IEO
Independent Evaluation Office
of the International Monetary Fund

BACKGROUND PAPER

BP/18-02/07

Emerging Technology-Related Issues in Finance and the IMF—A Stocktaking

Dimitri Demekas

Address. 700 19th Street, N.W., Washington, D.C. 20431, U.S.A. Telephone. +1 202 623 7312 Fax. +1 202 623 9990 Email. ieo@imf.org Website. www.ieo-imf.org

 BP/18-02/07

IEO Background Paper
Independent Evaluation Office
of the International Monetary Fund

Emerging Technology-Related Issues in Finance and the IMF—A Stocktaking

Prepared by Dimitri Demekas*

December 14, 2018

* IEO Consultant and former IMF staff.

Contents Page

ABBREVIATIONS

BCBS	Basel Committee on Banking Supervision
DLT	distributed ledger technology
Dos	denial-of-service
FFIEC	Federal Financial Institutions Examination Council
FSAP	Financial Sector Assessment Program
FSB	Financial Stability Board
FSOC	Financial Stability Oversight Council
FSSA	Financial System Stability Assessment
GFSR	*Global Financial Stability Report*
G7FE	G-7 Fundamental Elements of Cybersecurity for the Financial Sector
IOSCO	International Organization of Securities Commissions
MCM	Monetary and Capital Markets Department (IMF)
OCC	U.S. Office of the Comptroller of the Currency
OFR	Office of Financial Research
P2P	Peer-to-Peer
SDN	Staff Discussion Note
SPR	Strategy, Policy, and Review Department (IMF)
STA	Statistics Department (IMF)
SWIFT	Society for Worldwide Interbank Financial Telecommunication

EXECUTIVE SUMMARY

This paper provides a stocktaking of the IMF's work on three emerging technology-related issues in finance: (i) cyber risk and cyber security for financial systems; (ii) technology-driven innovation in the provision of financial services ("fintech"); and (iii) digital currencies or cryptocurrencies. Because these issues are relatively new, still evolving, and their economic impact is uncertain, it would be premature to try to assess the quality and impact of the Fund's engagement and policy advice. Instead, this paper casts a wide net and takes stock of a broad range of relevant Fund activities, including analytics, outreach, multilateral work—including work with the Financial Stability Board (FSB) and standard-setting bodies (SSBs)—as well as the coverage of these issues in bilateral surveillance.

The stocktaking shows that the IMF has been paying increasing attention to technology-related issues in finance, both from an analytical perspective and as a topic for bilateral surveillance. This engagement is in its early stages and still evolving. It has so far been more visible on fintech and digital currencies than on cyber security issues. In a handful of Article IV consultations and Financial Sector Assessment Programs (FSAPs) these issues have been discussed in some depth, but more generally coverage has varied widely, as might be expected, reflecting judgments on the importance of these issues in the jurisdictions concerned. At the same time, the Fund has used its convening power to raise awareness of these issues—particularly cyber risk—and facilitate knowledge-sharing among developing and emerging market member jurisdictions. Most recently, the IMF has worked together with the World Bank to develop the Bali Fintech Agenda, a framework for the consideration of high-level issues in these areas by the international community and individual member countries.

Looking forward, the challenge for the IMF is to continue working closely with member countries and relevant international bodies in order to best respond to the membership's needs in this area. The Bali Fintech Agenda is expected to help guide the focus of this work within the Fund's expertise and mandate, inform the dialogue with national authorities, and help shape the contributions of the Fund to the work of standard-setting bodies on fintech issues.

I. Introduction and Scope

1. This paper provides a stocktaking of the Fund's work on a number of emerging technology-related issues in finance. Although they are widely acknowledged—including by the Fund—to have potentially profound implications for the financial industry and, more broadly, for economic welfare, these issues are described as "emerging" for two reasons. *First*, because the technological innovations underlying them are relatively new, not widely understood, and in many cases still evolving rapidly, and their potential economic impact is not known with any certainty. *Second*, and relatedly, because they have only recently become the focus of national supervisory authorities in advanced economies and international standard-setting bodies.

2. The stocktaking focuses on three technology-related issues: (i) cyber risk and cyber security for financial systems; (ii) technology-driven innovation in the provision of financial services (fintech); and (iii) digital currencies, sometimes referred to as cryptocurrencies. The latter is a particular application of fintech, but one that has attracted significant attention by central banks and policymakers recently, and merits separate treatment.

3. It would be premature to try to assess the quality and impact of the Fund's engagement and policy advice in these areas. Because of their very nature as "emerging," as well as the dearth of relevant, high-quality data, these issues are not yet generally integrated in the analytical frameworks used by staff in surveillance. Instead, this paper casts a wide net and takes stock of the Fund's broad engagement with these issues, on the analytical front, in outreach and advocacy, and in multilateral and bilateral surveillance.

4. It is not the first time the Fund finds itself in the position to have to expand quickly its analytical and policy toolkit to cover new areas. Financial sector issues in general were considered peripheral to the Fund's mandate until the late 1990s and, despite the substantial progress made since then, the process of integrating them and mainstreaming them into surveillance is still ongoing today, two decades later. The process of learning and adaptation—and the obstacles to overcome in an institution like the Fund—are similar, and there are useful parallels to be drawn.

5. This stocktaking exercise covers the activities of the Fund in these areas during the period from 2013 to mid-2018, and is based on a review of Fund documents, publications, and outreach events; review of Fund country documents (Article IV staff reports and Financial System Stability Assessments—FSSAs) for 25 jurisdictions, spanning a range of financial sectors where technology-related issues are important (see Appendix); and interviews with authorities from a subset of these jurisdictions, Fund staff, and external experts which took place in Spring 2018.

II. Emerging Technology-Related Issues in Finance: An Overview

A. Cyber Risk and Cyber Security for Financial Systems

6. The risk of accidental or deliberate disruption to financial institutions' IT systems has long been recognized by the industry and regulators. However, for much of this time, it was treated as one of several sources of "operational risk." The concept of operational risk, clarified in the Basel II regulations for banks in the early 2000s,[1] was a catch-all category for risks arising from "inadequate or failed processes, people, and systems, or from external events," including fraud, legal risks, systems failure, terrorist attacks, employment practices, workspace safety, accounting errors, etc. (BCBS, 2004).

7. It was not until early this decade that cyber risk per se started becoming the focus of the financial industry and regulators, following a string of cyber attacks against governments and businesses in Estonia in 2007, Korea in 2009 and 2011, and the U.K. in 2012. In 2012, the World Economic Forum (WEF), in cooperation with Deloitte, published one of the first reports on cyber risk for business, though not specifically focused on the financial sector (WEF, 2012). In 2013, after the U.S. government identified financial services as "part of the nation's critical infrastructure, with assets, networks, and systems [...] that are vital to public confidence and the Nation's safety, prosperity and well-being" (White House, 2013), the U.S. Office of the Comptroller of the Currency (OCC) explicitly identified "increasingly sophisticated cyber-threats [and] expanding reliance on technology" as major sources of operational risk (OCC, 2013). Also, in 2013, the Bank of England's Financial Policy Committee issued a recommendation requesting that HM Treasury and regulators work with the core U.K. financial firms to put in place "a program of work to improve and test resilience to sophisticated cyber-attacks." In January 2015, Keidanren, the Japan Business Federation, which includes financial firms, published a Proposal for Reinforcing Cyber Security Measures,[2] and later that year, the ECB established a working group to study how euro area national supervisors and banks were dealing with cyber threats.

8. In the meantime, the number of cyber attacks against the financial services industry multiplied. The most prominent attacks include disrupting money transfers and erasing computer files in three Korean banks in 2013; hacking trading terminals in a Russian bank in 2014 and, several months later, executing fraudulent high-value dollar trades; and compromising a SWIFT software program installed on bank servers at the Central Bank of Bangladesh in February 2016. According to a survey by Verizon (referred to in Kopp and others, 2017), in 2015, financial services was the industry with the most incidents with confirmed data losses.

[1] Even the term "operational risk" itself, which was first coined in the early 1990s, did not gain widespread traction in supervisory circles until the Basel Committee started circulating the first Basel II documents for consultation in the late 1990s (Power, 2003).

[2] See Keidanren (2015).

9. Cyber risk has a number of characteristics that make an assessment of the likelihood and potential cost of events particularly challenging.

- The means of cyber attacks vary widely across firms and geographies, ranging from denial-of-service (DoS) attacks to attacks on ATMs, breaches of firewalls, internal databases or servers, and web application attacks.

- Vulnerability to cyber risk can arise not only from weaknesses in a firm's own systems but also in those of its clients, suppliers or service providers, and infrastructure providers.

- As the perpetrators are often not identified, their motivations and capabilities—and thus the degree of risk they represent—are not well understood.

- There are no comprehensive data on cyber attacks and their impact, rendering risk aggregation and the estimation of losses extremely difficult. Individual firms have an incentive not to reveal the scope and nature of breaches.

10. Despite the increasing frequency and impact of cybersecurity incidents, there has not yet been an incident with systemic consequences for the financial sector. Nevertheless, in the past few years, a consensus emerged that cyber risk can be systemic, and policy-makers and regulators are exploring a variety of policies and tools to mitigate it. In the U.S.A., the Financial Stability Oversight Council (FSOC) and the Office of Financial Research (OFR) have described how cybersecurity incidents in financial firms could undermine the stability of the entire financial system (OFR, 2016; 2017), and the Federal Financial Institutions Examination Council (FFIEC) has created an extensive cyber security assessment tool for financial institutions (FFIEC, 2017). U.K. financial regulators have developed CBEST, a scheme for testing financial firms' vulnerabilities against cyber attacks involving, in addition to the financial institution and the regulator, the intelligence community and private sector cyber security firms.[3] At the global level, the G-7 published in October 2016 the "G-7 Fundamental Elements of Cybersecurity for the Financial Sector" (G7FE), outlining some broad cybersecurity practices for public entities, public authorities, and financial firms, followed in 2017 by a more detailed document on the "Effective Assessment of Cybersecurity in the Financial Sector;"[4] and in mid-2016, CPMI issued guidance on cyber risk for financial market infrastructures (CPMI, 2016). And there is an ongoing debate between two opposing views on the regulation of cyber risk: one sees it like any other risk, for which the general principles for risk management (governance, setting of risk appetite, etc.) apply, and where specific rules might quickly become obsolete; the other emphasizes the special nature of cyber risk and argues for specific regulations to supplement those for other types of risk (FSI, 2017).

[3] On CBEST, see Bank of England (2018).

[4] See G7 (2016; 2017).

B. Technology-Driven Innovation in the Provision of Financial Services ("fintech")

11. The Financial Stability Board (FSB) has defined fintech as "technologically-enabled financial innovation that could result in new business models, applications, processes, or products with an associated material effect on financial markets and institutions and the provision of financial services" (FSB, 2017).[5] It is based on a number of inter-related technological developments, notably the growth of computing power, spread of high-speed internet connectivity, faster mobile networks, application programming interface (API), cloud computing, artificial intelligence, and cryptography.

12. Leading this wave of innovation are both large, established technology firms—such as Google, Amazon, Apple, and Facebook, and Chinese giants Baidu, Alibaba, and Tencent—as well as small, startup companies. From an estimated 1,600 fintech companies with about US$5.5 billion in funding in 2005, the global footprint has jumped to some 8,800 companies with over US$100 billion in funding (IOSCO, 2017). Fintech credit, i.e., credit facilitated by electronic platforms (either using their own balance sheet or matching investors with borrowers), where both large technology firms and small startups are active, has grown rapidly and today the stock is largest in China (almost US$100 billion outstanding in 2015), followed at a distance by the U.S. and the U.K. (CGFS & FSB, 2017). Fintech can also be extremely important in smaller markets, for instance in Kenya and other African countries, where it has enabled rapid expansion in access to financial services. Still, the sector remains small compared to the global financial industry.

13. The innovations cover a wide area, including credit and deposits; payment, clearing, and settlement services (mobile wallets, distributed ledger technology (DLT), P2P transfers); investment management (robo-advice), and market support services (big data analytics, security, and cloud computing) (IOSCO, 2017; BCBS, 2018). The implications of each of these applications vary widely, but it appears that at least some of them could usher in profound changes in the industry.

14. It could be argued that the existing financial services industry will overcome this challenge to its business model without any destabilizing effects, perhaps absorbing some of the startups and incorporating the most promising technologies. After all, banks have historically been resilient to disruption by technology owing to a number of structural barriers to entry: economies of scale in producing and distributing services, information asymmetries entrenched in client information and credit underwriting systems, high fixed costs of compliance with regulations, sovereign insurance of liabilities, and consumer inertia (Philippon, 2015; McKinsey, 2015).

15. While these barriers to entry are still present, there are several reasons why the potential for disruption may now be higher. Some of these are exogenous, such as the ubiquity of mobile devices, low initial fixed cost, demographics, and the decline of trust in banks. Others reflect

[5] In fact, the term "fintech" is older: it was first used in the early 1990s, when it was introduced by the Financial Services Technology Consortium, a project started by Citicorp (Hochstein, 2015).

certain characteristics of the recent innovations (easy access, network effects, and the generation and capture of a huge amount of data), as well as the fact that they target segments of financial intermediation that are particularly profitable for incumbents (origination and sales, investment management) (McKinsey, 2015; Dhar & Stein, 2017). The combination of these factors means that this time may indeed be different for the financial industry.

16. Fintech holds out the promise of reducing frictions and inefficiencies in financial intermediation to the benefit of the ultimate users of these services. This can take many forms: faster and safer payments and settlements through the use of DLT ("blockchain"); greater real-time control of personal and business finances by consumers and small businesses through APIs; simple person-to-person transfers—including cross-border remittances; easier mobilization of savings to fund investments through crowdfunding; cheaper investment management for small investors through robo-advice; and better and faster credit decisions through big data analytics. Looking farther into the future, some elements of fintech, especially DLT, could potentially transform processes through "smart contracts," intellectual property protection, and secure and immediate attestation services (e.g., proof of ownership of assets) (Swan, 2015; Diedrich, 2016).[6]

17. The risks of fintech range from risks to consumer privacy to risks for financial stability (Brainard, 2016; He and others, 2017; DTCC, 2017). The latter, which are generally considered still low, could include:

- new forms of credit and liquidity risk created by fintech companies that provide core banking functions (credit, liquidity, and maturity transformation);
- the possible emergence of new too-big-to-fail entities;
- increased risk of herd behavior as a result of automated processes; and
- the disruption of incumbents' profitability and business models.

18. The regulatory community is looking into the challenges posed by fintech. This includes regulators in advanced economies, struggling to balance the desire to encourage innovation against the need to contain the risks (for example, through regulatory "sandboxes" for fintech startups) and in emerging market and low-income countries, where certain implementations of fintech hold the potential to expand financial inclusion. Global regulatory bodies are trying to distill lessons for national regulators (IOSCO, 2017; IAIS, 2017; CPMI, 2017; BCBS, 2018). And

[6] Views differ on the potential of DLT. Some see DLT as no less than the means to "move away from an economic order centered around powerful but not always trustworthy intermediaries […] toward a more decentralized and democratic order" (Maupin, 2017). Others, noting the current technical limitations of DLT in terms of scalability and security, are more skeptical, conceding that the technology could be useful only to specific applications (Roubini and Byrne, 2018; Kay, 2017).

there is an active debate about the potential of fintech to transform financial regulation itself ("regtech"—see Arner and others, 2016; Philippon, 2017).

C. Digital Currencies

19. One particular application of fintech that has recently attracted a lot of public attention is digital currencies (or cryptocurrencies or virtual currencies). Bitcoin, which is almost ten years old, is perhaps the best known, but there are thousands of other digital currencies, with a total market cap of over US$500 billion (https://coinmarketcap.com/).

20. While there is no commonly agreed definition, the BIS has defined a digital currency as a means of payment that shares the following characteristics (CPMI, 2015):

- It is stored and used in transactions electronically.
- In contrast to other electronic payments systems, it can function like cash, in that it enables "trustless" P2P transactions, i.e., without a trusted financial intermediary.
- Unlike fiat currency (the liability of a central bank or government) and bank deposits, which are often treated as money (the liability of a commercial bank), a digital currency is not the liability of anyone. In that sense, it is akin to gold.

21. Digital currencies fall into several categories, depending on their primary purpose and design goal: digital cash (like Bitcoin, Monero, Bitcoin Cash) is primarily designed as a (quasi) anonymous and autonomous means of payment; payment tokens (like Ripple and Utility Settlement Coin—the latter currently under development by a consortium of banks) are meant to exploit technologies like DLT to complement existing payments systems at lower cost, higher speed, and greater reliability; and securities or utility tokens (RMG, Filecoin, Golem) are designed to represent a unit of a financial, physical, or digital asset (e.g., data storage) in order to facilitate P2P trading activity. Some digital currencies circulate only within a limited group, while others are in the public domain, like conventional currencies. Most digital currencies are built on DLT or "blockchain" or make use of this technology in some way.

22. The regulatory and policy concerns raised by digital currencies are mainly a reflection of certain characteristics, notably the extraterritoriality, anonymity, and personal crypto security they provide to users.

- The immediate concerns are about financial integrity (digital currencies can be used to facilitate illicit transactions and money laundering), consumer protection, and tax collection. These concerns have been underscored by a number of recent incidents, like the hacking of Mt. Gox, the largest bitcoin exchange platform, in Japan in 2014, the security breaches of Instawallet, Coincheck, and Bitstamp, and others.

- Although the scale of the phenomenon is still too small to represent a threat to financial stability, this could happen in the future, if it continues to spread and prices continue to be volatile. It could arise through interconnections with established financial institutions, leverage, and increasing concentration/counterparty risk.

- At the same time, it is recognized that the same technologies that power the spread of digital currencies (and the attendant risks), notably DLT, could also have beneficial effects on financial stability by making payment and settlements systems quicker and more secure. The challenge for regulators is thus to safeguard financial integrity, consumer protection and, prospectively, limit risks to financial stability while, at the same time, not preventing beneficial technological innovation (Quarles, 2017; Oliver Wyman, 2018).

23. The policy and regulatory response to this challenge is still in flux. Digital currencies were the subject of a high-visibility public statement by the head of the BIS[7] in February this year and shot to the top of the agenda of the G20: the Buenos Aires G20 communique on March 20, 2018, noting that while crypto-assets—this term is meant to underscore that digital currencies lack all the attributes of official currencies—do not yet pose a financial stability risk, the Financial Action Task Force (FATF) and standard-setters should continue to monitor them and "assess multilateral responses as needed."[8] Nevertheless, practices differ widely and the G20 could not agree on specific steps.[9] Some jurisdictions ban digital currencies and "initial coin offerings" launches; others recognize them as formal forms of payment and a type of financial asset; still others have adopted a "wait-and-see" approach. Some jurisdictions regulate the exchanges, while others have introduced prudential requirements for firms conducting digital currency "business," meaning buying, selling, transmitting, issuing, or administering digital currencies.

24. Finally, a separate aspect of the digital currency debate is the interest of several central banks to issue their own digital currency (discussed later in this paper). Depending on the design, this could be used to facilitate settlements, provide an alternative, safe, and convenient payment system to the public, or enhance monetary policy transmission. This project raises complex policy issues that the central banking community is just starting to tackle (CPMI, 2018).

III. THE FUND'S WORK ON TECHNOLOGY-RELATED ISSUES IN FINANCE

25. This section takes stock of the various strands of Fund work on the three technology-related issues described above. This stocktaking casts a wide net and captures Fund activities related to these three issues in four areas: (i) analytical and policy work; (ii) outreach and advocacy intended to raise awareness of, and share knowledge on, these issues globally;

[7] "Authorities should be prepared to act on cryptocurrencies," BIS (2018).

[8] See G20 (2018).

[9] "G20 leaders to hold fire on cryptocurrencies amid discord," see Canepa (2018).

(iii) multilateral surveillance, including contributions to the work of standard-setting bodies and other global stakeholders; and (iv) bilateral surveillance. For the latter, the stocktaking focuses on 25 jurisdictions where these issues are particularly relevant.[10]

26. Institutionally, different departments of the Fund are expected to take primary responsibility for each of these activities.[11] Given the nature of the issues, Monetary and Capital Markets Department (MCM) is the lead department for the first three: it is the natural locus of analytical and policy work on financial sector issues, on which it is expected to develop positions and provide guidance to country teams; it represents the Fund in, and contributes to the work of, standard-setting bodies and the FSB; it is in a position to raise awareness and disseminate knowledge among member countries through its capacity-building activities; and it prepares the *Global Financial Stability Report (GFSR)*. Area departments take the lead in bilateral surveillance, although FSAPs, which are led by MCM, are also part of bilateral surveillance.[12] As the main review department and one of the contributors to the analytical work of the Fund on these issues, Strategy, Policy, and Review Department (SPR) also plays a key role. Global outreach is led by Communications Department (COM), with Management often playing a visible role, and other departments also contribute: LEG is involved in the work of the FATF on fintech issues, which informs its capacity building activities on AML/CFT, as well as in the analysis of broader legal issues; Information Technology Department (ITD) functions as a knowledge hub for technological issues; Research Department (RES) is involved in policy and analytical projects in this field; and Statistics Department (STA) is working toward clarifying international concepts and standards related to digital currencies and fintech and their treatment in macroeconomic statistics, and collects data on mobile money as part of the Financial Access Survey (FAS) database.

A. Cyber Risk and Cyber Security for Financial Systems

27. While the IMF has been active in outreach and advocacy on cyber security issues, analytical and policy work to date has been more limited. As the IMF staff has become aware of the increasing importance of cyber risk, it has provided briefings to Management and has flagged the issue since July 2016 in the (unpublished) regulatory updates provided periodically to the Board, summarizing the debate among regulators and standard setting bodies. Cyber risk and cyber resilience are also highlighted as a focus for the Fund's work in the Managing Director's latest Global Policy Agenda. To date, however, the Fund has not taken a position on some important policy questions, e.g., whether cyber risk should be treated as any other kind of

[10] Australia, Belgium, Chile, China, the Euro area, Finland, France, Germany, Hong Kong SAR, India, Japan, Kenya, Korea, Luxembourg, Malaysia, Mexico, the Netherlands, Nigeria, Singapore, South Africa, Sweden, Switzerland, Tanzania, U.K., and U.S.A.

[11] Although individual departments are expected to take the lead on different activities, the work on fintech issues is shared among departments through the interdepartmental working group on financial and technology.

[12] From a legal point of view, only the financial stability assessment under the FSAP is part of surveillance, and only for jurisdictions with systemically-important financial sectors.

operational risk or merits a special risk management and regulatory framework. Recently, the staff has started to produce research on the potential impact of cyber risks on financial systems. For example, a Box on "cyberthreats as a financial stability risk" in the October 2017 *GFSR* examined the potential of cyber attacks to undermine financial stability and reported on recent regulatory initiatives to improve cyber resilience. At the multilateral level, the Fund is liaising with the G7 working group on cyber risk—which takes the lead on the policy work—but is not a member.

28. In interviews, staff indicated that the analytical work to date on cyber risk has been constrained by the lack of information about cyber attacks and data that would allow a meaningful quantitative analysis, as well as the view that developing policy/regulatory positions on cyber risk should be left to standard-setters, like the BCBS or CPMI. Staff also explained that the Fund had faced the challenge of building the necessary expertise at a time when such skills were generally in high demand. Some progress is being made with the creation of an inter-departmental working group on cyber risk and the hiring of two experts in MCM.

29. Notwithstanding the limited in-house analytical and policy work, the Fund has been active on cyber risk in the areas of **outreach, advocacy** and **capacity development** and, to a lesser extent, **bilateral surveillance**.

- Following the breach of the SWIFT servers in February 2016, several developing and emerging market countries approached the Fund for advice on limiting vulnerabilities to cyber risk in their systems. In response, MCM organized a workshop for about 30 country representatives during the 2017 Spring Meetings, and a larger workshop—in cooperation with the National Bank of Belgium—in late 2017, where representatives of about 60 developing and emerging market countries participated (Appendix Table A.1). This has been followed by a series of regional workshops in the Fund's regional technical assistance centers and bilateral technical assistance. A follow-up workshop for developing and emerging market countries is planned for December 2018, again in cooperation with the National Bank of Belgium.

- Aware of the growing preoccupation of country authorities, Article IV and FSAP reports for four advanced economies (Belgium, Germany, U.K., and U.S.A.—see Appendix Tables A.2 and A.3) covered cyber risk and the authorities' policy and regulatory initiatives. The degree of detail of the coverage varied from a few simple references to the issue to full-page boxes with a detailed presentation of the authorities' initiatives. Not surprisingly, the detail tended in most cases to be somewhat greater in FSAPs than in Article IVs. In all cases but one (Belgium FSAP), staff did not make specific policy recommendations but reported on the authorities' work and initiatives.

- In the context of the Article IV consultation with the U.S.A., the country team (together with MCM and ITD staff) took the initiative to produce a working paper on "Cyber Risk, Market Failures, and Financial Stability" (Kopp and others, 2017). This original and

innovative piece of work attempted to collect and report data on cyber incidents, provided an analytical framework to analyze cyber risk, and discussed policy options. In that sense, although mainly focused on the U.S.A., this paper has gone well beyond all other analytical work thus far done by the Fund—and many other agencies—on cyber risk. Given the scarcity of analytical work in this area around the world, the paper has attracted interest even outside the USA. Building on this paper, another Working Paper (Bouveret, 2018) proposed a methodology for estimating losses from cyber-attacks.

30. These Fund activities have been well received by the membership, notwithstanding some caveats. The initiative to reach out to emerging market and developing countries was generally praised, and the consensus was that the seminars had been useful for the emerging market and developing country participants. The fact that the Fund had not tried to dominate the proceedings but focused on facilitating knowledge-sharing among participants was universally commended. The discussion of cyber risk in the (few) Article IV consultations and FSAPs that covered it was also welcomed. The country representatives saw these discussions as part of the Fund's mission to learn from country experiences and disseminate good practices. And the U.S. Article IV Working Paper by Kopp and others (2017) was seen as a good first effort to insert some economics in the discussion of cyber risk, which often tends to be too narrowly technical.

31. Staff indicated that a key reason for why the coverage of cyber risk in bilateral surveillance has not been more extensive was limited expertise. This view was shared by the handful of country teams that covered this topic in Article IVs or FSAPs and by those that did not—they all would have welcomed more expert support from MCM. For example, one area department mission chief, who was cognizant of the keen interest of the authorities in this issue but did not cover it during the mission, explained "I would not know where to start" without some sort of guidance, a set of questions to frame the discussion, and a set of useful examples or experiences from other countries.

B. Technology-Driven Innovation in the Provision of Financial Services ('fintech')

32. The Fund started engaging publicly with fintech issues in 2016, including a number of high-profile **outreach** events, including speeches and blogs by the Managing Director, seminars and panel discussions—one chaired by the Managing Director—during the Spring and Annual Meetings, and several publications in Finance & Development, among others (Appendix Table A.1). While not going in depth into specific technologies or innovations, these activities highlighted the implications of a wide area of fintech applications, including those relevant for financial inclusion in developing or underbanked countries. These outreach activities raised significantly the public profile of the Fund on fintech issues globally.

33. This outreach built on staff **analytical** and **knowledge-management** work that had started earlier.

- MCM has monitored fintech developments since 2014, issuing a Working Paper on oversight issues for mobile payments—a key aspect of fintech for some developing countries (Khiaonarong, 2014)—and since 2015, disseminating information on broader fintech trends through an internal *Fintech Monitor* and occasional seminars.

- STA has been collecting data on mobile money accounts and transactions since 2014 through the Financial Access Survey (FAS). Based on these data, STA has produced several notes analyzing the growth of mobile money across the world, including the Mobile Money Note in October 2017 and the 2018 FAS Trends and Development in September 2018.

- A Staff Discussion Note (SDN) (He and others, 2016) on digital currencies—discussed in more detail in the next section—was prepared in 2015 and published in January 2016.

- An interdepartmental working group on finance and technology was formed in early 2016 with a broader brief, namely to "study the economic and regulatory implications of developments in the area of finance and technology."[13]

- A High-Level Advisory Group on Fintech was convened in March 2017, including 14 outside experts (technologists, regulators, lawyers, and academics) to advise the Fund and work closely with the aforementioned interdepartmental working group on fintech issues. The Advisory Group, which was expanded earlier this year to include representatives of the public sector and emerging markets, has only met once since its inaugural meeting but staff have been able to use individual members as sources of information and a sounding board.

34. These strands of work culminated in the issuance of an SDN prepared by an inter-departmental staff team (He and others, 2017), and presented to the Board for informal discussion. The SDN provided an overview of the key technological innovations; presented a general economic framework for the analysis of the market impact of fintech; and focused on the implications of fintech in the area of cross-border payments.

35. Staff also actively reached out to relevant central banks and regulatory agencies to seek their views and discuss the findings of the SDN—much as they did with the High-Level Advisory Group members—building a global network of contacts and staying on top of this rapidly evolving area.

[13] IMF (2017).

36. This effort has provided a strong foundation for further analytical work by the Fund in this area but has not yet reached maturity. Representatives of central banks and regulatory agencies were appreciative of staff efforts to reach out to them, and those that had seen the SDN/17/05 on fintech considered it a good first step. They noted, however, that the SDN provided policy prescriptions on the regulatory issues raised by fintech only in the most general terms.

37. At the **multilateral** level, in contacts at the FSB, the CGFS, and standard-setting bodies, the Fund is represented at a high level but did not participate in the various working level groups that prepared papers on analyzing trends and discussing the policy implications of fintech. At the technical and working group levels, MCM technical staff participates in the FSB Financial Innovation Network (FIN) and in specific technical workstreams such as RegTech and Monitoring, where the IMF is responsible for monitoring developments in non-FSB jurisdictions; and LEG staff is working with FATF, including on the amendments of the FATF standard to address digital currencies.

38. There appears to be some momentum for deepening the Fund's analytical and policy work in the area of fintech. A major challenge for anyone attempting to engage with the topic of fintech in general—and one that the Fund is already confronting—is the breadth, diversity, and rapidly evolving nature of the technological innovations. This calls for prioritization. The Fund so far—notably in SDN/17/05—seems to have prioritized studying the implications of fintech for cross-border payment and settlements. Staff explained this choice as being the closest to the Fund's institutional mandate for the stability of the international monetary system, and thus an appropriate entry point for the Fund in the discussion on fintech.[14]

39. Most recently, the Bali Fintech Agenda has been developed with the World Bank to provide a broad framework for guiding consideration of high-level fintech policy issues by the international community and member governments (IMF and World Bank Group, 2018). This agenda was set out in a joint IMF-World Bank staff paper discussed by the Boards of the Fund and the Bank, endorsed by the joint Bank/Fund Development Committee, and submitted to the IMFC during the 2018 Annual Meetings. The paper outlined in general terms twelve areas where fintech could have implications for financial stability, integrity, or development. The agenda will help guide the IMF and World Bank staff in their work on fintech issues within their expertise and mandate. While the Agenda does not represent a work program, the paper suggests that the IMF's initial focus will be on the implications of fintech for cross-border flows; national and global

[14] An alternative approach would be to prioritize the areas of fintech that have the biggest potential impact on financial market stability. Under this approach, it is doubtful that cross-border payment and settlements would come on top: other areas of fintech, such as innovations in investment management services (robo-trading) that have the potential to increase market volatility, or the role of AI and big data in disrupting the business models of traditional financial institutions, would probably be higher priorities.

monetary and financial stability; and the evolution of the international monetary system and the global financial safety net.

40. Fintech issues have been covered in **bilateral surveillance** in a range of countries. In contrast to the topic of cyber risk, the coverage has been greater in Article IV reports than in FSSAs (Appendix Tables A.2 and A.3). The coverage has typically focused on the aspects of fintech most relevant to the country. In many developing countries, such as Kenya and Tanzania, staff papers discussed technologies (such as mobile payments, e-wallets and, in the case of India, the deployment of biometric IDs) from the perspective of financial inclusion, where fintech can have a potentially transformative impact on economies where access to financial services has so far been quite limited. In a few countries, Article IV staff reports provided detailed descriptions of fintech trends in their jurisdictions, as well as a rich discussion of the policy and regulatory issues involved. This tended to be the case in countries where fintech is growing rapidly and is already an important issue for the authorities (e.g., Singapore and Hong Kong SAR). Representatives of the authorities in these jurisdictions welcomed the staff's initiative: although the Article IV staff were "clearly not experts" in these areas, they had generally been eager to engage and to learn.

41. By contrast, in the majority of the cases reviewed, the coverage of fintech issues was brief—often just a short reference to the potential of fintech, and support for the authorities' initiatives in this area. Article IV and FSAP staff teams that covered fintech issues lightly (or not all) in their reports explained that this choice reflected their assessment that these issues were not yet important enough to be systemic or macro-relevant in their countries, especially compared to other, higher priority topics. In some cases, they said they had discussed these issues with the authorities in depth but, due to the word limits for staff reports and the need for prioritization, they could not report on these discussions at length.

C. Digital Currencies

42. The Fund has been following the issue of digital currencies along with general fintech issues. It engaged with the topic as an **analytical** issue relatively early, with an SDN in January 2016 on "Virtual Currencies and Beyond: Initial Considerations" (He and others, 2016). The SDN described the technology underlying digital currencies, addressed the question whether they are "proper" currencies, and discussed the legal, policy, and regulatory issues they raise, albeit without making specific policy recommendations. The SDN was followed by a number of **outreach** activities (Appendix Table A.1) and, more recently, an interdepartmental was formed to study on central bank digital currencies.

43. Until recently, digital currencies received little attention in **bilateral surveillance**, as staff considered that their scale had not merited coverage in Article IV discussions or in FSAPs. In fact, there was no reference to digital currencies in Article IV staff reports or FSSAs in the 25 countries that were examined as part of this stocktaking. However, the situation changed in 2018 as some

countries have actively considered issuing their own official digital currency.[15] For example, in March 2018, the Republic of the Marshall Islands announced that it had decided to create the digital "Sovereign," recognized in law as legal tender.[16] Accordingly, this was discussed in the 2018 Article IV staff report, published in September (IMF Country Report No. 18/270), that contains a comprehensive analysis that will likely inform staff positions in other countries where the issue may be relevant. In fact, a number of staff teams in Asia reported that the issue had been discussed in the most recent consultation and were planning to study it in more depth in next year's consultation.

44. Outreach efforts centered around digital currencies have also stepped up recently. In 2017, following a number of security breaches in a few crypto-exchanges and wide gyrations in the price of Bitcoin, digital currencies entered the G20 agenda, and received much greater IMF attention. The Managing Director published a blog and the IMF organized a workshop in April 2018 on technology and finance—a large part of which was focused on digital currencies. A speech by the Director of MCM to that workshop provided a comprehensive, high-level discussion of the risks and regulatory response to digital currencies (Appendix Table A.1). The April 2018 *GFSR* included a Box on crypto-currencies ("crypto-assets" is staff's preferred nomenclature). Finally, digital currencies were mentioned in the Board paper on the "Bali Fintech Agenda," discussed in the previous section.

IV. CONCLUDING OBSERVATIONS

45. This stocktaking shows that the Fund has been paying increasing attention to technology-related issues in finance, both from an analytical perspective and—to a more limited extent—as a topic for bilateral surveillance. While this engagement is in its early stages and still evolving quickly, there is widespread understanding of the importance of these issues, clear commitment—indeed enthusiasm—among the staff, and a strong sense that Management considers them a priority. There is a core of staff that are well informed, strongly motivated, and have built a network of contacts around the world, including with the private sector.

46. These are issues where the official sector as a whole has had to scramble to keep up with innovations. Central banks and standard-setting bodies are only gradually developing their approaches, policies and regulatory frameworks for these issues. For its part, the Fund has been particularly active in outreach and convening efforts aimed at disseminating good practices among developing and non-G20 emerging market countries and facilitating knowledge-sharing between these and advanced economies. In addition, over the past couple of years, the Fund has strengthened its analytical and policy work and started to develop an institutional view on these

[15] For example, the Swedish Riksbank has been studying this issue for over a year now (Sveriges Riksbank, 2017). In February 2018, Venezuela launched the "petromoneda" or "petro," an official cryptocurrency backed by oil and mineral reserves. For a more complete list of country cases, see Prasad (2018).

[16] "This is the first country to adopt a cryptocurrency as its official currency," see Hosia and Perry (2018).

innovations and integrating these topics in surveillance. At the global level, the Fund has been more active on fintech and digital currencies, than on cyber risks. At the country level, Article IV and FSAP teams have discussed these issues in depth in a handful of cases, where they focused on cyber risk or general fintech issues, and more recently on digital currencies. Generally—as one might expect—the depth of coverage of technology-related issues in bilateral surveillance, varied widely, reflecting an assessment of the importance of these issues in the jurisdictions concerned.

47. Looking ahead, the IMF is committed to continue to build its expertise in this fast-moving area so as to meet the strong interest in member countries for guidance and support. Past experience when the Fund has faced a new or emerging issue has shown the importance of clear prioritization to focus on areas where the Fund can add value in areas related to its mandate, of ensuring adequate resources to build up necessary in-house expertise, and of working closely with partner institutions to maximize synergies.

APPENDIX. FUND DOCUMENTS AND PUBLICATIONS ON TECHNOLOGY-RELATED ISSUES IN FINANCE

The stocktaking exercise is based on a review of two sets of documents: (i) Fund documents, publications, and events, including the flagship publications of multilateral surveillance, published research (SDNs and Working Papers), articles, blogs, speeches, conferences, workshops, panel discussions during the Annual or Spring Meetings, etc., summarized in Table A.1; and (ii) Fund country documents (Article IV staff reports and Financial System Stability Assessments—FSSAs) for 25 jurisdictions for the period 2013 to mid-2018 (given the nature of the issues, there is virtually no mention of them in Fund documents before 2013), summarized in Appendix Tables A.2 and A.3.

The jurisdictions covered in the review are Australia, Belgium, Chile, China, the Euro area, Finland, France, Germany, Hong Kong SAR, India, Japan, Kenya, Korea, Luxembourg, Malaysia, Mexico, the Netherlands, Nigeria, Singapore, South Africa, Sweden, Switzerland, Tanzania, U.K., and U.S.A.. The sample includes most G20 jurisdictions, as well as several non-G20 jurisdictions, both advanced and developing, selected on the basis of an *a priori* assessment that technology-related issues are relevant in these.

It is important to stress that this is not a random sample: technology-related issues are more likely to have been discussed with the authorities in these jurisdictions during bilateral surveillance (Article IV missions and FSAPs) than in other Fund member countries. This review of country documents is therefore not representative of the coverage of these issues by the Fund in surveillance globally: the degree and depth of coverage in these jurisdictions is likely to be much higher than across the Fund membership as a whole.

At the same time, this bias in selecting the sample means that it is reasonable to expect that at least some of these issues would be discussed in the context of bilateral surveillance in most or all of these jurisdictions.

APPENDIX TABLE A.1. FUND PUBLICATIONS AND EVENTS ON EMERGING TECHNOLOGY-RELATED ISSUES IN FINANCE

Year	Topic	Type	Reference	Notes
2018	CR	SP	Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment, WP/18/143	A VaR-type methodology for assessing the potential costs of cyber attacks on financial institutions.
2018	DC	OUT	Fintech—Building Trust Through Regulation	Speech by the Director of MCM focusing on the risks and regulatory response to digital currencies.
2018	DC, CR, OTH	SP	Fintech, Inclusive Growth and Cyber Risks: Focus on the MENAP and CCA Regions, WP/18/201	Reviews the fintech landscape in the MENAP and CCA regions, identifies the constraints to the growth of fintech and its contribution to inclusive growth and considers policy options to unlock the potential.
2018	DC, CR, OTH	WKS	Emergence of FinTech: Opportunities and Challenges for the Arab World	High-level roundtable, organized with the Arab Monetary Fund, that gathered central bank governors and heads of institutions from the Arab Region.
2018	DC, OTH	SP	Measuring the Digital Economy	STA Policy Paper that includes a section on the challenges of digitalization for monetary and financial statistics, including e-money and digital currencies.
2017	CR	OUT	Cyber Defense Must Be Global, IMFBlog, October 26, 2017	Blog by the authors of WP/17/185 presenting the key findings of their paper
2017	CR	SP	Cyber Risk, Market Failures, and Financial Stability, WP/17/185	Detailed analysis of cyber risk, data or recent attacks, impact estimates, and underlying market failures. Analysis of potential financial stability impact and regulatory remedies.
2017	DC, OTH	OUT	Central Banking and Fintech--A Brave New World?	Conference speech by the MD on broad fintech implications (mainly on monetary policy and regulation). Claims IMF is "ideal platform" for these topics b/c of its "mandate for economic and financial stability and the safety of our global payments and financial infrastructure."
2017	OTH	SP	A Rapidly Changing Financial System	Chapter in book "Modernizing China: Investing in Soft Infrastructure," IMF (2017). Focused on China, mostly descriptive. P2P payments systems mentioned but no specific policy recommendations.
2017	CR	WKS	Regulatory and Supervisory Approaches in Managing Cyber Risk	By-invitation workshop organized jointly with the National Bank of Belgium for representatives from about 60 developing and emerging market countries on cyber risk.
2017	OTH	SP	Fintech and Financial Services: Initial Considerations, SDN/17/05	General introduction to fintech, financial services, and regulation; paper focuses mainly on cross-border payments.
2017	OTH	SP	Taxation and the Peer-to-Peer Economy, WP/17/187	WP focusing on the implications of P2P economy (gig economy, AIrBnB, Uber, BlaBlaCar, etc.) for tax policy and administration, and potential solutions.
2017	OTH	OUT	Banking on the Go, IMFBlog, June 23, 2017	Podcast by Paga founder on mobile payments in Nigeria.
2017	OTH	OUT	Democratizing the Money Market, IMFBlog, May 26, 2017	Podcast by external expert on general fintech issues.
2017	OTH	OUT	Fintech: Capturing the Benefits, Avoiding the Risks, IMFBlog, June 20, 2017	Blog by the MD based on the SDN on "Fintech and Financial Services."

Year	Topic	Type	Reference	Notes
2017	OTH	OUT	Fintech—A Brave New World for the Financial Sector?, IMFBlog, January 20, 2017	Blog by the MD on a speech in Dubai, also anticipating the SDN on "Fintech and Financial Services."
2017	OTH	OUT	Fintech: Challenges to Regulation and Central Banking	Panel chaired by the MD at the 2017 Annual Meetings, mainly focused on regulatory challenges of fintech.
2017	OTH	OUT	Fintech and the Transformation of Financial Services	Panel discussion with external experts at the 2017 Annual Meetings.
2017	CR	WKS	The role of supervision in building resilience against cyber risk	By-invitation roundtable at the 2017 Spring Meetings for central bank governors from about 30 jurisdictions.
2017	OTH	WKS	Driving Digital Inclusion in Africa	Seminar at the 2017 Spring Meetings on digital financial services, using Nigeria's PAGA as a case study and a contribution by the central bank governor of Tanzania.
2017	OTH	OUT	Key challenges from fintech (F&D)	Three articles in Sept. 2017 F&D on fintech, leveraging work already published by staff.
2017	DC, CR, OTH	SP	Fintech: Unlocking the Potential for the MENAP and CCA Regions	Chapter in the Regional Economic Outlook: Middle East and Central Asia, October 2017.
2016	DC	SP	Virtual Currencies and Beyond: Initial Considerations, SDN/16/03	SDN on digital currencies, including an economic foundation, discussion of potential implications in a number of areas, and (in general terms) regulatory/policy issues.
2016	DC	OUT	Virtual Currencies: The Public Impact of Private Money, IMFBlog, January 20, 2016	Blog on the SDN on "Virtual Currencies and Beyond: Initial Considerations."
2016	DC	OUT	The Internet of Trust, F&D, June 2016	Article on digital currencies and the underlying DLT technology.
2016	OTH	OUT	Leveraging Financial Technology for the Underbanked, IMF Country Focus, September 19, 2016	Article on IMF Country Focus online on fintech and financial inclusion, following a conference in Dakar.

Notes: DC: Digital currencies; CR: Cyber risk; OTH: General fintech issues.
SP: Staff paper or publication with analytical or policy content (WP, book, SDN, etc.); OUT: Outreach & advocacy (speech, blog, panel discussion, article in F&D or IMF Country Focus online, etc.); WKS: Workshop, conference, etc.

APPENDIX TABLE A.2. ARTICLE IV COVERAGE OF EMERGING TECHNOLOGY-RELATED ISSUES IN FINANCE[1]

Year	Topic	Country	Document	Notes
2018	OTH, CR	Belgium	SR	Brief reference to the "need for the financial sector to adapt to growing digitalization and step up protections against cyber risk".
2018	OTH	PR China	SR	Reference to the challenge of fintech for financial regulation and the authorities' strategy in this area.
2017	OTH	PR China	SR	Several references to "shadow banking" and the need to regulate it; reference to the previous year's regulatory initiative (see 2016 SR).
2016	OTH	PR China	SR	Several references to "shadow credit products" and calls for their "holistic supervision;" reference to a recent regulatory initiative of the authorities.
2015	OTH	PR China	SR	Several references to "shadow banking" and associated risks, and the need to tighten regulations.
2014	OTH	PR China	SR	Full page Box on "Growth in Shadow Banking and Internet Finance," but the latter focuses only on internet-based MMFs. Call to find the "right balance between investors, regulators, and policy-makers," no specific recommendations.
2017	OTH, CR	Hong Kong SAR	SR, SIP	Extensive and prominent discussion of regulatory efforts to coordinate approach to different fintech platforms, including the benefits and costs of fintech. SIP on "Fintech in Hong Kong: Opportunities and Challenges" provides an overview of regulatory initiatives. Reference to measures taken to bolster cyber security.
2016	OTH, CR	Hong Kong SAR	SR	Brief reference to the "challenges" of fintech and to authorities' preparedness to deal with cyber threats; no staff analysis. Brief discussion of authorities' macroprudential oversight of shadow banks.
2015	OTH	Hong Kong SAR	SR	Brief reference to macroprudential oversight of shadow banks.
2017	OTH	France	SR	Brief reference to how "fintech" could squeeze bank profits. No analysis or evidence, no discussion of policies.
2016	OTH	France	SIP	Fintech mentioned as one of the factors that could threaten banks' traditional business models. Reference to how banks adjust to this challenge. No staff analysis of potential implications or policies.
2017	OTH	India	SR	Box on Financial Inclusion focuses on initiatives to increase access to "basic banking services," especially for women; it includes a brief reference to "technology-driven initiatives" but no analysis or policy discussion.
2016	OTH	India	SR	Box on Enhancing Financial Inclusion provides overview of initiatives to widen access to banking services, including through biometric IDs and mobile payments but no analysis or policy discussion.
2015	OTH	India	SR, SIP	Reference to the use of new technologies (notably biometric ID) as a means of increasing financial inclusion. SIP on financial inclusion focuses on the links between firms' access to finance (a proxy for inclusion), output, and inequality.
2014	OTH	India	SR	Box on India's biometric ID scheme (*Aadhaar*) with a reference to its potential impact on financial inclusion.
2018	CR	Kenya	SR	Brief mention of a guidance note to banks issued by the regulator on cyber-security.

Year	Topic	Country	Document	Notes
2014	OTH	Kenya	SR	Discussion of mobile banking (M-Pesa) and deposit-lending for the poor (M-Shwari) in the context of financial inclusion. Full-page box on impact of mobile banking and inclusion on welfare. Subsequent program documents (2015-17) do not mention these initiatives.
2018	OTH	Luxembourg	SR	Brief reference to the challenge of fintech for financial regulation, but no discussion.
2017	OTH	Luxembourg	SR	Reference to the authorities' intention to follow up on the 2017 FSAP recommendations on, among others, "studies on bank-fund interlinkages and shadow banking."
2017	OTH	Luxembourg	SIP	Brief mention of "fintech" as one of example of innovative finance supported by a public-private partnership but no analysis or examples.
2017	OTH	Mexico	SR	Brief mention of "fintech" as one of the ways to enhance financial inclusion in reference to the authorities' Inclusion Strategy; no details.
2018	OTH	Nigeria	SR	Brief reference to the need to accelerate the financial inclusion strategy including through “reliable and inclusive mobile payments systems,” but no analysis.
2017	OTH	Nigeria	SR	Report on progress of the 2013 FSAP recommendation to "Revise the 2009 Regulatory Framework for Mobile Payment Services to level the playing field and intensify competition."
2016	OTH	Nigeria	SIP	Reference to authorities' progress in increasing banking penetration and facilitating other channels for savings "to move from the informal to informal sectors (e.g., innovative insurance products distributed through mobile distribution channels)."
2014	OTH	Nigeria	SR, SIP	Discussion of mobile payments platforms (e-wallet) for financial inclusion, including in SIP. Staff stress the need for proper regulatory oversight, e.g. protection of deposits in e-wallets and AML/CFT. Brief discussion of mobile payment platforms for banking, pension funds, and insurance.
2018	OTH	Singapore	SR	Reference to MAS’s support for fintech applications and attendant adaptation of regulations; discussion of risks is postponed to the 2019 FSAP. Appendix VII takes stock of the latest developments of fintech companies’ activities in Singapore and in the Asia region.
2017	OTH, CR	Singapore	SR, SIP	Brief mention of staff support to the authorities' initiatives in fintech and cyber security in SR (in the context of a "new growth model" of digital tech and automation). Full-page descriptive box on fintech and cyber risk in SIP on innovation and growth (but SIP focuses mostly on automation).
2016	OTH	Singapore	SR	Appendix on "Developments in Fintech" provides a detailed overview of fintech trends in Singapore and discussion of initiatives to support tech development, but not of regulatory issues.
2018	OTH	South Africa	SR	Brief reference to Fintech Unit at the SARB in the context of discussing the growth potential of digitalization for growth and financial inclusion, and some discussion of financial sector impact.
2017	OTH	South Africa	SR	Discussion of mobile payments in the context of financial development and inclusion (includes comparison to BRICS) - Annex II on financial inclusion. -References fintech as an option, based on int'l experience, to further financial inclusion -Reports on discussions with authorities on fintech and regulatory framework.
2014	OTH	South Africa	SR	Brief mention of mobile banking.

Year	Topic	Country	Document	Notes
2017	OTH	Sweden	SR	Appendix on FSAP recommendations reports that the financial supervisory authority joined the work program of the Joint Committee of the European Supervisory Authorities which included a task for the subcommittee on Consumer Protection and Financial Innovation that focuses on cross border supervision of financial services.
2017	OTH	Tanzania	PRG	Brief discussion of mobile and internet services and its impact on monetary policy: "The impact of the slow growth was partly dampened by gradual rise in the money multiplier and the velocity of circulation on the back of financial innovations especially the enhanced use of mobile phone financial services which has been boosted by interoperability across network operators."
2016	OTH	Tanzania	PRG	Extensive discussion of mobile money.
2015	OTH	Tanzania	PRG	Extensive discussion of mobile services in the context of financial sector development, cross-border money transfers, and regulation.
2017	CR	U.K.	SR	Cyber attacks mentioned as a medium risk in the RAM, but no analysis of potential impact or discussion of mitigation policies; no discussion in text.
2016	CR	U.K.	SR	Reference to the analysis of cyber risk in that year's FSSA.
2015	CR	U.K.	SR	Reference to the authorities' awareness of cyber risks; no staff analysis.
2018	CR, DC	U.S.A.	SR	Brief reference to the authorities' assessment that risks from unregulated financial institutions and activities (including cryptocurrencies and cyber risk) are moderate.
2017	CR	U.S.A.	SR	Extensive discussion of cyber risks in text and a full-page Box leveraging the analysis in WP/17/185. Reference to cyber attacks as a "Low" risk in RAM.
2015	CR	U.S.A.	SR	Brief reference to "need to increase cyber resilience" for CCPs; no reference in RAM.

Notes: DC: Digital currencies; CR: cyber risk; OTH: general fintech issues.
SR: Staff report; SIP: Selected Issues Paper; PRG: Program document.
[1] This is not an exhaustive list but an overview of the coverage of technology-related emerging issues in finance by staff in Article IV consultations in a sample of countries (see text for details on the selection of the sample). The reviewed documents include Article IV consultation documents from 2014 through mid-2018 for Australia, Belgium, Chile, China, the Euro area, Finland, France, Germany, Hong Kong SAR, India, Japan, Kenya, Korea, Luxembourg, Malaysia, Mexico, the Netherlands, Nigeria, Singapore, South Africa, Sweden, Switzerland, Tanzania, U.K., and U.S.A..

APPENDIX TABLE A.3. FSAP COVERAGE OF EMERGING TECHNOLOGY-RELATED ISSUES IN FINANCE[1]

Year	Topic	Country	Document	Topic Mentioned in		Notes
				Executive Summary	Table of Key Recommendations	
2018	CR	Belgium	FSSA	Y	Y	Discussion of oversight of SWIFT following recent incidents in its global user network and specific recommendation regarding the role of NBB in its oversight.
2018	CR	Euro Area	FSSA	N	N	Reference to cyber risk as a source of concern for financial institutions and the need for the SSM to develop a strategy.
2017	OTH	China	FSSA	Y	Y	Discussion of innovations in the context of shadow banking, as well as of inclusion; recommendations to level the regulatory playing field for all similar products and enhance the leg/reg framework for fintech. Box on financial engineering.
2017	OTH	India	FSSA	N	N	Discussion of digitalization in the context of inclusion, in the section on "fostering long-term market development."
2017	CR	Japan	FSSA	N	N	One paragraph referring to the authorities' policy framework on cyber crime. (TN on "Long-term challenges for financial intermediation" focuses on SMEs, ageing, etc. but not on any technology-related issues).
2017	OTH	Luxembourg	FSSA	N	N	Disruption due to "fintech" is mentioned as one of the risks in the RAM, but no discussion in text. No mention of cyber risk.
2016	CR	Germany	FSSA	N	N	Full page box on cyber risk and the regulatory response.
2016	CR	U.K.	FSSA	N	N	Full page box on cyber risk and the regulatory response.
2015	CR	U.S.A.	FSSA	N	N	References to the importance of cyber risk and cyber resilience in the sections on the supervision of banks, securities markets, and CCPs; in the RAM; and in the ROSCs.

Notes: DC: Digital currencies; CR: Cyber risk; OTH: General fintech issues.

[1] This is not an exhaustive list but an overview of the coverage of technology-related emerging issues in finance by staff in FSAPs that took place in a sample of countries (see text for details on the selection of the sample) from 2013 through mid-2018. The FSAPs reviewed are: Belgium (2018), Canada (2014), China (2017), Denmark (2014), the Euro area (2018), Finland (2016), Germany (2016), Hong Kong SAR (2014), India (2017), Ireland (2016), Italy (2013), Japan (2017), Korea (2014), Luxembourg (2017), Mexico (2016), the Netherlands (2017), Nigeria (2013), Norway (2015), Singapore (2013), Spain (2017), Sweden (2016), Switzerland (2014), U.K. (2016), and U.S.A. (2015).

REFERENCES

Arner, D.W., J. Barberis, and R.P. Buckley, 2016, "FinTech, RegTech and the Reconceptualization of Financial Regulation" *Northwestern Journal of International Law and Business* (forthcoming).

Bank of England, 2018, "Financial sector continuity," October. Available at https://www.bankofengland.co.uk/financial-stability/financial-sector-continuity.

Bank for International Settlements (BIS), 2018, "Authorities should be prepared to act on cryptocurrencies: Carstens," Press Release, February.

Basel Committee on Banking Supervision (BCBS), 2004, "International Convergence of Capital Measurement and Capital Standards: A Revised Framework", Bank for International Settlements. Available at https://www.bis.org/publ/bcbs107.pdf.

_____, 2018, "Sound Practices: Implications of Fintech Development for Banks and Bank Supervisors", February, Bank for International Settlements. Available at https://www.bis.org/bcbs/publ/d415.pdf.

Bouveret, A., 2018, "Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment," IMF Working Paper No. WP/18/143. Available at https://www.imf.org/~/media/Files/Publications/WP/2018/wp18143.ashx (Washington: International Monetary Fund).

Brainard, L., 2016, "The Opportunities and Challenges of Fintech," Remarks at the Conference on Financial Innovation at the Board of Governors of the Federal Reserve System. Available at https://www.federalreserve.gov/newsevents/speech/brainard20161202a.htm.

Canepa, Francesco, 2018, "G20 leaders to hold fire on cryptocurrencies amid discord: sources," Reuters, March.

Committee on the Global Financial System and Financial Stability Board (2017), "Fintech Credit: Market Structure, Business Models, and Financial Stability Implications," Financial Stability Board. Available at http://www.fsb.org/wp-content/uploads/CGFS-FSB-Report-on-FinTech-Credit.pdf.

Committee on Payments and Market Infrastructures, 2015, "Digital Currencies," November 2015, Bank for International Settlements. Available at https://www.bis.org/cpmi/publ/d137.pdf.

_____, 2016, "Guidance for Cyber Resilience for Financial Market Infrastructures," June 2016, Bank for International Settlements. Available at https://www.bis.org/cpmi/publ/d146.pdf.

_____, 2017, "Distributed Ledger Technology in Payment, Clearing and Settlement—An Analytical Framework," February 2017, Bank for International Settlements. Available at https://www.bis.org/cpmi/publ/d157.htm.

_____, 2018, "Central Bank Digital Currencies," March 2018, Bank for International Settlements. Available at https://www.bis.org/cpmi/publ/d174.pdf.

Depository Trust & Clearing Corporation (DTCC), 2017, *Fintech and Financial Stability*, White Paper, October 2017. Available at www.dtcc.com/~/media/Files/PDFs/Fintech%20and%20Financial%20Stability.pdf.

Dhar, V. and R.M. Stein, 2017, "Fintech Platforms and Strategy," MIT Sloan School Working Paper 5183-16, MIT. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2892098.

Diedrich, H., 2016, *Ethereum: Blockchains, Digital Assets, Smart Contracts, Decentralized Autonomous Organizations*, Wildfire Publishing.

Federal Financial Institutions Examination Council, 2017, *Cybersecurity Assessment Tool*, FFIEC. Available at https://www.ffiec.gov/cyberassessmenttool.htm.

Financial Stability Board (FSB), 2017, "Financial Stability Implications from FinTech: Supervisory and Regulatory Issues that Merit Authorities' Attention," June. Available at http://www.fsb.org/wp-content/uploads/R270617.pdf.

Financial Stability Institute (FSI), 2017, "Regulatory Approaches to Enhance Banks' Cyber-security Frameworks," *FSI Insights on Policy Implementation No. 2*, Bank for International Settlements. Available at https://www.bis.org/fsi/publ/insights2.pdf.

Group of Seven (G7), 2016, "G7 Fundamental Elements of Cybersecurity for the Financial Sector," October. Available at https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf?69e99441d6f2f131719a9cada3ca56a5.

_____, 2017, "G7 Fundamental Elements of Cybersecurity for the Financial Sector." Available at http://www.mef.gov.it/inevidenza/documenti/PRA_BCV_4728453_v_1_G7_Fundamental.pdf.

Group of Twenty (G20), 2018, "Communiqué of the First G20 Meeting of Finance Ministers and Central Bank Governors of 2018," March (Argentina).

He, D., and others, 2016, "Virtual Currencies and Beyond: Initial Considerations," IMF Staff Discussion Note SDN/16/03. Available at https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf (Washington: International Monetary Fund).

He, D., and others, 2017, "Fintech and Financial Services: Initial Considerations," IMF Staff Discussion Note SDN/17/05. Available at https://www.imf.org/~/media/Files/Publications/SDN/2017/sdn1705.ashx (Washington: International Monetary Fund).

Hochstein, M., 2015, "Fintech (The Word, That Is) Evolves," *American Banker,* October 5, 2015. Available at https://www.americanbanker.com/opinion/fintech-the-word-that-is-evolves.

Hosia, Hilary, and Nick Perry, 2018, "This is the First Country to Adopt a Cryptocurrency as its Official Currency," *Money*, March. Available at http://time.com/money/5186316/this-is-the-first-country-to-adopt-a-cryptocurrency-as-its-official-currency/.

International Association of Insurance Supervisors, 2017, *Fintech Developments in the Insurance Industry*, February. Available at https://www.iaisweb.org/page/news/other-papers-and-reports/file/65625/report-on-fintech-developments-in-the-insurance-industry.

International Monetary Fund (IMF), 2017, "IMF Managing Director Welcomes Establishment of High Level Advisory Group on FinTech," IMF Press Release No. 17/84, February (Washington).

International Monetary Fund and The World Bank Group, 2018, "The Bali Fintech Agenda—Chapeau Paper," October. Available at https://www.imf.org/~/media/Files/Publications/PP/2018/pp101118-bali-fintech-agenda.ashx.

International Organization of Securities Commissions (IOSCO), 2017, *Research Report on Financial Technologies*, February. Available at https://www.iosco.org/library/pubdocs/pdf/IOSCOPD554.pdf.

Kay, J., 2017, "Technological Change and the Future of Financial Intermediation," presentation at the 44th economics conference of the Oesterrechische Nazionalbank, June. Available at https://www.johnkay.com/2017/06/24/technological-change-future-financial-intermediation/.

Keidanren, 2015, "Proposal for Reinforcing Cybersecurity Measures (Summary)," February. Available at http://www.keidanren.or.jp/en/policy/2015/017_summary.pdf.

Khiaonarong, T., 2014, "Oversight Issues in Mobile Payments", IMF Working Paper No. 14/123. Available at https://www.imf.org/en/Publications/WP/Issues/2016/12/31/Oversight-Issues-in-Mobile-Payments-41747 (Washington: International Monetary Fund).

Kopp, E., L. Kaffenberger, and C. Wilson, 2017, "Cyber Risk, Market Failure, and Financial Stability," IMF Working Paper WP/17/185. Available at http://www.imf.org/~/media/Files/Publications/WP/2017/wp17185.ashx) (Washington: International Monetary Fund).

Maupin, J., 2017, "Blockchains and the G20: Building An Inclusive, Transparent and Accountable Digital Economy," Centre for International Governance Innovation Policy Brief No. 101, March 2017. Available at https://www.cigionline.org/publications/blockchains-and-g20-building-inclusive-transparent-and-accountable-digital-economy.

McKinsey & Company, 2015, "Cutting Through the FinTech Noise: Markers of Success, Imperatives for Banks," December 2015. Available at https://www.mckinsey.com/~/media/mckinsey/industries/financial%20services/our%20insights/cutting%20through%20the%20noise%20around%20financial%20technology/cutting-through-the-fintech-noise-full-report.ashx.

Office of the Comptroller of the Currency, 2013, *Semiannual Risk Perspective*, Fall 2013, OCC. Available at https://www.occ.gov/publications/publications-by-type/other-publications-reports/semiannual-risk-perspective/semiannual-risk-perspective-fall-2013.pdf.

Office of Financial Research, 2016, *2016 Financial Stability Report*, Office of Financial Research. Available at https://www.financialresearch.gov/financial-stability-reports/files/OFR_2016_Financial-Stability-Report.pdf.

_____, 2017, *2017 Financial Stability Report*, Office of Financial Research. Available at https://www.financialresearch.gov/financial-stability-reports/2017-financial-stability-report/.

Oliver Wyman, 2018, *Cryptocurrencies and Public Policy: Key Questions and Answers*, February 2018. Available at http://www.oliverwyman.com/our-expertise/insights/2018/feb/cryptocurrencies-and-public-policy.html.

Philippon, T., 2015, "Has the US Finance Industry Become Less Efficient? On the Theory and Measurement of Financial Intermediation," *American Economic Review*, vol. 105, No. 4, pp. 1408-38.

_____, 2017, "The Fintech Opportunity," BIS Working Paper No. 655, Bank for International Settlements. Available at https://www.bis.org/publ/work655.pdf.

Power, M., 2003, "The Invention of Operational Risk," Discussion Paper No. 16, Centre for Analysis of Risk and Regulation (CARR), London School of Economics and Political Science, Available at http://eprints.lse.ac.uk/21368/1/DP16.pdf.

Prasad, Eswar, 2018, "Central Banking in a Digital Age: Stock-Taking and Preliminary Thoughts," Hutchins Center on Fiscal & Monetary Policy Working Paper, April (Washington: The Brookings Institution).

Quarles, R., 2017, "Thoughts on Prudent Innovation in the Payment System," Remarks at the 2017 Financial Stability and Fintech Conference, sponsored by the Federal Reserve Bank of Cleveland, the Office of Financial Research, and the University of Maryland's Robert H. Smith School of Business. Available at https://www.federalreserve.gov/newsevents/speech/files/quarles20171130a.pdf.

Roubini, N. and P. Byrne, 2018, "The Blockchain Pipe Dream," Project Syndicate commentary, March 5, 2018. Available at https://www.project-syndicate.org/commentary/blockchain-technology-limited-applications-by-nouriel-roubini-and-preston-byrne-2018-03.

Sveriges Riksbank, 2017, *E-Krona Project Plan*, March 14, 2017. Available at https://www.riksbank.se/globalassets/media/rapporter/e-krona/2017/projektplan-e-kronan_170314_eng.pdf.

Swan, M., 2015, *Blockchain: Blueprint for a New Economy*, O'Reilly Publications.

White House, 2013, "Presidential Policy Directive—Critical Infrastructure Security and Resilience," Presidential Policy Directive PPD-21, February 12, 2013. Available at https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

World Economic Forum, 2012, *Risk and Responsibility in a Hyperconnected World—Pathways to Global Cyber Resilience*, WEF, Geneva. Available at http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf.