Comments to the Office of the Comptroller of the Currency on Supporting Responsible Innovation

Peter Van Valkenburgh & Jerry Brito
May 27, 2016

Introduction

Coin Center is a non-profit research and advocacy center focused on the public policy issues facing open and decentralized blockchain technologies. Specifically, our focus encompases cryptocurrencies (*e.g.* Bitcoin), decentralized computing platforms (*e.g.* Ethereum) and inter-ledger systems and protocols (*e.g.* sidechains). Our mission is to build a better understanding of these technologies and to promote a regulatory climate that preserves the freedom to innovate using them. We do this by producing and publishing policy research from respected academics and experts, educating policymakers and the media about decentralized blockchain technology, and by engaging in advocacy for sound public policy. In that spirit, please find below our comments on the recent OCC innovation white paper.

We applaud the OCC for engaging in this process. In its white paper on innovation, the OCC has modestly and transparently recognized that it may have a "low risk tolerance for innovative products and services" which can result in "a deliberate and extended vetting process that can discourage innovation inadvertently." This forthright observation will hopefully be the prescient and deliberate first step in a longer journey to re-enable American innovation in the financial services sector, a sector that is increasingly finding its home abroad.

This Comment will proceed in three sections. First, deficiencies in the current US regulatory landscape will be explored by comparison to other nations, in particular the UK and by extension the EU. Second, the nature of fintech innovation in the information age will be discussed, and three key concepts—open source software, open networks, and virtual currencies—will be briefly explained. Third, a regulatory solution to the poor state of US competitiveness will be proposed: a limited federal charter for fintech firms.

I. International Comparisons

The US approach to regulating financial technology stands in sharp contrast to the recent approach taken by UK regulators. In March of 2015, Her Majesty's Treasury, seeking to "create a world-leading environment for the development of innovative payments and

financial technology" crafted a plan for digital currency regulation that included public funding, standard setting, and regulatory clarifications.[1]

One year later, UK authorities have matched that encouraging talk with real action. The UK Financial Conduct Authority ("FCA") now makes it easy and quick for innovative startups and entrepreneurs to comply with appropriate consumer protection regulations and safely enter the market.[2]

While some US regulators have issued similarly encouraging statements[3]—including the Comptroller of the Currency[4]—little in the way of ameliorative action has materialized. Many in the press have identified the gap and warned of a coming exodus of innovative companies into the UK.[5] This is a particularly dire state of affairs for American fintech competitiveness given two troublesome structural features of US financial regulation not present in the UK: *federalism*, and a *rules-based rather than principles-based approach*. These two structural issues are not a product of mistakes or miscalibration at the OCC or any other agency specifically; they are features of the larger landscape of financial regulation in the US. We focus on these issues in this comment because the OCC is uniquely positioned to address them.

---

[1] Specifically the plan called for: (1) Clarification and application of anti-money laundering regulation to digital currency exchanges to prevent criminal use. (2) Training, resources, and legislation to ensure that law enforcement bodies can effectively address criminal activity conducted with digital currency. (3) Cooperation from the British Standards Institute and the digital currency industry to develop a set of best practices for consumer protection that does not impose an extreme regulatory burden on players in the space. (4) Creation of a research initiative with leading institutions within the UK to study digital currencies and increase public funding for digital currency research to £10 million. *See* HM Treasury, *Digital currencies: response to the call for information* (Mar. 2015) *available at* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/414040/digital_currencies_response_to_call_for_information_final_changes.pdf

[2] Among other things, participants in the FCA's Innovation Hub receive from the regulator: A dedicated team and contact for innovator businesses, help for these businesses to understand the regulatory framework and how it applies to them, assistance in preparing and making an application for authorisation, to ensure the business understands our regulatory regime and what it means for them, and a dedicated contact for up to a year after an innovator business is authorised. *See* Financial Conduct Authority, *Innovator businesses: Project Innovate* (last accessed May 2016), https://innovate.fca.org.uk/.

[3] For example, in a recent special address, CFTC Commissioner J. Christopher Giancarlo has articulated "The Need for a "Do No Harm" Regulatory Approach to Distributed Ledger Technology."J. Christopher Giancarlo, *Special Address Before the Depository Trust & Clearing Corporation 2016 Blockchain Symposium* (Mar. 2016) *available at* http://www.cftc.gov/PressRoom/SpeechesTestimony/opagiancarlo-13.

[4] With regard to virtual currencies and blockchain technology, the Comptroller has said that "[t]hese innovations are potentially revolutionary in their impact, and are advancing at a breakneck pace. The current regulatory regime, which is rooted in 20th century concepts and approaches, will need to change and adapt in order to remain relevant into the 21th century." Thomas J. Curry, *Remarks Before the Institute of International Bankers Washington, D.C* (Mar. 2015) *available at* http://www.occ.treas.gov/news-issuances/speeches/2015/pub-speech-2015-32.pdf.

[5] *See generally,* Jeff Lynn, "Why Britain is beating the U.S. at financial innovation" *TechCrunch* (May 2016) http://techcrunch.com/2016/05/13/why-britain-is-beating-the-us-at-financial-innovation/.

A. Federalism, Redundancy, and Non-Uniformity

Special programs and friendly rhetoric aside, the UK *already* offers fintech innovators a substantially safer harbor than the US. In the UK there is a one-stop-shop for financial regulation: Her Majesty's Treasury. In the US, however, many fintech firms will often be found to be a money services business and, more narrowly, a money transmitter. As a money transmitter, a firm must be prepared to interface with multiple federal regulators[6] as well as regulators in every one of the several states wherein they have or expect to have customers.[7] Little coordination exists between these several regulatory bodies and conflicting approaches and non-uniformity abound.[8]

By marked contrast, the simplicity of the UK's purely national approach extends to the entire EU single market. Once authorized to do business in an EU member state, a firm can passport into every other.[9] No such regulatory coordination—uniformity, passporting, or reciprocity—exists across the several US states for firms deemed to be money transmitters.[10]

Moreover, profound criminal penalties await an innovator who ignores the states, or who wishes to hazard a liberal interpretation of when an activity is *not* money transmission, or who—succinctly—chooses to seek forgiveness rather than permission.[11] The innovator need not even have knowledge that what she has built will be construed as unlicensed money transmission to be convicted under the Bank Secrecy Act, because PATRIOT Act amendments to the BSA stripped the law of all scienter requirements, effectively creating a strict liability regime.[12] Such liabilities can even extend to a firm's investors, managers, or employees,

---

[6] MSBs are subject to regulation by FinCEN under the Bank Secrecy Act as well as being potentially regulated by the CFPB under the Dodd Frank Act, the FTC under Unfair and Deceptive Acts and Practices standards. Additionally, if the firm engages in margin trading or derivatives exchange it will be regulated by the CFTC and potentially the SEC.

[7] Specifically, 53 states and territories have individual licensing requirements for money transmission. *See* Thomas Brown, *50-STATE SURVEY: Money Transmitter Licensing Requirements* (last accessed May 2016) http://abnk.assembly.ca.gov/sites/abnk.assembly.ca.gov/files/50%20State%20Survey%20-%20MTL%20Licensing%20Requirements(72986803_4).pdf.

[8] For example, as of 2016, the Uniform Law Commission's *Uniform Money Services Act* has only been adopted by legislatures in nine states and territories. The UMSA was finalized in 2000. After 16 years it has only modestly remedied the issue of disparate standards for money transmission regulation across the several states. *See* Uniform Law Commission, *Uniform Money Services Act* (last accessed May 2016) http://www.uniformlaws.org/Act.aspx?title=Money%20Services%20Act.

[9] *See* European Banking Authority, *Passporting and supervision of branches* (last accessed May 2016) https://www.eba.europa.eu/regulation-and-policy/passporting-and-supervision-of-branches.

[10] *See infra* note 8.

[11] *See* 18 U.S. C § 1960 - Prohibition of unlicensed money transmitting businesses, *available at* https://www.law.cornell.edu/uscode/text/18/1960.

[12] *See id. See id. See also* Brian Klein, "Does 18 U.S.C. § 1960 create felony liability for bitcoin businesses? A Backgrounder for Policymakers" *Coin Center* (Jul. 2015) *https://coincenter.org/2015/07/does-18-u-s-c-%C2%A7-1960-create-felony-liability-for-bitcoin-businesses/*

generating a culture of knee-jerk caution likely to chill experimentation, or send it to safer, simpler shores.[13]

B. Rules rather than Principles

Additionally, the US approach to regulation of financial intermediaries—particularly state money transmission licensing law—is, more often than not, rules-based.[14] There are, generally, no flexible standards for consumer protection.

Firms are not left to calibrate their own policies using their own internal expertise and understanding of risk in the shadow of a principles-based standard. Instead, a business is prescriptively told to mitigate risks through a set of rigidly defined compliance requirements (*e.g.* hold surety bonds of specific amounts for customers in each of the several states,[15] submit extensive and specific licensing applications dealing with many factors inapplicable to their particular, novel business model,[16] and file suspicious activity reports, currency transaction reports, and forward customer data along with the funds for every transaction above a certain dollar threshold[17]). Businesses are required to meet uniform standards of minimum capitalization regardless of the scale of their activities,[18] and business models deliberately developed in order to genuinely mitigate risks by dealing only in low-value transactions or by holding custody of consumer funds only briefly (or not at all) are granted no special or particularized treatment.[19] If their volume and value at risk would never justify a market capitalization above the minimum required by the state, then they simply cannot operate in compliance.

These rules are inflexible and calibrated to a technological and commercial environment that has long-since become outmoded. These rules are difficult to interpret for new firms, because they deal in specific prescriptive obligations sensible for legacy businesses but often irrelevant or confounding for new technologies (*e.g.* a purely online business must obtain a

---

[13] *See id.*
[14] *See generally,* Jeff Lynn, "Why Britain is beating the U.S. at financial innovation" *TechCrunch* (May 2016) http://techcrunch.com/2016/05/13/why-britain-is-beating-the-us-at-financial-innovation/.
[15] *See* Thomas Brown, *50-STATE SURVEY: Money Transmitter Licensing Requirements* (last accessed May 2016) http://abnk.assembly.ca.gov/sites/abnk.assembly.ca.gov/files/50%20State%20Survey%20-%20MTL%20Licensing%20Requirements(72986803_4).pdf.
[16] *See id.*
[17] *See* FinCEN, *BSA Requirements for MSBs* (last accessed May 2016) https://www.fincen.gov/financial_institutions/msb/msbrequirements.html.
[18] *See* Brown, *50-State Survey, supra* note 15.
[19] No states offers a *de minimis* or low value exemption for money transmission licensing requirements. Coin Center has advocated that such exemptions should be considered when states look to develop virtual currency specific licensing laws or regulations. As of this comment, only New York has implemented such a policy, with a provisional license for small virtual currency companies. *See* New York Department of State Department of Financial Services, *New York Codes, Rules and Regulations Title 23. Department of Financial Services Chapter 1. Regulations of the Superintendent of Financial Services Part 200. Virtual Currencies*, available at http://www.dfs.ny.gov/legal/regulations/revised_vc_regulation.pdf.

license whose requirements are calibrated based on the number of physical locations in a state;[20] a global service must hold surety bond specifically and exclusively for the benefit of customers in each state;[21] a platform that predominantly allows persons to send money to other persons *without intermediaries* may need to send customer data to the "receiving financial institution" for every transaction[22]). And these prescriptive obligations are triggered by performing an activity that is statutorily defined using terms of art from tools and business models of the past (*e.g. "transmit," "payment instrument," "check cashing," "money transmission," "pre-paid account,"* or *"electronic funds transfer"*). And, finally, amending the rules or interpreting them to better address the risks and rewards offered by evolving technological opportunities is a slow and difficult process because the very nature of rules as compared with principles is that they are intended to be inflexible and stable.

By contrast, a principles-based approach, exemplified by the recent FCA Innovation Hub in the UK, forgoes these rigid, often obsolete, and check-the-box requirements in favor of a cooperative dialog between innovators and regulators, a dialog aimed at achieving a set of principles—adequate protection of consumer funds, prevention of systemic risks to the economy, and effective transparency for law enforcement—in light of the fresh opportunities and limitations of some new technology or business model.[23]

The problem of rules-based regulation is amplified by the presence of overlapping, multi-state regulation discussed earlier. Each state has a unique definition of money transmission,[24] a unique and highly comprehensive licensing application,[25] and each a unique set of rules that licensees must follow to remain compliant.[26] This panoply of requirements necessitates herculean compliance costs for fintech startups who engage in activities found to be money transmission. As will be explained in the following subsection, this may be the majority of innovative fintech companies. The state of the art in financial network architecture often makes it impossible for a firm to innovate without engaging, itself, in activities classified as money transmission.

II. Open Source and Open Network

In the 21st century, responsible financial innovation is *open* innovation, both open source and open network. Before asking how the OCC can facilitate increased responsible innovation, it is important to discuss how open source software and open network architecture are essential for security and competition in today's information economy. Encouraging experimentation is important, but as the white paper's title suggests, we should

---

[20] *See* Brown, *50-State Survey, supra* note 15.
[21] *See id.*
[22] *See* FinCEN, *BSA Requirements for MSBs* (last accessed May 2016) https://www.fincen.gov/financial_institutions/msb/msbrequirements.html.
[23] *See* Financial Conduct Authority, *Innovator businesses: Project Innovate* (last accessed May 2016), https://innovate.fca.org.uk/.
[24] *See* Brown, *50-State Survey, supra* note 15.
[25] *See id.*
[26] *See id.*

encourage *responsible* systems that truly improve financial services by increasing security and interoperability.

Open source refers to the source code that comprises a particular piece of software. Software can be developed alone, in secret within a firm, and that secrecy can be protected by using copyright law to aggressively prevent unauthorized use or distribution. Alternatively software can be developed publicly amongst multiple contributors—some within the firm, some outside as contractors, or even complete strangers who happen to also take an interest in the software's development. To avoid copyright liability for this open set of participants, permissive licenses are used.[27]

Particularly in applications where interoperability and network security are critical—Internet web servers and operating systems—open source software has come to dominate the market. Among active websites on the Internet, 50% are powered by the open source Apache web server; the next most popular server is nginx, also open source, with 16% market share as of November 2015.[28] The Android mobile operating system is also open source, and it dominates smartphone computing globally with over 80% market share in the fourth quarter of 2015.[29]

Similarly, the networks that allow software to communicate and interoperate between multiple users can be proprietary or open. Today, most consequential networks are made up of open, shared, multi-purpose communications infrastructure that employs packet switching protocols, most commonly the Internet Protocol or IP.[30] Even voice calls now often travel over IP,[31] as do web pages, streaming video, the SWIFT payments network in Europe,[32] and FedWire in the US.[33]

Despite using IP networks, SWIFT and FedWire continue to use a server-client network architecture, wherein users send messages to a centralized server that then validates and forwards the payment message to the other party. These centralized servers remain vulnerabilities in network architecture. If the server is hacked or overloaded, the system fails.

---

[27] *See generally* Open Source Initiative, *Licenses & Standards* (last accessed May 2016) https://opensource.org/licenses.
[28] *See* Netcraft, *November 2015 Web Server Survey* (Nov 2015) http://news.netcraft.com/archives/2015/11/16/november-2015-web-server-survey.html.
[29] *See* Gartner, *Worldwide Smartphone Sales Grew 9.7 Percent in Fourth Quarter of 2015* (Feb. 2016) http://www.gartner.com/newsroom/id/3215217.
[30] *See* Don Parker, "Basic Journey of a Packet" *Symantec Connect* (Nov 2010) http://www.symantec.com/connect/articles/basic-journey-packet.
[31] *See* Federal Communications Commission, *Voice Over Internet Protocol (VoIP)* (last accessed May 2016) https://www.fcc.gov/general/voice-over-internet-protocol-voip
[32] In 2005 SWIFT completed its move to an all IP network infrastructure, known as SWIFTNet. *See* SWIFT, *SWIFT for high-value payment market infrastructures* (Feb 2009) https://marketinfrastructures.swift.com/sites/marketinfrastructures/files/swift_for_high_value_payment_brochure.pdf.
[33] *See* Federal Reserve Bank of New York, *Fedwire: The Federal Reserve Wire Transfer Service*, (Mar. 1995), and Adam Gilbert, Dara Hunt, and Kenneth C. Winch "Creating an Integrated Payment System: The Evolution of Fedwire," *Federal Reserve Bank of New York Economic Policy Review*, July 1997, available at www newyorkfed.org/research/epr/97v03n2/9707gilb html.

The vulnerabilities of these architectures were highlighted by the recent failure of the SWIFT network to prevent $81 million in fraudulent transactions (and very nearly $1 billion in additional transactions) initiated by a hacker who gained access to SWIFT software and credentials through the Bangladeshi central bank.[34] Newer network architectures utilize peer-to-peer Internet protocols to ensure redundancy in the event any particular intermediary step in the communications line fails or is corrupted by hackers.[35]

Privacy may be seen as a concern in these peer-to-peer systems because any transaction message could travel across the hardware of any other participant in the open network. These concerns are addressed using cryptography so that even if the encrypted communication travels over several intermediary peers in the network, only the sender and recipient have the keys to decode the message and understand what the transaction was. Similarly, if any one of the several participants initiates messages claiming to originate from another player (*i.e.* sockpuppeting or identity theft), cryptographic digital signatures can make this attempt at fraud more difficult.[36] Even though the network infrastructure is open, the ability to make authoritative statements on that network is contingent on proving one's identity (at least pseudonymously).[37]

To ensure that a transaction message is truly unique and not an attempt to send the same funds to multiple recipients simultaneously, these networks will often employ a blockchain or ledger of all transactions that is shared across all members of the peer-to-peer network. Before accepting a transaction, the recipient checks this ledger to make sure that the sender has not previously spent the funds she now purports to send. With a blockchain, we do not need to take our counterparty at her word, an authoritative shared record exists to ensure all participants play fair and don't try to double spend.

If the network is truly open and decentralized it must employ an incentive system to ensure that participants do not collude to commit fraud as they update and maintain the authoritative ledger.[38] To dispense these incentives without a centralized point of control, the network will need to automatically reward honest participants using the same scarce token that travels on that network for settlement or payment purposes. If the reward was a

---

[34] *See* Peter Bright, "Billion dollar Bangladesh hack: SWIFT software hacked, no firewalls, $10 switches," *ArsTechnica* (Apr. 2016) http://arstechnica.com/security/2016/04/billion-dollar-bangladesh-hack-swift-software-hacked-no-firewalls-10-switches/.

[35] *See* Larry Greenemeier, "Bitcoin-Based Blockchain Breaks Out," *Scientific American* (Apr. 2015) http://www.scientificamerican.com/article/bitcoin-based-blockchain-breaks-out/ ("Bitcoin operates on a peer-to-peer network that consists of computers—run by "miners" set up specifically to verify the validity of a transaction and record it in the blockchain. The first computer to solve a cryptographic puzzle accompanying each transaction is awarded bitcoins. Other computers in the network check the solution, creating a redundancy designed to guard against transaction fraud.").

[36] *See id.*

[37] *See* Adam Ludwin, "How Anonymous is Bitcoin? A Backgrounder for Policymakers," *Coin Center* (Jan. 2015) http://coincenter.org/2015/01/anonymous-bitcoin/.

[38] Within Bitcoin, this incentive structure is referred to as "mining." *See* Peter Van Valkenburgh, "What is Bitcoin Mining, and Why is it Necessary?" *Coin Center* https://coincenter.org/2014/12/bitcoin-mining/.

valuable item outside of the network, say dollars,[39] there would need to be a system outside of the network to judge honest participation and dispense those rewards. That system, itself, would then be a vulnerable centralization of power generating risks for users on the network. This is why several fintech firms are experimenting with virtual currencies rather than simple bookkeeping ledgers. There is no way to have the security and interoperability of a decentralized and open blockchain without a valuable token or virtual currency involved.

Many new fintech firms wish to experiment with decentralized blockchains because of the added security provided by the absence of centralized weak-points in the network, and the interoperability inherent in an open network. However, this means that experimenting with "fintech" will often constitute more than simply writing software that existing financial intermediaries can employ. In many cases a fintech firm, simply by participating in the open network, will automatically be holding or exchanging funds (the scarce tokens or virtual currencies that travel on these networks) potentially subjecting an innovator to the full consequences of money transmission law from day one, merely because of interconnectivity with a virtual currency network.[40]

While open software and open networks may carry regulatory risks, they have great potential to substantially reduce operational risks. Proprietary software is not always effectively vetted by a large enough community of security professionals. Open source software is developed in public with potentially thousands of independent auditors testing the code for weaknesses and bugs.[41] Open networks add to this resilience because they do not rely on perimeter security and maintenance on the part of centralized servers or consortium members to prevent unauthorized access or network failure. Unlike a client-server architecture, which fails if vulnerabilities hidden in the internal processes of the server are revealed to the public, open architectured systems are designed to exist in public, where sunlight is the best disinfectant.

---

[39] At least until a digitized dollar is deployed by the Federal Reserve.

[40] According to FinCEN guidance from March of 2013, exchanging virtual currencies or transmitting them on behalf of others constitutes money transmission under the Bank Secrecy Act. *See* FinCEN, "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies" FIN-2013-G001 (Mar. 2013) *available at* https://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf. Several innovators in the virtual currency space were caught somewhat off-guard by that guidance. Firms that believed that they were doing something outside of the normal realm of money transmission suddenly had to deal with the compliance consequences of being a money transmitter simply because the platform they had helped to develop involved a virtual currency component. *See, e.g.*, Sarah Todd and Ian McKendry, "What Ripple's Fincen Fine Means for the Digital Currency Industry," *American Banker* (May 2015) http://www.americanbanker.com/news/bank-technology/what-ripples-fincen-fine-means-for-the-digital-currency-industry-1074195-1.html.

[41] The idea of security by way of massive public auditing and transparency has come to be called "Linus' Law" and it is commonly expressed as ""Many Eyes Make All Bugs Shallow." See Jeff Jones, "Linus's Law aka "Many Eyes Make All Bugs Shallow"" Microsoft Cyber Trust Blog (Jun. 2006) https://blogs.microsoft.com/cybertrust/2006/06/07/linuss-law-aka-many-eyes-make-all-bugs-shallow/.

Perimeter security and proprietary software create security weaknesses which inevitably will be exploited on the day the perimeter is breached or the source code leaked. In the 21st century, responsible financial innovation *is* open innovation, both open source and open network. The US regulatory landscape, however, remains inhospitable to these open innovations because of the issues of federalism and rules-based regulation discussed in the previous sections. The OCC is ideally positioned to change all of that.

III. Facilitating American Innovation

As discussed, the lack of a single, centralized, and flexible regulator for fintech products—as the UK has in Her Majesty's Treasury—is the primary barrier to innovation in the US. The OCC is already in a prime position to play that regulatory role; it can, therefore, remove the barriers to American competitiveness far more rapidly than any other regulatory or political strategy.

In its White Paper, the OCC asks "How can [we] facilitate responsible innovation by institutions of all sizes?" The simplest and most promising answer is to create a lightweight, limited-purpose federal charter for fintech firms that mirrors the regulatory environment of the UK: principles-based regulation with passporting across the several states.

Innovative firms have, principally, two needs that such a federal charter could satisfy. (1) A federal charter could be made to preempt state money transmission regulation and grant the firm a passport enabling them to operate in any and all of the several states. (2) A federal charter could facilitate access to the payment system so that the fintech firm need not struggle to obtain banking services from existing financial institutions who may be risk averse.[42]

The OCC, by virtue of being a federal agency with preemptive power over state law, is ideally positioned to address the first concern. The OCC need not fully preempt state authority in this space, but can—instead—craft a new federal alternative to state money transmission regulation for fintech firms who choose to seek a limited charter. Similarly, the OCC is the ideal choice for crafting and enforcing flexible, principles-based rather than rules-based regulations because of its history of working closely and flexibly with other federally chartered institutions.

The OCC could also effectively limit its own risk by establishing a limited federal fintech charter. Primarily, the OCC would be taking real steps to ensure that American institutions remain relevant in the development of the future global financial system. Migration of innovative firms to other nations would narrow the window that US regulators have into

[42] Virtual currency firms in particular have found it difficult to establish banking relationships. *See* Pratin Vallabhaneni, David Fauvre, and Andrew Shipe, "Overcoming Obstacles to Banking Virtual Currency Businesses" *Coin Center Report* (May 2016) https://coincenter.org/wp-content/uploads/2016/05/banking-obstacles.pdf.

financial networks and hamstring the US's global policy objectives. Second, the OCC could craft a risk-mitigating charter that *only* enables fintech firms to engage in *some* of the core activities of banks. Given the risks associated with deposit-taking and lending, fintech firms could be limited in their charters to performing the check payment function. Effectively, the firm only gains access to ACH or Fedwire in order to facilitate exchange or interoperability between virtual currencies and the dollar. In this potential model of a limited charter, the fintech firm would have the key benefits of federal regulation, preemption of state law, and access to the payments system, but would not engage in risk-generating activities like deposit taking or credit extension.

Conclusion

Nations like the UK are already taking substantial steps to encourage fintech innovation, especially in the realm of virtual currencies. Substantial structural impediments to innovation exist within the US regulatory landscape: federalism and a rules-based approach. Responsible innovation is open innovation, which will often involve the use of virtual currencies, money transmission, and—by inevitable extension—even greater regulatory confusion. The OCC can and must act to remove these impediments and ensure continued American competitiveness in the coming global financial technology revolution.