfilment of predefined trigger conditions – hence, free of human intervention – can be instrumental in facilitating the running of these organisations, for instance by enforcing the collective decisions of the community of members of a DAO, without the involvement of fund managers.[446] At the time of writing, the most prominent example of the DAO concept was *The DAO*, explored in more detail later in this chapter: *The DAO* illustrates the legal uncertainties surrounding this type of smart contract-enabled innovative association, as well as the interaction between the computer code (i.e., the software) in which a smart contract is written and the legal system of a jurisdiction external to (but relevant to the operation of) a DAO. Suffice it to note here that, at the time of writing, there was no settled legal view in terms of the precise company law status of DAOs, the law or laws subject to which they

444. While smart contracts do not depend, for their operation, on artificial intelligence, developments in artificial intelligence could see smart contracts 'interact', more autonomously, with the outside world (for instance, to judge the quality of the work of an employee, so as to effect or release a bonus payment, or to assess whether goods delivered from a seller to a buyer were of 'satisfactory quality').

445. 'DAOs are funded by members using Ether and will usually provide its members with tokens, proportional to their investment, representing voting and ownership rights. DAO tokens are freely transferable and their price may vary over time, in a manner not dissimilar to company shares' (Allen & Overy LLP, *Decentralized Autonomous Organizations*, 2016 (Allen & Overy, 2016), 3).

446. Capital allocation decisions are made by the anonymous stakeholders themselves, who can vote directly on any major decision to allocate the DAO's funds. Companies or individuals who want to tap the crowdfunding-raised funds are to submit a proposal; proposals are published online, with stakeholders voting which proposals to adopt, and what share of the total funds to allocate to each of them.

may operate, or whether their investor-members could be liable, as shareholders, for any debts incurred (or any damages caused) by a DAO.[447]

The most notable practical example, to date, of the convergence between DLTs and smart contracts is the decentralised platform operated by the *Ethereum Foundation*, a Swiss non-profit organisation, crowdfunded in 2014.[448] In common with *Bitcoin*, *Ethereum* is a distributed network composed of thousands of nodes running the *Ethereum* Blockchain-type software. However, unlike *Bitcoin*, which exists to record, in its distributed ledger, the creation and transfer of *bitcoin*, *Ethereum* not only records the creation and transfer of *Ether* (its native virtual currency, the first ever with in-built, general-purpose smart contract execution capability) but also runs smart contract applications on a customised Blockchain, serving as a shared global infrastructure that can simultaneously represent ownership in assets, and which platform participants (nodes) can use to 'create' markets, store logs of debts or promises, and move funds or other value in accordance with predetermined instructions, free of human intermediation. It follows that, although inspired by *Bitcoin*, *Ethereum* marks an improvement upon *Bitcoin's* functionally limited scope through its smart contract capabilities, which allow agreements to be written in code and to be executed automatically through its network of multiple participants.

§5.02 BENEFITS OF DLT-ENABLED SMART CONTRACTS

Smart contracts, within the meaning of the definition proposed earlier in this chapter, have been possible for as long as computers have existed. What is genuinely novel about DLT-enabled smart contracts is the programmable use that they make of DLTs and Blockchain, and the benefits that this particular feature of theirs is likely to come with for financial market actors, in terms of *certainty of execution of contractual agreements*, *immutability/censorship resistance* and *cost savings*. The core benefits of DLT-enabled smart contracts are briefly examined below.[449]

As explained earlier in this study, distributed ledgers are, in principle, more secure and less error prone compared to conventional, centralised ledgers, on account of their shared nature, and the absence, in their case, of the need for data reconciliation. In a Blockchain or other DLT environment, automated (or automatable) contracts for the transfer of assets or value could provide contracting parties with a greater degree of certainty in terms of the performance of their predetermined contractual obligations, in accordance with the terms stored in their software. In the same way that they can ensure the validity of ledger updates, DLTs can also cater for the faithful

447. For instance, it has been argued that '[I]f "management" of an organization is conducted automatically by code, legal systems will have to determine who to hold accountable if laws are broken and disputes arise. The legal frameworks around corporations and other business associations would have to adapt to the concept of distributed management' (Mills et al., 2016, 29).

448. For an account of the Ethereum Blockchain-based platform, *see* V. Buterin, *A Next-Generation Smart Contract and Decentralized Application Platform, Ethereum*, White Paper, 2013.

449. For a more detailed account of the benefits of smart contracts, *see* A. Wright and P. De Filippi, 2015, 24-29.

execution of smart contracts, free from external tampering, generating an environment of commercial trust in which perfect strangers can trade with one another without the need for a trusted intermediary or another comparable gatekeeper to assume responsibility for contract execution. Financial transactions aside, DLT-based smart contracts could be used to facilitate the conduct of fully disintermediated E-commerce transactions, free of intermediaries such as e-commerce sites, payment-processing companies and, ultimately, courts or other external adjudicative mechanisms.

The substitution of trust in intermediaries with trust in computer code, as part of the contract-creation process, is not the only benefit of DLT-run smart contracts. The automated nature of such smart contracts can narrow down (or altogether eliminate) the scope for human error (except in the design of the computer code itself), while at the same time being conducive to the formation of contracts that are virtually unbreakable (meaning that none of the parties thereto can invoke duress, unconscionability or coercion in their formation, so as to deprive them of legal effect). Equally important, the automated nature of smart contracts can drastically remove the costs (and the inconvenience) inherent in the exchange of paper-based contractual documentation, while at the same time facilitating the process of the execution of contractual transactions.

In a nutshell, DLT-embedded smart contracts hold a number of tantalising promises. The *first* is to facilitate the formation of contractual transactions that are incorruptible and tamper-proof, thereby shielding their parties from the consequences of undesirable, malevolent external interference; the *second* is to provide a reliable record of the entire transacting history between contracting parties; the *third* is to automate buy, sell and supply transactions; and the *fourth* is to decrease the marginal cost of contracting by, *inter alia*, disposing with time-consuming and resource-intensive formalities for the formation of contracts, promoting standardisation in the contract-formation process, and removing the ambiguities often built into contractual agreements drafted in natural, rather than in computer language, as well as the need for lawyers to interpret them.

Without prejudice to the foregoing, smart contracts also raise a number of legal challenges and practical questions, addressed in more detail later in this chapter.

§5.03 LEGAL NATURE OF SMART CONTRACTS

As the reader will have appreciated from the foregoing discussion, smart contracts are computer codes that allow agreements to execute themselves once certain real-life conditions have been met. By emulating the logic of contractual agreements, smart contracts hold the promise of *complementing* or, *in extremis*, *displacing* conventional contracts. Is this to say that smart contracts qualify, legally, as contracts in their own right, in the sense that they can be the source of rights and obligations for the parties to them? This core question is examined in the remainder of this section.

[A] Introductory Remarks

It has been argued that the term 'smart contracts' is a double misnomer: the arrangements brought under their umbrella are neither 'smart' nor binding, in the strict legal sense of the term.[450] Indeed, it can be asserted that to the extent that the formation, execution and recording of a smart contract is triggered by the fulfilment of a pre-agreed and pre-programmed condition or the occurrence of a contractually relevant, ascertainable event, rather than by a genuinely autonomous, own-initiative 'decision' of the software in which a smart contract is embedded, the latter cannot meaningfully be termed 'smart'. Moreover, to the extent that certain smart contracts exist to implement other, *existing* contracts (rather than mere framework agreements), they cannot *sensu stricto* qualify as contracts in their own right but, rather, as settlement mechanisms or follow-up, accessory arrangements, the function of which is to merely implement *prior* contractual agreements, or, alternatively, as *mere evidence* of a contract, the full terms of which may (or may not) be ascertainable on the basis of their software. The legal implication of the foregoing observations is that smart contracts would only be legally binding on their parties if their execution were to in no way contradict a prior contractual arrangement between the parties nor any mandatory public law provisions applicable thereto at the time of their 'formation', and if their terms were complete and ascertainable on the basis of their software. What this, in turn, entails is that computer code will not invariably be 'law', meaning that the software in which a smart contract is embedded cannot (always) be the source of legally binding obligations. How warranted are the above conclusions?

Three introductory observations are in order before it is attempted to provide the elements of an answer to the above core question. A *first* observation is that the moniker 'smart contract' need not be conclusive in terms of the legal characteristics of the underlying phenomenon: the appropriate frame of reference is that of national contract law, as interpreted and applied by domestic courts, rather than the nomenclature opted by the creators and advocates of smart contracts. A *second* related observation is that much will turn on the features of a particular smart contract (which may incorporate, by reference, the terms of another, conventional contract), as well as on national law prescriptions in the jurisdiction where the question arises:[451] smart contracts will differ from one another, and the same is true of national contract law, which need not necessarily accommodate them.[452] The final observation is that, despite the challenges it poses, the question of the exact legal status of smart contracts

450. C. Lim, T.J. Saw and C. Sargeant, *Smart Contracts: Bridging the Gap Between Expectation and Reality*, 11 July 2016, Oxford Business Law Blog (Lim et al., 2016).

451. For an account of the main parameters of an answer to this question, in a number of leading jurisdictions, *see* R3/Norton Rose Fulbright, *Can Smart Contracts Be Legally Binding Contracts?*, White Paper, 2016 (R3/Norton Rose Fulbright, 2016).

452. One notable example of a jurisdiction that had explicitly addressed, at the time of writing, some of the legal enforceability issues associated with the use of smart contracts and signatures ensured through Blockchain technology was the US State of Arizona, which, in March 2017, enacted dedicated legislation, with a focus on the recognition of the validity of transactions relating to the sale of goods, leases, and titles. The US States of Delaware and Vermont had earlier passed legislation recognising Blockchain technology under state corporate law, and

merits an answer – even if, for the reasons explained here, this can only be a general one – given the seminal role that contracts and contract law play in the organisation of economic relations in contemporary societies: whatever the appetite for innovation, and notwithstanding the malleability and adaptability of contract law,[453] there is bound to be a measure of scepticism vis-à-vis innovations that purport to improve on or, *a fortiori*, to altogether dispense with the need for conventional contracts and, by implication, with the time-honoured legal safeguards and protections that conventional contracts provide to their contracting parties.

[B] Smart Contracts and the 'Code Is Law' Doctrine

In a seminal 1999 publication, the view was advanced that computer code operates *outside* the legal framework, and that 'Code is law',[454] in the sense that computer code provides the normative underpinning of cyberspace, which conventional legal frameworks cannot meaningfully be expected to regulate. Applied to smart contracts (a phenomenon that had yet to manifest itself at the time when the 'Code is law' thesis was propounded), the foregoing doctrine would militate in favour of the conclusion that whenever computer code is implemented through a network of computers running on a decentralised platform, it is the computer code alone that carries legal weight, as the code in question 'resides nowhere and everywhere'.[455]

In spite of its common sense attraction, and the insights that it provides on the intersection between law and technology (in particular, on the potential of technology to challenge the foundations of the modern commercial legal order), it is submitted that the 'Code is law' doctrine places the very concept of smart contracts under severe stress, for three reasons no less. The *first* is that it misrepresents the limitations of computer code and, in particular, the degree of difficulty inherent in transposing *legal* into *technical* rules: simple, unambiguous legal rules may well lend themselves to encoding, but the same need not be true of more complex, less straightforward ones, the application of which may involve an element of interpretation, discretion or appreciation, rendering the task of their implementation into code something of a challenge.[456] The *second* is that it glosses over the continuing (indeed, overarching)

making it possible for Blockchain-generated digital records to be adduced as evidence admissible before a court of law.

453. *See* E. Mik, 'Formation Online', in M. Furmston and G.J. Tolhurst (eds), *Contract Formation: Law and Practice* (OUP 2010), 159.
454. '… [i]n cyberspace, we must understand how code regulates … *Code is law*' (L. Lessig, *Code and Other Laws of the Cyberspace* (Basic Books 1999), 89). Another scholar had earlier referred to this incipient body of rules as 'Lex Informatica' (J.R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 (3) Texas Law Review (1998)).
455. P. Vigna and M.J. Casey, *The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order* (St. Martin's Press 2015), 66.
456. 'Yet, the practice of transposing legal rules into technical rules is not an easy task. As opposed to legal rules, written as general rules in a natural language that is inherently ambiguous, technical rules can only be implemented into code, and thus necessarily rely on formal algorithms and mathematical models. Regulation by code is therefore always more specific and less flexible than the legal provisions it purports to implement' (P. De Filippi and S. Hassan,

relevance of external legal rules in the regulation of human behaviour in cyberspace: despite the libertarian exuberance inspired by the advent of the Internet,[457] traditional legal concepts of property, contract and criminal law continue to play a dominant role in the regulation of the online activities of human agents in cyberspace,[458] and they are likely to continue doing so, for the foreseeable future, refuting the thesis that cyberspace operates in a legal vacuum or that smart contracts are, effectively, jurisdiction-free arrangements.[459] A *third* reason (and, perhaps, the most powerful objection to the application of the 'Code is law' doctrine to smart contracts) is the following: to accept that the 'Code is law' is to *ipso facto* accept that the parties to an automated contract are to invariably be bound by the consequences of its digital execution, courtesy of its computer code, without any possibility of judicial review, even when the computer code in question has 'malfunctioned', whether on account of a bug or due to an original technical design fault, or has been hacked into by intruders or malicious users, or has otherwise led to manifestly unintended results, not foreseen by the parties to a commercial transaction at the time of the drawing up of the relevant computer code, and which are contrary to their interests. Code correctness is, in other words, something that the 'Code is law' doctrine merely postulates, without regard to the concrete consequences of the counterfactual scenario. In this regard, the precedent of the 'attack' on *The DAO* is highly instructive.[460]

The DAO was launched on the *Ethereum* Blockchain as a decentralised, computer-operated crowdfunding and capital-management platform, intended to operate *without* a fund manager. *The DAO* was to allocate funds collected from its users, i.e., its investor-members (in the form of *Ether*) to third-party projects, in line with the wishes of its investor-members, similar to a venture capital fund. The voting rights of the users of *The DAO* (which reflected the amount of *Ether* that users had pledged in exchange for tokens)[461] were governed by its computer code, with 'curators' (permissioned users) selecting projects for funding and putting them up for a vote.[462] On 17 June 2016, an unknown user exploited a loophole (or a weakness) in the computer code of *The DAO* to drain from it an estimated 3.6 million of *Ether* (or one-third of the

Blockchain Technology as a Regulatory Technology: From Code Is Law to Law Is Code, 21 (12) First Monday (2016) (De Filippi and Hassan, 2016)).

457. *See*, for instance, J.P. Barlow, *A Declaration of the Independence of Cyberspace*, 1996; and D. Bradbury, *Is Bitcoin a Digital Currency or a Virtual One?*, CoinDesk.com, 19 March, 2014.
458. The adoption of entire rafts of legislation not only on both sides of the Atlantic but also globally, at around the time when the Internet went mainstream (such as, for instance, the E-Commerce Directive in the EU, the Digital Millennium Copyright Act in the US, and the Anti-counterfeiting Trade Agreement) testify to the predominant role of the law in regulating human activities carried out through use of modern communication technologies.
459. *See* M.S. Miller, T. Van Cutsem and B. Tulloh, 'Distributed Electronic Rights in Java Script', in M. Felleisen and P. Gardner (eds), *Programming Languages and Systems* (Proceedings of the 22nd European Symposium on Programming ESOP 2013, held as part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2013, Rome, Italy, March 2013, Springer).
460. For an account of the attack on *The Dao*, *see* A. Kraińska, *What the History of The DAO Says About the Law, in Blockchain, Smart Contracts and DAO* (Wardyński & Partners, 2016), 25-28.
461. Investors paid in *Ether* and, in return, they received tokens, which entitled them to vote on how the funds accumulated by *The Dao* should be invested.
462. Mills et al., 2016, 29, fn. 41.

net worth of *The DAO*, at the material time), which he abusively channelled into a 'child DAO', for a project he had proposed.[463] Some members of *The DAO* argued in favour of a 'hard fork' (effectively, a change in *Ethereum's* protocol), so as to reverse transactions in each block, and refund the misdirected *Ether*; whereas other users opposed this solution, as it would contradict *Ethereum's* credentials as an immutable record of past transactions, and violate the irreversibility of its code.[464] Was the 'attack' on *The DAO* a hacking incident or was it, instead, an illustration of a programming feature of a computer code producing effects that were at odds with the contracting parties' intentions?

Far from implementing the presumed contractual agreement that bound together the users of *The DAO*, its software had worked in ways that *contradicted* that agreement. Interestingly, the contract between *Slock.it*, the entity behind *The DAO*, and its user community stated that:

> [A]lthough the word 'contract' is used in The DAO's code, the term is a programming convention and is not being used as a legal term of art. The term is a programming convention, not a representation that the code is in and of itself a legally binding and enforceable contract. If you have questions about legal enforceability, consult with legal counsel.

The above statement would appear to suggest, on the one hand, that the smart contracts built into *The DAO* were never intended to qualify as binding contracts in their own right, to the extent that they were unsupported by conventional contractual documentation between the parties, allowing their genuine intentions to be surmised, and, on the other, that, if in doubt, it is the law of contract, and any conventional contractual documentation between the parties, that was intended to prevail over the computer code. While the foregoing, case-specific conclusion need not be decisive as to the connotation attaching to the term 'contract', as applied to *other* smart contracts, it does question the extent to which smart contracts are to always be perceived as stand-alone agreements, in the context of which computer code is the only arbiter of the agreement it represents, or instead, as digital versions of conventional contracts, actual or implied, or, worse, as mere automated settlement tools operating in a DLT environment.

It has been argued that the 'attack' on *The DAO* 'demonstrates the risk of disintermediation of financial services intermediaries that can result from DLT deployment', as well as 'the risk of flaws in smart contract coding, [and] questions about the application of the law to smart contracts'.[465] Perhaps more importantly, what the 'attack' on *The DAO* shows is that, conceptual considerations aside, and as a matter of public policy, there is no obvious interest in treating computer code as law, at least in

463. The computer code weakness in question allowed the exploiter of *The DAO* ('Exploiter') to circumvent its code (rather than to hack into it) and be paid extra amounts of Ether held by the DAO when executing so-called split proposals (the reference is to a process through which anyone who does not agree with a proposal can take her tokens and, with them, her investments into a new 'child' DAO, operating under the Exploiter's control).
464. Allen & Overy, 2016, 4-5.
465. IOSCO, 2017, 58.

the case of smart contracts: if the 'Code is law' doctrine were to be accepted here, acts similar to those perpetrated in the case of *The DAO* would not fall to be treated as instances of abuse but, instead, as rightful actions, and as non-actionable incidents of the exploitation of particular features of a smart contract's computer code, to the actor's advantage. This outcome would be manifestly absurd, both because it would leave no room to interpret the genuine intentions of the parties to an electronic contract, however obvious these may be, and to deduce their presumed shared understanding of its conditions, and because it would exclude all scope for remedial action, aimed at reversing the real-world consequences of the operation of computer code.[466] Conventional contracts that prove 'defective' can be amended, whether at the instance of the parties, or by operation of law: it is not readily obvious why smart contracts should be treated any differently.

If, in the context of smart contracts, computer code cannot (or should not) be law, is this to say that law itself cannot be transformed into computer code (or, even, drafted in computer code, to start with)? Taking a step back, it is acknowledged that most law is *human* code: its aim is to prescriptively codify human behaviour into socially or privately acceptable behavioural patterns and to normatively ban or disincentivise transgressions.[467] The difference between law and computer code is that law is to be executed by humans, rather than by computers, and that, unlike computer code, which is self-executory, law requires a support structure to operationalise its application (in the form of an administration of justice system), as legal prescriptions are often imperfect without reference to definitions, to a normative background and a surrounding legal fabric, to overarching legal policy considerations and to the exercise of human judgment in their application. Thus, whether or not law (and, by extension, legal language) can be transformed into computer code (or computer language) is a distinct question to the one treated earlier in this chapter. It is also a question to which no universal answer is possible: much will depend on the concrete legal rules and prescriptions each time in question and on the degree of their complexity and clarity. That said, the advent of smart contracts is likely to provide the necessary impetus for more systematic reflection on the viability (or otherwise) of encoding private and public law rules, in ways that computers can grasp and act upon, whether in order to self-execute digital contracts (as in the case of smart contracts) or in order to otherwise organise financial or other interactions, so as to achieve predictable and verifiable outcomes, similar to those of the application of conventional legal norms and provisions. Indeed, one of the most significant (but, possibly, unintended) contributions of smart contracts could be in accelerating the pace of digitalisation of legal rules, both with regard to the private law applicable in the context of contractual relations and in

466. On 16 October 2012, Germany's Federal Court of Justice held in Az. X ZR 37/12 (https://openjur.de/u/592082.html) that, when in doubt, declarations of will constituting an electronic contract shall be interpreted by taking into account how a human being would interpret the contract. This approach detaches itself from the actual code running the software.
467. It is telling that the earliest known Legal Code, the Ur-Nammu Code, was formulated as a series of conditional statements, linking specific acts to concrete consequences ('[I]f a man commits murder, that man shall be killed').

only if they could inspire confidence, in terms of their reliability, resilience, constant availability and the legal certainty guarantees that their use would come with, that technology-driven alternatives to established payment media, novel payment rails or innovative means of creating tradable assets and settling transactions over them would stand any realistic chance of challenging the dominance of traditional payment media, clearing and settlement processes or established financial intermediaries. Assessing the market prospects of DLTs, Blockchain and virtual currencies, gauging their likely impact on the facilitation and delivery of financial services and measuring their genuine transformative potential, oblivious to the surrounding hype, are risk-fraught endeavours, as with any attempt to predict the future.[761] Although it is not the aim of this author to risk making predictions, he would nevertheless posit that a number of logical inferences can be drawn on the basis of this study, which, once reduced into general observations, should help the reader, whatever her inclinations, policy-driven, academic, professional or other, with her own thoughts around the future of FinTech, the likelihood of its more wide-spread adoption and its probable scope of application. By way of epilogue, the author proceeds to formulate, below, *six* such 'qualitative' observations, on the understanding that these are borne out by the facts, such as they were known to him at the time of writing, and in the hope that they will not be taken, by the reader, as definitive statements of the shape of things to come but, instead, as plausible deductions, following logically from the analytical component of this work.

A *first* observation is that, by promising to 'simplify the settlement chain, reduce its cost, and raise its speed while increasing resilience',[762] digital financial innovations in general, and DLTs in particular, have the potential to substantially impact on financial markets, in terms of both *how* financial services are delivered and by *whom*. Referring to distributed ledgers, it has aptly been observed that these 'may sound incredibly dull, but innovations in this space have been game changers in the past',[763] with the potential to revolutionise the financial markets ecosystem. Besides, as explained earlier in this study, the use of DLTs has the potential to strengthen the operational robustness of market infrastructures processing retail payments and securities transactions, enhance market transparency, promote market access and reduce settlement costs and, possibly, also times. That said, opinions can legitimately differ in terms of the extent of the transformative potential of FinTech: some may see

761. It has aptly been suggested that, 'the development of digital currencies in general, or more broadly any new technology for making payments, is also subject to considerable uncertainty. One reason is the rapid evolution of technology. For instance, agents maintaining the Bitcoin network are trying to improve its transaction processing capacity, which is a necessary condition for Bitcoin to handle any nontrivial fraction of the realistic volume of transactions routinely processed by networks such as Visa and MasterCard. In addition, how the legal and regulatory system will react to the changes is equally hard to predict' (Lo and Wang, 2014, 17-18).
762. M. Carney, *Enabling the FinTech transformation: Revolution, Restoration, or Reformation?*, Speech at the Lord Mayor's Banquet for Bankers and Merchants of the City of London at the Mansion House, London, 16 June 2016 (Carney, 2016), 7.
763. C. Wilkins, *Fintech and the Financial Ecosystem – Evolution or Revolution?*, Remarks at Payments Canada, Calgary, Alberta, 17 June 2016 (Wilkins, 2016). Wilkins adds, by reference to the work of Max Weber and Robert Schumpeter, that 'the invention of double-entry bookkeeping has been credited as one factor enabling capitalism'.

in it a genuine game-changer, capable of reshaping financial services in general, and banking in particular, from a silo into a collaborative model-type business, where traditional intermediaries, such as banks, would either operate as 'platforms' or perish in the face of competition, while others may only see in it a force of gradual, evolutionary change. Moreover, it is fair to assume that the impact of FinTech on the payments or securities landscape will not only be a function of the inherent potential of digital financial innovations but also evolving consumer and investor preferences and habits, the shape of which cannot easily be predicted at the present juncture. As suggested earlier in this study, where the potential of FinTech is at its strongest is where known inefficiencies subsist in the *modus operandi* of financial markets, which recourse to digital financial innovations could attenuate or, even, extinguish. The processing of cross-border payments, the sending of foreign remittances, the management, by financial intermediaries, of back-office processes and asset servicing, the execution of straightforward, 'either or' type (binary) transactions and the setting up of peer-to-peer lending platforms are good examples of possible use cases for digital financial innovation, where its application could help overcome inefficiencies, reduce costs and complexities, and compress timelines. But, for the reasons explained earlier in this study, the author is of the view that there is only a limited probability of FinTech making more significant inroads into the contemporary payments or securities issuance, clearing and settlement space and, in particular, in their tiered, intermediated architecture: despite their inefficiencies and costs, contemporary payments and securities issuance, clearing and settlement systems have proved their worth, including at times of crisis. Besides, some of the financial sector inefficiencies identified over the years have largely been addressed through conventional avenues,[764] while solutions to subsisting ones could still be sought through enhancements in the operation and capacity of existing large-value or retail payment systems (including credit card-processing networks).[765] Notwithstanding the allure of DLTs and Blockchain, it is not clear that there is a compelling case for recourse thereto, to overhaul the contemporary financial system, as opposed to merely improving, incrementally, the *modus operandi* of established value exchange platforms and the entities responsible for their management and operation. Similarly, it is not yet clear whether, even if an overhaul were to be necessary, Blockchain and DLTs would be the right tools through which to achieve it. Thus, while mature and duly calibrated DLT has the potential to improve the operation of financial markets, *first*, it is not a panacea, *second*, there are alternatives to it, using the current technological and market infrastructures, and *third*, it 'is still in

764. A prime example is TARGET2 Securities, which goes a long way towards addressing several of the Giovannini Report barriers (in this regard, *see* ECB, *Giovannini Barriers to Be Reduced by T2S*, available at: https://www.ecb.europa.eu/paym/t2s/about/html/giovannini.en.html).
765. For instance, in 2016, the Eurosystem launched an investigation to assess the needs of market participants for instant payment settlement services (TIPS), available 24/7/365. Public consultations on the user requirements took place in early 2017, and a final decision on the future of the TIPS project was taken in the summer of 2017. More information on TIPS is available at: https://www.ecb.europa.eu/paym/initiatives/html/index.en.html.

its relative infancy as a technological development', making it difficult to 'say with any certainty whether and how it could change the financial ecosystem'.[766]

Linked to the foregoing, a *second* observation is that, whatever their scale, the DLT-fostered disintermediation and efficiency benefits touted by the advocates of FinTech do not appear likely to materialise in the short to medium term. Despite the sustained incursion of non-financial firms, such as *Apple* or *Google*, in the field of financial services (with an emphasis on retail payments), the gradual shift in client demands towards mobile technology-driven, real-time access to financial services and the theoretical potential of DLTs 'to replace entire transaction systems, including core payment systems',[767] neither commercial banks, nor CSDs, nor CCPs are destined to be ousted and substituted, anytime soon, by peer-to-peer, Blockchain or similar, distributed consensus logic networks or platforms for *legal*, *practical* and *economic* reasons alike. Of the various legal reasons touched on earlier in this study, the three salient ones have to do with the role of financial intermediaries as reference points for regulatory compliance and third-party liability, the utility of the checks, validations and reconciliations they perform for the creation of trust in the ability of the financial system to credibly record and finally settle counterparty obligations, and their instrumentality in ensuring legal certainty in terms of the existence and ownership status of financial assets (all of which are conditions precedent for financial and systemic stability). The practical reasons alluded to above are bound up with concerns over the scalability of the technology underlying digital financial innovations and their practical applications, the cyber-resilience of alternative value exchange platforms, and their interoperability, making of 'the implementation of a DLT environment a multifaceted endeavour',[768] which is likely to require time and careful consideration. A few words are also in order on the economic reasons accounting for the author's second observation, which, although left for last, are no less crucial than the preceding ones: for all its merits, technological innovation cannot do away with the rationales for financial intermediation (namely, maturity and liquidity transformation, leverage and credit risk transfer). For as long as those rationales remain relevant to the operation of financial markets, so will financial intermediaries. Thus, even if it could dent demand for the services of financial intermediaries, as it seems capable of, the advent of FinTech is unlikely to signal their precipitous downfall, with the process of the adoption of Blockchain and DLTs as a means of approaching and resolving financial market inefficiencies looking set to be 'slow and deliberate, with improvements and change manifesting incrementally over time'.[769]

766. Mersch, 2016a.
767. Wilkins, 2016.
768. Mersch, 2016a.
769. FIS-Payments Leader, *Don't Believe the Distributed Ledger Hype*, 28 April 2016. The same report also states that, '[I]ncreasingly, reports are suggesting that it will be another four to five years before we see truly big developments in key financial markets, and a decade before blockchain is deployed industry-wide. But we can expect many niche markets to rollout blockchain within 18 months. This last point is critical to the acceptance of blockchain; to ensure continued investment, it is important that practical uses of the technology, in controlled non-critical processes, begin to be launched. For the longer term it is vital that the offerings coming to market are robust, but more importantly, some long-term investment in time and resources is

A *third* observation is to do with the future of (public) money and, in particular, cash and the competition that both of them face from virtual currencies, as the leading form of 'private money' in circulation. While some virtual currencies (and, especially, *bitcoin*) have been a qualified success, they have not, so far, managed to 'outshine competition when it comes to serving as a store of value and a medium of exchange',[770] both because they are devoid of the coveted status of legal tender and because of their inherent volatility, either of which is apt to seriously undermine their claim to serving as genuine substitutes for public money. Regarding physical cash, it is submitted that this remains the benchmark against which to assess the merits and shortcomings of alternative payment media, conventional and innovative alike, with cash continuing to enjoy an advantage over the competition (virtual currencies included), in terms of both finality and anonymity, despite its shortcomings. The above is without prejudice to the possible introduction, in the medium term, of central bank-issued digital currencies and of their circulation in parallel with cash, as complements thereto, rather than as substitutes thereof. The monetary policy needs of contemporary sovereign states or federal structures look set to provide a lasting source of demand for centrally issued currencies, whatever the format of their issuance and the modalities through which their issuing central banks are to grant access to them: at the time of writing, virtual currencies did not appear capable of satisfying those needs, for practical and legal reasons alike, linked to their 'private money' (non-legal tender) status, the fact that they did not represent claims against the balance sheet of an identifiable issuer, and their limited public acceptance, the combination of which inevitably raises concerns, prima facie warranted, in terms of the scalability of virtual currencies, and their utility as payment media, especially for large-value transactions.

A *fourth* observation is derived from the pivotal role of *legal considerations* to any rational discussion of Blockchain, DLTs and FinTech and to any dispassionate assessment of the prospect of their widespread adoption and use in the context of financial markets. As explained earlier in this study, there are a number of crucial legal issues to be resolved before DLTs can unfold their perceived benefits and deliver on their tantalising promises, which, in this author's view, have not so far featured as prominently as they should have in the public debate on FinTech. Depending on the precise configuration of a distributed ledger and on the particulars of its underlying technology, the issues in question include lack of legal certainty with regard to the legal basis of distributed ledgers, and of any 'assets' constituted digitally or, merely, recorded on a DLT ledger, ambiguity in terms of the finality attributes of transactions settled in a distributed ledger environment, lack of clarity on the extent to which DLT records qualify, legally, as 'securities accounts' within the meaning of the relevant national law definition and, in the affirmative, on the *locus* of such 'accounts', concerns with the protection afforded by alternative trading platforms to privacy and data confidentiality, question marks in respect of the allocation of liability for their operation and the consistency of DLT network validation and record-keeping methods

needed by a large number of leading market players to agree common and open standards before implementation can begin.'
770. Wilkins, 2016.

with those applicable in the jurisdiction (or jurisdictions) of their establishment, lack of certitude in respect of DLT network compliance with national law rules (*inter alia* on matters of AML/CTF, KYC and securities issuance and account maintenance) and, last but not least, challenges in identifying *which law* or laws govern payment, securities or other financial transactions processed in a DLT environment, and which court could rightfully assert subject matter jurisdiction over disputes arising from, or in connection with, their processing. On the litany of legal issues specific to the issuance and/or use of virtual currencies and smart contracts, the reader is referred to the detailed analysis in Chapters 4 and 5, respectively; suffice it to note here that these touch on issues of relevance to the definition, legal characterisation and regulatory treatment of virtual currencies and smart contracts, the extent to which the combination of DLTs and smart contracts can create legally binding agreements between the parties to a transaction involving the transfer of financial assets and the precise legal attributes of virtual currencies, hence, on a wide range of issues that go to the very core of virtual currencies and smart contracts as legal phenomena. Thus, even if one were willing to accept that FinTech holds the promise of helping resolve some of the contemporary financial markets' inefficiencies by, for instance, facilitating retail payments or promoting more efficient securities clearing and settlement, one would also need to acknowledge that its advent and eventual application in the context of financial markets is apt to be a source of novel vulnerabilities, many of which are legal in nature; a robust (and concerted) response to them appears necessary, if DLTs, Blockchain and other forms of FinTech are to stand any chance of widespread adoption in the highly regulated world of financial markets.

Related to the foregoing, a *fifth* observation is linked to the *regulatory acceptance hurdles* that FinTech would need to negotiate and overcome before it could see an increase in its take-up and the nature of the *regulatory response* thereto. It has been observed that due to 'the weight of various historical indicators and in the wake of significant recent events, regulators adopted an incredibly aggressive approach to enforcing existing regulations against the drastically new, different, and emerging technology', with the 'resulting barriers to entry and climate of legal stigma … stifling the nascent decentralised technology industry and preventing further innovation'.[771] Whatever its proportions, the regulatory acceptance hurdles faced by FinTech are significant. For instance, regulators will need to balance the need for a level playing field amongst established financial service providers and the multitude of new players likely to take a business interest in FinTech's potential against the need to avoid legislating unnecessary barriers to entry, grapple with the tension between the third-party intermediaries focus of the current financial markets regulatory framework and the distributed (hence 'impersonal') logic of FinTech's underlying technologies, gauge the potential of the latter to transform financial services in ways that, while not yet sufficiently well understood, could help overcome current inefficiencies but, also, undermine market integrity and public trust in the operation of payment systems, SSS and financial markets (which regulators should guard against, alleviate or neutralise),

771. Reyes (2016), 194.

and reflect on the scope for factoring technical code into the regulatory debate, as a means of governing the use of modern technology for the delivery of financial services and the achievement of regulatory outcomes. All things considered, regulators are in the non-enviable position of having to reconcile two conflicting aims: preserve the potential benefits of digital innovation, as applied to the provision of financial services while, at the same time, tempering its less benevolent aspects, with targeted, proportionate, risk-focused regulation, putting FinTech into perspective and integrating it into the fabric of contemporary financial regulation.[772] Whether the regulatory community will manage to tackle these challenges, free of regulatory failures, and how regulators will go about responding to the digital financial innovation phenomenon will largely determine its fortunes and impact on financial markets, which, without regulatory support, is destined to remain limited. Turning to the concrete nature of the regulatory response to FinTech, it is submitted that the need for it, in the first place, will not only depend on the risks and opportunities of FinTech, which, as suggested in this study, can be substantial but also on consumer, investor and financial markets' demand for technological innovation, while its precise contours will inevitably turn on the public policy interests that regulation will seek to achieve in this space, and on the relative weight it would attribute to the regulatory objectives of consumer protection, financial stability and the promotion of competition amongst incumbents and new entrants. It remains to be seen whether regulators and policymakers will opt to reduce barriers to market entry for FinTech firms, so as to reap the benefits of enhanced competition, or whether they will, instead, choose to err on the side of caution, by either denying them the benefit of regulatory recognition or subjecting them to the same regulatory constraints as those applicable to established financial service providers, thereby risking to forsake their benefits for the sake of averting too substantial an effect on the process of financial intermediation and the position of established financial intermediaries.[773]

A *sixth*, and final, observation is to do with the need for some measure of global cooperation (or, ideally, coordination), both to facilitate the adoption of digital financial innovations and to help address the challenges, legal and other, that their introduction would inevitably throw up. As explained earlier in this study, FinTech can operate across borders, across asset classes and across different types of service providers, making FinTech 'an international issue'.[774] Similarly, as both the perceived benefits of FinTech and its many challenges are global in nature, the same should, presumably, be true of the response to them, to ensure a level playing field across different jurisdictions, consistency in terms of the national regulatory responses to FinTech and, last but not least, the efficiency of those responses at tackling what is a global phenomenon. The present lack of regulatory consistency, which, in this author's view, is partly attributable to differences in national legal traditions and partly the

772. 'Fintech should neither be the Wild West nor strangled at birth' (Carney, 2016, 10).
773. At the time of writing, the authorities in Switzerland appeared to be opting for the first approach. For an account of the incipient Swiss regulatory framework *see* T. G. Albert, *Fintech, Blockchain and Digitalisation: Is Switzerland the New e-Eldorado?*, 32 (8) Journal of International Banking Law and Regulation (2017), 367-371.
774. IMF, 2017, 6.