ADBI Working Paper Series

REGULATING FINTECH: OBJECTIVES, PRINCIPLES, AND PRACTICES

Marlene Amstad

No. 1016
October 2019

Asian Development Bank Institute

Marlene Amstad is a professor at the School of Management and Economics, The Chinese University of Hong Kong, Shenzen, and vice chair of the board at the Swiss Financial Market Supervisory Authority.

The views expressed in this chapter are those of the author and do not necessarily represent those of FINMA.

Suggested citation:

Amstad, M. 2019. Regulating Fintech: Objectives, Principles, and Practices. ADBI Working Paper 1016. Tokyo: Asian Development Bank Institute. Available: https://www.adb.org/publications/regulating-fintech-objectives-principles-practices

Please contact the authors for information about this paper.

Email: marleneamstad@cuhk.edu.cn

Asian Development Bank Institute
Kasumigaseki Building, 8th Floor
3-2-5 Kasumigaseki, Chiyoda-ku
Tokyo 100-6008, Japan

Tel: +81-3-3593-5500
Fax: +81-3-3593-5571
URL: www.adbi.org
E-mail: info@adbi.org

Abstract

We provide an overview and key elements on the ongoing debate of whether and how to regulate fintech. The paper reviews three objectives of financial regulation (investor protection, market integrity, safeguarding financial stability) in the context of recent fintech developments, covers three guiding principles many regulators follow (legal certainty, technology neutrality, and proportionality), and ends with a suggested synopsis of current fintech regulatory practices: “wait-and-see”, “same risk, same rules” (“duck typing”), or “new functionality, new rules” (“coding”).

Keywords: fintech, financial technology, digital currency

JEL Classification: G15, F65, O16

Contents

1. INTRODUCTION

Two events have shaped the financial system over the past 10 years: the global financial crisis and the rise of the digital finance ecosystem, broadly labelled as financial technology or fintech.[1] Both raised questions about appropriate regulatory response. The lessons learned after the crisis have been widely discussed and the response broadly agreed upon—though not yet fully implemented[2]—in the global regulatory framework Basel III. However, whether and how to regulate fintech is still in its early stages and is a topic of an active policy and academic debate.

In the context of recent fintech developments, this paper reviews the objectives of financial regulation, covers key guiding principles regulators follow, and ends with a suggested synopsis of the current regulatory practices. Given the very diverse and rapidly developing fintech landscape, it is beyond the scope of this article to aim for completeness; rather, the goal is to offer an overview and focus in each section on a few key regulatory elements. In that, it identifies three core objectives, three guiding principles, and three regulatory practices.

2. OBJECTIVES

A precondition of good regulation is clarity about needs and goals. The finance literature commonly gives at least three forms of market failures for which regulation is needed: information asymmetry, importance of externalities (moral hazard), and monopoly power (Armour et al. 2016; Brunnermeier et al. 2009; Freixas and Rochet 2008). From these, among others, core objectives such as investor and consumer protection, financial stability, and market integrity take shape.[3] While the hierarchy of goals varies in each jurisdiction, most regulators cover these core elements in some form. This section touches on each in the context of fintech. While the introduction of fintech poses new challenges and opportunities, the core objectives of regulation likely can also provide appropriate guidance, both on whether or not and how to regulate digital finance.

2.1 Reduce Information Asymmetry: Investor and Consumer Protection

Information asymmetries motivate investor protection or, more broadly, protection of consumers of financial services. Digital finance introduces possibilities to both increase and decrease information asymmetry.

[1] Different terms are used, among which the most prominent ones are crypto-currencies, crypto-assets, and digital assets; less common is virtual or distributed ledger technology (DLT) asset. The terms fintech and digital finance will be used interchangeably in this paper.

[2] See Hohl et al. (2018) for a recent review on implementation of the Basel framework for 100 jurisdictions. Special focus is given to how implementation is shaped following the principle of proportionality (covered in section 3.3).

[3] While several additional objectives are discussed, like the contribution to financial sector competitiveness, those can, in many cases, be achieved indirectly via a successful implementation of the aforementioned investor protection, financial stability, and market integrity.

2.1.1 Risks of Increased Information Asymmetry

A key risk for information asymmetry lies in the code that underpins digital finance. While disclaimers testify to the need for some financial and legal knowledge, the ability to know whether the code, public or otherwise, does what it promises is a potential additional obstacle. This is particularly the case when a code (or proof of work or consensus finding, as is present in distributed ledger technology [DLT]) substitutes a third party. This seems more than a theoretical risk as illustrated by initial coin offerings (ICOs), which may offer the possibility for the governance and protection of investors to be executed by a computer code ("smart contracts") instead of the traditional legal mechanisms of a non-digital IPO. Indeed, Cohney et al. (2018) investigated the top 50 ICOs in 2017 regarding the promises[4] made by promoters and found that the code and disclosures often do not match.

One of the key characteristics of fintech versus traditional finance is that it operates differentially, entailing elements of decentralization, summarized as DLT. While the additional challenge of digital knowledge is largely undisputed, the impact of decentralization is controversial. On the one hand, decentralization may increase information asymmetry, e.g., when comparing an ICO with an IPO. At least in their early days, ICOs often did foresee a less restrictive set of rules for the information-providing issuer and did not involve an underwriter that could potentially soften any asymmetries. By contrast, in an IPO, it is generally mandatory to file a registration statement in the form of a publicly available prospectus, as well as a private filing for the regulator.[5] On the other hand, decentralization may, over time, lower information asymmetries following the traditional Hayek argument (1945) that says decentralized markets process information better than a centrally planned economy and thus allocate resources more efficiently. It is yet too early to tell whether the emergence of digital platforms will eventually facilitate frictionless decentralization and deepen coordination.

2.1.2 Opportunities to Lower Information Asymmetry

Digital finance can also lower information asymmetries in several ways, not least under the rubric of financial inclusion. Some fintech initiatives particularly aim at not only lowering costs, but also lowering information asymmetries in providing financial product access to a broader audience. The information asymmetry can potentially be lowered on both the supply as well as the demand sides of financial services.

On the demand side, proximity to a well-developed commercial area used to be a determining factor for the breadth of financial products and services, as well as the competitiveness of their prices. Digital technology has changed that, as consumers in remote and less-developed regions are empowered to enjoy equal access to financial products and services and information allowing for less costly comparisons, and to build a credit history simply by, for example, using their mobile phones. In underbanked regions with no legacy system like bank branches, these developments have been particularly fast and impactful, in some respects even leapfrogging traditional markets, with the People's Republic of China as an oft-cited example (Institute of Digital Finance 2018; Luohan Academy Report 2019).

[4] Specifically, the authors checked whether, if ICO white papers so promised, the code actually restricted the supply of their crypto-assets and the transfer of those allocated to insiders according to a vesting or lockup plan. Further, they investigated whether ICO promoters used code to retain the power to modify the smart contracts, and, if so, whether they disclosed this in natural language.

[5] Such documentation provides financial statements of the company, the background of the management, insider holdings, any legal problems faced by the company, etc.

On the supply side, banks might be more willing to provide credit to customers they know better through data collections and to tailor their services closer to their needs. Meanwhile, the promise of technology goes beyond that and may potentially lower the entrepreneurship disparities between regions, gender, income, and age. However, as a precondition for this, the World Bank (2018) identifies many skill-related obstacles that can hamper inclusive growth, including limited access to education, lack of a basic social safety net, and weak institutions. One of the most well-known examples of overcoming these obstacles is M-Pesa launched in 2007 in Kenya, which innovated on the back of existing infrastructure by using SIM cards, allowing basic phones, even without the functionality of applications, to provide financial services.[6]

2.2 Financial Stability

In addition to ensuring the solvency and liquidity of individual financial institutions, regulation aims at the soundness of the financial system as a whole. Stability risks are usually associated either with the relative size or the connectivity of a financial market participant, that is, being either "too big to fail" or "too interconnected to fail".

In terms of threats through size, the Committee on the Global Financial System (2017) and the Financial Stability Board (2017), among others, concluded that, at this stage, the size of fintech-era credit in many jurisdictions is still small enough to limit the systemic impact. At the same time, a range of benefits and risks was identified in cases where fintech might grow further. Particularly, the recent entry of large technology firms (Bigtech) presents new and complex trade-offs between financial stability, competition, and data protection (BIS 2019).

In terms of risks related to connectivity, cybersecurity[7] emerged as a key challenge for regulators and is as much related to financial stability as it is to market integrity (covered in the next section). However, it is notoriously difficult to quantify cyber-risks' overall impact as data are scarce due to lack of common measurement standards and firms' small incentive to report. Early, widely cited estimates are annual losses of $375–$575 billion (McAfee 2014), with cybercrime being the second-most reported economic crime with 32% of organizations affected (PwC 2016).

The financial sector is a favorite target for cybercrime according to several industry reports. Cybercrimes come in different formats, including data theft,[8] asset theft,[9] and (Distributed) Denial of Service attacks.[10] The attacks are far from being limited to

[6] The FinAccess household survey carried out by the Central Bank of Kenya, the Kenya National Bureau of Statistics and FSD Kenya found in 2019 that 83% of Kenyans had access to formal financial services, up from 29% in 2006. These positive advances were also attributed to the growth of mobile money platforms like M-Pesa (FSD Kenya 2019).

[7] Defined by Cebula and Young (2010) as, "operational risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems."

[8] For example, in one of the biggest data breaches in history, over 80 million accounts at JP Morgan were affected in 2014.

[9] At least 10 attacks using fraudulent SWIFT messages causing initial losses of $171 million for Union Bank of India in July 2016, $81 million for the Bangladesh Central Bank in February 2016 and $60 million for Far Eastern International Bank (Taipei,China) in October 2017 (estimated losses as reported by ORX news and Financial Times).

[10] In the US in 2012, the websites of Bank of America, PNC, JPMorgan, US Bancorp, Wells Fargo, BBT, Capital One, HSBC, Region Financial, and SunTrust were targeted and disrupted. In 2013 in the Czech Republic, the central bank, three large banks, and the stock exchange were disrupted, with estimated damages of $500,000. In Norway on 8 July 2014, seven major financial institutions were attacked, leading to disrupted services during the day. In Finland in 2014, three banks (Op Pohjola, Danske Bank, and

banks and increasingly also involve securities dealers, particularly in the context of fintech. Cyberattacks on fintech firms (mainly online exchanges allowing the trading of crypto-currencies and providing wallet services) have resulted in at least $1.45 billion in losses since 2013 (Bouveret 2018).[11]

Given its world-spanning nature, cybersecurity has triggered a series of international initiatives from the G20, Financial Stability Board, Committee on Payments and Market Infrastructures, and the International Organization of Securities Commissions, all expressing the need to monitor cyber-risk arising from fintech and issuing guidance for regulatory responses. The worry is shared among the industry as illustrated in a recent survey where only 42% of respondents considered their institution to be extremely or very effective in managing cyber-risk (Deloitte 2016). Yet, in a 2019 global survey (risk.net 2019) among chief risk officers and operational practitioners, the first, second, and fifth[12] among the top 10 major operational risks were related to cyber-security.

2.3 Market Integrity

The third core objective of regulation and supervision is to maintain market integrity. Whether digital or not, trust is the basis of financial transactions, emphasizing the need to safeguard the system from illicit activities and fraud. New technologies have the potential to spur financial innovation, efficiency, and inclusion, and, at the same time, create new risks to market integrity, making zero tolerance of illicit behavior as much in the interest of a truly innovative industry as regulators and supervisors.

Among the several risks to market integrity from fintech, money laundering stands out. The recommendations by the independent inter-governmental body Financial Action Task Force (FATF) are recognized as the global anti-money laundering and counter-terrorist financing standard. In 2014, FATF issued recommendations focusing on digital currencies. With the rise of anonymity-enhanced digital currencies and the emergence of other virtual asset ecosystems, including ICOs, the approach broadened since 2015. Particularly, in October 2018 and June 2019, FATF amended Recommendation 15 on New Technologies to clarify definitions and to specifically describe how countries and obliged entities must prevent the misuse of virtual assets for money laundering and terrorist financing and the financing of proliferation (FATF 2019), a step welcomed by G20 and Financial Stability Board, with the latter further exploring the possible implications of decentralized financial technologies and how regulators can engage other stakeholders.

Remaining vigilant to existing and emerging risks to market integrity has further elements. With increased importance of data, corresponding privacy issues are heightened. While these hurdles are particularly high for individuals, they often show the classic privacy paradox (Barnes 2006; Athey et al. 2017), where people claim to be very concerned about their own privacy, while largely ignoring these risks in their online behavior.

The EU in May 2018 was among the earliest jurisdictions to implement tight consumer safeguards around data disclosure with their General Data Protection Regulation (GDPR), which requires firms to report a data breach within 72 hours and provide customers with access to their own data, in some cases enabling them to correct or erase

Nordea) suffered Distributed Denial of Service attacks that rendered their online services unavailable and, for one bank, prevented customers from withdrawing cash and making card payments.

[11] The largest initial losses occurred at Coincheck in January 2018 with $534 million and MT Gox in January 2014 with $470 million.

[12] No. 1: data compromise; No. 2: IT disruption; No. 5: theft and fraud.

it. Failure to comply with the requirements can lead to fines up to EUR20 million or 4% of global annual turnover, whichever is higher. With digital technology being part of the problem as well as the solution (e.g., via encrypting), regulation and supervision must be especially alert to strike the right balance in order to inform and protect the privacy of financial market participants.

3. PRINCIPLE-BASED REGULATION

To achieve the objectives covered in the previous section, many regulators use a broad set of principles and outcome-focused rules ("principle-based") rather than detailed prescriptions ("rules-based regulation"). Overall, the principle-based regulatory approach seems to have somewhat gained in importance in the light of fintech developments. One reason might be that it adapts more easily and cost-effectively to new and quickly developing business models, due to its less-demanding frequency and volume of legislation adaptations.

While the principles, their implementation, and their hierarchy vary, at least the following three have emerged across different jurisdictions and are widely accepted among regulators: legal certainty, technology neutrality, and proportionality (or often also referred to as risk-based). In the following, we cover each of these principles in the context of fintech. All principles aim toward a level playing field for market participants: make sure that everyone is on the same page legally (3.1), treat technologies equally (3.2), and find a balance between risk exposure and regulatory requirements. All three principles keep or even heighten their relevance in the context of digital finance.

3.1 Legal Certainty

A key principle to any regulation is to provide legal certainty. This includes a robust definition of regulatory perimeters as well as transparent application of the law. Unclear terminology and classification encourage regulatory arbitrage and ultimately hamper a robust legal framework and financial innovation, alike. It therefore comes as no surprise that many fintech projects are eager to be regulated as this instills the legal certainty needed to attract investors. Further, there is a risk that coding regulator approaches at an early stage of development is normative and might even intentionally or unintentionally steer innovation from the public sector.

In the context of fintech at least three challenges to legal certainty arise. First, the high speed of development of fintech in terms of different business models and from basically nil to taking center-stage in discussions on the financial system within just a decade contrasts with the usually time-consuming procedures for new regulatory rules commonly embedded in a system of public consultation of the most important involved stakeholders. The second challenge pertains to the number of involved government institutions. Financial regulation in many jurisdictions involves a variety of institutions (including the central bank, financial supervisory bodies, other government departments such as the tax administration, legislative and anti-money laundering regulator). The scope of different regulatory authorities ("regulatory perimeter"), which varied significantly even before the digital age, potentially overlaps even more when regulating digital asset activities. This is illustrated by the finding that, on average, three distinct national bodies per jurisdiction have issued official statements on digital assets, including warnings (Cambridge 2019). The third challenge is, vis-à-vis regulators and market participations, fintech increasingly mandates computer science and coding knowledge in addition to the usual legal and financial market knowledge.

One possible answer to all three challenges is regulatory sandboxes. While the format of sandboxes varies significantly in different jurisdictions (Cambridge Centre for Alternative Finance 2019), they usually allow testing new business models without immediate full-fledged legislation. In addition, further attempts to provide legal certainty have been undertaken in several jurisdictions in the form of either a fintech license (usually for a dedicated business model, or, in a few cases, in the form of a horizontal license covering several financial services banks, insurance and asset managers, and financial infrastructure at once) or legislation covering distributed ledger technologies (DLTs).

3.2 Technology Neutrality

Technology neutrality entails regulators looking through the technology and focusing mainly on the functionality that a financial service provides. For example, with the onboarding of new clients, which is a key element in financial services, a technology-neutral regulation defines specific requirements regarding anti-money laundering, regardless of whether the on-boarding is done non-digitally at the classic bank counter or through a dedicated online solution.

Several reasons bolster technology-neutrality as a key regulatory principle. First, technological change is very fast and getting faster. It might be neither possible nor efficient to constantly review and update regulations accordingly. As of mid-2019, there are over 2,500 different crypto-currencies available[13] and the term DLT is only a placeholder for a diverse set of functionalities and parameters.[14]

Another reason for regulators to abstain from picking one technology over the other is that taking sides invokes potential responsibility. The risk of unwillingly being perceived as an implicit guarantee may lower industry incentives to identify imperfections and flaws in the technology favored by a regulator. In the extreme, it could even cause the industry to innovate less as the official technology has an advantage.

3.3 Proportionality

The Basel framework sets minimum regulatory requirements for internationally active banks in the traditional framework. Within these limits, it allows national authorities proportionality in setting lower regulatory requirements for financial services that are of limited risk due to factors such as firm size, systemic importance, complexity, and risk profile. The concept of proportionality aims to limit public intervention in the form of regulatory duties and particularly to avoid excessive compliance costs or regulatory burdens for smaller and non-complex banks (Basel Committee on Banking Supervision 2019; Lautenschläger 2017).

Some of the new business models of fintech engage only in one particular aspect of banking (e.g., payments), insurance (e.g., convenience in processing refunds), or asset management (e.g., advisory). Also, at least some are of relatively small size and, so far, limited systemic importance (Ch. 2.2). This raised the question of the extent to which fintech should be required to live up to a full-fledged banking, insurance, or infrastructure license, or whether it could be regulated only for the specific function of its business model. Two key criteria regarding the risks fintech poses are whether it is involved in maturity transformation and whether deposits are on the balance sheet and directly accessible by the fintech company. In that context, the limit between

[13] Coinlore.com. Number of all coins retrieved July 2018.

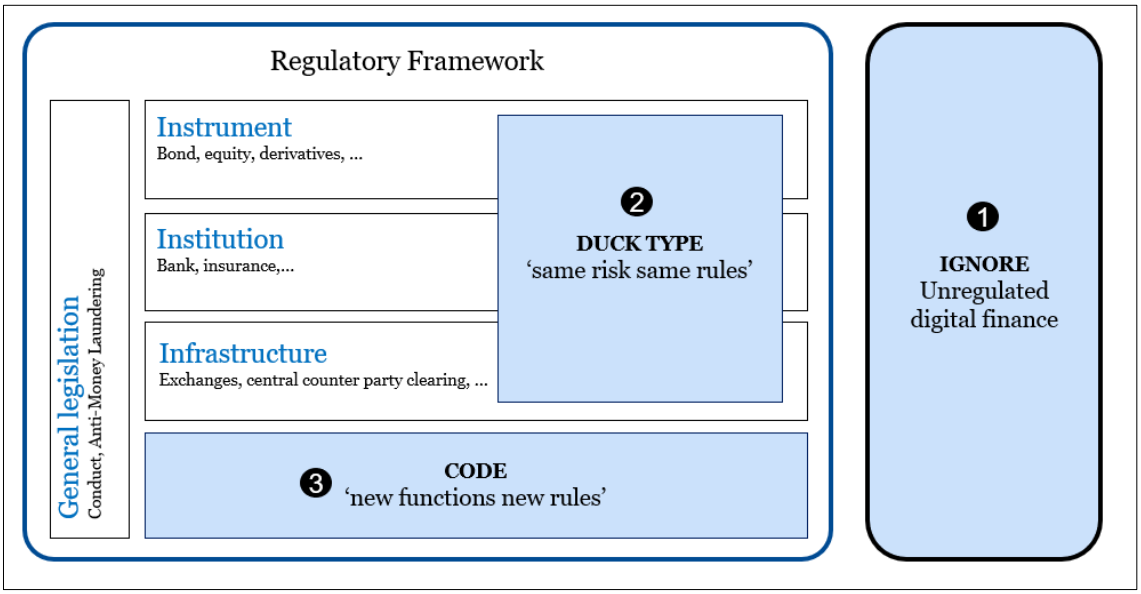
[14] E.g., Rauchs et al. (2018b) introduce a DLT landscape map that differentiates 12 systems.

providing only a pure software solution and actual financial services has been tested by digital finance.

4. REGULATORY PRACTICES IN FINTECH: A SYNOPSIS

In the traditional regulatory framework, a few aspects, such as conduct and anti-money laundering regulations, apply to the full financial universe. However, in most aspects, the regulatory framework differs by instrument, institution, and infrastructure (see Figure 1). Where does fintech fit into this landscape? The answer is not trivial as fintech encapsulates a broad spectrum of activities. A one-size-fits-all regulatory approach risks stifling innovation and discouraging new market entrants. Accordingly, Claessens et al. (2018) for fintech credit and Kaal (2018) for ICOs, both find that the current regulatory responses differ widely across types of fintech activities and jurisdictions. This section shows how, despite these differences, regulators essentially have three options in this regard: ignore, duck type, or code (Amstad 2019).

Figure 1: A Synopsis for Regulatory Options in Fintech



Source: Amstad (2019).

4.1 Ignore: "Keep It Unregulated"

The first option is to leave fintech largely unregulated. In the early days of fintech, regulators in most jurisdictions chose "wait and see". Bitcoin, as a catalyst of the fintech ecosystem, started in 2008 with the seminal paper by Satoshi Nakamoto. However, many jurisdictions had their initial statements issued only in 2013 (Rauchs et al. 2018).[15] At that time, some fintech companies felt hampered in their activities as they could not

[15] Rauchs et al. (2018): "the first official report mentioning cryptoassets by a regulatory authority was published in 2011 by the French AML regulator Tracfin, followed by the European Central Bank in 2012. By 2014, 93% of analyzed jurisdictions. Interestingly, the vast majority (75%) of, the same year the market experienced the largest bubble since the inception of Bitcoin in 2009."

benefit from the legal certainty of regulation, a criticism that contrasts with the sometimes anti-government approach of at least some fintech activities.

The aggregate market capitalization of crypto-assets skyrocketed from $30 billion to over $800 billion in early January 2018, before falling back to around $200 billion (Rauchs et al. 2018). With increased fintech-era volumes, levels of fraud, inappropriate market practices, and Ponzi schemes also increased. Hesitant to overregulate, but increasingly seeing the need for a response to ensure investor and consumer protection and market integrity, several jurisdictions resorted to issuing warnings to the market. In detailing the case of ICOs, Zetzsche et al. (2018) documented the issuance of warnings as likely the least interventionistic of all regulatory options.

To wait and see was the predominant option as long as the market volume in fintech stayed low. However, a range of benefits and risks were identified in cases where fintech might grow further (CGFS and FSB 2017). If regulation seems appropriate, the fundamental question arises as to whether fintech's risks and rewards can be integrated into the existing framework, or whether a new paradigm is required.

4.2 Duck Type: "Same Risk, Same Rules"

The second option is to "duck type"[16] fintech rules into the existing regulation. Some fintech models are essentially digital or crypto representations of an instrument, an institution, or a financial infrastructure platform. A straightforward approach to regulating these models is to focus on their economic function or, more specifically, their underlying risk. The same risk—whether digital or not—would need the same regulatory answer, be it reporting requirements, a license, or a ban. This strategy refers to the famous Howey test,[17] and is often simplified as the "duck test" that says, "if it looks like a duck, swims like a duck, and quacks like a duck, then it probably is a duck."

Duck typing regulation applies two widely used, previously mentioned regulatory principles: it is principle-based, as it regulates the same risk with the same rule, and it is technology-neutral as it focuses on the economic function. An example is the ICO guidelines by the Swiss Financial Market Supervisory Authority (FINMA): "In assessing ICOs, FINMA will focus on the economic function and purpose of the tokens (i.e., the blockchain-based units) issued by the ICO organizer" (FINMA 2018). Accordingly, ICOs are classified into payment, utility, and asset tokens. Compliance with respective existing regulations and, in all cases, with anti-money-laundering legislation is required. Duck typing regulates the function, rather than the instrument, institution, or infrastructure platform. However, fintech innovations may also lead to new functionality. Regulators need to identify these new functions and, if need be, code them into new regulations that specifically address them.

4.3 Code: "New Functionality, New Rules"

The third option is to code fintech using regulations that are specifically tailored to new functionality made possible through technological innovation. Duck typing regulation works as long as fintech operates in the same way as traditional finance. Despite technological change, the underlying core risks in financial markets, such as market, credit, liquidity, and operational risks, have remained largely the same.

[16] I borrow the term "duck-typing" from computer programming.

[17] It goes back to a case in the Supreme Court in 1946, which created a test that looks at an investment's substance, rather than its form, as the determining factor for whether it is a security.

However, with ongoing financial innovation, new combinations of risks might emerge. Alternatively, the core risks might show in forms only made possible through using new technology. Both scenarios might need additional specific regulations. Similarly, new risks stemming from interconnected financial markets were brought to the forefront during the global financial crisis. While underlying risks would stay the same, it became clear that safeguarding individual financial institutions is insufficient and a separate additional macroprudential layer is necessary.

Indeed, current research suggests that fintech might lead to new functionality based on, among other elements, on: (a) the specific features of blockchain technology; (b) the new combination of business models; and (c) new digital operational challenges. In the following we provide examples for each characteristic.

Blockchain technology. Cong and He (2018) demonstrated that blockchains have profound economic implications on consensus generation, industrial organization, smart contract design, and anti-trust policy. Specifically, in the traditional system—largely due to contract incompleteness—sellers cannot offer prices contingent on the success of delivering the goods. In contrast, blockchains, via decentralized consensus, enable agents to contract based on service outcomes and to automate contingent transfers. They conclude that this new functionality can deliver higher social welfare and consumer surplus through enhanced entry and competition, yet it may also lead to greater collusion. Consequently, they suggest an oft-neglected regulatory solution to separate usage and consensus generation on blockchains, so that sellers cannot use the consensus-generating information for the purpose of sustaining collusion.

Another example for functionality made possible through blockchain is the “fork”, as an either accidental or intentional change in protocol. Biais et al. (2017) illustrated that forks might be an integral part of blockchain applications, leading to orphaned blocks and persistent divergence between chains.[18] Again, it is not straightforward to see a direct analogy to a fork in the non-digital world and therefore how to mirror it using current regulations, at least taking into consideration whether dedicated regulations are needed.

New functionality might also arise from decentralization, which, for example, allows for greater ease in benefitting from regulatory arbitrage. Makarov and Schoar (2018) found that price movements in cryptocurrencies are largely driven not by transaction costs or differential governance risk, but rather by avoiding regulation.

New combination (of business models and jurisdictions). Fintech is characterized by a strong and increasing cross-segment expansion instead of limiting itself to the value chain of a classic bank or insurance company. Rauchs et al. (2018) found that 57% of crypto-asset service providers were operating across at least two market segments to provide integrated services for their customers. This led some to declare fintech a new asset class. Findings by Hu et al. (2018) support this view, showing that cryptocurrencies are highly correlated among each other—likely driven by Bitcoin serving as vehicle currency in the cryptocurrency space—but are largely orthogonal to traditional assets. It is still too early to tell whether cryptocurrencies’ distinct behavior is a testament to the rise of a new asset class justifying its own regulation.

New digital operational risks can appear across the digital financial services and market value chain. Digital technology also enables the generation and analysis of vast amounts of customer and transaction data, i.e., “big data”, which introduces its own set of benefits and risks that should be managed (G20 2018).

[18] They also show how forks can be generated by information delays and software upgrades.

An additional need for dedicated regulation may arise from the fact that digital blockchain records must be enforced in the physical world. “While blockchains can keep track of transfer of ownership, proper enforcement of possession rights is still needed, except in the case of (fiat) cryptocurrencies” (Abadi and Brunnermeier 2019). The enforcement of rights and duties in fintech may differ from those found in traditional assets.

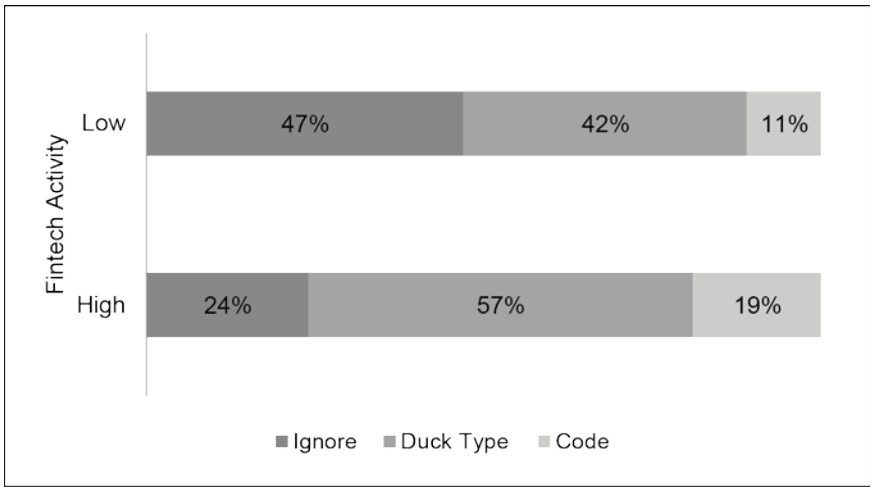
4.4 Current Regulatory Practices

To gauge the importance of each of the three previously mentioned regulatory answers, we use a survey done by Cambridge (2019) and map their categories in the above-suggested synopsis. The survey includes 108 jurisdictions. The categorization applies to secondary market activities.

The importance of each category varies depending on the level of activity of the fintech industry in a jurisdiction. The classification between “high” and “low” level of crypto-asset activities is based on the number of crypto asset firms operating, the number of ICOs launched, and the level of mining activities recorded. Of the jurisdictions with low fintech activity, the main regulatory answer is, with almost 50%, “wait and see”. If “ignore” is not an option, then duck typing is 42% of regulation, while only in 10% of the jurisdictions would code a bespoke fintech answer.

Meanwhile, “wait and see” is an option only for 24% of jurisdictions that face an active fintech industry. Here, the predominant strategy of regulators with 57% is to duck type existing regulations. In already a fifth of the cases, the regulators even adapt by coding tailor-made regulations (see Figure 2).

Figure 2: Regulatory Answers



Notes: “Ignore” (outside of financial regulatory framework) represents “other existing or unregulated”, “Code” represents “bespoke” and “duck type” represents “retrofitted or prohibited”. These regulatory responses only apply to secondary market activities. The classification between “high” and “low” levels of crypto-asset activities is based on the number of crypto-asset firms operating in the country, the number of ICOs launched, and the level of mining activities recorded in the country.

Source: Author’s representation based on an expanded sample of 108 jurisdictions by Cambridge (2019).

Table 1 presents an overview of several countries’ new regulations and licenses (“coding”) introduced since 2015. It further illustrates that, as of now, the way in which public policy balances risks and benefits differs quite a bit, as no consensus has emerged so far.

Table 1: Selected Features of Dedicated Fintech Credit Policy Frameworks

Jurisdiction	Tax Incentives	Regulations[a]	Licensing/ Authorization[a]	Investor Protections[a]	Risk Management Requirements[a]
Australia	—	—	—	—	—
Brazil	—	✓	✓	✓	—
Canada	—	—	—	—	—
Chile	—	—	—	—	—
People's Republic of China	✓	✓	✓	✓	✓
Estonia	—	—	—	✓	—
Finland	—	✓	✓	—	—
France	✓	✓	✓	✓	✓
Germany	—	—	—	—	—
Japan	✓	—	—	—	—
Rep. of Korea	—	—	—	—	—
Mexico	—	✓	✓	—	✓
Netherlands	—	—	—	✓	—
New Zealand	—	✓	✓	—	✓
Singapore	—	—	—	—	—
Spain	—	✓	✓	—	✓
Switzerland[b]	—	✓	✓	✓	✓
United Kingdom	✓	✓	✓	✓	✓
United States	—	—	—	—	—

[a] Specific rules for fintech credit that are separate from pre-existing rules for other financial intermediaries.

[b] New rules effective from 2019.

Source: Adapted from Claessens et al. (2018).

5. CONCLUSION

Regulators and supervisors face a challenging balancing act to stay innovation-friendly and, at the same time, show zero-tolerance for criminal behavior. As with previous non-digital forms, fintech regulations need to be motivated by a clear set of objectives and guiding principles for their implementation. The traditional core objectives of non-digital financial regulation as investor and consumer protection, market integrity, and safeguarding financial stability, keep their relevance also for fintech. In very early days and at small volumes of fintech, ignore or wait-and see approaches were dominant. In cases where regulation seemed appropriate, however, similar activities were treated in similar ways to limit incentives for regulatory arbitrage. At the same time, regulators would be well-advised to remain alert to the limits of duck typing and aim to identify early on new functionalities that may require conceptually distinct regulation of technology-enabled finance. In harnessing the benefits of financial innovation, while containing risks, it will be instrumental that all relevant stakeholders such as regulators, the fintech industry, and academia engage in an open dialogue to assure a common understanding of fintech activities and business models, as well as the motivation and implementation of regulatory measures, alike.

REFERENCES

Abadi, J., and M. K. Brunnermeier. 2019. Blockchain Economics. National Bureau of Economic Research (NBER) Working Paper No. 25407.

Amstad, M. 2019. Regulating Fintech: Ignore, Duck Type or Code. *Voxeu.com*, 23 March.

Armour, J., et al. 2016. *Principles of Financial Regulation*. Oxford: Oxford University Press.

Athey S., C. Catalini, and C. E. Tucker. 2017. The Digital Privacy Paradox: Small Money, Small Costs, Small Talk. National Bureau of Economic Research (NBER) Working Paper No. 23488.

Barnes S. B., 2006. A Privacy Paradox: Social Networking in the United States. *First Monday* 11, ISSN 1396-0466 119.

Basel Committee on Banking Supervision (BCBS). 2019. Proportionality in Banking Regulation and Supervision–a Survey of Current Practices. March. BCBS.

Bank for International Settlements (BIS). 2019. Big Tech in Finance: Opportunities and Risk. BIS Annual Economic Report 2019. BIS.

Biais, B., C. Bisière, M. Bouvard, and C. Casamatta. 2018. The Blockchain Fork Theorem. Toulouse School of Economics Working Paper No. 17–817.

Bouveret, A. 2018. Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment. International Monetary Fund working paper 18/143.

Brunnermeier, M., A. Crockett, C. Goodhart, A. D. Persaud, and H. S. Shin. 2009. The Fundamental Principles of Financial Regulation. *Geneva Report on the World Economy* 11.

Cambridge Centre for Alternative Finance. 2019. Early Lessons on Regulatory Innovations to Enable Inclusive FinTech: Innovation Offices, Regulatory Sandboxes, and RegTech. Cambridge: University of Cambridge.

Cebula, J. J., and L. R. Young. 2010. A Taxonomy of Operational Cyber Security Risks, Technical Note CMU/SEI-2010-TN-028, Software Engineering Institute, Carnegie Mellon University.

Committee on the Global Financial System and Financial Stability Board (CGFS and FSB). 2017. FinTech Credit: Market Structure, Business Models and Financial Stability Implications. CGFS Papers, May.

Claessens, S., J. Frost, G. Turner, and F. Zhu. 2018. Fintech Credit Markets around the World: Size, Drivers and Policy Issues. *BIS Quarterly Review* September.

Cohney, S., D. Hoffman, J. Sklaroff, and D. Wishnick. 2018. Coin-Operated Capitalism. *Columbia Law Review* 119(3): 591–676.

Cong, W. and Z. He. 2018. Blockchain Disruption and Smart Contracts. *Review of Financial Studies*, forthcoming.

Deloitte. 2016. Global Risk Management Survey, 10th edition.

Financial Action Task Force (FATF). 2019. Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. FATF.

FINMA. 2018, Guidelines for Enquiries Regarding the Regulatory Framework for Initial Coin Offerings. Bern: FINMA.

Freixas, X., and J.-C. Rochet. 2008. *Microeconomics of Banking*, MIT Press.

FSD Kenya. 2019. FinAccess Household Survey 2019.

G20. 2016. High-Level Principles for Digital Financial Inclusion.

Hayek, F. 1945. The Use of Knowledge in Society. *The American Economic Review* 35(4): 519–530.

Hohl, S., M. C. Sison, T. Stastny, and R. Zamil. 2018. The Basel Framework in 100 Jurisdictions: Implementation Status and Proportionality Practices. *FSI Insights on Policy Implementation* 11.

Hu, A. S., C. A. Parlour, and U. Rajan. 2018. Cryptocurrencies: Stylized Facts on a New Investible Instrument. Available at SSRN: https://ssrn.com/abstract=3182113.

Institute of Digital Finance, Peking University. 2018. Digital Inclusive Finance Index Report 2011–2017. Beijing: Institute of Digital Finance.

Kaal, W. 2018. Initial Coin Offerings: The Top 25 Jurisdictions and their Comparative Regulatory Responses. Working paper, University of St. Thomas School of Law.

Lautenschläger, S. 2017. Is Small Beautiful? Supervision, Regulation and the Size of Banks. Speech at International Monetary Fund seminar, Washington DC, 14 October.

Luohan Academy Report 2019. Digital Technology and Inclusive Growth. Luohan Academy.

Makarov, I., and A. Schoar. 2018. Trading and Arbitrage in Cryptocurrency Markets. working paper. Available at SSRN: https://ssrn.com/abstract=3171204.

Rauchs, M., A. Blandin, K. Klein, G. Pieters, M. Recanatini, and B. Zhang. 2018. 2nd Global Cryptoassets Benchmarking Study. Cambridge Centre for Alternative Finance, University of Cambridge.

Rauchs, M. et al. 2018. Distributed Ledger Technology Systems: A Conceptual Framework. Cambridge Centre for Alternative Finance, University of Cambridge.

Risk.net. 2019: Top Operational Risks for 2019. Survey. 14 March. https://www.risk.net/risk-management/6470126/top-10-op-risks-2019 (accessed 18 August 2019).

World Bank. 2018. Universal Finance Access by 2020. http://www.worldbank.org/en/topic/financialinclusion/brief/achievinguniversal-financial-access-by-2020 (accessed 18 August 2019).

Zetzsche, D. A., R. P. Buckley, D. W. Arner, and L. Föhr. 2018, The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators. European Banking Institute (EBI) Working Paper Series no. 18. EBI.