Boston College Law Review

Volume 62 | Issue 2 Article 3

2-24-2021

Payments Failure

Hilary J. Allen
American University Washington College of Law, hjallen@wcl.american.edu

PAYMENTS FAILURE

HILARY J. ALLEN

PAYMENTS FAILURE

HILARY J. ALLEN*

Abstract: The processing of retail payments traditionally has been the domain of regulated banks, but technologically sophisticated players like Venmo, AliPay, Bitcoin, and Ripple, and potentially, Facebook's Libra, are making incursions into the market. Even within regulated banks, payments processing is becoming increasingly reliant on new technologies—JPMorgan Chase's "JPMCoin" is just one example. Limited attention, however, has been paid to the new kinds of operational risks associated with these methods of processing retail payments. This Article argues that technological failures at a payments provider—either a bank or non-bank—could be amplified in unexpected ways as such failures interact with technological failures at other payments providers. In a worst-case scenario, a cascading failure of payments technologies could cause significant parts of the retail payments system to shut down—an eventuality that would harm the broader economy if people were unable to transact for a prolonged period of time. This Article is the first to raise the possibility of a financial crisis precipitated primarily by operational failures. Such a crisis would look more like a rolling blackout than a bank run. Because of this possibility, this Article argues that it is insufficient to approach the risk of payments failure with a purely prudential strategy. This Article therefore makes the case for a complementary "macro-operational" approach to regulation, rooted in complexity theory, to deal with the possibility that the systemic interactions of operational risks could hobble our retail payments system—and the broader economy. Using this framework, this Article analyzes the potential threats posed by different technologies and business models to the orderly functioning of our retail payments system. Further, this Article suggests the beginnings of what proactive macro-operational regulation of the retail payments system might look like.

INTRODUCTION

Imagine that, even if you had the money, you were suddenly unable to pay for goods and services. Imagine how quickly your day-to-day life would be impacted if you could not pay for food, gas, or rent. How long would it take

* Associate Professor, American University Washington College of Law. Many thanks to Dan Awrey, Dick Berner, Pat McCoy, David Min, JB Ruhl, Rory Van Loo, Yesha Yadav and to participants in the National Business Law Scholars Conference and the American University Washington College of Law Business Faculty Workshop series for helpful discussions and comments on earlier drafts.

for an economy to contract if consumers were no longer able to transact with businesses and employers were no longer able to pay their employees? A cyber attack could certainly generate these nightmarish outcomes, and there is nascent work being done on managing the systemic risks associated with cyberthreats to the financial system.[1] But cyber attacks are not the only threat we should be concerned about. This Article argues that even in the absence of any nefarious attack, the financial system could be incapacitated by compounding technical glitches. As retail payments processing becomes increasingly technologically complex, we need to consider the possibility of a financial crisis driven primarily by technological failures cascading through the financial system—a crisis, in other words, that looks more like a rolling blackout than a bank run. After all, as economists Kirilenko and Lo have quipped, "[W]hatever can go wrong will go wrong faster and bigger when computers are involved."[2]

Fears of payments failure have long motivated government intervention in the financial system, but in the past, when consumers predominately made retail payments with cash or checks, catastrophes could be kept at bay so long as the banks responsible for providing deposit accounts and processing checks remained safe and sound.[3] The government has developed a repertoire of regulatory and emergency measures (known as "prudential regulation") over the decades to shore up confidence in banks, reduce the risk of runs, and ensure that payments can continue to be made.[4] Such measures have been reasonably successful in preserving the payments system—even during the financial crisis of 2007–2008, retail payments were not interrupted. The retail payments landscape is becoming increasingly technologically complex, however, with the entry of new fintech firms into the market.[5] These fintech firms are not typically chartered as banks, and thus avoid most prudential regulation. Furthermore, prudential regulation—which focuses on addressing credit and liquidity risks that may impact institutional solvency—does not fully contemplate or address

---

[1] Enhanced Cyber Risk Management Standards, 81 Fed. Reg. 74,315 (proposed Oct. 26, 2016); THOMAS M. EISENBACH ET AL., FED. RSRV. BANK OF N.Y., CYBER RISK AND THE U.S. FINANCIAL SYSTEM: A PRE-MORTEM ANALYSIS 1 (2020), https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr909.pdf [https://perma.cc/K3ZC-F26F].

[2] Andrei A. Kirilenko & Andrew W. Lo, *Moore's Law Versus Murphy's Law: Algorithmic Trading and Its Discontents*, 27 J. ECON. PERSPS. 51, 52 (2013).

[3] *See* FED. RSRV., FEDERAL RESERVE POLICY ON PAYMENT SYSTEM RISK 3 (effective Oct. 1, 2020), https://www.federalreserve.gov/paymentsystems/files/psr_policy.pdf [https://perma.cc/DFY3-9AXJ] [hereinafter FEDERAL RESERVE POLICY] (stating in its policy on payments system risk that "[t]he safety and efficiency of these systems may affect the safety and soundness of U.S. financial institutions and, in many cases, are vital to the financial stability of the United States").

[4] *See* RICHARD SCOTT CARNELL ET AL., THE LAW OF FINANCIAL INSTITUTIONS 119 (6th ed. 2017) (explaining that courts and regulators know that banks pose particular hazards to the economy, and therefore warrant specific regulation).

[5] *See infra* notes 172–291 and accompanying text.

the possibility of a crisis driven primarily by operational risks.[6] As a result, even the banks involved in processing retail payments are inadequately regulated.

An analogy to the prudential regulatory strategies adopted before the last crisis illustrates the inadequacy of our current approach to regulating operational risk. Pre-crisis prudential regulation largely was predicated on the assumption that so long as individual banks were safe and sound, the system as a whole also would be robust.[7] However, steps that individual banks took to preserve their own solvency—most notably, selling assets at "fire sale" prices—created problems for entire asset markets (and the institutions that participated in them), which made the financial system as a whole much weaker.[8] It is similarly possible that leaving operational risk management to individual payments providers will make the retail payments system more fragile, if the steps taken internally to manage operational risk have consequences for other payments providers.[9] This Article is the first to argue for "macro-operational" regulation, designed to deal with a potential new breed of financial crises that could arise from systemic interactions of technological operational risks.

Such crises would have more in common with the failure of complex infrastructure systems, such as power grids, than with the financial crises of the past. This Article therefore argues that complexity science, particularly the literature on cascade failures, provides an important framework for assessing fragilities in the retail payments system. This literature identifies five different dimensions of robustness in complex systems: reliability, efficiency, modularity, scalability, and evolvability.[10] Of these dimensions, improved modularity, scalability, and evolvability are most likely to protect the system from cascading failures.[11] Somewhat counterintuitively, focusing too heavily on improving the reliability of the individual components of the system can render it more susceptible to catastrophic failure—a state that complexity science refers to as "robust yet fragile."[12] Unfortunately, however, existing regulation of opera-

---

[6] *See infra* notes 33–49 and accompanying text.

[7] Luca Enriques et al., *Network-Sensitive Financial Regulation*, 45 J. CORP. L. 351, 357 (2020).

[8] *See* Markus K. Brunnermeier, *Deciphering the Liquidity and Credit Crunch 2007–2008*, 23 J. ECON. PERSPS. 77, 94 (2009) (describing "fire-sale externalit[ies]," as occurring when "[e]ach individual speculator takes future prices as given and hence does not take into account that unloading assets will cause some adverse effects on other speculators by forcing them to sell their positions as well").

[9] *See infra* notes 89–127 and accompanying text.

[10] J.B. Ruhl, *Managing Systemic Risk in Legal Systems*, 89 IND. L.J. 559, 570 (2014) (citing David L. Alderson & John C. Doyle, *Contrasting Views of Complexity and Their Implications for Network-Centric Infrastructures*, 40 IEEE TRANSACTIONS ON SYS., MAN, & CYBERNETICS 839, 840 (2010)). Part I.B elaborates on these dimensions in more detail. *See infra* notes 50–88 and accompanying text.

[11] Ruhl, *supra* note 10, at 594.

[12] *Id.* at 562.

tional payments risk focuses primarily on encouraging banks to minimize their own operational risks—in other words, the focus is squarely on the reliability of some of the system's component parts. Regulators have done little to promote the modularity, scalability, and evolvability of the system as a whole. Macro-operational regulation could begin to improve these dimensions of the retail payments ecosystem.

Admittedly, complexity science is reasonably pessimistic about our ability to contain the failures of complex systems, and we should not expect macro-operational regulation to entirely eliminate the possibility of cascading operational failures.[13] That does not mean that regulation is a wasted effort, however: well-designed regulation can render the retail payments ecosystem more robust to such failures.[14] Furthermore, well-designed regulation can establish, in advance, emergency measures that regulators and payments providers can take to mitigate damage once a cascade failure begins. Of course, what constitutes "well-designed regulation" always will be somewhat subjective and uncertain in the context of the highly complex retail payments ecosystem. In my previous work, I have argued strenuously that when it comes to financial stability, policymakers should take a precautionary approach, erring on the side of caution when dealing with uncertainty—even at some cost to efficiency.[15] Retail payments processing is both critical to economic functioning and facilitated by a complex system that is robust yet fragile.[16] Accordingly, this Article argues that policymakers should view the system as critical infrastructure that deserves prospective regulation because of the potential for catastrophic failures.

It is already well recognized that the existing payments infrastructure in the United States is antiquated and in dire need of improvement.[17] New fintech

---

[13] *See* CHARLES PERROW, NORMAL ACCIDENTS: LIVING WITH HIGH-RISK TECHNOLOGIES 5 (2d ed. 1999) (pointing out that new methods of regulation not only fail to prevent accidents in complex systems, but can sometimes make certain kinds of accidents more likely to occur); Alderson & Doyle, *supra* note 10, at 839 (noting that traditionally we have failed to successfully address "the fragilities created by our complex networks, from global warming to ecosystem destruction, global financial crises").

[14] *See* Ruhl, *supra* note 10, at 564–65 (explaining that although efforts to increase systemic robustness might actually increase complexity and thus the chance that the system will fail, "the balance between robustness and fragility is something we can hope to influence").

[15] Hilary J. Allen, *A New Philosophy for Financial Stability Regulation*, 45 LOY. U. CHI. L.J. 173, 178 (2013).

[16] *See generally* Morgan Ricks, *Money as Infrastructure*, 2018 COLUM. BUS. L. REV. 757 (providing an excellent discussion of the financial system as public infrastructure).

[17] In 2014, the New York Superintendent of Financial Services lambasted the financial industry for the state of payments systems: "At a certain point, enough is enough . . . . Four decades of slow-to-non-existent progress in the bank payments system seem like fair warning." Ian McKendry, *Lawsky to Banks: Speed Up Payments Innovation—Or Else*, AM. BANKER (Dec. 18, 2014), https://www.americanbanker.com/news/lawsky-to-banks-speed-up-payments-innovation-or-else [https://perma.cc/47UJ-Q29Z].

technologies are being hailed by many as the solution, but it is an open question whether these technologies will make our financial system more robust—both in the prudential sense and from the macro-operational risk perspective articulated in this Article. This Article briefly will explore the vulnerabilities of several new fintech payments technologies to runs, before assessing these technologies from the perspectives of modularity, scalability, and evolvability.

The surveyed payments innovations that rely on the "new rails" of distributed ledger technology do have the potential to increase modularity within the retail payments ecosystem, as they aspire to create an alternative path for processing payments that can function even if the "old rails" are compromised. These innovations do not assure modularity, however. Even if payments innovations initially promote systemic modularity, the retail payments system may ultimately lose this modularity through efficiency-driven innovations in interoperability that link the new rails to the old rails—and to other new rails.[18] The modularity of the retail payments system also will be reduced if a new payments provider outcompetes its rivals to establish a monopoly on retail payments processing. Then there will be no alternative path. Uncertainties regarding the governance structure of many of the distributed ledgers also suggest concerns about how the technology will be able to scale and evolve—a static ledger ultimately may become overwhelmed as usage patterns change over time.

Because new fintech technologies are not a silver bullet for creating a robust retail payments ecosystem, regulators, central bankers, and legislators need to consider the types of regulatory strategies that they themselves might deploy to reduce the risk of crises driven by operational failures, or to respond to them once they have occurred. This Article offers the very beginnings of a discussion on strategies that regulators could adopt to reduce the fragility of the retail payments system. The intention of this Article is to inspire a debate on these issues, rather than to provide concrete and comprehensive macro-operational policies. Even at this early stage, however, it is clear that the expertise of complexity and data scientists will be critical to macro-operational regulation, and regulators should prioritize hiring persons with such expertise.

The Article proceeds as follows. Part I introduces the extant prudential approach to financial stability regulation, before offering an alternative complexity perspective that is more apt when considering the possibility of financial crises caused by operational failures.[19] Part II then analyzes existing pay-

[18] *See* David Mills et al., *Distributed Ledger Technology in Payments, Clearing, and Settlement* 23 (Fed. Rsrv. Bd., Working Paper No. 2016-095, 2016), https://www.federalreserve.gov/econresdata/feds/2016/files/2016095pap.pdf [https://perma.cc/34E7-5F2S] (discussing why interoperability is considered an important goal for new payments innovations by many in the financial industry).

[19] *See infra* notes 29–127 and accompanying text.

ments regulation from a complexity perspective, and finds it wanting in terms of its ability to make the retail payments ecosystem as a whole more robust to failure.[20] Part III considers a sample of recent payments innovations to assess *their* potential to improve or threaten the robustness of the retail payments ecosystem, and (because the credit-related risks associated with these new technologies are undertheorized) considers whether they pose prudential concerns as well.[21] Part IV makes some initial policy recommendations, drawn from complexity theory, that could function as the beginnings of a macro-operational regulatory framework.[22]

Before proceeding any further, it is helpful to have a brief introduction to the basics of payments processing and some of the terminology used in this Article. Non-cash payments are essentially accounting transactions, debiting the payer's account and crediting the payee's account.[23] Payments processing requires a system that can accept requests to initiate these transactions, validate them, and then—if the request is found to be valid—check whether specified conditions precedent, such as the availability of funds, have been met.[24] Only after these processes have been completed can the payment be settled by crediting the payee's account.[25] Confusingly, the term "payments system" can refer to both a discrete system for processing payments offered by a single provider and to the overarching national, and sometimes international, architecture for payments processing.[26] Some payments systems exist to process wholesale payments, where the users are typically financial institutions, large commercial firms, or other firms providing payment services.[27] This Article, however, focuses on the systems that facilitate retail payments—the types of payments made by consumers and businesses in daily commerce.[28] To avoid confusion—

---

[20] *See infra* notes 128–171 and accompanying text.

[21] *See infra* notes 172–291 and accompanying text.

[22] *See infra* notes 292–348 and accompanying text.

[23] CARNELL ET AL., *supra* note 4, at 72.

[24] Mills et al., *supra* note 18, at 5.

[25] *Id.*

[26] *See id.* at 5, 9 (noting that transfers of funds between parties often are carried out by payments systems and that "a set of large and complex electronic networks of participants and processes . . . comprise the financial architecture and are often broadly called *the* U.S. payment system").

[27] Dan Awrey & Kristin van Zwieten, *The Shadow Payment System*, 43 J. CORP. L. 775, 781–82 (2018).

[28] To supply a definition, "[r]etail payments usually involve transactions between two consumers, between consumers and businesses, or between two businesses." *Retail Payment Systems Overview*, FED. FIN. INSTS. EXAMINATION COUNCIL (FFIEC) IT EXAMINATION HANDBOOK INFOBASE, https://itbooklets.ffiec.gov/it-booklets/retail-payment-systems/retail-payment-systems-overview.aspx [https://perma.cc/W9GD-CCZZ]. They often are contrasted with "[w]holesale payments [that] are typically made between businesses." *Id.* Furthermore, "[a]lthough there is no definitive division between retail and wholesale payments, retail payment systems generally have higher transaction volumes and lower average dollar values than wholesale payment systems." *Id.*

and using lexicon inspired by the complexity science literature—this Article will refer to the overarching architecture for retail payments processing as the "retail payments ecosystem." This Article will use the term "payments provider" to refer to individual participants in that ecosystem.

I. Perspectives on Financial System Failure

Past experience suggests that the broader economy will suffer if there is a significant disruption in the credit that ordinarily is extended by and to financial institutions.[29] The regulatory apparatus that has been adopted to promote financial stability is largely informed by a desire to avoid the disruption of such credit channels.[30] If we become too beholden, however, to this narrative of crises as being transmitted through credit channels, we may miss other important ways in which the stability of our financial system, and the health of our broader economy, may become compromised. The primary goal of financial regulation should be to avoid any systemic failure that harms broader economic growth—regardless of *how* the system fails.[31] This Part demonstrates that future financial crises could be driven primarily by operational failures, and focuses specifically on vulnerabilities that may originate in, and be communicated by, the retail payments ecosystem. Crisis prevention discussions, however, often neglect operational risk, perhaps because there is little precedent for such crises in our historical narrative.[32]

A. The Credit-Channel Perspective

In their seminal history of financial crises, Reinhart and Rogoff observed that most of the financial crises that have occurred in modern developed economies have started out as banking panics.[33] These banking panics then metas-

---

[29] *See* Ben Bernanke, Brookings Inst., The Real Effects of Disrupted Credit: Evidence from the Global Financial Crisis 3 (2018), https://www.brookings.edu/wp-content/uploads/2018/09/BPEA_Fall2018_The-real-effects-of-the-financial-crisis.pdf [https://perma.cc/EU5J-ST3D] (explaining that the weaknesses in the financial system prior to the last financial crisis resulted in credit disruptions and widespread panic).

[30] *Id.* at 6.

[31] Hilary J. Allen, *Putting the "Financial Stability" in Financial Stability Oversight Council*, 76 Ohio St. L.J. 1087, 1093 (2015).

[32] One welcomed exception is a recent Staff Report from the Federal Reserve Bank of New York, which seeks to integrate the literature on a particular type of operational risk (cyber risk) into the literature on bank runs, and conduct a "pre-mortem" of what *wholesale* payments failure might look like. *See* Eisenbach et al., *supra* note 1, at 1 (beginning their discussion by noting that "[i]n some ways, losses related to cyber attacks are similar to other operational loss events that can trigger liquidity runs and lead to solvency issues").

[33] Carmen M. Reinhart & Kenneth S. Rogoff, This Time Is Different: Eight Centuries of Financial Folly 141, 146 (2011).

tasized into financial system failures that had macroeconomic repercussions once the compromised financial system was unable to provide credit to the broader economy.[34] The classic formulation of a banking panic is as a series of bank runs, pithily described by Diamond and Dybvig as follows:

> During a bank run, depositors rush to withdraw their deposits because they expect the bank to fail. In fact, the sudden withdrawals can force the bank to liquidate many of its assets at a loss and to fail. In a panic with many bank failures, there is a disruption of the monetary system and a reduction in production.[35]

In other words, banking panics occur when depositors refuse to continue to provide credit (their deposits are in fact loans to banks), with the result that the banks themselves are unable to provide the credit (including mortgages and business loans) that is necessary to fuel economic growth.

This run dynamic also was central to sparking the 2007–2008 financial crisis, although it manifested in a more sophisticated way. Instead of a run caused by depositors refusing to extend credit to banks, the crisis involved "a run on the sale and repurchase market (the repo market), which is a very large, short-term market that provides financing for a wide range of securitization activities and financial institutions."[36] Once financial institutions were unable to use the repo market to access what was functionally credit, they were, as in a classic bank run, forced to liquidate many of their assets at a loss. These crippled institutions were no longer able to provide credit to businesses, and the institutions that did have funding often lacked the confidence to lend. As a result, expansion and growth were limited.[37]

In a recent influential paper, former Federal Reserve Chair Ben Bernanke reiterated the importance of credit channels in both generating and transmitting crises.[38] A credit-driven crisis certainly could impact the ability of the retail

---

[34] *Id.* at 141, 146–47.

[35] Douglas W. Diamond & Philip H. Dybvig, *Bank Runs, Deposit Insurance, and Liquidity*, 91 J. POL. ECON. 401, 401 (1983).

[36] Gary Gorton & Andrew Metrick, *Securitized Banking and the Run on Repo*, 104 J. FIN. ECON. 425, 425 (2012).

[37] *See* Brunnermeier, *supra* note 8, at 90 (explaining that in the midst of the financial crisis, financial institutions took measures to protect themselves against the failings of other banks, and credit markets tightened overall).

[38] BERNANKE, *supra* note 29, at 5. Bernanke concludes:

> [R]ecent experience and research highlight the need for greater attention to credit-related factors in modeling and forecasting the economy. Standard models used by central banks and other policymakers . . . do not easily accommodate financial stresses of the sort seen in 2007-2009, including the evident disruption of credit markets.

payments ecosystem to function, and regulation that seeks to avoid such crises has been implemented in part to ensure the continuing availability of bank-based payments systems.[39] There also is credit risk embedded in many traditional forms of retail payment, such as checks and credit cards, where the payment could take several days to ultimately settle, leaving at least one party to the transaction exposed to default.[40] Many newer payment methods, however, are being provided by non-banks, aim for real-time settlement, and are thus less reliant on credit and more reliant on technological innovation for their operation.[41] With many of these new payment services, the intermediary is not compensated for taking on the credit risks associated with settlement (or at least, much less of the compensation relates to that risk).[42] Instead, users pay fees for the efficiency and convenience associated with the mechanical processing of payments.[43] But even as some of the credit-related vulnerabilities in the retail payments ecosystem are being addressed, new operational risks are being introduced.

Payments systems have become vulnerable to mass technological failures in recent decades as reliance on electronic processing and communication has increased.[44] Such vulnerability will only be exacerbated by the increasing speed and complexity of new innovations in payments processing.[45] Because of the relative novelty of these operational risks, it is not surprising that there is no historical precedent for a full-blown crisis generated by operational failures

---

Id. Bernanke's seminal work on the banking panics that led to the Great Depression informed the Federal Reserve's response to the 2007–2008 crisis. REINHART & ROGOFF, *supra* note 33, at 146–47.

[39] Awrey & van Zwieten, *supra* note 27, at 794, 796. Lacker observes that although the United States has experienced events that impacted the functioning of the interbank payments system, none yet have had a significant detrimental impact on retail payments processing. Jeffrey M. Lacker, *Payment System Disruptions and the Federal Reserve Following September 11, 2001*, at 24 (Fed. Rsrv. Bank of Richmond, Working Paper No. 03-16, 2003), https://www.richmondfed.org/~/media/richmondfedorg/publications/research/working_papers/2003/pdf/wp03-16.pdf [https://perma.cc/HPM2-BC42] (noting that in all the past crises, "bank runs either did not occur or were secondary; the main event in all was the interbank payment system").

[40] Ross P. Buckley & Ignacio Mas, *The Coming of Age of Digital Payments as a Field of Expertise*, 2016 U. ILL. J.L. TECH. & POL'Y 71, 76.

[41] *Id.* at 72.

[42] *Id.* at 73. Or at least, much less of the intermediary's compensation relates to that risk. *Id.*

[43] *Id.*

[44] Lacker, *supra* note 39, at 25.

[45] J.B. Ruhl, *Governing Cascade Failures in Complex Social-Ecological-Technological Systems: Framing Context, Strategies, and Challenges*, 22 VAND. J. ENT. & TECH. L. 407, 410 (2020); *see* Kirilenko & Lo, *supra* note 2, at 52 (explaining that although there are many benefits of "computer-based automation," it has drawbacks because the financial industry increasingly will use such technology and the "regulatory framework that is supposed to oversee such technological and financial innovations" is insufficient).

in the retail payments system.[46] A failure of the infrastructure supporting retail payments processing could certainly be systemic, however, and could be at least as debilitating as a financial crisis transmitted through credit channels.[47] The retail payments system performs functions that are key to consummating everyday transactions—it stores and keeps funds safe for customers and it allows for those funds to be transferred to provide consideration for transactions.[48] If a widespread failure of retail payments infrastructure were to compromise the storage and/or transfer of funds, that could be more immediately harmful than any systemic problem conveyed through the credit channels.

Because there is a lack of historical precedent from which to draw lessons about how operational risks might trigger, or transmit, broader economic harm, we need a new framework within which to consider what may arise as our retail payments infrastructure evolves. This new framework is vital from both an ex ante and an ex post perspective: our current narrative may blind us to existing vulnerabilities in the financial system, and also may prescribe unsuitable remedies if a payments failure does occur. Bernanke has noted that the emergency measures adopted by governments in response to the financial crisis of 2007–2008 did not differ significantly from those that Walter Bagehot would have recommended in the nineteenth century.[49] Similar measures probably will continue to be appropriate as long as crises are primarily communicated by credit channels, but traditional methods of emergency support are likely to be of limited utility if the problem is an immediate cessation of the ability of market participants to transact, rather than a drying up of credit. Financial stability regulation needs to be reconsidered in light of the possibility of crises precipitated by, and transmitted through, operational failures.

B. A Complexity Perspective

To facilitate such exploration, this Section of the Article provides a new framework within which to consider the possibility of cascading technological failures. Adopting a new and complementary theoretical framework will force us to divorce ourselves from the theoretical path dependency that comes from

---

[46] Lacker notes two instances—a Bank of New York software glitch in 1985 and September 11, 2001—where there were technological problems that initiated problems in the interbank payments system. Lacker, *supra* note 39, at 24. Neither of these impacted the retail payments system, however, and to the extent that their impacts rippled through the wholesale banking system, it was as a result of credit channels. *See id.* (noting that runs only occurred as a result of the initial failures).

[47] *See* Kristin N. Johnson, Essay, *Managing Cyber Risks*, 50 GA. L. REV. 547, 553 (2016) (discussing a similar argument with respect to cyber attacks specifically).

[48] Dan Awrey & Kristin van Zwieten, *Mapping the Shadow Payment System* 7 (SWIFT Inst., Working Paper No. 2019-001, 2019), https://swiftinstitute.org/wp-content/uploads/2019/10/Mapping-the-Shadow-Payment-System-vFINAL.pdf [https://perma.cc/H37J-8BU7].

[49] *See* BERNANKE, *supra* note 29, at 1.

following historical precedent too closely. Literature from the discipline of complexity science, which provides a more general understanding of complex adaptive systems through their features and failures, can help provide such a theoretical framework.[50]

Complex adaptive systems are complex in the number and diversity of their components and complex in the interactions of their components, with the result that the behavior of the system as a whole is complex and not predictable from merely examining the components in isolation.[51] These systems tend to be "robust yet fragile," in the sense that steps taken to make the system more robust unwittingly create fragilities that only become evident when parts of the system interact in unanticipated ways.[52] Such unexpected interactions can trigger failures with catastrophic consequences.[53] These types of failures are often referred to as "cascade[] failures," because they are transmitted by interconnections amongst the system components, and magnified through the transmission process.[54]

Many prominent economists and legal scholars already have observed that the financial system exhibits the features of a complex adaptive system, and have turned to complexity science for its explanatory power in illuminating how the financial system functions.[55] When scholars have applied the complexity science literature to the financial system, however, they have often done so retroactively, seeking to illuminate the dynamics of past crises, often with a particular focus on credit transmission channels.[56] The related field of network theory *has* been used prospectively, primarily by economists, to gain some insight as to how systemic risks might propagate in networks of financial institutions and markets in the future, but this literature again is focused on

---

[50] *See* Ruhl, *supra* note 10, at 562 (discussing the application of complexity science to the realm of law and other social sciences). Notwithstanding that the discipline evolved from the hard sciences, complexity science also has proved to have many applications to social systems like economies. *See id.*

[51] *Id.* at 567–68 (quoting Alderson & Doyle, *supra* note 10, at 840) (citing MELANIE MITCHELL, COMPLEXITY: A GUIDED TOUR 12–13 (2009)).

[52] *See id.* at 562, 564–65 ("[T]he 'robust yet fragile' (RYF) dilemma . . . is an inherent quality of any complex adaptive system . . . ." (citing Alderson & Doyle, *supra* note 10, at 843)).

[53] *Id.* at 564–65.

[54] Dirk Helbing, *Globally Networked Risks and How to Respond*, 497 NATURE 51, 51 (2013).

[55] *See* Lawrence G. Baxter, *Betting Big: Value, Caution and Accountability in an Era of Large Banks and Complex Finance*, 31 REV. BANKING & FIN. L. 765, 861–68 (2012) (discussing the operational and regulatory complexity of financial markets). *See generally* Andrew G. Haldane & Robert M. May, *Systemic Risk in Banking Ecosystems*, 469 NATURE 351 (2011) (comparing the financial system and its evolution to that of complex ecosystems).

[56] *See* Baxter, *supra* note 55, at 866 ("The newly perceived importance of developing better methods for predicting potential system failures is one of the byproducts of the Financial Crisis."); Haldane & May, *supra* note 55, at 353 (noting that one of the leading issues of the last financial crisis was the interruption of loans and credit channels between banks).

credit transmission channels.[57] In contrast, this Article seeks to use the complexity literature to explore potential vulnerabilities in our financial system that do not arise from the extension of credit. Because a future payments failure may resemble a blackout more than a bank run, this Article turns to the literature on cascading failures of complex systems like the electrical grid, to help assess threats that may emerge as our payments system evolves.[58] The literature on complex systems also can inform the development of regulatory measures designed to make the payments ecosystem more robust to operational risk, without exacerbating its fragility.

As with any complex system, "[p]ower transmission systems are heterogeneous networks of large numbers of components that interact in diverse ways."[59] Components of power transmission systems can fail for a variety of reasons. They can be disconnected for safety reasons, for example, or damaged as a result of "aging, fire, weather, poor maintenance, or incorrect design or operating settings."[60] If a component fails for any of these (or other unanticipated) reasons, then power will be redistributed to other components of the system and "flows all over the network change."[61] Flows of power also can be altered by changes in the behavior of the human actors using the power (for example, increased use of air conditioners during a heatwave).[62] These changes cause the remaining components of the system to interact in new and unanticipated ways, and the more loaded the remaining components are, the stronger their interactions are likely to be.[63] If further component failures ensue as a result, the system will become more fragile and stressed, with the possibility of "the propagation of many rare or unanticipated failures in a cascade."[64] The events that trigger these cascade failures "can seem random and trivial in isola-

---

[57] *See* Enriques et al., *supra* note 7, at 361 ("Network theory is . . . a well-developed and scientifically advanced conceptual framework to analyze contexts in which connections are relevant, [and] it provides a rigorous set of tools to identify, describe, and measure connections." (citing SANJEEV GOYAL, CONNECTIONS: AN INTRODUCTION TO THE ECONOMICS OF NETWORKS 2 (2012))). *See generally* Paul Glasserman & H. Peyton Young, *Contagion in Financial Networks*, 54 J. ECON. LITERATURE 779 (2016) (providing a review of this economic literature on network theory that emphasizes its focus on credit and leverage).

[58] *See* Ian Dobson et al., *Complex Systems Analysis of Series of Blackouts: Cascading Failure, Critical Points, and Self-organization*, 17 CHAOS 026103, 026103-1 (2007) ("Cascading failure is the usual mechanism by which failures propagate to cause large blackouts of electric power transmission systems.").

[59] *Id.* at 026103-2.

[60] *Id.*

[61] *Id.*

[62] M. Rosas-Casals et al., *Knowing Power Grids and Understanding Complexity Science*, 11 INT'L J. CRITICAL INFRASTRUCTURES 4, 7 (2015).

[63] Dobson et al., *supra* note 58, at 026103-2.

[64] *Id.*

tion," but "[o]nce the cascade starts . . . it can be virtually unstoppable."[65] One important insight from the complexity science literature is that even if a faulty component can be identified after a problem, it is incomplete to say that that component caused the problem. Rather, the faulty component served as the trigger, but the problem was in fact caused by the complexity of the system in which the component was embedded.[66]

This concept of cascade failure has significant descriptive power not only for electrical grids, but for all kinds of complex systems. The next Section will therefore use this complexity framework as the basis for conjecture about how a cascading failure in the retail payments system might transpire.[67] A complexity science framework is not only descriptive, though; it also provides suggestions for making a complex adaptive system less prone to catastrophic failures.

In an excellent paper outlining systemic risks in legal systems, Professor J.B. Ruhl synthesizes the complexity science literature in a way that is accessible to legal scholars. To assist in determining how to design a system that is less susceptible to cascading failures and thus more likely to continue to discharge its functions, Ruhl provides a taxonomy of five dimensions of robustness: reliability, efficiency, scalability, modularity, and evolvability.[68] Ruhl notes that it is usually not possible to maximize all five dimensions of robustness; sacrifices in one dimension are sometimes needed to avoid a system that is robust yet fragile to certain shocks.[69]

Sacrificing efficiency in the name of stability is reasonably intuitive, although often politically challenging. The mechanisms that allow a financial system to move capital around more efficiently are equally as efficient in transmitting shocks.[70] "Shortcuts" that allow for direct links between components of a complex adaptive system are therefore likely to increase the risk of cascade failure within that system, whereas inhibiting the flow of any complex system slows down the transmission of problems from component to compo-

---

[65] Ruhl, *supra* note 45, at 410 (citing Raissa M. D'Souza, *Curtailing Cascading Failures*, 358 SCI. 860, 861 (2017)).

[66] SAMUEL ARBESMAN, OVERCOMPLICATED: TECHNOLOGY AT THE LIMITS OF COMPREHENSION 12 (2016).

[67] *See infra* notes 89–127 and accompanying text.

[68] Ruhl, *supra* note 10, at 564, 570 (quoting Alderson & Doyle, *supra* note 10, at 840). The framework provides: "*Reliability* involves robustness to component failures. *Efficiency* is robustness to resource scarcity. *Scalability* is robustness to changes to the size and complexity of the system as a whole. *Modularity* is robustness to structured component rearrangements. *Evolvability* is robustness of lineages to changes on long time scales." Alderson & Doyle, *supra* note 10, at 840.

[69] Ruhl, *supra* note 10, at 575–76. Ruhl cites the work of complexity scientists Alderson and Doyle, who have concluded that if the priority is the reduction of risk of systemic failure, then scalability, modularity, and evolvability should be prioritized over efficiency and reliability. *Id.* at 594 (citing Alderson & Doyle, *supra* note 10, at 841).

[70] Baxter, *supra* note 55, at 858.

nent.[71] Sacrificing reliability in order to prevent systemic risk is a little more counterintuitive, but it stems from the same idea. Incremental steps that are taken to make individual components of a system more reliable in the face of known problems reduce the risk of those problems, but by ensuring that those components will continue to function, and by increasing the complexity of the system as a whole, those incremental steps can combine to facilitate the transmission of unanticipated large problems.[72] This does not mean that systems designers and policy-makers should seek to *maximize* inefficiency and unreliability—this would pyrrhically reduce systemic risk by creating a system that fails to work even in normal times. The key is to find balance with the dimensions of robustness that are more likely to promote the stability of the system as a whole—which may require "investing in some inefficiency and sloppiness."[73]

Scalability, modularity, and evolvability are all dimensions of robustness that relate to the system's ability to continue functioning well amidst changes. In the case of scalability, the relevant changes are to size and complexity. The modularity of a system refers to its ability to cope with changes to the organization of the system's components: "[m]odularity promotes system robustness by allowing systems to work in parallel and to reconfigure, either in response to a component failure or as an adaptive move, without crashing the system."[74] Evolvability is particularly important in the context of an adaptive complex system, because it denotes an ability to adapt as the system changes over time.[75] It is often impossible to predict how a system will be used in the future, but a system that is robust from an evolvability perspective can withstand many unanticipated changes in usage. This concept of evolvability is particularly important in the context of a highly regulated system, where the industry is likely to change its behavior in response to regulations. Such behavioral changes

---

[71] Ruhl, *supra* note 45, at 417, 419 (quoting Amir Bashan et al., *The Extreme Vulnerability of Interdependent Spatially Embedded Networks*, 9 NATURE PHYSICS 667, 667 (2013)) (citing Alderson & Doyle, *supra* note 10, at 843); *see also* Dobson et al., *supra* note 58, at 026103-11 (explaining that there is a point of "critical loading at which the probability of cascading failure sharply increases").

[72] *See* Ruhl, *supra* note 10, at 564–65 (discussing how "[o]ver time, as each local failure is met with new fail-safe strategies, system architecture grows more complex, and systemic risk becomes embedded in the system"). In the context of power transmission systems, Dobson et al. have observed that "measures to reduce the frequency of small blackouts can eventually reposition the system to have an increased risk of large blackouts." Dobson et al., *supra* note 58, at 026103-10. Dobson et al. further remark that "[t]he possibility of an overall adverse effect on risk from apparently sensible mitigation efforts shows the importance of accounting for complex system dynamics when devising mitigation schemes." *Id.* (citing B.A. CARRERAS ET AL., HAW. INT'L CONF. ON SYS. SCI., BLACKOUT MITIGATION ASSESSMENT IN POWER TRANSMISSION SYSTEMS (2003), http://iandobson.ece.iastate.edu/PAPERS/carrerasHICSS03.pdf [https://perma.cc/JD7S-7VSZ]).

[73] Ruhl, *supra* note 10, at 594.

[74] *Id.* at 573.

[75] *Id.* at 574.

subsequently inspire new regulations and more behavioral responses, resulting in a continually changing system.[76]

There are a number of measures that can be adopted to promote these types of robustness. According to the complexity scientists, "redundancy, sensors, and feedback" mechanisms are the measures on which regulators seeking to avoid catastrophic failures should focus.[77] Redundancy is a relatively familiar concept, with "redundancy in components and system subparts, although not always contributing to efficiency . . . [being] a well-studied and common strategy in systems application."[78] Redundancy may promote modularity, but it will not necessarily create the scalability and evolvability that are desirable in any complex adaptive system.[79] Sensors built into the system can detect internal and external changes that may pose threats to the continued functioning of the system, and feedback protocols can act on the input of those sensors, allowing the system to grow and evolve.[80] Ensuring the quality of the components of the system themselves is also a relevant fail-safe strategy, but this contributes primarily to the reliability of the system, rather than its scalability, modularity, or evolvability. Thus, if our primary concern is with systemic risk, component quality should not be the only fail-safe mechanism.[81] As Ruhl summarizes, "The core idea is to avoid constructing a rigid, highly integrated network of ultraquality, homogenous components with few sensors and centralized system actuators."[82]

It is important to note that incorporating redundancy, sensors, and feedback protocols will reduce, but not eliminate, the risk of cascade failures within the system.[83] The term "normal accident" was most famously formulated by Charles Perrow, and he uses it to describe accidents that are produced by cascade failures facilitated by the "interactive complexity and tight coupling" of highly complex systems.[84] He uses the word "normal" to convey his view that

---

[76] Lawrence G. Baxter, *Adaptive Financial Regulation and RegTech: A Concept Article on Realistic Protection for Victims of Bank Failures*, 66 DUKE L.J. 567, 594 (2016).

[77] Ruhl, *supra* note 10, at 594.

[78] *Id.* at 580.

[79] *See id.* at 581 ("Ultraquality and redundancy techniques 'can be effective at providing robustness in the face of component uncertainty, but they do not help achieve robustness to the external environment.'" (quoting Alderson & Doyle, *supra* note 10, at 841)).

[80] *Id.*

[81] *See id.* at 579 ("One obvious approach for managing component-level constraints on system robustness is to improve the quality of the system components so they rarely fail."). Cost and technological limitations also may place finite limitations on the level of quality that can be achieved.

[82] *Id.* at 594.

[83] *See id.* at 584 (discussing how fail-safe mechanisms such as "components, sensors, redundancies, feedback mechanisms, and actuator protocols" increase both the robustness and the complexity of the system).

[84] PERROW, *supra* note 13, at 5.

such accidents are a fundamental, perhaps unavoidable, feature of such highly complex systems.[85] Systems will always remain vulnerable to unanticipated risks, because sensors may not look for these, and feedback protocols will give no guidance as to how to react.[86] Furthermore, once risks are anticipated, the inclusion of any sensors and feedback protocols to address them will further complexify the system, potentially generating the conditions for different kinds of cascade failures.[87] That does not mean that measures to increase robustness are always futile, though. As Ruhl notes, "[S]ome degree of systemic risk is inherent in any complex adaptive system—but the balance between robustness and fragility is something we can hope to influence."[88]

C. Cascading Retail Payments Failure

Retail payment services are provided to customers by a heterogeneous global network of central banks, banks and clearinghouses, and, increasingly, non-banks providing payment services.[89] These institutions and firms are themselves composites of software, hardware, and humans: the retail payments ecosystem therefore can be characterized as a system of systems, with the individual components interacting with each other and with customers in diverse ways. These interactions will continue to evolve as consumer usage patterns change and retail payments providers enter and exit the market—and such interactions are not overseen or coordinated by any overarching centralized control. The retail payments ecosystem thus qualifies as a complex adaptive system and is susceptible to cascade failures.[90]

It is difficult to provide a prospective description of what a cascade of operational failures in the retail payments ecosystem might look like. There are certainly no historical examples that provide any insight into how our modern retail payments ecosystem might fail. The so-called "back office" crisis that disabled the stock markets in the late 1960s was caused by paper backlogs rather than the interactions of complex technologies, and although it resulted in the insolvency of many broker-dealers, it impacted only those who trade

---

[85] *Id.*

[86] *See* Ruhl, *supra* note 10, at 587 (noting that one reason fail-safe mechanisms cannot eliminate systemic failure entirely is that mechanisms designed to ward off known dangers might be at risk of failure from unknown dangers).

[87] *Id.* at 588 (citing Alderson & Doyle, *supra* note 10, at 842).

[88] *Id.* at 565.

[89] Regarding new non-bank payment services, see *infra* notes 172–291 and accompanying text.

[90] One definition of "complex adaptive systems" is: "large networks of components with no central control and simple rules of operation give rise to complex collective behavior, sophisticated information processing, and adaptation via learning or evolution." MITCHELL, *supra* note 51, at 13.

stocks[91]—a much smaller subset of the population than those who need to make and receive retail payments. Following the 9/11 terrorist attacks, there were some problems with processing wholesale payments amongst financial institutions, but retail payments were not compromised to any significant extent.[92] The week-long "bank holiday" declared by President Roosevelt in 1933 *was* "a complete stoppage of the entire U.S. payments system," but a voluntary suspension of retail payments in the 1930s tells us nothing about how payments technology might inadvertently fail in 2021.[93] The 1933 bank holiday also reveals little about the economic cost of a frozen retail payments system: given the economic turmoil of the Great Depression, it is hard to parse the precise economic cost of this suspension of payments processing. In fact, many have argued that the bank holiday actually improved the economic situation by reestablishing the credibility of retail payments processing.[94]

When attempting to divine the potential economic cost of a modern-day payments outage, a helpful, though imperfect, analogy can be drawn with the outages experienced by the mobile money platform M-Pesa in Kenya. Although this Article is focused on retail payments processing in advanced economies—and thus does not consider the operational risks associated with the mobile money platforms that have been extremely successful in developing economies—Kenyan citizens' widespread use of M-Pesa illustrates the potential for technological problems with a payments systems to compromise a nation's economy. For example, M-Pesa experienced a significant outage in December 2018 and then again in May 2019—both of these lasted approximately two hours and were attributed to a "database problem."[95] A prior outage also had occurred in 2017, when, for unexplained reasons, "the operator had lost connectivity in its core network and the redundant path."[96] Even these relatively short outages had noticeable economic consequences,[97] and the Kenyan

[91] For a discussion regarding the paper logs and broker-dealer failures that caused the back office crisis, see Walter Werner, *The SEC as a Market Regulator*, 70 VA. L. REV. 755, 770 (1984); Wyatt Wells, *The Remaking of Wall Street, 1967 to 1971*, HARV. BUS. SCH. (Oct. 2, 2000), https://hbswk.hbs.edu/archive/the-remaking-of-wall-street-1967-to-1971 [https://perma.cc/9KGP-F2RG] (discussing the Wall Street crisis in the late 1960s as one that occurred in the "back offices" of financial firms).

[92] Lacker, *supra* note 39, at 7, 24.

[93] WILLIAM L. SILBER, FED. RSRV. BANK OF N.Y., WHY DID FDR'S BANK HOLIDAY SUCCEED? 21 (2009), https://www.newyorkfed.org/medialibrary/media/research/epr/09v15n1/0907silb.pdf [https://perma.cc/GZL3-4LZD].

[94] *Id.* at 19.

[95] Njenga Hakeenah, *Countrywide M-Pesa Outage Hits Safaricom, Kenyans Again*, THE EXCHANGE (May 17, 2019), https://theexchange.africa/countries/kenya/m-pesa-outage-countrywide-safaricom-bills-shopping-sanctions/ [https://perma.cc/DP5D-XX9R].

[96] *Id.* Furthermore, the Chief Executive of Safaricom, the company behind M-Pesa, released a statement saying that "This shouldn't happen. It is unusual that both failed." *Id.*

[97] *Id.*

Treasury Department has since recognized that if M-Pesa were to be compromised for a more prolonged period of time, the Kenyan government's tax revenues ultimately would be impacted. The Kenyan Treasury Department therefore has designated the possibility of a "technological disaster" as a "plausible fiscal risk."[98]

This Article argues that policy-makers dealing with more developed financial systems also should consider the economic costs of operational failures in the retail payments ecosystem, although two commenters on the payments industry recently downplayed such concerns. Buckley and Mas hypothesized that "[w]hile it may prove highly inconvenient to many people, it is difficult to imagine the failure of a payments provider causing financial market contagion in the manner that the collapse of Lehman Brothers did."[99] This observation, however, seems predicated on the assumption that, in the absence of credit channels linking payments providers, there are no mechanisms for contagion to spread amongst them. Alternative contagion channels may exist, though.[100]

In their "pre-mortem" of cyber risks to the stability of the wholesale payments system, Eisenbach et al. have focused on events that could compromise the availability of data or systems, and events that could compromise the integrity of data.[101] The functioning of the retail payments ecosystem could be similarly compromised by disruptions to the availability and integrity of its data and systems. Such disruptions could be the result of a cyber attack, but they also could arise from other operational problems. For example, different payments providers might rely on shared infrastructure, such as cloud data storage, and thus be equally compromised by a problem with that infrastructure that prevents them from, say, identifying whether a particular payer has sufficient funds to satisfy a request for a payment.[102] Or a payments provider might succumb to a software bug that prevents it from transmitting payment instructions from payer to payee. That provider might try to route their customers' payment orders to a second payments provider while the bug is being fixed, but the second provider may be suffering the same problem simultaneously (financial

---

[98] *See* NAT'L TREASURY, REPUBLIC OF KENYA, 2017 BUDGET POLICY STATEMENT: CONSOLIDATING ECONOMIC GAINS IN AN ENVIRONMENT OF SUBDUED GLOBAL DEMAND 83 (2016), http://treasury.go.ke/component/jdownloads/send/172-budget-policy-statement/459-2017-budget-policy-statement.html (last visited Nov. 17, 2020) (noting that the economic risk comes from "mobile money transfer services" in particular).

[99] Buckley & Mas, *supra* note 40, at 87.

[100] *See* EISENBACH ET AL., *supra* note 1, at 1 ("Technological linkages through which cyber attacks can spread are likely to be different from solvency and linkages arising from business interactions.").

[101] *Id.* at 5.

[102] *See id.* at 31 ("Vulnerabilities arising from third-party service providers is viewed as a prominent sources of cyber risk especially when a provider is common to many institutions.").

services providers are increasingly sourcing their technology from the same third-party vendors, so such an outcome is becoming increasingly likely).[103] Or the second provider might have been functioning well initially, but its systems could buckle under the increased load of payment instructions it receives as a result of the first provider's technological problem.[104] Experience with power grids suggests that stressed alternative infrastructure will be more vulnerable to its own failure—it is the stress of high loads that typically bring about blackouts.[105] If payments providers are compromised by an increased load of instructions routed from other struggling providers, the remaining payments architecture could become overloaded—even across national borders.

The technological glitches that have plagued the trading of stocks and treasuries over the last decade also may provide some indication of how operational failures might cascade through the retail payments ecosystem. As these markets have become more technologically complex, trading decisions have been increasingly delegated to algorithms. Algorithms can malfunction (sometimes for a reason as simple as a mistaken key being pressed on a keyboard—often referred to as a "fat finger" error),[106] and on several occasions over the last decade, these algorithms have interacted in ways that have caused problems to cascade through markets, resulting in unexpected gyrations in the trading of assets, and thus, their prices.[107] The initial triggers and cascading failures that caused such gyrations can remain inscrutable long after the event.[108]

A technical failure at a payments provider (again, perhaps something as simple as a fat finger error or a lurking software bug) could interact with the automated components of other payments providers' systems to create a cascade of similarly inscrutable and problematic responses.[109] The likelihood of

---

[103] *See* FIN. STABILITY BD., FINANCIAL STABILITY IMPLICATIONS FROM FINTECH: SUPERVISORY AND REGULATORY ISSUES THAT MERIT AUTHORITIES' ATTENTION 19 (2017), http://www.fsb.org/wp-content/uploads/R270617.pdf [https://perma.cc/T7NV-ZKVP] (explaining that multiple companies might be impacted if they all rely on the same compromised third-party service).

[104] Ruhl, *supra* note 45, at 421 ("[O]verload failures occur when the system responds to a perturbation . . . by rerouting network flow to the point that a node fails and immediately sheds the overload to other nodes, some of which fail and shed even more overload into the system.").

[105] Dobson et al., *supra* note 58, at 026103-6.

[106] Yesha Yadav, *The Failed Regulation of U.S. Treasury Markets*, 121 COLUM. L. REV. 1, 35 (forthcoming 2021), https://ssrn.com/abstract=3365829 [https://perma.cc/3NYX-8NX4].

[107] *Id.* at 35–36. Furthermore, "the costs of these errors can compound incrementally as prices across the system rapidly incorporate these problems far too fast for human traders to contain the damage." *Id.* at 35.

[108] *See id.* at 36 (recounting how a year after one such event, multiple regulators were unable to discern its cause).

[109] The economic impacts of widespread technological problems in the retail payments system are likely to be much more immediate than the consequences of any trading glitch. As I have previously argued, cascading pricing failures in the equities markets could impact financial stability if financial institutions exposed to the mispriced assets engaged in fire sales of other assets to remain solvent (or

such transmission could be increased by the growing use of "application programming interfaces," (APIs) which allow the different software programs used by different payments providers to communicate directly with one another.[110] From a complexity science perspective, these APIs can be viewed as shortcuts that allow for payment instructions to flow more efficiently between the providers; increasing the number of shortcut links that exist between different parts of the retail payments ecosystem also will make it easier to transmit problems from one part of the ecosystem to another.[111]

Retail payments providers typically commit to getting critical processing systems back up and running within a specified time period after an operational failure (for example, by the end of the day), but these commitments might ultimately prove unrealistic.[112] If payments providers plan to recover by routing payments through an uncompromised alternative payments provider, they may be falling prey to the assumption that failures occur in isolation. As this Part has already explored, it is quite possible that other providers will suffer from the same problem at the same time, or will be overloaded by the additional traffic. The entire payments ecosystem could be compromised to varying degrees, leaving little in the way of alternative processing routes. It is an open question how long and how widespread an outage would have to be before broader economic growth were to become compromised, but any event that prevents a payments provider from identifying and/or transferring user funds would cut off commerce immediately for all users who rely on that provider for their exclusive means of transacting (because of identity verification requirements, establishing access to an alternative electronic payment typically takes users some time).[113] Even if a user already had established access to a

---

even failed as result of exposure to those assets). Such failure would impact the broader economy, however, primarily through fire sale or credit channels, and to date glitches have been resolved before their impact could be so transmitted. Hilary J. Allen, *Driverless Finance*, 10 HARV. BUS. L. REV. 157, 179–80 (2020). *See generally* Yadav, *supra* note 106 (discussing treasury trading markets and their weaknesses).

[110] *See* Perry Eising, *What Exactly IS an API?*, MEDIUM (Dec. 7, 2017), https://medium.com/@perrysetgo/what-exactly-is-an-api-69f36968a41f [https://perma.cc/3VZF-CPBP] (explaining that an API is a piece of code that permits communications between different platforms).

[111] *See* Ruhl, *supra* note 45, at 417–19 (regarding systemic risks associated with shortcut links).

[112] *See* FFIEC, RETAIL PAYMENT SYSTEMS: IT EXAMINATION HANDBOOK 47 (2016), https://it handbook.ffiec.gov/media/274860/ffiec_itbooklet_retailpaymentsystems.pdf [https://perma.cc/VW6U-6MZL] (explaining that financial institutions and other financial providers should develop "business continuity plans" that aim for a service restoration time that is "reasonable for internal business units, other dependent financial institutions, and counterparties").

[113] Some countries (most notably India) are implementing national digital identities. Ross P. Buckley et al., *Sustainability, FinTech and Financial Inclusion* 17 (Univ. of Luxembourg, Working Paper No. 2019-006, 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3387359 [https://perma.cc/4LY3-2HEX]. Buckley et al. note that "Axis Bank was the first Indian bank to offer an eKYC facility in 2013, reducing the turnaround time for opening bank accounts from 7-10 days to just

substitute system for effecting payments, they would nonetheless be impaired if their transaction partners did not also have an alternative means of exchanging funds with them. In other words, the inability of consumers to pay for goods and services would prevent the suppliers of those goods and services from receiving the *funds* they need to make their own payments, even if those suppliers had access to alternative physical means of making payments.

Although the events of the financial crisis of 2007–2008 seemed to transpire very quickly, the transmission of harm to the broader economy through credit channels was not instantaneous.[114] Commercial activity, however, as well as the provision of many public services, could be impacted immediately if everyday transactions were disrupted.[115] Without payments systems, people might be unable to make basic and time-critical purchases for things like food, transportation, and shelter.[116] We might even see an immediate increase in theft and looting by people otherwise unable to obtain basic goods. The macroeconomic consequences would be swift if creditors, suppliers, and employees were to remain unpaid for a prolonged period of time, preventing the "positive

---

one day." *Id.* They go on to observe that, "[t]oday, many traditional banks and licensed payments banks in India offer accounts which can be opened and used instantly with eKYC." *Id.* Other countries, however, may be averse to allowing the government to establish such a national identification system, meaning that some kind of private digital verification would be needed before a payments system could be used—if this has not been established in advance, then users still will face a lag time before they can access an alternative payments system.

[114] Economist Robert Solow provides an excellent description of how this transpired:

> What happened in the course of the financial crisis is that banks, insurance companies, and credit unions—all sorts of institutions whose normal business is to finance industry and people who want to buy cars and houses—they've been paralyzed. So businesses that would normally be investing in a new computer or a new fleet of trucks or whatever that would need to borrow, can't borrow. And if they could borrow, they would be paying a very high rate of interest. So they stop. And then the real economy begins to slow down, and people lose their jobs because their firms can't sell to consumers, can't sell to other businesses. A modern economy is a more complicated piece of machinery than a simple barter economy. Production is very complicated. You start with God knows what, and you end up with some extraordinarily complicated piece of equipment or the machinery that appears in my dentist's office when I sit down. That can't be directed without a good deal of action which is taken now and can only pay off many stages later. And that's where the credit mechanism comes in. Industry that depends on it has to slow down, simply because it can't get the funds that enable each stage in production to pay off the previous stage.

What IF the Banking System Failed?, PBS NEWS HOUR (Jan. 11, 2011), https://www.pbs.org/newshour/economy/what-if-the-banking-system-fai [https://perma.cc/ZUM7-4FRF].

[115] Johnson, *supra* note 47, at 552–53.

[116] *See* Awrey & van Zwieten, *supra* note 27, at 799 (explaining that one of the risks in some types of payments systems arises when users employ that system for their everyday expenses and payments).

externalities" that flow from general commerce and trade.[117] Collectively, fewer transactions also would generate less tax revenue, and lowered tax revenues typically result in greater government debt,[118] or even painful austerity measures.[119]

Thus far, this Part has focused only on the potential impact of cascading technological problems. In reality, however, such cascading failures in the payments system are likely to implicate and intertwine technological and economic forces. Because some of the component parts of the financial system are human actors, feedback effects are likely to be less predictable than in a purely technical system.[120] Panic could create a run-like dynamic that harms the broader economy:[121] for example, even if alternative payments processing were to remain technically available, panic regarding payments technology nonetheless might inspire withdrawals from banks and other payments providers as people try to hoard cash. Alternatively, people could limit the transactions they carry out "with consumers delaying fund transfers to other businesses and households to which they owe a payment, and which transferees were relying on those funds to satisfy other debts or operational expenses."[122] Such a chain of events could impact the macroeconomy.[123] Or people might start to purchase and hoard goods because they fear that they will not be able to transact in the future. As we have seen in economies afflicted with hyperinflation, such hoarding renders goods scarce, and if it persists, the economy begins to deteriorate.[124]

The potential for an economic catastrophe to arise from cascading operational failures in the retail payments system justifies a more comprehensive approach to regulating for operational or infrastructure-related systemic risks.

---

[117] *See* Ricks, *supra* note 16, at 839 (quoting Richard Epstein, *Freedom of Association and Antidiscrimination Law: An Imperfect Reconciliation*, LAW & LIBERTY (Jan. 2, 2016), https://lawliberty.org/forum/freedom-of-association-and-antidiscrimination-law-an-imperfect-reconciliation/ [https://perma. cc/ZM22-XL2G]) (discussing the importance of the payments system to the commercial system); *see also* Awrey & van Zwieten, *supra* note 27, at 809 (discussing how in the event that a payments system entity declares bankruptcy and regulators decide not to intervene, there are "potential externalities stemming from the inability of customers to pay creditors, suppliers, and employees").

[118] REINHART & ROGOFF, *supra* note 33, at 142.

[119] *See* Allen, *supra* note 31, at 1106–07 (explaining the social cost of austerity measures).

[120] Steven L. Schwarcz, *Regulating Complexity in Financial Markets*, 87 WASH. U. L. REV. 211, 233 (2009).

[121] *See* EISENBACH ET AL., *supra* note 1, at 6 ("Like any operational risk event, a cyber attack can trigger a liquidity run and lead to solvency issues.").

[122] Christina Parajon Skinner, *Regulating Nonbanks: A Plan for SIFI Lite*, 105 GEO. L.J. 1379, 1418 (2017).

[123] *Id.*

[124] Kimberly Amadeo, *Hyperinflation: Its Causes and Effects with Examples*, THE BALANCE (July 1, 2020), https://www.thebalance.com/what-is-hyperinflation-definition-causes-and-examples-3306097 [https://perma.cc/979C-TMC9].

Although the prognosis for preventing normal accidents within the retail payments system is not particularly good, complexity science nonetheless offers suggestions on how to improve systemic robustness.[125] Given the potentially catastrophic consequences of cascading payments failure, even incremental improvements are a worthwhile policy objective.[126] Accepting the inevitability of normal accidents in the retail payments system also can spur good policy by encouraging the design of thoughtful emergency measures that might respond to future technological failures, to serve as a complement to regulation that seeks to make such failures less likely to occur in the first place. Although the retail payments system is in a moment of rapid change—which makes it challenging to assess the robustness of the system and how to improve it—the following Parts nonetheless will consider traditional retail payments providers as well as more recent entrants to the retail payments industry in terms of their impact on the overall robustness of the retail payments ecosystem. Building on this analysis, Part IV provides some policy suggestions intended to prioritize the robustness dimensions of modularity, scalability, and evolvability.[127]

II. Operational Risks in the Bank-Based Retail Payments System

The purpose of the retail payments system is to "facilitate the transfer of funds from debtors (payors) to creditors (payees) in satisfaction of financial obligations."[128] To do this, the payments system must be able to protect funds prior to and during transfer, and also must ensure that the transfer actually occurs, at full value, in a timely fashion.[129] Payments made using checks, cards, or electronic transfers are processed as a series of accounting changes to the parties' deposit accounts as represented on ledgers maintained by the parties' banks: a payer's account is debited and a credit is made to the payee's account in a corresponding amount.[130] Because payers and payees often do not have accounts with the same bank, mechanisms are needed to reconcile accounting ledgers at different banks and transfer funds between them.

For domestic payments, this process—known as clearing and settlement—is facilitated by the existence of a central bank, such as the Federal Re-

---

[125] *See* Arbesman, *supra* note 66, at 102 (noting that although increasingly complex systems can lead to additional issues, these same issues also can help us figure out how to fix problems in interconnected systems).

[126] *See generally* Allen, *supra* note 15 (providing an explanation of why a precautionary approach to financial stability regulation is justified).

[127] *See infra* notes 292–348 and accompanying text.

[128] *See* Awrey & van Zwieten, *supra* note 27, at 781 (describing this transfer as an important component of both wholesale and retail payments systems).

[129] *Id.* at 782–83.

[130] Carnell et al., *supra* note 4, at 71–73.

serve.[131] Deposit-taking banks all have accounts with the central bank, and so debits can be made to the payer's bank's account at the central bank and credits can be made to the payee's bank's account.[132] Over time, clearinghouses have emerged that make this process more efficient; "after sorting [payment instructions received from banks] and aggregating payments destined for the same bank, [they] then transmit information to each participating bank regarding the details of payments to be made to their accountholders."[133] In the United States, the clearinghouse for domestic retail payments is the Clearing House Interbank Payments System (CHIPS).[134] The clearing and settlement of cross-border payments is more complicated. This requires the settling of accounts through a network of correspondent banks—and there is often significant cost and delay associated with processing cross-border transactions.[135]

Because banks historically have provided the bulk of retail payment services—which have synergies with their deposit-taking and other functions—concerns about threats to the proper functioning of the retail payments system typically have been subsumed into discussions of the prudential regulation of banks, under the assumption that as long as banks remain safe and sound, retail payments processing will be protected.[136] To be clear, the existing bank regula-

---

[131] *Id.* at 73.

[132] The banks involved also will make the appropriate adjustments to the payer's and payee's individual accounts. *Id.* at 71–73.

[133] Awrey & van Zwieten, *supra* note 27, at 792.

[134] *Id.*

[135] Mills et al., *supra* note 18, at 18 (first citing COMM. ON PAYMENTS & MKT. INFRASTRUCTURES, BANK FOR INT'L SETTLEMENTS, CORRESPONDENT BANKING (2016), http://www.bis.org/cpmi/publ/d147.pdf [https://perma.cc/C34F-YCY7]; and then citing MCKINSEY & CO., GLOBAL PAYMENTS 2015: A HEALTHY INDUSTRY CONFRONTS DISRUPTION 22–24 (2015), https://www.mckinsey.com/~/media/McKinsey/dotcom/client_service/Financial%20Services/Latest%20thinking/Payments/Global_payments_2015_A_healthy_industry_confronts_disruption.ashx [https://perma.cc/8L8N-3APR]). Mills et al. have noted:

> Currently, electronic cross-border payments are effected by credit (and sometimes debit) transfers that convert funds from bank to bank through a series of correspondent banking relationships, often with an assessment of multiple fees. . . . According to one report, the settlement times for cross-border payments can take up to five days for the most common currency pairings, generally with limited clarity regarding the total amount of fees to be charged and the timing of settlement.

Id.

[136] *See* Awrey & van Zwieten, *supra* note 27, at 784 (explaining that regulators typically have focused on regulating banks when attempting to regulate payments systems in general). Broadly construed, prudential rules manage the risks that financial institutions typically encounter with the goal of ensuring that such institutions fulfill their commitments to other financial institutions. They tend to focus on "capital adequacy, solvency, and liquidity" with less attention paid to operational risks. Iman Anabtawi & Steven L. Schwarcz, *Regulating* Ex Post*: How Law Can Address the Inevitability of Financial Failure*, 92 TEX. L. REV. 75, 87 (2013) (citing Kristin N. Johnson, *Macroprudential Regulation: A Sustainable Approach to Regulating Financial Markets*, 2013 U. ILL. L. REV. 881, 884).

tory apparatus does not ignore operational risks. The regulatory agencies supervising banks expect those banks to have "internal controls and information systems appropriate to the size of the institution and to the nature, scope, and risk of its activities and that provide for, among other requirements, effective risk assessment and adequate procedures to safeguard and manage assets."[137] Regulatory agencies also expect banks to implement business continuity plans and cybersecurity risk management strategies and, starting in 2022, regulations will require banks to take into account past operational risk losses in calculating their regulatory capital requirements.[138] There also are other regulatory measures targeted specifically at operational risks that might arise from the retail payments activities of banks, which will be explored in detail in this Part. All of these measures, however, are best thought of as "micro-operational regulation," because they focus only on improving operational risk management at individual banks, without thinking about potential systemic interactions of such risks.[139] Complexity theory suggests that focusing only on the reliability of individual components will make the system more fragile.[140] This Part instead assesses existing payments regulation in terms of its ability to promote the varieties of robustness that are more likely to insulate the retail payments ecosystem from cascade failures. It concludes that there is a need for a "macro-operational" approach that promotes the modularity, scalability, and evolvability of the retail payments ecosystem as a whole.

A. The Principles for Financial Market Infrastructures

The Federal Reserve recently issued a Policy on Payment System Risk, which informs banks and bank holding companies supervised by the Federal Reserve of how they are expected to manage the risks associated with their payments processing activities.[141] A significant and prescriptive portion of this policy statement is concerned with the terms on which the Federal Reserve

---

[137] Enhanced Cyber Risk Management Standards, 81 Fed. Reg. 74,315, 74,317 (proposed Oct. 26, 2016).

[138] BANK FOR INT'L SETTLEMENTS, OPERATIONAL RISK STANDARDISED APPROACH—EXECUTIVE SUMMARY 1, 2, https://www.bis.org/fsi/fsisummaries/oprisk_sa.pdf [https://perma.cc/B82B-7HL4]. Starting in 2022, new regulations will require banks to take into account past operational risk losses in calculating their regulatory and capital requirements. *Id.*

[139] Concerns even have been raised about the neglect of systemic interactions of operational risks *within* individual financial institutions. Joshua Rosenberg, Exec. Vice President & Chief Risk Officer, Fed. Rsrv. Bank of N.Y., Thrive in Any Environment: Strengthening Resilience Through Risk Management (Nov. 6, 2019), https://www.newyorkfed.org/newsevents/speeches/2019/ros191106 [https://perma.cc/Q3L3-WEL9].

[140] Ruhl, *supra* note 10, at 562 (citing Alderson & Doyle, *supra* note 10, at 839).

[141] FEDERAL RESERVE POLICY, *supra* note 3, at 3.

will provide intraday credit to smooth payments processing.[142] This portion of the policy is focused on the credit risks inherent in the bank-based payments system, and seeks to address these concerns by preventing the transmission of shocks through interbank credit exposures.[143] The Federal Reserve's policy also considers operational risk, however, which it defines as "the risk that deficiencies in information systems or internal processes, human errors, management failures, or disruptions from external events will result in the reduction, deterioration, or breakdown of services provided."[144] Although the policy does not engage with the possibility of operational failures cascading through the retail payments ecosystem, it does recognize that an operational risk at one payments provider may be transmitted through the *credit channels* to other payments providers.[145] This is reason enough for the Federal Reserve to address operational risks in its policy, which it does by reference to the Principles for Financial Market Infrastructures (PFMI) disseminated by the Committee on Payment Settlement Systems and the Technical Committee of the International Organization of Securities Commissions.[146]

PFMI 17 provides that any provider of financial markets infrastructure:

> should identify the plausible sources of operational risk, both internal and external, and mitigate their impact through the use of appropriate systems, policies, procedures, and controls. Systems should be designed to ensure a high degree of security and operational reliability and should have adequate, scalable capacity. Business continuity management should aim for timely recovery of operations and fulfillment of the FMI's obligations, including in the event of a wide-scale or major disruption.[147]

Principle 17 is complemented by Principles 2 and 3, which require internal governance and risk-management structures to be implemented to facilitate the identification and reduction of operational risk.[148] Furthermore, Principle 20

---

[142] *Id.* at 15–31.

[143] *Id.*

[144] *Id.* at 5.

[145] *See id.* (explaining that one financial institution's issues "could create credit or liquidity problems for participants and their customers, the system operator, other financial institutions, and the financial markets").

[146] *Id.* at 7–8.

[147] *Id.* at 35.

[148] *See id.* at 33 (explaining that Principle 2 requires institutions to develop effective governance standards as a means to "support the stability of the broader financial system," and that Principle 3 requires "a sound risk-management framework for comprehensively managing legal, credit, liquidity, operational, and other risks").

provides that "[a]n FMI that establishes a link with one or more FMIs should identify, monitor, and manage link-related risks."[149]

With the exception of Principle 20, these principles should be viewed as promoting the reliability of individual components of the retail payments ecosystem, because they focus on steps taken by each payments provider *on its own* to protect itself by minimizing its risks. Principle 20 requires some consideration of spillover effects to other institutions, but is far from comprehensive. Although Principle 20 recognizes the possibility of links between institutions that could transmit shocks from operational risks, it focuses on links that have been formally and consciously established (for example, through contract), while neglecting the possibility of unanticipated additional linkages that could arise in a time of stress.[150] There is insufficient focus within the PFMIs (and thus the Federal Reserve's Policy on Payment System Risk) on the resilience of the retail payments ecosystem as a whole, in terms of its scalability, modularity, and evolvability.

Separate and apart from the PFMIs, the Federal Reserve Policy does include a general direction to payments providers to be mindful of systemic-level risks and externalities.[151] It is questionable, however, whether individual payments providers have the incentives, or the capacity—in terms of both access to system-wide information and the ability to compel coordinated action—to address systemic operational risks on their own.[152] Even banks with the best intentions face challenges in trying to coordinate to address systemic risks—although the Payments Risk Committee does provide one forum for such cooperation.

---

[149] *Id.* at 35.

[150] *See id.* (requiring that linked FMIs should be aware of and address "link-related risks").

[151] *Id.* at 11, 13.

[152] Allen, *supra* note 31, at 1103. For example, a wide-reaching survey of banking executives and other personnel involved with cybersecurity found that banks have limited motivation to coordinate to reduce the operational risks associated with cyber attacks. SAS SEC. INTEL. SOLS., CYBERRISK IN BANKING: A REVIEW OF THE KEY INDUSTRY THREATS AND RESPONSES AHEAD 2, 3 (2013), https://www.kroll.com/-/media/kroll/pdfs/publications/cyber-risk-in-banking.ashx [https://perma.cc/4ZT7-DEX3]. There are a few reasons for this lack of motivation:

> Because many banks are typically only financially liable when their own systems are compromised, there is little incentive for them to cooperate with other stakeholders when it comes to cybersecurity. Although there are exceptions, many financial institutions operate in silos—or only work with each other through industry associations—while expecting others, primarily governments, to deal more effectively with deterring cybercriminals.

Id. at 3.

B. Payments Risk Committee

The Payments Risk Committee is a private entity sponsored by the Federal Reserve Bank of New York (New York Fed) that has "worked to identify, analyze and address risks in payments, clearing and settlement of financial transactions since its founding in 1993."[153] The New York Fed appreciates that the Committee could "be subject to antitrust scrutiny because [it] may bring together competitors to discuss economic, financial, and market conditions," and thus requires the participant banks to abide by established antitrust guidelines that note that information sharing and coordinated action amongst Committee members may be problematic in some circumstances.[154] The New York Fed's Antitrust Guidelines do allow for the promulgation of jointly developed best practices, however, and the Committee has devised Best Practices for Payments, Clearing, and Settlement Activity that are intended to guide banks' payments activities.[155]

As with the Federal Reserve Policy discussed in the previous Section, there is a significant focus within the Committee's Best Practices on mitigating the credit risks associated with delayed settlement of payments, but they also deal with operational risk and business continuity planning.[156] For example, banks are encouraged to "[c]onduct frequent testing to help ensure the capacity, durability and redundancy of payment infrastructure in times of stress."[157] They also are encouraged to "[c]ommunicate with customers, external [payments, clearing, and settlement] system providers, and other stakeholders as applicable should they experience an outage to avoid further delays in payment execution."[158] Relevantly, banks are advised to:

> Fully document and test business continuity/resiliency plans as part of operational risk management. These plans should include scenarios that examine a significant interruption in access to the [large

---

[153] PAYMENTS RISK COMM., FED. RSRV. BANK OF N.Y., CHARTER 1 (last revised Nov. 2018), https://www.newyorkfed.org/medialibrary/microsites/prc/files/PRC-Charter-November-2018.pdf [https://perma.cc/RH9D-8WZK].

[154] FED. RSRV. BANK OF N.Y., ANTITRUST GUIDELINES FOR MEMBERS OF THE FEDERAL RESERVE BANK OF NEW YORK'S ADVISORY AND SPONSORED GROUPS 1 (2018), https://www.newyorkfed.org/medialibrary/media/aboutthefed/Antitrust_Guidelines.pdf [https://perma.cc/NFL2-S7T8] (discussing why groups and committees under the purview of the Federal Reserve Bank of New York are regulated by antitrust laws).

[155] *See generally* PAYMENTS RISK COMM., FED. RSRV. BANK OF N.Y., BEST PRACTICES FOR PAYMENTS, CLEARING, AND SETTLEMENT ACTIVITIES (2019), https://www.newyorkfed.org/medialibrary/microsites/prc/files/Best_Practices_for_Payments_Clearing_and_Settlement_Activities.pdf [https://perma.cc/XEA3-8KTV] (discussing best practices for financial institutions).

[156] *Id.* at 10, 11.

[157] *Id.* at 6.

[158] *Id.*

> value payment systems], as well as an alternative process to continue to execute time critical payments. The plan should be tested regularly to ensure effectiveness and to minimize impact from a range of disruptive events, including minor system outages, facility disruptions such as power outage, or a catastrophic scenario.[159]

As with the Federal Reserve's policy, the focus here is on the resilience of the individual providers within the retail payments ecosystem, with insufficient attention paid to possible systemic interactions. For example, a bank might adopt a business continuity plan that routes payments traffic to other providers in an emergency, without consideration of whether those other providers will be able to tolerate the overload without suffering some kind of operational breakdown themselves.[160] In October 2012, the Committee did stage a simulated exercise involving multiple banks that was intended as a training exercise on how to respond to a hypothetical data corruption affecting multiple banks, but that simulation was the exception rather than the rule.[161] In reporting on the exercise, the Committee noted that firms typically "conduct[ed] their own business continuity and resilience exercises."[162]

C. Financial Market Utility Regulation

At present, the primary way of regulating *systemic* operational risk in the retail payments system is through Title VIII of the Dodd-Frank Act, which authorizes the Financial Stability Oversight Council (FSOC) to "designate those financial market utilities or payment, clearing, or settlement activities that the Council determines are, or are likely to become, systemically important" for enhanced regulation by the Federal Reserve.[163] The only domestic retail payments utility or activity that has been designated to date is CHIPS.[164] Title VIII contemplates that much of the regulation of designated utilities and activities will take the form of capital and margin requirements—again, reflecting an

---

[159] *Id.* at 8–9.

[160] *See supra* notes 104–105 and accompanying text. For an analogous discussion of the stresses of high load that typically bring about blackouts, see Dobson et al., *supra* note 58, at 026103-6.

[161] *See* PAYMENTS RISK COMM., FED. RSRV. BANK OF N.Y., BUSINESS CONTINUITY PLANNING: LESSONS FROM A COMMUNICATIONS EXERCISE 1 (2013), https://www.newyorkfed.org/medialibrary/microsites/prc/files/report130709.pdf [https://perma.cc/8DP3-YBH4] (discussing the exercise and its results).

[162] *Id.*

[163] Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) § 804, 12 U.S.C. § 5463.

[164] *See Designated Financial Market Utilities*, FED. RSRV. (Jan. 29, 2015), https://www.federalreserve.gov/paymentsystems/designated_fmu_about.htm [https://perma.cc/RX8G-3KEP] (defining CHIPS as a "multilateral payment system typically used for large dollar payments").

expectation that harms will be transmitted through credit channels.[165] It also, however, gives the Federal Reserve broad leeway to consider other issues, including "the ability to complete timely clearing and settlement of financial transactions" to "support the stability of the broader financial system."[166]

To implement Title VIII, the Federal Reserve has adopted Regulation HH.[167] In doing so, it has drawn heavily on the PFMIs, so it is not surprising that Regulation HH focuses heavily on credit risk, and leaves much of the management of operational risk to the financial market utility itself.[168] Nonetheless, Regulation HH contains important directions to Financial Market Utilities (FMUs) to focus on scalability and evolvability in establishing their operational risk management policies and procedures.[169] It also sets out parameters for business continuity planning in the event of an operational failure, establishing the goal of same-day resumption of settlement services even in a worst-case scenario.[170] Section 234.4(b) of Regulation HH also expressly authorizes emergency changes to be made to a FMU's rules, procedures, and operations if its ability to provide services in a safe and sound manner is compromised.[171] Viewed through the complexity science framework, this provision allows for feedback protocols to be implemented, quickly altering the operation of the system to increase robustness in response to identified problems.

In summary, most of the existing regulation of the bank-based retail payments ecosystem attempts to limit the impact of operational risks on individual banks, but neglects the possibility of *systemic* operational risks. Regulation HH is incomplete, but as a mechanism for promoting the robustness of a complex payments processing ecosystem, it does have some helpful features. Changes are afoot in the retail payments industry, though, and to the extent that new entrants are neither banks nor covered by Regulation HH, any existing efficacy of the current regulatory system will be undermined. It is possible that these

---

[165] *See* MARC LABONTE, CONG. RSCH. SERV., R41529, SUPERVISION OF U.S. PAYMENT, CLEARING, AND SETTLEMENT SYSTEMS: DESIGNATION OF FINANCIAL MARKET UTILITIES (FMUS) 20 (2012), https://fas.org/sgp/crs/misc/R41529.pdf [https://perma.cc/45DE-C5EP] (discussing the relevant capital and margin requirements).

[166] Dodd-Frank Act § 805.

[167] 12 C.F.R. § 234.1 (2020).

[168] *See supra* notes 141–152 and accompanying text.

[169] 12 C.F.R. § 234.3(a)(17). Regulation HH requires a "designated financial market utility" to enact "a robust operational risk-management framework" that, relevantly, "[h]as systems that have adequate, scalable capacity to handle increasing stress volumes and achieve the designated financial market utility's service-level objectives" and "[h]as comprehensive physical, information, and cyber security policies, procedures, and controls that address potential and evolving vulnerabilities and threats." *Id.*

[170] *Id.* § 234.3(a)(17)(vi)–(vii).

[171] *See id.* § 234.3(b) (noting that "[t]he Board, by order, may apply heightened risk-management standards to a particular designated financial market utility" if it thinks it is necessary to address risks).

new entrants could promote the robustness of the retail payments ecosystem in other ways, including by abandoning complex legacy systems and by providing alternative payments processing services that increase redundancy in the ecosystem. If these new entrants lack the capacity to scale up and evolve, however, then they may increase the complexity of the retail payments system in a way that makes normal accidents more likely. The next Part, therefore, evaluates selected payments developments from a complexity perspective. Because the credit risks posed by these new entrants have yet to be theorized fully, and because credit and operational risks can intertwine in a crisis, the next Part also considers the risks that these new entrants may pose from a credit perspective.

III. Recent Retail Payments Innovations

Existing financial regulation seeks to ensure the stability of the retail payments ecosystem by applying prudential rules to the banks that currently provide the bulk of the retail payments processing services, and to financial market infrastructure like CHIPS. As Part I of this Article has explored, these regulatory approaches were developed in light of historical understandings of how financial crises evolve, and as a result, their focus on operational risk is insufficient. Operational risks are becoming an increasingly important issue as the technological complexity of new payments providers increases. To illustrate these evolving risks, this Part looks at the case studies of Venmo, Alipay, Bitcoin, Ripple, JPMCoin, and Facebook's Libra. This is by no means a complete list of new payments innovations, but the providers chosen here serve as a reasonably representative selection of retail payments innovations in developed economies as of the time of this writing.[172]

This Article focuses on operational failures, but operational failures of retail payments systems would most likely intertwine with, and be exacerbated by, the defaults, runs, and credit crunches that have characterized past crises.[173] For example, an operational failure could sap public confidence in the ability of payments providers to ensure the safe custody and transfer of customer funds, triggering a run on one or more payments providers. An affected payments provider then may be forced to default on customer requests to withdraw their funds or to liquidate assets, which, if the payments provider in question also provides credit, could lead that provider to stop lending. The inverse

[172] *See generally* Awrey & van Zwieten, *supra* note 48 (providing a more complete taxonomy and survey of fintech payments providers). Important innovations, such as M-Pesa, that have been implemented in countries with less-developed financial sectors are beyond the scope of this Article. *See supra* notes 95–98 and accompanying text (discussing the M-Pesa payments platform in Kenya).

[173] *See* EISENBACH ET AL., *supra* note 1, at 6–7 (explaining that operational failures can lead to runs and insolvency that can spread among financial institutions and throughout the economy as a whole).

is also possible: a payments provider experiencing a run could find that its technological infrastructure is unable to support the increased load of withdrawal requests and fail, which would only further damage confidence in that provider and reinvigorate the vicious cycle.

Although this Article has critiqued the operational risk regulation of banks as insufficient, existing *prudential* regulation does a good, if imperfect, job of addressing the runs and credit crunches that an operational failure at a bank could trigger. The same cannot be said for the newest crop of non-bank payments providers, which are often purposely structured to avoid prudential regulation. As a result, customer funds held with non-bank payments providers typically do not have the protection of deposit insurance, nor are they exempted from bankruptcy regimes that could freeze customer assets at any moment.[174] In the absence of such protections, customers have incentives to withdraw their funds at the first sign of trouble with the payments provider—particularly because the complexity of the technology makes the risks more opaque and therefore more difficult to assess.[175] When approaching these new types of payment services, policymakers therefore should be concerned about operational risks acting as a trigger for runs, as well as the systemic interactions of operational risks. This Part considers both operational and credit risks for these new technologies.

A. Venmo

Venmo is a peer-to-peer payments provider that describes itself as a way to "[s]end and receive money with Venmo friends."[176] In addition, Venmo serves as something of a social media platform, permitting "users to attach subject lines, emojis and comments to a transaction, which then populate a single feed."[177] In 2018, Venmo facilitated sixty-two billion dollars worth of payments, which users can make with money held in a Venmo account or a linked bank account.[178] Users who receive funds through Venmo can quickly move those funds to a linked bank account, but it is also possible for a user to

---

[174] Awrey & van Zwieten, *supra* note 48, at 11–12.

[175] *See* Richard B. Berner et al., *Stress Testing Networks: The Case of Central Counterparties* 1 (Nat'l Bureau of Econ. Rsch., Working Paper No. 25686, 2019), https://www.nber.org/system/files/working_papers/w25686/w25686.pdf [https://perma.cc/RU8T-V4GB]. For a discussion of complexity, opacity, and runs, see Glasserman & Young, *supra* note 57, at 783.

[176] VENMO, https://venmo.com [https://perma.cc/5MT2-QUHW].

[177] Sara Salinas, *A Mobile Payments App from US Banks Is Less Than a Year Old, but Rivals Venmo's Volume*, CNBC (Feb. 23, 2018), https://www.cnbc.com/2018/02/23/mobile-payments-zelle-has-rival--paypals-volume-in-under-a-year.html [https://perma.cc/YX3V-2J2B].

[178] Lila MacLellan, *Venmo Is Finally Venmo-ing Big Revenue to Its Less Cool Parent*, QUARTZ (Jan. 31, 2019), https://qz.com/1539489/paypal-earnings-venmo-is-sending-big-revenue-to-its-parent-company/ [https://perma.cc/AMS6-TYH3].

maintain a balance in a Venmo account.[179] Because it is not a bank, however, Venmo is not authorized to take deposits.[180] It therefore uses carefully structured and well-disclosed relationships with regulated banks to avoid regulators construing balances carried in Venmo accounts as unauthorized deposits.[181] Instead, users have only an unsecured claim against Venmo until the funds are transferred to a linked bank or credit card account.[182] Although not a bank, Venmo does qualify as a "money transmitter," and is therefore covered by the Bank Secrecy Act and subject to various registration, reporting, and record-keeping requirements designed to address money laundering.[183] Furthermore, Venmo is subject to state money transmitter laws, and has money transmitter licenses in all forty-eight states that require them.[184]

Using the traditional prudential lens to assess new technological payments providers like Venmo, Awrey and Van Zwieten have raised concerns about their financial stability implications.[185] Venmo customers assume that funds held in a Venmo account will always be immediately available for transactions, but customers may be surprised to learn that Venmo may have deployed the funds for other purposes or the funds may be commingled with

---

[179] *Send & Receive*, VENMO, https://venmo.com/about/product/ [https://perma.cc/2TQ2-PZ4U].

[180] *See* Ricks, *supra* note 16, at 769 (noting that banks' "legal monopoly" comes not from lending but from providing users with deposit accounts).

[181] *See* John L. Douglas, *New Wine into Old Bottles: Fintech Meets the Bank Regulatory World*, 20 N.C. BANKING INST. 17, 25–26 (2016) (discussing how companies might avoid banking regulations through "properly structur[ing], document[ing] and disclos[ing] [their] relationships").

[182] Ricks, *supra* note 16, at 834; *User Agreement*, VENMO, https://venmo.com/legal/us-user-agreement/ [https://perma.cc/L8MC-UHC5].

[183] *See* 31 C.F.R. § 1010.100(ff)(5)(i)(A) (2019) (defining a money transmitter as one who "provides money transmission services"); *id.* § 1022.210 (delineating the requirements imposed on money transmitters). Venmo has come under scrutiny in the past for the inadequacy of its anti-money laundering compliance program. Jameson McRae, *Venmo Is Under Scrutiny of the FTC After Investigation of Their AML Program*, LINKEDIN (Apr. 29, 2016), https://www.linkedin.com/pulse/venmo-under-scrutiny-ftc-after-investigation-aml-program-mcrae [https://perma.cc/T984-BWCN]. In contrast, ApplePay was able to structure its business model to avoid falling within the definition of "money transmitter" or "money services business," and thus is not required to comply with anti-money laundering regulation. Samuel Rubenfeld, *Apple Pay Faces Lighter Compliance Than Paypal, Google*, WALL ST. J. (Oct. 20, 2014), https://www.wsj.com/articles/BL-252B-5374 [https://perma.cc/KF5W-4R79].

[184] *See Licenses*, VENMO, https://venmo.com/legal/us-licenses/ [https://perma.cc/8D3Q-JX6E] (providing a list of all the states in which PayPal, Inc., Venmo's owner, is licensed as a money transmitter). "[W]hile requirements vary from state to state, [these licenses] typically include some form of minimum net worth, maintenance of a bond, annual audits, examinations by regulators, recordkeeping, AML programs, and a list of permissible investments for funds received and held." Douglas, *supra* note 181, at 43–44 (citing JAMES SIVON ET AL., UNDERSTANDING FINTECH AND BANKING LAW: A PRACTICAL GUIDE 88 (2014)).

[185] *See generally* Awrey & van Zwieten, *supra* note 27 (discussing the emergence of a "shadow payment system," the risks of failing to regulate this system in the same way as traditional banks, and strategies regulators might take to address these risks).

Venmo's other assets in a bankruptcy situation.[186] Venmo would be unable to take advantage of measures like deposit insurance and special resolution regimes that disincentivize runs by assuring *bank* customers that their funds will continue to be available at all times.[187] As a result, fear about the unavailability of their funds may cause Venmo customers to withdraw their funds rapidly in the future—a dynamic very similar to a run.[188]

The concerns raised by Awrey and Van Zwieten are valid. We also should consider payments providers like Venmo from a complexity science perspective, however. In that light, prudential regulation designed to allay the concerns that Awrey and Van Zwieten have raised would increase the reliability of Venmo (and similarly structured payments providers) as individual components of the retail payments ecosystem. But, as discussed in Part I.B, steps taken to make individual components of the payments system more reliable are, in isolation, insufficient to make the system as a whole more robust. Attention also must be paid to the impact of Venmo on the modularity, scalability, and evolvability of the retail payments ecosystem.

With or without prudential regulation, there are reasons to be concerned that the rise of new payments providers like Venmo will make the payments system as a whole more fragile.[189] Venmo is essentially an intermediary that facilitates the transfer of funds from one regulated bank account to another—albeit in a fun and efficient way.[190] Although Venmo has sped up and simplified the consumer experience in terms of effecting payments, it has in fact complicated the legal path of funds from user to user by adding extra intermediaries to the chain of institutions involved in processing the payment.[191] Venmo, and other digital payment services like it, have therefore been de-

---

[186] *See id.* at 805–06 ("[A]s the shadow payment system continues to grow and evolve, the pressure to generate profits may drive institutions to bundle payment functions with more conventional forms of financial intermediation . . . .").

[187] *See id.* at 806 (pointing out that the regulation of traditional banks is designed to protect payments system during times of financial stress, but that these same regulations do not apply to nonbank payments providers).

[188] *See id.* (hypothesizing that during times of financial stress, shadow payments system customers are likely to move their funds to traditional banks, where their funds will be protected by government-sponsored deposit insurance).

[189] Although Venmo is subject to money transmitter regulation, that regulation also fails to address the possibility of systemic operational risks. For a discussion of the content of state and federal money transmitter laws, see Awrey & van Zwieten, *supra* note 48, at 32–37.

[190] *See* Douglas, *supra* note 181, at 25–26 ("As a general proposition, unless an entity is already a chartered bank, it must place customer funds in another insured depository institution . . . on behalf of its customers.").

[191] *See* Tom C.W. Lin, *Infinite Financial Intermediation*, 50 WAKE FOREST L. REV. 643, 656, 660 (2015) (explaining how new financial technologies, although perhaps making payments easier for users, actually have added intermediaries that in fact make the process more complicated).

scribed as "new technologies running on old rails."[192] Complexity scientist Sam Arbesman has observed that one of the major causes of technological glitches is the building of a new system on the foundation of an outdated legacy system.[193] To rephrase this using the terminology from Part I.B, being tethered to outdated payments rails could limit the scalability and evolvability of new components of the payments system, necessitating complicated, and likely error-prone, fixes if Venmo wants to grow and change over time.

To some degree, modularity is improved by adding new payments providers like Venmo to the retail payments ecosystem, but if a problem occurs in the bank payments infrastructure upon which Venmo and others rely (as opposed to Venmo's proprietary system), then any improvement to the modularity of the system is illusory. All payments providers relying on that infrastructure will be incapacitated together. In such circumstances, rather than serving as an alternative module or substitute, Venmo actually makes the system more fragile by increasing the number of interconnections in the payments system, and thus the number of opportunities for something to go wrong.[194] In sum, the increased complexity that comes from adding another link to the chain of institutions involved and from building more layers of code on legacy bank payments systems, coupled with the speed at which payments are effected, should give us pause. Because of their additional complexity and speed, we should be concerned about all of the new mobile payment services providing shortcuts between outdated rails—even those, like ApplePay, that do not allow users to store positive balances of funds and therefore do not seem particularly concerning when viewed through a prudential lens.[195]

B. AliPay

AliPay is a Chinese payments provider that was established in 2004, initially to facilitate purchases on the Alibaba e-commerce platform.[196] It has since evolved into a leading payments platform that facilitates "peer-to-peer" transactions between acquaintances, as well as allowing customers to pay mer-

---

[192] MICHAEL S. BARR ET AL., FINANCIAL REGULATION: LAW AND POLICY 823 (2d ed. 2018).

[193] ARBESMAN, *supra* note 66, at 39–40.

[194] *See* Ruhl, *supra* note 10, at 417 (discussing how the more interconnected a system is, the more likely the system as a whole will fail if one node fails).

[195] Awrey and van Zwieten have suggested that mobile payments systems, such as ApplePay, are not particularly worrisome from a prudential perspective, because they are merely technology platforms and "do not perform any custodial or transactional storage function." Awrey & van Zwieten, *supra* note 27, at 800.

[196] Gwynn Guilford, *Alibaba Has a New Way of Explaining Its Controversial Alipay Spinoff*, QUARTZ (June 16, 2014), https://qz.com/221635/alibaba-has-a-new-way-of-explaining-its-controversial-alipay-spinoff/ [https://perma.cc/9K7C-PU4C].

chants directly for goods and services.[197] Payment instructions are sent by scanning a QR code—a type of barcode assigned to every user of AliPay—which sends a message to debit and credit the respective AliPay digital wallets.[198] Only one party to the transaction needs to be online and scan the QR code to consummate the transaction.[199] Like Venmo, AliPay is not operated by a bank, but money is transferred into and out of the AliPay system by linking to a bank account,[200] although users often carry a balance in their AliPay digital wallet or even invest the funds in other financial products offered by companies affiliated with AliPay.[201] Unlike Venmo, however, which ultimately uses bank payments infrastructure to process payments, AliPay operates on its own proprietary infrastructure.[202] Furthermore, AliPay has over one billion users and processes more than twenty trillion worth of payments annually, a reach far exceeding that of Venmo.[203] Indeed, AliPay and its main competitor, the popular WeChat Pay, have become so successful that the Chinese retail payments system is no longer viewed as "bank-based,"[204] which has necessitated a change in how prudential risks are managed in China.[205]

A fulsome discussion of the Chinese mobile payments system is beyond the scope of this Article, but AliPay is discussed here because its use is not limited to China. In the United States, AliPay has established relationships with high-end retailers, duty-free stores, taxi companies, and the Walgreens drug store chain, thus allowing customers to pay by scanning a QR code with their phones, just as they would in China.[206] AliPay's stated ambition is to pro-

---

[197] AARON KLEIN, BROOKINGS INST., IS CHINA'S NEW PAYMENT SYSTEM THE FUTURE? 9–10 (2019), https://www.brookings.edu/wp-content/uploads/2019/06/ES_20190620_Klein_ChinaPayments.pdf [https://perma.cc/7WGN-SMY5]; Evan Bakker, *Dominant Alipay Adds P2P Payments and Further Broadens Its Mobile Commerce Platform*, BUS. INSIDER (July 9, 2015), https://www.businessinsider.com/dominant-alipay-adds-p2p-payments-and-further-broadens-its-mobile-commerce-platform-2015-7 [https://perma.cc/VG78-P6AE].

[198] KLEIN, *supra* note 197, at 9–10.

[199] *Id.* at 7.

[200] BIS, ANNUAL ECONOMIC REPORT 58 (2019), https://www.bis.org/publ/arpdf/ar2019e.pdf [https://perma.cc/4FWT-XYDD].

[201] KLEIN, *supra* note 197, at 14.

[202] BIS, *supra* note 200, at 57–58.

[203] *See* KLEIN, *supra* note 197, at 8 (providing data about the number of Alipay's users and the amount of payments it processes).

[204] *Id.* at 5–6.

[205] BIS, *supra* note 200, at 70.

[206] Erica Pandey, *Alipay in America*, AXIOS (Feb. 15, 2019), https://www.axios.com/alibaba-alipay-america-expansion-walgreens-118df09f-55f6-425f-b3e7-d5a77ccf1a5e.html [https://perma.cc/TS8D-558F]; Jennifer Surane & Christopher Cannon, *Why China's Payment Apps Give U.S. Bankers Nightmares*, BLOOMBERG (May 23, 2018), https://www.bloomberg.com/graphics/2018-payment-systems-china-usa/ [https://perma.cc/UQ5Z-ZHPS].

vide services for Chinese nationals visiting or living in the United States,[207] which makes sense in light of the inadequacies of the current system for processing cross-border payments.[208] Many believe, however, that AliPay eventually will compete for business from U.S. residents at large.[209] U.S. merchants might be amenable to using AliPay because it dispenses with the significant processing fees currently charged to them in connection with credit card transactions.[210] Although there are other costs associated with using AliPay and there are many other reasons to be skeptical about AliPay's ability to take over significant market share in the United States and other developed economies, such an outcome is not impossible.[211] Furthermore, even if it remains a niche service, it is worth considering the impact that AliPay could have on the robustness of the retail payments ecosystem in the United States.

Given that AliPay operates on its own proprietary infrastructure, it could enhance the modularity of the retail payments ecosystem in the United States. In the event that bank-based payments infrastructure is compromised, the AliPay system could continue to work in parallel, offering a potential alternative for purchasing some goods and services. It is particularly noteworthy that payments can be consummated on AliPay as long as one party to the transaction is online, even if the other party's technology is compromised.[212] Also, because it is not weighed down by legacy systems, AliPay may be more scalable and evolvable than something like Venmo, even though Venmo and AliPay seem to provide similar services to their customers.

AliPay would only work as a true alternative, however, to the extent that users maintained a balance in their AliPay digital wallets and did not need to transfer funds into those wallets from their bank accounts. Furthermore, despite the potential contributions to the robustness of the retail payments ecosystem, it may not be good policy to rely on redundancy generated by a payments provider that is so integrally involved with a foreign government (the United States recently prevented Ant Financial, AliPay's parent company, from acquiring MoneyGram International, a U.S. money transfer company, because of potential

---

[207] *See* Surane & Cannon, *supra* note 206 (noting that Alipay says its forays into the American market are inspired by the goal of helping Chinese tourists).

[208] *See* Mills et al., *supra* note 18, at 18 (discussing the current difficulties in processing cross-border payments).

[209] *See* Surane & Cannon, *supra* note 206 (explaining that even though Alipay claims its expansion is geared towards Chinese visitors, "few in the payments industry believe it will stop there").

[210] KLEIN, *supra* note 197, at 13. The average processing fee in the United States is 2% for cards like Visa and MasterCard. *Id.*

[211] *See id.* at 22 (arguing that AliPay is unlikely to experience wide adoption in the United States).

[212] *See id.* at 6 (explaining that for AliPay to work, only one party needs to be online).

national security threats).[213] The remainder of this Part therefore considers other "alternative payments rails" that could improve the modularity of the U.S. retail payments ecosystem, and are not as closely linked to any foreign government.

C. Bitcoin & Ripple

Bitcoin was the first significant "cryptocurrency," a type of privately-issued money that relies on cryptography for the verification of transactions.[214] For the purposes of this Article's examination of the robustness of payments processing, the most important feature of Bitcoin is the distributed ledger on which transactions are recorded. A "distributed ledger" is essentially an online database that provides a permanent record of all the transactions that have ever been verified by the persons maintaining that ledger.[215] The ledger technology is "distributed" in the sense that there are multiple devices serving as "nodes" that run the software that hosts the database.[216] The devices that serve as nodes will have varying abilities, depending on the protocol that is adopted by the developers of the distributed ledger.[217] For example, some nodes may only be able to validate new transactions; others may also be authorized to alter the code of the ledger itself, or to issue new "coins" or "tokens."[218]

A payment effected using a distributed ledger is settled when it is recorded on that ledger, after the transaction has been verified by the relevant nodes.[219] In a permissionless distributed ledger, the rules embodied in its protocol confer the right to verify transactions, and to accept the updated version of the ledger, upon *all* of the nodes in the system, which decide by consensus.[220] With this sort of distributed ledger, some mechanism is needed to protect the ledger from nodes controlled by nefarious actors. For example, Bitcoin protects its permissionless ledger by requiring that a node complete a mathe-

---

[213] Greg Roumeliotis, *U.S. Blocks MoneyGram Sale to China's Ant Financial on National Security Concerns*, REUTERS (Jan. 2, 2018), https://www.reuters.com/article/us-moneygram-intl-m-a-ant-financial/u-s-blocks-moneygram-sale-to-chinas-ant-financial-on-national-security-concerns-idUSKBN1ER1R7 [https://perma.cc/24D4-R7F8].

[214] Hilary J. Allen, *$=€=Bitcoin?*, 76 MD. L. REV. 877, 885–86 (2017).

[215] *Id.* at 882; Marcel T. Rosner & Andrew Kang, Note, *Understanding and Regulating Twenty-First Century Payment Systems: The Ripple Case Study*, 114 MICH. L. REV. 649, 650 (2016); Brandon Ferrick, Note, *Modernizing the Stockholder Shield: How Blockchains and Distributed Ledgers Could Rescue the Appraisal Remedy*, 60 B.C. L. REV. 621, 623 (2019).

[216] Mills et al., *supra* note 18, at 10.

[217] A protocol is "a syntax and set of procedures that define how members of the arrangement interact." *Id.* at 13.

[218] Shaanan Cohney et al., *Coin-Operated Capitalism*, 119 COLUM. L. REV. 591, 600 (2019) (defining coins and tokens as the units issued to fund new ventures); Mills et al., *supra* note 18, at 12.

[219] Mills et al., *supra* note 18, at 31.

[220] *Id.* at 12.

matical proof of work before it participates in the consensus process.[221] If the distributed ledger relies on authorized persons rather than a cryptographic process to ensure the validity of the transactions on the ledger, however, it is referred to as a "permissioned" distributed ledger.[222] Whether permissioned or permissionless, because all transactions are recorded as transfers of ownership on a single distributed ledger, distributed ledger technology avoids the inefficiencies and errors associated with reconciling disparate bank ledgers to process payments.[223]

As I have argued previously, the efficiencies associated with the use of the distributed ledger reduce the need for credit to smooth the settlement process, and therefore, can eliminate some of the credit-related risks inherent in the payments system.[224] When a distributed ledger is used to facilitate transactions in bitcoins, however, a new type of run risk is introduced into the system. Bitcoin's viability as a means of exchange is entirely dependent on the willingness of market participants to accept it at any given moment. Because Bitcoin is not backed by a government, central bank, or commodity, confidence that it will continue to be accepted is fragile, and there could be runs on it if that confidence were to evaporate.[225] Recognizing this fragility, Ripple Labs created a distributed ledger that can be used to process transactions in sovereign currencies, in addition to its native virtual currency, XRP.[226]

Like Bitcoin, the Ripple distributed ledger relies on a decentralized, albeit permissioned, network of users to verify transactions.[227] From a complexity perspective, decentralized distributed ledgers have some features that will ren-

---

[221] Allen, *supra* note 214, at 929–30 (discussing the complicated proof-of-work mechanism that is used to validate Bitcoin transactions).

[222] Angela Walch, *The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk*, 18 N.Y.U. J. LEGIS. & PUB. POL'Y 837, 840 & n.15, 841 (2015). Many in the crypto-community argue that any currency associated with a permissioned ledger should not be called a "cryptocurrency," but such definitional intricacies are not relevant to this Article's discussion of operational risks. Aaron Hankin, *JPM Coin Is Not a Cryptocurrency, Says Crypto Advocacy Group*, MARKETWATCH (Feb. 15, 2019), https://www.marketwatch.com/story/jpm-coin-is-not-a-cryptocurrency-says-crypto-advocacy-group-2019-02-14 [https://perma.cc/QFF3-VDCZ].

[223] *See* Allen, *supra* note 214, at 909 (first citing TIM SWANSON, CONSENSUS-AS-A-SERVICE: A BRIEF REPORT ON THE EMERGENCE OF PERMISSIONED, DISTRIBUTED LEDGER SYSTEMS 1, 24, 28 (2015), http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf [https://perma.cc/FM2T-HBAW]; and then citing Walch, *supra* note 222, at 846) (noting that minors only need consider one ledger, whereas banks must combine multiple ledgers).

[224] *Id.* at 908–09; *see also* Rosner & Kang, *supra* note 215, at 674 (noting that although credit risk is significant for traditional financial institutions, it poses less of an issue for Ripple).

[225] Allen, *supra* note 214, at 881–82.

[226] Rosner & Kang, *supra* note 215, at 650, 660–61. Part of the business case for Ripple is its ability to process cross-border payments more efficiently than bank-based systems. *See id.* (noting the benefits of Ripple's cross-border payments system).

[227] *See id.* at 663 ("[V]alidating nodes must update Ripple's ledger and vote to approve a transaction . . . .").

der the payments system more fragile, and others that will enhance its robustness. Unlike payments made using Venmo, payments processed using distributed ledger technologies are not burdened by legacy system foundations or links to the traditional payments processing infrastructure. Instead, they can be considered to be their own payment rails—independent modules that could generate redundancy and robustness of the payments ecosystem.[228] Furthermore, the decentralized nature of these payments rails means that if one participating node were to fail, the payments system could continue to function. In this way, these distributed ledger networks have significant redundancy built into their core technologies and create redundancy at the systemic level by providing alternative payments processing.[229] These technologies also were developed in an era of cyber attacks, and therefore were designed from the outset to be robust to them.[230]

These are real contributions to the robustness of the payments system, but their benefits may dissipate over time. Work is being undertaken to make different distributed ledgers "interoperable."[231] APIs and other programs could tether the different ledgers so that they are more likely to fail together.[232] Additionally, there is the potential for quality control issues to arise, particularly if the APIs are user-created.[233] There also are other features of these distributed ledger technologies that are likely to introduce new fragilities into that system. The software protocols underpinning the distributed ledgers themselves are complex, error-prone systems.[234] Remedial steps continually are being taken to improve the quality of these protocols, but in doing so, the complexity of the

---

[228] *See id.* at 651 (discussing how Ripple might function as a piece of the payments system, "provid[ing] the rail on which payments move" (citing Telephone Interview with Ryan Zagone, Dir. of Regul. Rels., Ripple Labs, Inc. (Apr. 20, 2015))).

[229] *See* Karen Gifford & Jessie Cheng, *Implementation of Real-Time Settlement for Banks Using Decentralised Ledger Technology: Policy and Legal Implications*, *in* 20 FINANCIAL STABILITY IN THE DIGITAL ERA, FIN. STABILITY REV. 143, 149 (2016) (noting that thousands of redundancies have been built into decentralized distributed ledger systems, which decreases risk to the system as a whole); Mills et al., *supra* note 18, at 11 (discussing how distributed ledger technology "enables a single party to maintain its database records across multiple nodes, for purposes including increased operational resiliency").

[230] Walch, *supra* note 222, at 860–61. These technologies may not be quite as impervious to cyber attacks as they claim to be, however. *See id.* (describing how Bitcoin could be attacked by an entity controlling a majority of Bitcoin's mining capabilities).

[231] Brian Patrick Eha, *Inside Ripple's Plan to Make Money Move as Fast as Information*, AM. BANKER (June 14, 2017), https://www.americanbanker.com/news/inside-ripples-plan-to-make-money-move-as-fast-as-information [https://perma.cc/WB73-R3UQ].

[232] *See supra* notes 110–111 and accompanying text (discussing APIs).

[233] *See* Mills et al., *supra* note 18, at 14 (explaining that APIs can "provide user-friendly interfaces that make using the technology easier for a broader set of potential users").

[234] *See* Walch, *supra* note 222, at 855–56 (noting that Bitcoin's software and other central features pose certain risks including inherent problems, such as persistent software errors, that might make it unreliable "as financial market infrastructure").

protocols is increased, rendering them more fragile to unanticipated events.[235] In addition, software protocols that are decentralized and open source, such as those used for Bitcoin and Ripple Labs,[236] require consensus from a broad group to implement changes that may be needed to fix problems or cope with greater volumes of payments, which may limit their scalability and evolvability.[237]

It is challenging to coordinate changes to any software when there is no one "in charge" of it.[238] Even when there is agreement amongst the code developers, the lack of centralized control can result in coordination problems, and the situation becomes significantly more challenging if the developers disagree on proposed changes. Ultimately, changes cannot take effect unless they are adopted by the majority of the users in the network, which means that necessary fixes will not be adopted if the majority does not approve.[239] One way of addressing this gridlock is to create a "hard fork," a situation where the distributed ledger splits in two with each branch using a different software protocol from that time on[240] (one journalist described the concept of a hard fork using the analogy of "a new version of Microsoft Word, which generates documents that can no longer be opened via the older versions").[241] In August 2017, for example, a hard fork was used to resolve the "civil war" over the size of the blocks of data in the Bitcoin distributed ledger (changes to the block size would allow for quicker processing of Bitcoin transactions).[242] Successive hard forks that split the distributed ledger into increasingly smaller subsets, however, are not a sustainable solution to the problems of scalability and evolvability.

---

[235] *See id.* at 858–59 (discussing the lists that Bitcoin developers create to catalogue bugs and the steps they take to address those bugs).

[236] *See* Rosner & Kang, *supra* note 215, at 651 (explaining that Ripple is open source); Walch, *supra* note 222, at 841 (noting that Bitcoin is a "decentralized, open-source software"). "Open-source software is software that makes its 'source code' (i.e., its human language instruction manual) freely available to the world. Software that is open-source is made available to users through a license agreement that gives the user permission to alter the source code." Walch, *supra* note 222, at 875 (footnote omitted).

[237] *See* Mills et al., *supra* note 18, at 14 (noting that, depending on the form of consensus protocol adopted, it "can have consequences for the scalability and performance" of the system).

[238] Rosner & Kang, *supra* note 215, at 668; Walch, *supra* note 222, at 869–70.

[239] Rosner & Kang, *supra* note 215, at 664; *see* Walch, *supra* note 222, at 867 (explaining that any changes to the Bitcoin ledger protocol can be implemented only by majority agreement).

[240] 26 C.F.R. § 1.61-1 (2020); Rev. Rul. 2019-24, 2019-44 I.R.B. 1004.

[241] Zheping Huang, *Bitcoin Cash "Hard Fork": Everything You Need to Know About the Latest Cryptocurrency Civil War*, S. CHINA MORNING POST (Nov. 15, 2018), https://www.scmp.com/tech/blockchain/article/2173389/bitcoin-cash-hard-fork-everything-you-need-know-about-latest [https://perma.cc/6T6D-FZND].

[242] *Id.*

After all, payments systems benefit from network effects—the more users they have, the more useful they become.[243]

These limitations on scalability and evolvability are likely to be less constraining for permissioned blockchains, as the same central authority that grants permission to nodes to approve transactions can pressure those nodes to adopt changes to the underlying software.[244] For example, although there still may be some coordination problems for the Ripple protocol, many of the users who have been granted permission to use it are financial institutions who could be directed to act in a particular way by a financial regulator or self-regulatory organization.[245] Ripple's integration with regulated banks creates other problems, however. Fragilities at individual financial institutions could come to impact the Ripple blockchain. In other words, it would undermine the modularity of the retail payments ecosystem, if banks and Ripple are all likely to fail together.

D. JPMCoin

Whereas bitcoins and Ripple's XRP are purely digital assets, some of the newer virtual currencies have been designed to derive their value from tangible, real world assets in an attempt to moderate their volatility. Virtual currencies backed by some form of collateral typically are referred to as "stablecoins."[246] JPMCoin, however, goes further than stablecoins by converting directly into U.S. dollars held by JPMorgan Chase Bank, N.A., at a 1:1 ratio.[247] Launched in February 2019, JPMCoin is a prototype virtual currency that the bank is now testing with its institutional clients.[248] JPMCoin can be distinguished from Bitcoin and Ripple because it is redeemable for U.S. currency at a pegged rate.[249] It also can be distinguished because it will run on its own proprietary centralized permissioned ledger, meaning that JPMorgan, rather than members of the public, will hold the power to approve transactions and

---

[243] For a discussion of hard forks and network effects, see Rosner & Kang, *supra* note 215, at 679.

[244] *See* Walch, *supra* note 222, at 867 (noting that in contrast to the disagreements caused by Bitcoin's decentralized structure, in the case of "permissioned blockchains," all who use the network can be forced to adopt any changes).

[245] Rosner & Kang, *supra* note 215, at 670–71.

[246] For discussion on stablecoins, see Marco Dell'Erba, *Stablecoins in Crypoteconomics: From Initial Coin Offerings to Central Bank Digital Currencies*, 22 N.Y.U. J. LEGIS. & PUB. POL'Y 1 (2019).

[247] *J.P. Morgan Creates Digital Coin for Payments*, J.P. MORGAN (Feb. 14, 2019), https://www.jpmorgan.com/global/news/digital-coin-payments [https://perma.cc/L52T-B9S7].

[248] *Id.*

[249] *See id.* (explaining that JPMCoin is different from cryptocurrencies such as Bitcoin and Ether because JPMCoin is "1:1 redeemable in fiat currency held by J.P. Morgan (e.g., US$)").

make changes to the software operating the ledger.[250] In short, JPMCoin has dispensed with proof of work and other design features that make cryptocurrencies so complex, and pared down the distributed ledger into a pure payments processing technology.

For those in the crypto community who are ideologically committed to payments without centralized control, the development of JPMCoin is deeply unsatisfying.[251] As one journalist observed, "[I]t lacks the fundamental qualities that have made cryptocurrencies so radical: the freedom from middlemen and from regulatory oversight."[252] JPMCoin has some clear advantages over Bitcoin and Ripple, however. By dispensing with the cryptographic elements of transaction verification, using JPMCoin to effect payments will be much more efficient than using Bitcoin.[253] Furthermore, JPMCoin is issued by JPMorgan Chase Bank, N.A., a highly regulated bank that is subject to significant levels of prudential regulation, which will contribute to its reliability. More important than efficiency and reliability from a complexity science perspective, though, is the fact that JPMCoin will operate on a centralized, permissioned blockchain.[254] This means that it will be easy to implement changes to the distributed ledger's code as it needs to adapt—thus improving the scalability and evolvability of this payments processing method. From a credit perspective, JPMCoin also seems reasonably insulated from runs: it is issued by a bank that has access to the Federal Reserve as a lender of last resort and deposit insurance from the FDIC, and it is backed by JPMorgan Chase's "$2.6 trillion balance sheet."[255]

Although JPMCoin initially might seem like a beneficial development from a stability perspective, it is questionable whether it will actually increase redundancy within the retail payments ecosystem. Payments services gain utility from network effects, meaning that they become more valuable when they allow for payments to a larger group of recipients. At present, you need to be a JPM customer to send or receive JPMCoin, so it does not serve as a good

---

[250] *See* Hankin, *supra* note 222 (noting that "JPM coin is anything but permissionless" because it is based on a blockchain operated by JPMorgan).

[251] *See id.* (arguing that because JPMCoin is neither permissionless nor decentralized, it should not be considered a cryptocurrency).

[252] Michael J. de la Merced & Nathaniel Popper, *JPMorgan Chase Moves to Be First Big U.S. Bank with Its Own Cryptocurrency*, N.Y. TIMES (Feb. 14, 2019), https://www.nytimes.com/2019/02/14/business/dealbook/jpmorgan-cryptocurrency-bitcoin.html [https://perma.cc/P3DB-A2KS].

[253] For a discussion of the inefficiencies of Bitcoin's transaction verification process, see Allen, *supra* note 214, at 930–32.

[254] *See supra* notes 69–73 and accompanying text (discussing why scalability, modularity, and evolvability are often more important than efficiency and reliability when it comes to establishing robust systems).

[255] *See J.P. Morgan Creates Digital Coin for Payments*, *supra* note 247 (explaining that JPMCoin will be protected by JPMorgan's "$2.6 trillion balance sheet" and the various banking regulations to which JPMorgan, as a large bank, is subject).

substitute for most existing payment methods, which do not require payers and payees to be affiliated with the same financial institution.[256] Therefore, at present, JPMCoin is unlikely to make the overall retail payments ecosystem more robust. One commentator, however, has noted that JPMorgan's ledger "is designed to interact with any 'standard' blockchain," and it is possible that in the future JPMCoins could be used to transact outside of JPMorgan's proprietary distributed ledger.[257] Increased interoperability could make JPMCoin more useful as a payment method, but also could create a situation where the different ledgers are more likely to fail together. It is therefore unclear at present whether JPMCoin's net impact on the stability of our payments system is likely to be positive or negative.

If, however, JPMCoin were to achieve significant scale as a means of payment, it could compromise the Federal Reserve's ability to use monetary policy to address future financial instability—which is a key feedback mechanism used to make the financial system more robust.[258] This certainly would be a negative impact. JPMorgan has stated that it created JPMCoin solely to allow it to use distributed ledger technology to facilitate speedier payments.[259] However, "[s]keptics questioned why a blockchain ledger was necessary to move money between JPMorgan bank accounts."[260] Although it has not made any public statements to this effect, JPMorgan also may be seeking to benefit from the seigniorage it can receive for creating JPMCoins.[261] A bank like JPMorgan already can profit from seigniorage when it creates new money by extending U.S. dollar loans to others,[262] but regulations, such as reserve and capital re-

---

[256] *See* de la Merced & Popper, *supra* note 252 (pointing out that, at first, JPMCoin will be confined to JPMorgan's own payments systems).

[257] Aaron Brown, Opinion, *JPM Coin Is the Wildest Big Bank Idea in Many Years*, BLOOMBERG (Mar. 21, 2019), https://www.bloomberg.com/opinion/articles/2019-03-21/jpmorgan-proposes-a-wild-idea-for-crypto-and-banks [https://perma.cc/W2VT-YMLB].

[258] Awrey and van Zwieten have noted that "as an increasing proportion of funds become held by institutions outside the conventional banking system, this may undercut the ability of central banks to use existing monetary policy tools to manage the money supply in pursuit of price stability, financial stability, and other policy objectives." Awrey & van Zwieten, *supra* note 27, at 779.

[259] *J.P. Morgan Creates Digital Coin for Payments*, *supra* note 247 ("Exchanging value, such as money, between different parties over a blockchain requires a digital currency, so we created the JPM Coin.").

[260] de la Merced & Popper, *supra* note 252.

[261] Brown, *supra* note 257. "Seigniorage" is the profit that represents the difference between the face value of money, and the cost of producing and distributing that money.

[262] *See* Robert C. Hockett, *Rousseauvian Money* 45–46 (Cornell L. Sch., Research Paper No. 18-48, 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3278408 [https://perma.cc/YM7P-KFUX] (discussing the historical development of "seignorage" as banks' lucrative "practice of issuing more notes than they had" and the idea that "[t]he only 'natural' constraint on the bank is what loans can be made profitably").

quirements, impose limits on the ability of private banks to extend loans in U.S. dollars,[263] and thus, cap private seigniorage profit.

Furthermore, banks have no right to create U.S. dollars for their own spending—that right belongs solely to the Federal Reserve. JPMorgan could create JPMCoins for its own spending, though.[264] At least at present, JPMCoins are not subject to reserve and capital requirements, and so JPMorgan could also theoretically make unlimited loans in JPMCoins.[265] Market participants may be willing to pay more than one dollar for a JPMCoin if it is a more useful payment mechanism than a U.S. dollar.[266] As the first global bank to develop a proprietary distributed ledger, JPMorgan may be in a position to achieve this outcome by using its ledger as a bottleneck to squeeze out competitors.[267] In short, JPMCoin could become a very lucrative business line, and to the extent that significant volumes of transactions are consummated in JPMCoins, the Federal Reserve will have lost some of its control of the money supply—and with it, its ability to take emergency actions to address financial instability.[268]

E. Libra

Whereas JPMCoin is an example of an established financial institution diversifying its technological offerings, the inverse also is happening: the largest technology companies are starting to make moves into the finance space.[269] Perhaps no technological venture into finance has generated more controversy than that proposed by the Libra Association, a not-for-profit organization pioneered and currently led by Facebook.[270] In June 2019, the Libra Association

---

[263] *See* CARNELL ET AL., *supra* note 4, at 240–41 (discussing the importance of capital and reserves to understanding the banking system).

[264] Brown, *supra* note 257.

[265] *See id.* (distinguishing between spending and lending with U.S. dollars and spending and lending with JPMCoin).

[266] *See id.* (discussing the possibility that JPMorgan could sell JPMCoins for more than one dollar).

[267] *See* Allen, *supra* note 214, at 934 (noting ways in which individual financial institutions might compete for distributed ledger technology dominance).

[268] *See* Rosa Maria Lastra & Jason Grant Allen, *Virtual Currencies in the Eurosystem: Challenges Ahead*, 52 INT'L LAW. 177, 201 (2019) (discussing the impact of virtual currencies on the current financial system). "If [Venture Capital (VC)]-based payment systems were used to the exclusion of cash and book-money, VCs could take whole economies outside the conventional monetary system, which would in turn erode both commercial banks' role in the monetary system and central banks' power over the money supply and monetary policy." *Id.*

[269] BIS, *supra* note 200, at 61. Their doing so "reflects strong complementarities between financial services and their core non-financial activities, and the associated economies of scope and scale." *Id.*

[270] LIBRA ASS'N MEMBERS, AN INTRODUCTION TO LIBRA 3–4 (2019), https://libra.org/en-US/wp-content/uploads/sites/23/2019/06/LibraWhitePaper_en_US.pdf [https://perma.cc/9UHS-XXL3] [hereinafter LIBRA WHITE PAPER 2019]. Some of this skepticism derives from concerns about Facebook's

issued a white paper introducing the world to its proposal for a "a simple global currency and financial infrastructure that empowers billions of people."[271] After receiving significant pushback from national authorities, the Libra Association issued a second white paper in April 2020 that made some changes and offered some clarifications to the initial proposal. Most notably, the second white paper includes a proposal to issue Libra coins denominated in dollars, Euros, and several other sovereign currencies, in addition to the global Libra currency announced in 2019.

Both of the white papers are relatively short, but they include enough information to provide a preliminary analysis of Libra's potential impact on the retail payments ecosystem. The first white paper outlines the following three key features of Libra:

> 1. It is built on a secure, scalable, and reliable blockchain;
> 2. It is backed by a reserve of assets designed to give it intrinsic value;
> 3. It is governed by the independent Libra Association tasked with evolving the ecosystem.[272]

The proposed Libra blockchain bears many similarities to the distributed ledgers already discussed in this Part. It will be decentralized but permissioned, with each of the members of the Libra Association charged with maintaining one of the validation nodes.[273] Because it aspires to create a new payment rail that can be used to facilitate domestic and cross-border payments, this blockchain could facilitate a more modular retail payments ecosystem. By using a reserve of assets identified as "cash or cash equivalents and very short-term government securities"[274] to back each type of Libra coin, Libra is seeking to solve the volatility problems that have so far prevented cryptocurrencies like Bitcoin from becoming a real alternative to existing payments processing methods.[275]

---

handling of privacy and data in the past. One question now asked is whether Facebook created Libra to generate more data about its users and their purchasing habits, which it could then monetize. Mike Isaac & Nathaniel Popper, *Facebook Plans Global Financial System Based on Cryptocurrency*, N.Y. TIMES (June 18, 2019), https://www.nytimes.com/2019/06/18/technology/facebook-cryptocurrency-libra.html [https://perma.cc/86LS-Z89Y]. For a discussion of tech companies seeking new sources of payments data, see BIS, *supra* note 200, at 62.

[271] LIBRA WHITE PAPER 2019, *supra* note 270, at 1.

[272] *Id.* at 3 (emphasis omitted).

[273] *Id.* at 4, 8.

[274] LIBRA ASS'N MEMBERS, WHITE PAPER V2.0, at 2 (2020), https://wp.diem.com/en-US/wp-content/uploads/sites/23/2020/04/Libra_WhitePaperV2_April2020.pdf [https://perma.cc/R54T-9YAT] [hereinafter LIBRA WHITE PAPER 2020].

[275] *See* LIBRA WHITE PAPER 2019, *supra* note 270, at 3 (explaining that Libra reserves are structured so that Libra will maintain a stable value); Lastra & Allen, *supra* note 268, at 201–02, 207

From a prudential perspective, the proposal to rely on a reserve of assets to maintain a stable value for each type of coin is the most problematic feature of Libra. The first white paper states that Libra coins will have an "intrinsic" value,[276] but in reality, that value will vary depending on the composition and valuation of the reserve of assets.[277] In this sense, Libra bears similarities to money market funds. When someone invests in a money market fund, they are purchasing a share in a mutual fund that invests in short-term liquid assets that are considered to be reasonably safe.[278] The value of a share in a money market fund will fluctuate depending on the market value of the assets that the fund has invested in, but because those assets are considered to be largely risk-free, the SEC has authorized money market funds to use a specific form of accounting that allows the share to consistently be valued at one dollar, so long as the underlying asset value does not drop too far.[279] This creates the perception that a share in a money market fund has a stable value. As with money market funds, however, assurances from the Libra Association that each Libra has a stable value are likely to make the currency more susceptible to runs if something goes awry. In 2008, a money market fund with investments in Lehman Brothers was unable to maintain its one dollar per share value (in industry parlance, it "broke the buck").[280] This resulted in a widespread fear that *all* money market funds might be less stable than previously thought, and significant numbers of investors sought to redeem their shares.[281] To satisfy these redemption requests, funds sold their best and most liquid assets for cash, creating incentives for remaining investors in the funds to redeem *their* shares as quickly as possible, lest they be left with a share in a fund that already had disposed of all of its good investments.[282]

A similar run dynamic could befall Libra. The Libra white papers anticipate that a holder of a Libra coin will be able to exchange it for their preferred

(pointing out that virtual currencies, such as Bitcoin, experience high volatility and that other issues such as speed, supply, and computing power interfere with their success).

[276] LIBRA WHITE PAPER 2019, *supra* note 270, at 3.

[277] *Examining Facebook's Proposed Cryptocurrency and Its Impact on Consumers, Investors, and the American Financial System: Hearing Before the H. Comm. on Fin. Servs.*, 116th Cong. (2019) (written statement of proposed testimony by Katharina Pistor, Edwin B. Parker Professor of Comparative Law and Director, Center on Global Legal Transformation, Columbia Law School), https://www.congress.gov/116/meeting/house/109821/witnesses/HHRG-116-BA00-Wstate-PistorK-20190717-U1.pdf [https://perma.cc/9GVU-LUA3] [hereinafter *Examining Facebook's Proposed Cryptocurrency*].

[278] Hilary J. Allen, *Money Market Fund Reform Viewed Through a Systemic Risk Lens*, 11 J. BUS. & SEC. L. 87, 90 (2010) (citing Gartenberg v. Merrill Lynch Asset Mgmt., 694 F.2d 923, 925 (2d Cir. 1982)).

[279] *Id.* at 90–91.

[280] *Id.* at 94.

[281] *Id.* at 95.

[282] *Id.*

sovereign currency. Libra holders will be reliant on third-party dealers to exchange their Libra coins for sovereign currencies, except in extreme circumstances when the Libra Network (a subsidiary of the Libra Association that will manage the reserves) will facilitate "burning Libra Coins for end users and liquidating assets comprising the Reserve to make payment as appropriate."[283] In these circumstances, the Libra Network presumably would have to start exchanging or selling the most liquid assets from their reserve to meet the conversion requests.[284] Remaining holders of Libra coins who feared that the value of their coins would plummet against sovereign currencies as the reserve is depleted would be incentivized to convert their Libra into sovereign currencies as early as possible, creating a vicious cycle. This vicious cycle would likely have impacts outside of Libra itself. As Professor Katharina Pistor notes:

> All of this would matter less if Libra were just one of many other cryptocurrencies that have entered and exited, risen and fallen, over the past decade. Libra's ambition, however, is of a different kind. It wants to be a global currency and, if allowed to go forward, would be rolled out at breathtaking speed by Facebook, a company that currently has over 2.5 billion users worldwide.[285]

There would likely be significant feedback effects from a run on Libra, with assets from the reserve being dumped into the markets at an unprecedented scale. Such asset fire sales can generate significant externalities for the financial system as a whole.[286]

The money market fund panic of 2008 ultimately was staunched by guarantees from the Federal Reserve, but there would be no equivalent body to perform that function for the global Libra coins.[287] With respect to the Libra coins that are denominated in sovereign currencies, the relevant national authorities would have more scope to intervene, but bailouts for Facebook might prove politically challenging to pursue. Libra thus poses risks from a credit perspective; we also should be concerned about Libra from an operational perspective.

---

[283] LIBRA WHITE PAPER 2020, *supra* note 274, at 13.

[284] Pistor has noted that the triggers for a run on Libra could range from "a truly exogenous shock, to major operational problems, or to heightened safety concerns about assets held in the Reserve." *Examining Facebook's Proposed Cryptocurrency*, *supra* note 277, at 5. She further speculates that "the transmission mechanism would most likely be a combination of price signals in critical asset markets and social media, which would put billions of Libra holders around the globe on notice." *Id.*

[285] *Id.*

[286] Anil K. Kashyap et al., *The Macroprudential Toolkit*, 59 IMF ECON. REV. 145, 146 (2011).

[287] *See* Allen, *supra* note 278, at 96–99 (discussing the emergency programs implemented by the Federal Reserve for money market mutual funds). There is no equivalent body to the Federal Reserve where Libra is concerned, notwithstanding that the Libra Association has stated that it would "welcome the oversight and control over [Libra] . . . by a group of regulators and central banks." LIBRA WHITE PAPER 2020, *supra* note 274, at 12.

Although it is free from the baggage of legacy systems, the software establishing the Libra blockchain is intended to be open source, meaning it will itself become a legacy system that complicates the development of the products designed to be built on top of it.[288] User-designed applications also may create linkages between this blockchain and legacy payments systems, thereby undermining the modularity of the system. Libra also has the potential to undermine redundancy within the retail payments ecosystem. Given the number of Facebook users around the world, the network effects of a Facebook-run payments system would be significant, and it is plausible that Libra could outcompete other payments systems to become the dominant global infrastructure.[289]

Also troubling from an operational perspective is the lack of clarity regarding the governance of the Libra Association. As with Bitcoin and Ripple, the scalability and evolvability of Libra will depend on the ability to coordinate changes to its distributed ledger as circumstances change. The first white paper claims that the Libra blockchain will be designed to "prioritize scalability . . . and future adaptability."[290] If there are impediments to coordinating changes, however, then Libra will become more fragile, and if it becomes an important component of the retail payments ecosystem, then the whole ecosystem will become more fragile. The white paper provides little clarity on how the members of the Libra Association will interact. Professor Chris Brummer has queried:

> Are members required to act in the best interest of the currency (and by extension the currency stakeholders) or are they permitted to put their financial interest first? Are there any public policy or contractual commitments they have with respect to assisting in the maintenance of financial stability and financial integrity?[291]

---

[288] *See* LIBRA WHITE PAPER 2019, *supra* note 270, at 3, 4 (providing that the Libra software is open source).

[289] *See* BIS, *supra* note 200, at 67 ("Once a captive ecosystem is established, potential competitors have little scope to build rival platforms. Dominant platforms can consolidate their position by raising entry barriers. They can exploit their market power and network externalities to increase user switching costs or exclude potential competitors.").

[290] LIBRA WHITE PAPER 2019, *supra* note 270, at 3.

[291] *Examining Facebook's Proposed Cryptocurrency and Its Impact on Consumers, Investors, and the American Financial System: Hearing Before the H. Comm. on Fin. Servs.* 7, 116th Cong. (2018) (written statement of testimony by Chris Brummer, Agnes N. Williams Research Professor Director, Institute of International Economic Law, Georgetown University Law Center), https://financialservices.house.gov/uploadedfiles/hhrg-116-ba00-wstate-brummerc-20190717.pdf [https://perma.cc/T4JS-9DML] (emphasis omitted). Finally, Libra has ambitions to transition to a permissionless blockchain eventually, which would further complicate its scalability and evolvability as a payments provider. *See* LIBRA WHITE PAPER 2019, *supra* note 270, at 4 (discussing Libra's future as a permissionless blockchain); *supra* notes 237–244 and accompanying text (discussing the limits on scalability and evolvability in permissionless blockchains).

IV. A Macro-Operational Approach

The new payments innovations surveyed in the previous Part seem to be a mixed bag in terms of their contributions to the modularity, scalability, and evolvability of the retail payments ecosystem. As such, it is hard to predict whether the process of fintech innovation will have a net positive or net negative impact on the robustness of our retail payments ecosystem. We therefore should not expect individual firms in the private sector to be able to resolve concerns about operational risk in the retail payments ecosystem. Given the possibility that cascading operational failures could incapacitate society's ability to transact, policy-makers and regulators need to engage with evolving operational risks proactively.

The previous Part also raised the possibility of new forms of prudential risk arising from new retail payments innovations. Although these are still evolving, academics and policy-makers already are starting to consider how to address them. The Chinese central bank, for example, recently has required non-bank payments providers, like AliPay, to sequester all customer funds in a reserve account in order to promote confidence that those funds will continue to be available—and to reduce the risk of runs.[292] Other reform possibilities that have been discussed include establishing private third-party insurance of funds used in unregulated payments systems, and requiring payments providers to have a relationship with a regulated bank.[293] Although important, prudentially oriented reform efforts such as these are insufficient if the retail payments ecosystem is viewed through a complexity theory lens. At best, prudential rules can improve the resilience of the new components of the retail payments ecosystem, but they will not directly address the scalability, modularity, and evolvability dimensions of the ecosystem as a whole. At worst, such prudential reform efforts could create a false sense of security—rendering the components themselves more robust to expected problems while making the payments ecosystem as a whole more susceptible to unexpected problems that could trigger catastrophic cascade failures. Regulatory approaches targeted at the robust yet fragile dimensions of the retail payments ecosystem are a necessary complement to prudential regulatory policy.

At present, the specter of systemic operational risk is dealt with by regulating the FMUs, like CHIPS, where such risk is concentrated.[294] This Article has argued not only that this approach is presently insufficient, but also that if new technologies (particularly distributed ledger technology) succeed in taking

---

[292] BIS, *supra* note 200, at 70.

[293] Awrey & van Zwieten, *supra* note 27, at 810–13.

[294] Mills et al., *supra* note 18, at 27 (explaining that risks, including operational risks, are currently addressed by regulating financial market infrastructures).

over a significant amount of retail payments processing, then focusing solely on CHIPS will be an even more inadequate approach to addressing systemic operational risk. Just as financial regulators have moved towards a "macro-prudential" approach to managing credit-related risks in the decade since the last crisis, a new "macro-operational" perspective is needed that contemplates the possible systemic impacts of cascading operational failures.[295] To use the complexity science terminology adopted in Part I.B, macro-operational policy should seek to promote redundancy within the ecosystem, and to establish sensors and feedback mechanisms to detect and respond to macro-operational threats.[296] This Part explores possible measures of this kind, which are designed to make cascading operational failures less likely and to respond when such failures do occur.

Before doing so, however, this Part briefly discusses why ex ante regulation is necessary. Given the sometimes inevitable nature of "normal accident[s],"[297] there is a temptation to be somewhat fatalistic about their occurrence and focus primarily on ex post mechanisms to deal with such accidents once they occur.[298] Although ex post mechanisms will likely remain necessary and should be planned for in advance, past experience with financial crises suggests that such ex post responses are often insufficient to fully contain the damage unleashed by such crises.[299] Furthermore, the ex post strategies that are currently in the regulatory arsenal have been developed to respond to the credit-driven dynamics of financial crises and are therefore inadequate to respond to crises that are driven primarily by operational failures.[300] As such, both new ex ante and new ex post tools need to be developed.

Historically, one of the most effective ways of mitigating emerging financial instability has been for a central bank to act as a lender of last resort, lending freely to banks against good collateral to prevent those banks from having to sell their assets at a steep discount into a distressed market—thus preventing a temporary liquidity problem from transforming into a solvency problem.[301] A

---

[295] For discussion of this shift, see Samuel G. Hanson et al., *A Macroprudential Approach to Financial Regulation*, 25 J. ECON. PERSPS. 3, 3 (2011); Kashyap et al., *supra* note 286, at 146.

[296] *See supra* notes 50–88 and accompanying text.

[297] PERROW, *supra* note 13, at 5.

[298] *See generally* Anabtawi & Schwarcz, *supra* note 136 (advocating for such a focus on *ex post* measures).

[299] Allen, *supra* note 31, at 1103–07. This insufficiency is why I have argued elsewhere that strong *ex ante* prudential regulation should not be abandoned. *See id.* (explaining why *ex post* regulation alone is not enough).

[300] *See* EISENBACH ET AL., *supra* note 1, at 8 ("[D]ue to the unique properties of cyber events, traditional policy tools such as ex ante capital requirements or ex post liquidity provision may not be as effective.").

[301] This description of the lender of last resort function is drawn from Walter Bagehot's classic work. *See generally* WALTER BAGEHOT, LOMBARD STREET: A DESCRIPTION OF THE MONEY MAR-

lender of last resort would have a very limited role to play, however, during a cascade of operational failures through the retail payments ecosystem. At best, a lender of last resort could assist by mitigating any credit-related fallout that might arise if people lose confidence in financial institutions as a result of their inability to transact. The Federal Reserve took steps in this direction in the wake of September 11, 2001, following classic Bagehotian policy in making credit available to lubricate interbank payments following massive operational failures.[302] A lender of last resort would not be equipped to resolve any technological glitch, or to provide alternative processing infrastructure, however.

Special resolution and deposit insurance regimes for banks are also designed to maintain confidence so as to prevent the runs that could incapacitate those banks.[303] Again, these safety nets seek to address concerns about the solvency of banks and their ability to satisfy creditors, and they would not be able to stop a cascading operational failure that could spread even without a depletion of confidence in the system.[304] Instead, different kinds of regulatory strategies—again, both *ex ante* and *ex post*—are required to better insulate the retail payments system from cascading operational failures. The complexity framework provides a way of thinking about how regulation should respond to an uncertain future.

A. Sensors and Feedback

A system can be made more robust to internal and external shocks by putting in place sensors that enable the system "to evaluate itself internally, to detect changes in its environment, and to measure its interactions with other . . . systems."[305] A robust retail payments ecosystem therefore requires reporting mechanisms that facilitate the transfer of information regarding operational problems from the providers that comprise that system to a central regulator.[306] Ideally, the information would be reported in real time, and at a granular level, but real-time regulatory monitoring is highly experimental at present, with limited resources being devoted to experimentation with operational risk monitor-

KET (1873) (discussing the idea of a lender of last resort as an essential component in a financial system).

[302] Lacker, *supra* note 39, at 3.

[303] CARNELL ET AL., *supra* note 4, at 222, 401.

[304] For a discussion of purely technological cascade failures, see *supra* notes 100–105 and accompanying text. Although to be clear, depletions of confidence would most likely accompany and exacerbate any cascading operational failure. *See* EISENBACH ET AL., *supra* note 1, at 6 (noting that if one bank identifies a cyber attack, other banks will not know immediately if the attack affected them as well, which would create uncertainty and potentially panic).

[305] *See* Ruhl, *supra* note 10, at 582 (discussing the use of sensors in the American legal system, a complex system).

[306] EISENBACH ET AL., *supra* note 1, at 9.

ing.[307] It is not unrealistic to expect that such technology eventually will be developed, but unless and until that happens, information transfer will have to take the more traditional form of somewhat delayed reports from regulated entities to their regulator about operational problems that have occurred. The utility of these types of reports is also limited because financial regulators lack jurisdiction over many of the new payments providers. An extension of regulatory jurisdiction, authorizing the appropriate regulators to compel reports of operational mishaps from non-bank providers, would help address this—but such a proposal is beyond the scope of this Article.

Assuming they have the necessary jurisdiction, regulators also could devise their own sensors, designed to look for systemic interactions. For example, existing prudential regulation uses stress tests as sensors to evaluate how the largest financial institutions would fare in hypothetical scenarios of great economic stress. The regulatory capital requirements for those institutions then are adjusted in light of the results of those stress tests; this works as a feedback mechanism.[308] A macro-operational approach to payments system regulation also should incorporate stress tests; here, the stress scenario would focus less on negative macroeconomic indicators and more on hypotheticals about worst case technical failures. As I have argued previously, when it comes to assessing the new risks created by fintech technologies, the stress scenarios employed should not be "engineered towards testing for a particular outcome, but instead should be designed to find out 'what would happen if.'"[309] Our sense of the types of entities and activities that pose the greatest risks to the financial system could shift as we start testing for cascading technological failures, rather than limiting the focus of testing to the ability of institutions to comply with capital requirements under stressed economic conditions.

Netflix uses something called "chaos monkey" to shut down parts of its system randomly in order to learn more about the connections therein, as well as the ability of those connections to transmit cascade failures.[310] Although the consequences of payments failure are much greater than an unavailable movie, some variation on this theme—perhaps a simulation of shutting down parts of the system—could assist in understanding the pathways through a constantly

---

[307] *See* SIMONE DI CASTRI ET AL., FIN. STABILITY INST. (FSI), FSI INSIGHTS ON POLICY IMPLEMENTATION NO 19: THE SUPTECH GENERATIONS 10 (2019), https://www.bis.org/fsi/publ/insights19.pdf [https://perma.cc/93ML-SKEA] (providing a graphical representation of the share of suptech innovation devoted to reporting, misconduct analysis, data management, virtual assistance, market surveillance, microprudential supervision, and macroprudential supervision).

[308] For background information on prudential stress testing, see Berner et al., *supra* note 175, at 3–6. It should be acknowledged that adjustable regulatory capital requirements make the financial system as a whole more complex, and thus more fragile in some respects.

[309] Allen, *supra* note 109, at 200.

[310] ARBESMAN, *supra* note 66, at 107.

evolving ecosystem. Breakthroughs are also being made in the field of novelty detection, where artificial intelligence is being utilized to "find unexpected outcomes in a system."[311] Recently, this type of technology has been used to detect changes in retail payments flows that could serve as early warning signals of credit-related problems with payments providers.[312] Presumably, it also could be used to identify unusual payments flows that signal operational problems.

Novelty detection and other new technologies could prove very helpful as sensors for evaluating the robustness of an evolving retail payments ecosystem. Before these types of sensors can be effective, however, some kind of map of the components of the retail payments ecosystem and their relationships with one another will be required.[313] Again, fragmented jurisdiction over retail payments providers is likely to limit our understanding of the systemic dimensions of operational risks. Assuming that these jurisdictional issues can be solved sufficiently to allow regulators to test for and detect problems with systemic potential, regulators will have a range of options.

In the face of an impending cascading failure, some form of circuit breaker could be deployed to stop the problem from spreading to the rest of the system. For example, to avoid overloading other parts of the retail payments ecosystem, regulators might intervene to prevent a compromised payments provider from routing its customers' payments through other providers. Although this certainly would have significant ramifications for those dependent on the compromised provider for transaction processing, it could preserve the overall retail payments ecosystem, and thus, protect economic growth more broadly. Such decisions are not easily made, however, because of the unequal distribution of their consequences—without any due process, unelected officials will sacrifice the ability of some people to transact in order to preserve the ability of others to do so. Similar issues were raised in late 2019 when PG&E cut power to some, but not all, residents of the San Francisco Bay area to thwart the spread of local wildfires.[314] Financial regulators might therefore be loath to use a circuit breaker except in the most dire circumstances.

---

[311] *Id.* at 127.

[312] *See* Leonard Sabetti & Ronald Heijmans, *Shallow or Deep? Detecting Anomalous Flows in the Canadian Automated Clearing and Settlement System Using an Autoencoder* 2 (De Nederlandsche Bank, Working Paper No. 681, 2020), https://ssrn.com/abstract=3581595 [https://perma.cc/YP9D-YAMG] (discussing the goal of "detect[ing] anomalous payment flows . . . automatically by applying an unsupervised anomaly detection method").

[313] In their discussion of macroprudential stress testing, Berner et al. note that "[c]hallenges remain in collecting granular data . . . and in developing methodologies to reconstruct the full network from partial information." Berner et al., *supra* note 175, at 2.

[314] Annie Lowrey, *Alone in the Dark in the Bay Area*, THE ATLANTIC (Oct. 12, 2019), https://www.theatlantic.com/ideas/archive/2019/10/californias-power-outage/599935/ [https://perma.cc/TE92-Z8JN?type=image].

If a cascade failure is not imminent, a more measured response to a detected problem might be to revise operational risk management regulations. As discussed in Part II, Section 805 of Dodd-Frank authorizes the Federal Reserve to implement rules that are more comprehensive than the current Regulation HH. Specifically, Section 805 allows the Federal Reserve to prescribe standards for any payments activities that the FSOC has designated as systemically important.[315] As an example of the type of standards that might work as macro-operational regulation, complexity scientist Sam Arbesman has noted that computer programmers often pay little attention to features of programs like "how numbers get stored and rounded when performing calculations."[316] These types of errors could metastasize into significant operational risks, and regulation could provide some rigor and consistency here. Implementing new regulations will inevitably increase the complexity of the ecosystem, however.

Regulatory complexity is particularly likely to increase if distributed ledgers with dispersed governance become more prominent, as there is often no identifiable person responsible for managing the operational risk associated with those ledgers, and thus, no obvious candidate for regulation.[317] Workarounds for this type of problem, such as regulating virtual currency intermediaries in lieu of those operating the distributed ledger itself—as New York's BitLicense has done—will make the regulatory landscape even more complex.[318] Given the fragilities that result from increasing complexity, in some circumstances the correct approach might be to refrain from making new rules, and simply to study the detected glitch to learn more about how payments infrastructure operates as a system. In this way, interconnections that can produce much larger cascade failures may be better understood.[319] Arbesman has argued that when it comes to exceedingly complex systems, the best approach is to "examine the anomalies and malfunctions to gain insights, even if we don't fully understand the system as a whole."[320] The understanding gleaned from such an approach, albeit imperfect, will be key to interpreting information provided by sensors in the future and determining whether some type of circuit breaker is warranted in the event of an emergency.

---

[315] *See* Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) § 805, 12 U.S.C § 5464 (defining the goals and scope of the "[s]tandards for systemically important financial market utilities and payment, clearing, or settlement activities").

[316] ARBESMAN, *supra* note 66, at 97.

[317] Allen, *supra* note 109, at 181–82.

[318] For a discussion of regulating Bitcoin through intermediaries, see Allen, *supra* note 214, at 921–23.

[319] For an argument in favor of observing glitches purely to understand, rather than to fix problems, see ARBESMAN, *supra* note 66, at 103–05.

[320] *Id.* at 110.

Unfortunately, the natural candidate to perform these types of functions in the United States, the Office of Financial Research (OFR), has seen its resources decimated under the Trump administration.[321] Rebuilding the OFR should be a priority for the Biden administration—but it should not be rebuilt solely with personnel guided by the credit theory of financial crises. The Biden administration should seek to hire data and complexity scientists as it rebuilds the OFR, so that the agency does not view data about operational glitches solely through established narratives about how financial crises occur.[322]

B. Recovery and Repair

Dirk Helbing has argued that, in order to facilitate recovery and repair, "it is necessary . . . to prepare and exercise contingency plans for all sorts of possible failure cascades."[323] In theory, this makes eminent sense, but it may not always be practically possible to do so. As challenging as it is to predict the types of cascade failures that could incapacitate the retail payments ecosystem, it is doubly challenging to figure out how to resolve such failures should they occur. Eisenbach et al. have noted that "if a cyber attack were to compromise the integrity of banks' systems, the reconciliation and recuperation process would be an unprecedented task."[324] The same can be said for any technologically driven cascade failure, even if not initiated by a nefarious actor. It will first take time to determine the systemic interactions that generated the problem—merely identifying the trigger will not be enough.[325] Even assuming an accurate diagnosis, solutions will be difficult to develop, and take time to implement. In the interim, something drastic like a regulator-mandated suspension of all payment services may be needed to allow payments providers time to recover and repair the impacted systems.[326] Even if such a suspension is the most expeditious way to restore payments services, there still will be significant economic fallout. Thus, given the challenges involved with recovery and repair, it makes sense to consider policies designed to ensure that there is an alternative way of transacting available.

---

[321] Pete Schroeder, *Trump Administration Cuts Staff at Financial Markets Watchdog: Source*, REUTERS (Aug. 8, 2018), https://www.reuters.com/article/us-usa-ofr-cuts/trump-administration-cuts-dozens-of-staff-at-financial-markets-watchdog-source-idUSKBN1KT23O [https://perma.cc/SJ9A-6SY6].

[322] For a detailed policy proposal for restaffing the Office of Financial Research, see Hilary J. Allen, Resurrecting the OFR (Nov. 9, 2020) (unpublished manuscript) (on file with author).

[323] Helbing, *supra* note 54, at 55.

[324] EISENBACH ET AL., *supra* note 1, at 36.

[325] ARBESMAN, *supra* note 66, at 12–13.

[326] *See* EISENBACH ET AL., *supra* note 1, at 8 (noting that a "bank holiday" might be necessary "to recover the affected systems").

C. Measures to Ensure Redundancy

Because building in redundancy is a well-recognized way of increasing the robustness of complex systems, a macro-operational approach to payments regulation should contemplate measures that promote redundancy within the retail payments ecosystem.[327] At the same time, payments systems benefit from network effects, and thus, become more convenient, efficient, and valuable when a provider allows for payments to a larger group of recipients.[328] A more modular retail payments ecosystem with redundant parts would be deprived of some of these network effects, likely requiring the retention of some of the cross-ledger reconciliation processing that currently slows down payments processing (particularly at the cross-border level).[329] Regulatory policy therefore will face a challenging balancing act between promoting redundancy and efficiency.

The appropriate balance ultimately will be informed by our confidence in the sensors, feedback loops, and recovery mechanisms available. Less redundancy in the retail payments ecosystem would be required if: (1) sensors existed that could alert regulators to issues that arise as payments systems take on increasing numbers of transactions and incorporate new technological developments; (2) feedback loops could be implemented that allowed regulators time to respond to signals from those sensors before a crisis develops; and (3) if recovery and repair measures could be designed in advance.

If, however, we have limited faith in these sensors, feedback loops, and recovery measures, a prudent approach to macro-operational risk management would be to build extra redundancy into the retail payments ecosystem, even at the cost of efficiency. At least while macro-operational sensors and intervention mechanisms are in their experimental phase, regulators should err on the side of caution and encourage such redundancy.[330]

There are a number of regulatory strategies that could be employed to promote redundancy in the retail payments ecosystem. Perhaps the most politically palatable strategy would be to lower regulatory barriers to entry to encourage entrepreneurs and innovators to make inroads into the industry and provide alternative payments processing services. Many jurisdictions are doing just this, with the adoption of regulatory sandboxes and special purpose char-

---

[327] *See* Ruhl, *supra* note 10, at 580 (explaining that redundancy is a technique often used to increase robustness in complex systems).

[328] BIS, *supra* note 200, at 62.

[329] *See* Morgan Ricks et al., *FedAccounts: Digital Dollars*, GEO. WASH. L. REV. (forthcoming 2021) (manuscript at 3), https://ssrn.com/abstract=3192162 [https://perma.cc/85SM-GPP2] ("[P]ayment system fragmentation—involving thousands of separate ledgers stitched together through various correspondent and clearing arrangements—creates massive inefficiencies.").

[330] *See supra* note 15 and accompanying text.

ters designed to reduce the amount of regulation applicable to fintech innovators.[331] In theory, adopting measures such as these could "allow a thousand payment systems to bloom," creating a diversity of payments processing modules. In reality, however, the network effects associated with payments processing make such an outcome unlikely. When the provider of payments services is a large tech company, such as Facebook, the likelihood of industry consolidation is particularly strong because such firms "can establish and entrench their market power through their control of key digital platforms, e.g., e-commerce, search or social networking."[332] Indeed, because of tendencies in the tech industry towards monopoly, simply reducing regulatory barriers to entry could very well result in fewer redundancies, not more.

If reducing regulation will not promote redundancy, adapting existing regulatory structures might be able to do so. Pursuant to Section 805 of Dodd-Frank, the Federal Reserve theoretically could promulgate rules that limit the volume of transactions that a particular payments provider could process, promoting modularity by making room for competitors. As a complementary approach, the Federal Reserve could adopt rules limiting interoperability under Regulation HH. There are, however, reasons to be skeptical that such inefficiency-inducing steps would be viable in our current political climate (before the Federal Reserve can regulate payments infrastructure or activities, they must first be subjected to heightened regulatory standards by the FSOC which is chaired by the Treasury Secretary—a political appointee).[333] There are therefore, at least at present, limitations on the ability of regulators to use Title VIII to prevent consolidation in the payments industry. Moreover, antitrust laws, which also could have a role to play in promoting redundancy,[334] are underutilized in the United States when it comes to financial infrastructure.[335]

Another alternative would be for national authorities to themselves provide a substitute payments service that adds redundancy to the system—perhaps

---

[331] Hilary J. Allen, *Experimental Strategies for Regulating Fintech*, 3 J. L. & INNOVATION 1, 19–24 (2020).

[332] BIS, *supra* note 200, at 73.

[333] *See* Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) §§ 111(b)(1), 804, 12 U.S.C. §§ 5321, 5463 (explaining how the FSOC determines whether certain payments systems are or will be "systemically important," thus rendering them part of the Federal Reserve's regulatory purview).

[334] *See* BIS, *supra* note 200, at 68 ("[B]ig techs' activity in finance may warrant a more comprehensive approach that encompasses not only financial regulation but also competition and data privacy objectives.").

[335] For a discussion of this issue, albeit with a focus on derivatives clearinghouses rather than retail payments processing infrastructure, see Felix B. Chang, *Financial Market Bottlenecks and the "Openness" Mandate*, 23 GEO. MASON L. REV. 69, 70–71 (2015).

as a "payment system of last resort."[336] There is currently significant interest in developing central bank-sponsored virtual currencies to "protect the pre-eminence of public money in a digitalised economy."[337] These essentially would be digital versions of sovereign currencies and certainly could function as a distinct and alternative payments rail that improves the robustness of the retail payments ecosystem. Some have expressed credit-related reservations about these virtual sovereign currencies, though. The concern is that if people prefer these currencies to bank deposit accounts as a place to store their money, banks will be deprived of much of the deposit funding they currently rely upon to make loans, thus limiting the availability of credit and growth.[338] Concerns have also been raised about the ability of central banks to carry out monetary policy, which they traditionally have implemented through their interactions with privately-owned banks, if private banks are rendered superfluous.[339] In a recent white paper, however, Ricks et al. have argued that even if depositors place their funds with a central bank, there can be a continued role for privately owned banks as lenders who engage in the time-intensive activity of screening borrowers—funding those loans with money borrowed from the central bank.[340] From a credit perspective, then, the adoption of digital sovereign currencies may not be problematic. Indeed, Ricks et al. have argued that the provision of retail payments services by a central bank is a solution to the many credit-related fragilities that can inspire panics in our current financial system.[341]

In fact, Ricks et al. have even argued that no virtual currency is needed to create a new central bank-sponsored retail payments processing system.[342] They have proposed that instead of relying on distributed ledger technology, the Federal Reserve simply should scale up its existing ledgers to allow for crediting and debiting balances for retail customers, which it already does for wholesale customers.[343] Using these ledgers, the Federal Reserve could just start offering bank accounts to retail customers, so that "[a] user-friendly web and smartphone interface would support free and instant peer-to-peer payments between FedAccount holders."[344] Even though Ricks et al. make a series of

---

[336] *See* EISENBACH ET AL., *supra* note 1, at 9 ("[T]he provision of dedicated back-up facilities in core markets could reduce the impact of availability and integrity events." (citation omitted)).

[337] Jean-Pierre Landau, *Central Banks Should Issue Digital Currencies of Their Own*, FIN. TIMES (July 1, 2019), https://www.ft.com/content/ad1a6ae8-9be5-11e9-9c06-a4640c9feebb [https://perma.cc/W8KW-6XBD].

[338] *Examining Facebook's Proposed Cryptocurrency*, *supra* note 277, at 11.

[339] Lastra & Allen, *supra* note 268, at 201.

[340] Ricks et al., *supra* note 329, at 20–21.

[341] *Id.* at 13–14.

[342] *Id.* at 27–31.

[343] *Id.* at 30–31.

[344] *Id.* at 6.

compelling arguments as to why their proposal would improve financial stability from a prudential perspective, operational concerns remain. From a redundancy perspective, the most obvious risk is that any government-provided payments service—be it the FedAccount proposed by Ricks et al. or a central bank-sponsored virtual currency—would be too successful, outcompeting all the private sector alternatives to become the only viable processor of payments.

One partial solution to the need for redundancy may be to implement policies that preserve the usefulness of cash (meaning physical currency issued by a sovereign government). Although electronic transfers are increasingly supplanting the use of cash for day-to-day payments[345]—some commentators have even gone so far as to call for the abandonment of cash altogether[346]—part of the solution to macro-operational risks in our retail payments ecosystem may be to ensure that we do not lose existing redundancies that might be able to pick up the slack if the electronic alternatives fail entirely. For example, Congress could amend its definition of "legal tender" in 31 U.S.C. § 5103 to require private persons to accept cash as payment for goods and services—they are not currently required to do so, and many businesses have "gone cashless" as a result.[347] Such an amendment certainly would inject inefficiencies into the retail payments ecosystem, but the redundancy would improve the robustness of the overall system.[348]

CONCLUSION

There is no foolproof way of preventing technological problems from cascading through our retail payments ecosystem, amplifying as they interact to paralyze the workings of our economy. The potential gravity of such a failure, however, justifies policy measures that seek to make such an outcome less likely or less severe. Unfortunately, our extant framework of crisis-prevention tools neglects the possibility of normal accidents and cascading operational

---

[345] Nathaniel Popper et al., *Will Cash Disappear?*, N.Y. TIMES (Nov. 14, 2017), https://www.nytimes.com/interactive/2017/11/14/business/dealbook/cashless-economy.html [https://perma.cc/E7UJ-72JS].

[346] Kenneth Rogoff, in his book, *The Curse of Cash*, made one of the more provocative calls for abandoning cash. *See generally* KENNETH S. ROGOFF, THE CURSE OF CASH (2016) (examining why and how governments should begin to transition away from physical currencies).

[347] *See Legal Tender Status*, U.S. DEP'T TREASURY (Jan. 4, 2011), https://www.treasury.gov/resource-center/faqs/Currency/Pages/legal-tender.aspx [https://perma.cc/V9WD-Z9CE] (explaining that 31 U.S.C. § 5103 currently does not require businesses and individuals to accept cash payments).

[348] As an aside, such a policy also would benefit the many members of society who do not have access to electronic financial services, and who are thus increasingly marginalized in a cashless society. For a report on this issue, see Ginia Bellafante, *How the Cashless Economy Shuts Out the Poor*, N.Y. TIMES (Dec. 6, 2018), https://www.nytimes.com/2018/12/06/nyregion/how-the-cashless-economy-shuts-out-the-poor.html [https://perma.cc/C8TN-CA2H].

failures. A new regulatory framework is therefore needed that takes the potential systemic interactions of operational risks seriously. This Article has argued for the development of a "macro-operational" regulatory approach that is based in the lessons of complexity theory. Such an approach is only becoming more necessary as new financial technologies are developed that make our retail payments system even more complex, and thus, more prone to cascading failures.

This Article's conclusion regarding the need for macro-operational regulation is not just applicable to the retail payments system; the increasing complexity of the financial system ensures that *all* financial regulators need to be open to the possibility of cascading operational failures that can impact financial stability. This Article has provided some preliminary thoughts on what macro-operational regulation of the retail payments ecosystem might look like, but a broader conversation regarding macro-operational regulation could find its start in the Advance Notice of Proposed Rulemaking (ANPR) promulgated in 2016 by the OCC, Federal Reserve, and FDIC on Enhanced Cyber Risk Management Standards.[349] Although this endeavor was shelved, this ANPR poses probing questions about how to determine which sectors' operations are critical enough to deserve heightened regulation, how to assess which entities pose systemic operational risk, and which methodologies are best for measuring cyber risks. This inquiry should be broadened beyond cyber-related risks to operational risks more broadly—the answers to these questions could then generate the beginnings of a new regulatory approach designed to address the possibility of future financial crises that could develop outside of the credit channels of systemic risk.

[349] *See generally* Enhanced Cyber Risk Management Standards, 81 Fed. Reg. 74,315 (proposed Oct. 26, 2016) (proposing rules on "enhanced standards to increase the operational resilience" of financial institutions).