Maurer School of Law: Indiana University

Digital Repository @ Maurer Law

Articles by Maurer Faculty

Faculty Scholarship

2019

"Gatekeepers" Are Vital Participants in Anti-Money-Laundering Laws and Enforcement Regimes as Permission-less Blockchain-Based Transactions Pose Challenges to Current Means to "Follow the Money"

Sarah Jane Hughes

Indiana University Maurer School of Law, sjhughes@indiana.edu

Follow this and additional works at: <https://www.repository.law.indiana.edu/facpub>

Part of the [Commercial Law Commons](#), and the [E-Commerce Commons](#)

Recommended Citation

Hughes, Sarah Jane, ""Gatekeepers" Are Vital Participants in Anti-Money-Laundering Laws and Enforcement Regimes as Permission-less Blockchain-Based Transactions Pose Challenges to Current Means to "Follow the Money"" (2019). *Articles by Maurer Faculty*. 2764.

<https://www.repository.law.indiana.edu/facpub/2764>

This Article is brought to you for free and open access by the Faculty Scholarship at Digital Repository @ Maurer Law. It has been accepted for inclusion in Articles by Maurer Faculty by an authorized administrator of Digital Repository @ Maurer Law. For more information, please contact rvaughan@indiana.edu.

LAW LIBRARY
INDIANA UNIVERSITY
Maurer School of Law
Bloomington

“Gatekeepers” Are Vital Participants in Anti-Money-Laundering Laws and Enforcement Regimes as Permission-less Blockchain-Based Transactions Pose Challenges to Current Means to “Follow the Money”

by

Sarah Jane Hughes[‡]

[‡] Sarah Jane Hughes is the University Scholar and Fellow in Commercial Law at the Maurer School of Law, Indiana University, Bloomington, Indiana. She recently served as the Reporter for the Uniform Law Commission’s Uniform Regulation of Virtual-Currency Businesses Act (2017) and the Uniform Supplemental Commercial Law for the Uniform Regulation of Virtual-Currency Businesses Act (2018). From 2000 to 2002, she was the American Bar Association’s Advisor to the Uniform Law Commission’s Money Services Business Act. Professor Hughes has written and given presentations about the deterrence and detection of money laundering since 1992 and has published numerous articles about virtual-currency service providers and the manner of their regulation since 2011. Her first work on electronic payment systems was published in 1997, shortly after early virtual currency and mobile payments efforts in the United States occurred. She is an elected member of the American Law Institute, and prior to joining the faculty at Maurer, held staff and line positions at the Federal Trade Commission related to payments and financial privacy. SSRN=408848.

The research for this essay was conducted from late 2018 through FATF’s approval in June 2019 of new rules for cryptocurrencies, which are discussed in this essay. The majority of the research was completed by May 31, 2019. Readers should anticipate that, given the pace of change in blockchain technologies and products and services available, some or all of what is written here could be seriously outdated by the time this essay is in print. Thus, what is here may be considered as starting points for consideration and research.

Professor Hughes would like to thank Professors Thomas Vartanian and Robert Ledig for the invitation to participate in the May 16, 2019 Public Policy Conference on The Future of Financial Regulation, sponsored by the Program on Financial Regulation & Technology, Law & Economics Center, George Mason University, Antonin Scalia Law School, and for suggesting the topic of this essay. She sends special thanks to Professors Vartanian and Ledig, Professor Paolo Saguato of George Mason University’s Antonin Scalia Law School, Professor Julie Hill of the University of Alabama Law School, and Professor Lawrence J. Trautman of Western Carolina University-College of Business; Ms. Elizabeth Rosenberg, Center for New American Security; Peter A. Wayner, technology author and programmer; Brian Brooks, Coinbase, Inc.; Richard Levin of Polsinelli, LLP, and A. Patrick Doyle, Arnold & Porter Kaye Scholer, for kind comments on topics covered in this essay. She also thanks every journalist and scholar whose works are mentioned in this essay. Despite so many helpful comments and extant work in this field on which to draw, Professor Hughes claims all errors in the pages that follow.

I. Introduction

Two phenomena dominate reports about blockchain-based transactions—that they will disrupt and displace legacy banking, securities, and trade intermediaries, and that they present new or greater opportunities for hiding proceeds of crimes or corruption. This essay does not deal with the former topic. Rather, the organizers of the symposium at George Mason University’s Antonin Scalia School of Law asks me to consider the latter question. It proved to be a tough assignment.

This essay looks at the separate questions of (1) the degree to which permission-less blockchain transactions will disrupt current anti-money laundering (AML) regimes and enforcement efforts, and (2) what efforts governments that have agreed to pursue goals of deterrence and detection of money laundering may need to initiate as blockchain-based transactions become more common.

My thought process has moved through stages and, finally, has focused on three silos of potential concerns about blockchain technologies. In the first silo are blockchain technologies as technologies. I assign to this first silo the lowest level of concerns because of their potential for inclusion, security and integrity. I do not favor regulating technologies; such regulation will be outdated too fast.

The second silo contains cryptocurrencies and other crypto-assets or products and services related to them that are offered in compliance with applicable domestic laws where the user of the product or services is domiciled. I assign a low-to-low-middle level of concern to these crypto assets but recognize and discuss below that this “grade” could change.

In the third silo, I have bad actors whose products and services are designed for illicit purposes, and opportunists that offer products and services they do not have and that have no intention of delivering products or services or allowing redemption of value delivered to them. This third silo gets a big red flag from me – and this silo will require continued attention from domestic and global law enforcement agencies.

Part of the reason that I see a low or low-to-low-middle level of concern for the first two silos is that, for the immediate future at least, that traditional financial services “gatekeepers” in payments, securities, and commodities will continue to play vital roles in deterring and detecting money laundering and terrorism finance efforts here and abroad. The presence of regulated “gatekeepers” may not forestall the need for new legal requirements or enforcement systems forever, but their presence in the marketplaces of today reduce the need for immediate action and allow legislatures and regulators more time to observe crypto innovations and determine their next steps.

As a subset of the third silo, for the time being at least, are the new brands of government-backed cryptocurrencies, such as the Petro from Venezuela and those that Russia, China, and other governments, and the special challenges they may pose to AML legal regimes and, separately, to the United States Dollar as the global reserve currency that it has represented since World War II. These government-backed cryptocurrencies also challenge longstanding concepts of sovereigns’ control over

“legal tender”¹ inside their own borders and their potential sponsors are designing them to avoid economic sanctions imposed by other governments.

The balance of this essay proceeds as follows: Part II provides background on permission-less blockchains and, separately, recent interest by governments in issuing cryptocurrencies themselves. Part III provides background on the three stages of value laundering – (1) initial “placement” of illicit proceeds, (2) “layering” through multiple forms of property or banks or banking systems to obscure its source or ownership, and (3) “integration” or emergence of assets that look legitimate to the outsider.

Part IV reviews different challenges to traditional means of detecting value laundering that non-government-issued cryptocurrencies, permission-less blockchains, and government-sponsored cryptocurrencies pose. This Part looks at the vital roles that “gatekeepers” play in AML enforcement in the United States. Part IV also explains how (1) regulators and law enforcement authorities are already using new tools to trace and identify blockchain-based transactions that are in furtherance of illicit activities, and (2) government-issued cryptocurrencies and more private and opaque cryptocurrencies may make detection of money laundering more difficult. Part V explains my view that permission-less blockchains are not our major problem in the global campaigns against money laundering (regardless of the purposes for which money laundering is attempted) but finding someone to regulate in future may be.

Part VI briefly evaluates efforts by global authorities, such as the G-20’s Financial Action Task Force (“FATF”) regarding the regulation of cryptocurrencies and the European Parliament’s 5th Anti-Money Laundering Directive (“AMLD5”), some of which goes into effect on January 10, 2020,² to re-frame the AML and market-protection regulatory recommendations to cover issues relating to cryptocurrencies and other crypto-assets.

Part VII states some conclusions and identifies questions for additional research.

II. Permission-less Blockchains, Cryptocurrencies and Other Crypto-Assets, and Special Issues Raised by Government-sponsored Cryptocurrencies

Cryptocurrencies and crypto-assets on permission-less blockchains offer time-stamped publicly viewable records of transfers of rights that rely on peer-to-peer distributed “servers to generate computational proof of the chronological order of transactions” that itself is “secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.”³

This Part looks at types of blockchain technologies, potential risks associated with some cryptocurrencies and crypto-assets, and special issues raised by government-sponsored cryptocurrencies.

¹ 31 U.S.C. § 5103 (2018) (“United States coins and currency (including Federal reserve notes and circulating notes of Federal reserve banks and national banks),” legally served to pay debts, charges, taxes, and dues, originally from the Coinage Act of 1965).

² Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing and amending Directive 2009/138/EC and 2013/36/EU (Text with EU relevance), at para. 53, Document 32018L0843, <http://data.europa.eu/eli/dir/2018/843/oj>.

³ Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 1 (undated), www.bitcoin.org (allowing electronic payment systems to work based on “cryptographic proof ... without the need for a trusted third party”) [hereinafter “Nakamoto”].

Before proceeding, it is important to establish a baseline understanding of what a blockchain is. I asked three experts from different backgrounds about the terms “distributed ledger technologies” and “blockchain.” These three views are shown in the order in which I received them:

Patrice Lyons, a technology attorney based in Reston, Virginia and Washington, D.C., responded:

From my perspective, a blockchain is considered a “digital entity” (see definition in ...ITU-T Recommendation X.1255), and there are many ways of configuring digital entities in this context. The origins of this technology go back many years ...⁴

My co-panelist at the “Smart Regulation” Public Policy Conference, Peter A. Wayner, a programmer and author of several books on cryptocurrencies and blockchains, has explained a blockchain as:

A chain of blocks that track the sequence of transactions for cryptocurrencies provide a unique opportunity for public analysis of spending patterns. While the nominal identity of each person is not recorded as a human readable name or common identification value like the Social Security number, the public key used to sign the transaction can provide much of the same value. All of the transactions associated with the key of a particular person are easy to find on the blockchain as the publicly accessible information. Even if the transactions are routed through different exchanges or intermediaries, all of the cryptocurrencies that flow through the wallet can be flagged.⁵

Michigan State University’s Professor Carla Reyes explains distributed ledger technologies, which are broader than the universe of blockchains, as follows:

... uses the [distributed ledger technology or DLT] to refer generally to ‘computer software that is distributed, runs on peer-to-peer networks, and offers a transparent, verifiable, tamper-resistant transaction-management system maintained through a consensus mechanism rather than by a trusted third-party intermediary that guarantees execution.’⁶

In simplified terms, then, a blockchain is a method of storing records of ownership or of assets and transactions that uses a version of a distributed ledger.⁷ A distributed ledger keeps records “in many

⁴ Patrice A. Lyons, email to Sarah Jane Hughes, June 8, 2019 4:53 PM. Copy on file with Sarah Jane Hughes. Ms. Lyons also directs attention to the term “Digital entity data model” in ITU-T Recommendation X. 1255 at § 7.1, which focuses on “[t]he essential fixed attribute of a DE is its associated unique persistent identifier” This, she explains, is “an evolution in the technology of the early Internet where IP addresses resolve to ports on machines.” Patrice A. Lyons, email to Sarah Jane Hughes, June 11, 2019 4:10 PM. Copy on file with Sarah Jane Hughes. Ms. Lyons is affiliated with the Corporation for National Research Initiatives (CNRI) in Reston, VA. For further, highly useful analysis, see Patrice A. Lyons and Robert E. Kahn, *Blocks as digital entries: A standards perspective*, in NFAIS Conference: Blockchain for Scholarly Publishing (Bonnie Lawlor, ed.), 38 J. Inform. Servs. & Use, 173-185 (2018), <https://content.iopress.com.443/journals/information-services-and-use>.

⁵ See Peter A. Wayner, HANDBOOK OF OPTICAL PROPERTIES: DIGITAL CASH: COMMERCE ON THE NET, 2 (AP Professional 1997).

⁶ Carla L. Reyes, *If Rockefeller Were a Coder*, 87 GEO. WASH. L. REV. 373, 379-380 & n. 21 & 28 (2019) [hereinafter “Reyes 2019”]. For additional background, see Carla L. Reyes, *Conceptualizing Crypto Law*, 96 NEB. L. REV. 384, 390-91 (2017).

⁷ See Artemis Caro, BLOCKCHAIN: THE BEGINNERS GUIDE TO UNDERSTANDING THE TECHNOLOGY BEHIND BITCOIN & CRYPTOCURRENCY 12 (Cryptonaire Press, 2018).

different locations simultaneously.”⁸ And a distributed ledger theoretically is auditable, verifiable, and transparent.

A. Distinctions Between “Permissioned” and “Permission-less” Blockchains

A matrix of blockchains would reveal several options: public and less public “permission-less” blockchains and permissioned blockchains. It is important to differentiate these forms of blockchains for a variety of reasons.

1. *Public, permission-less blockchains*

In a public, permission-less blockchain, such as Bitcoin or Ethereum, all participants are theoretically equal.⁹ There is no centralized management or authority that can be required by law to report data or keep a set of records prescribed by a government other than those inherent to their business model, or even any central authority to respond to legal process. The exception to this “equality” principle is that some participants play key roles in validating transactions on the blockchain, including “miners” of bitcoins who perform verification and validation functions but are not known to all participants. (The subject of the unknowable validators of public, permission-less blockchains is discussed by Professor Angela Walch in the paper she presented at the May 2019 “Smart Regulation” Public Policy Conference, which at the time was entitled “Intermediaries Who Must Not Be Named? The Keepers of the Public Blockchain.”¹⁰)

Transactions on public blockchains are all open-to-view and relatable to each other in a chain. They are time-stamped. One can follow a chain of transfers from the first entry to the latest entry in time, and to ascribe to the last entry the status of being the “owner” or custodian of the related crypto assets at that time. It also is possible to follow transfers from one address to another by comparing the relative lengths of the chains with similar initial addresses to the current “owner” or custodian. My co-panelist, Peter A. Wayner, demonstrated how the public can follow transactions at the “Smart Regulation” Public Policy Conference.

2. *Public, permissioned blockchains*

A public, permissioned blockchain is a category under which EOS and Ripple belong. Some participants in this category of blockchain are more equal than others.¹¹ The network appoints certain participants to be privileged over others.¹² These participants can run the node, and they have abilities not shared by the general public.¹³ Key features of these blockchains is the ability of the privileged participants to keep certain records. For this reason, privilege holders on these networks might be required to report specific types of records of customers and transactions or to respond to legal process.

⁸ See *id.*, at 12.

⁹ See Arnold Daniels, “The rise of private permissionless blockchains-part 1, October 18, 2018, <https://medium.com/ltoneetwork/the-rise-of-private-blockchains-part-1-4c39bea2e2be> (hereinafter “Daniels”).

¹⁰ Angela Walch, *Intermediaries Who Must Not Be Named? The Keepers of the Public Blockchain*, draft paper presented at the Public Policy Conference on Smart Regulation and the Future of Financial Services Regulation, Antonin Scalia Law School, George Mason University, May 16, 2019. Copy available from Professor Walsh, at awalsh@stmarytx.edu.

¹¹ *Id.*

¹² *Id.*

¹³ *Id.*

A public, permissioned blockchain is one source of future public records systems, such as those for recording ownership of tangible property or providing public notice of security-interest claims.

The third and fourth categories are private blockchains, which are not the focus of this essay. The discussion below, accordingly, is for completeness of description.

3. *Private, permission-less blockchains*

A private, permission-less blockchain has nodes that “will only acknowledge [other nodes’ existence], but not share any data” with them to this point in time.¹⁴

One attraction of the private, permission-less blockchains is that each “smart contract” that may be used “*automatically creates a private (side-) chain associated with that contract.*”¹⁵ In addition, although a node may hold more than one “side-chain,” one node will not hold all of those in existence for the larger chain.

Each node still operates as a repository.¹⁶ Only designated persons or organizations get permission to read specific nodes; designated persons will require cryptographic signatures to gain access to reading.¹⁷ To have reading privileges, one needs both the unique identifier (address) and the URL of the node that has a copy of the smart contract and associated chain.¹⁸ Also, each node will hold only data needed to service its users – an “agent-centric” solution.¹⁹ These chains inside private chains make the task of ferreting out specific transactions more complicated because they are not visible.

These blockchains represent more powerful opportunities to hide assets because “smart contracts on these private networks, not only define who is allowed to perform contract actions but also who is allowed to read the contract and all related data.”²⁰ First, the “smart contract” manages any contract actions required and created by this node, making it an ideal “location” from which to move those assets in the intermediate “layering” steps needed for traditional money laundering. Owners of crypto assets on private, permission-less blockchains are not likely to spend them outside a narrow sphere of prospective counterparties. This narrow sphere of prospective counterparties and the restrictions on permissions help protect the identities of users of these blockchains.

Experimentation with private, permission-less blockchains has been limited so far. As of October 2018, one commentator, Arnold Daniels, had identified only three chains – the Holochain, LTO Network, and Monet. Holochain allows “users share information peer-to-peer on a need-to-know basis.”²¹ The LTO Network is Daniels’ own project: it “run[s] trustless workflows, targeting multinationals and governments.... The process has a strong focus on privacy and GDPR compliance.”²² The last, as of February 2019, is Monet. Monet may be the most likely to be used to hide proceeds of financial crimes: it allows users to build “ad-hoc, short-lived chains, with mobile devices acting as nodes for the

¹⁴See *id.* at 2.

¹⁵ *Id.* (emphasis original).

¹⁶ *Id.*

¹⁷ See *id.*

¹⁸ See *id.*

¹⁹ See *id.* at 2-3.

²⁰ *Id.*

²¹ *Id.* at 3.

²² *Id.*

participants.”²³ Other crypto assets are in development that will enhance privacy protections for users.²⁴

Private, permission-less blockchains share features with a cluster of “burn phones” or “bearer” instruments -- each facilitating the placement, layering or re-emergence of the assets or transactions involved. Daniels’ observations cemented this image: “Collaborations are fluid as both participants come and go and nodes may be discovered based on location.”²⁵ Private, permission-less blockchains offer a lava-lamp-like fluidity of opportunity, a nearly perpetual series of opportunities to share data with only those with a need-to-know for a phase or a part of a part of a transfer or storage of assets. These blockchains certainly appear to be more powerful potential tools for money launderers than any bearer bond or other bearer instrument – based outsiders at least know who the issuer of the instrument is because that party is named in the instrument. This does not mean that all private, permission-less blockchains are designed for nefarious purposes. It means that they bear watching as they develop.

4. Private, permissioned blockchains

The last category is a private, permissioned blockchain. This category includes examples such as include Hyperledger Fabric and the Enterprise Ethereum Alliance.²⁶ How do these systems handle permissions? We look again to “smart contracts,” which “do define permissions.”²⁷ Using a private, permission-less network drives some of the activity to a private “side-chain” – one associated with a “smart contract,” in particular.²⁸

This private, permissioned category both enables assets to be moved when a pre-established event coded at inception of a relationship or series of transactions triggers the next phase of the transaction and to be stored in an environment in which it likely will be harder for an outsider to observe them, but that allows the assets to be moved via “smart contracts” and transfer onwards. Accordingly, this fourth category – like the third – creates new opportunities to use blockchains and “smart contracts” to transact financial crimes or launder assets to emergence in “clean” form on pre-established timetables or the occurrence of the prescribed event. Will these transactions be observable in the open at all? It seems that they are not intended to be.

However, as I discuss later, when it comes time to exchange the assets for tangible assets or bank credits, the legacy entities – my “gatekeepers” -- that laws here and elsewhere currently requires to know-their-customers, maintain records, and report certain types of transactions—will face civil and criminal liabilities if they do not comply with applicable legal requirements.

Permissioned blockchains are not the focus of this essay, however. The requirement of permission to use these blockchains takes them out of the scope of the assignment that Professors Vartanian and Ledig asked me to undertake. Where “permission” is required, a key feature of other blockchains – their lack of centralized management of the technology and the records that contributes

²³ *Id.*

²⁴ Peter Van Valkenburg, conversation with Sarah Jane Hughes, May 17, 2019. No transcript of this conversation is available.

²⁵ *Id.* at 4.

²⁶ *Id.* at 2.

²⁷ *Id.*

²⁸ *Id.*

to trust and integrity of records – is not present. Private, permissioned blockchains also offer opportunities to replace current databases of records, including those created and managed by banks and securities firms.

B. Special Issues Raised by Government-sponsored Cryptocurrencies

Governments such as the Russia Federation have spoken publicly of their intentions to create “official cryptocurrencies.”²⁹ Russia’s announced purpose is to thwart economic sanctions imposed on Russian organizations and citizens.³⁰

It is unclear whether governments such as Russia that sponsor cryptocurrencies will use their sovereign rights to deem their sponsored cryptocurrencies as “legal tender,” the legal means to pay taxes and debts.³¹ If not, this cryptocurrency might operate only as an external currency, not for domestic purposes, such as China’s current, external-only version of the yuan or renminbi, referred to as the CYH.³² It also is unclear whether owners of Russia’s cryptocurrency will be allowed to exchange it for rubles, Russia’s legal tender.

Russia and China also have indicated their plans to issue gold-backed cryptocurrencies for their own internal or external-trade reasons.³³ Another goal is to replace the US Dollar as the world’s reserve currency.³⁴ Russia’s has used cryptocurrencies such as the Venezuela-government owned Petro,³⁵ itself

²⁹ See Rachel McIntosh, *Oil-Backed Cryptocurrency Could Hit Russian Markets Soon*, FINANCEMAGNETS.COM (February 25, 2019 8:48 GMT+1), <https://www.financemagnates.com/cryptocurrency/news/oil-backed-cryptocurrency-could-hit-russian-markets-soon/>.

³⁰ See Helen Partz, *Russia’s Central Bank to Consider Gold-Backed Cryptocurrencies for Mutual Settlements*, COINTELEGRAPH.COM, May 23, 2019, <https://cointelegraph.com/news/russias-central-bank-to-consider-gold-backed-cryptocurrencies-for-mutual-settlements> (citing Elvira Nabiullina, head of the Russia Central Bank, giving testimony before the Duma).

³¹ The Case of Mixed Money in Ireland, Trin. 2 James I. a.d. 1605 (Davies’s Reports) (upholding the sovereign’s authority to make, change or debase its money as well as its designation of “mixed money” as legal tender for payments of taxes and debts; establishing a value that some of the governed found to their disadvantage; and clarifying that the definition of legal tender is “the stamp, the prince, and the value”). For a recent discussion of methods that the U.S. has used to thwart competition to the dollar, see Stephen T. Middlebrook and Sarah Jane Hughes, *Substitutes for Legal Tender: Lessons from History for the Regulation of Virtual Currencies*, in RESEARCH HANDBOOK ON ELECTRONIC COMMERCE LAW, Edward Elgar, 2016, Paper 316, Indiana Legal Studies Research Papers, https://papers.ssrn.com/sol3/cf_dev/AbsByAuth.cfm?per-id=408848.

³² Jeremy Cook, *Why does China have two currencies?* at 1 (March 14, 2018), <https://www.worldfirst.com/uk/blog/international-business/foreign-exchange-international-business/china-two-currencies/>.

³³ See Daniel Palmer, *Russian Central Bank to Consider Gold-Backed Cryptocurrency*, INDESK.COM, MAY 23, 2019 14:30 UTC, <https://www.coindesk.com/russian-central-bank-to-consider-gold-backed-cryptocurrency>; Sean Adl-Tabatabai, *Russia and China Roll Out 100% Gold-Backed Currency*, March 25, 2018, <https://newspunch.com/russia-china-gold-backed-currency/>.

³⁴ *Id.*

³⁵ See Sujha Sundararajan, *Venezuelan President announces oil-backed cryptocurrency*, COINDESK.COM (December 4, 2017 4:15 UTC, updated 8:14 UTC), <https://www.coindesk.com/venezuelan-president-announces-petro-oil-backed-cryptocurrency>.

on the U.S. Treasury Department's SDN list,³⁶ to help Venezuela evade U.S. economic sanctions,³⁷ or to assist Russia's operations in Crimea,³⁸ suggest the scope of this threat.

Cryptocurrencies, given the speed at which transfers can be settled compared with legacy bank transfers, also enhance risks associated with rapid movements of values from nation to nation and could contribute to broader instability in world markets and national economies. Use of crypto assets to avoid national securities regulatory regimes or to engage in market manipulation is also worrisome.³⁹

However, depending on the location of the owners of these Russian or Chinese cryptocurrencies, the opportunity to locate assets and trace beneficial ownership may still exist. When the owners seek to move this wealth into more stable financial systems in Europe or Asia than those from which they come, they are likely to require services of one or more "gatekeeper" intermediaries subject to the "Four R's." For example, investigations of Danske Bank and Deutsche Bank reveal that Russian oligarchs using banks in Estonia, Denmark, and elsewhere have transferred wealth to more stable banking systems and onwards to invest in real estate and other assets.⁴⁰ Movement of funds into more stable financial systems in the EU, Canada or the United States are examples of safety-seeking and the "emergence" or integration that is the last stage of money laundering.

III. Background on Money Laundering Methods

³⁶ President Donald J. Trump, , Executive Order 13827 of March 19, 2018, Taking Additional Steps to Address the Situation in Venezuela, March 19, 2018, <https://www.whitehouse.gov/presidential-actions/executive-order-taking-additional-steps-address-situation-venezuela/> [hereinafter "Executive Order 13827-Venezuela"]. For additional discussion, see Nikhilesh De, *Trump orders new sanctions against Venezuela's crypto*, WWW.CONDESK.COM (March 19, 2018 17:00 UTC, updated March 20, 2018 8:59 UTC), <https://www.coindesk.com/trump-orders-new-sanctions-against-venezuelas-national-cryptocurrency>.

³⁷ See Simon Shuster, *Exclusive: Russia Secretly Helped Venezuela Launch a Cryptocurrency to Evade U.S. Sanctions*, TIME.COM, March 20, 2018, <https://time.com/5206835/exclusive-russia-petro-venezuela-cryptocurrency/> (describing the Petro as a "joint venture" between Venezuela and Russia to avoid U.S. sanctions and describing a September 2017 white paper explaining how cryptocurrencies could "overcome the dominance of Western currencies" and displace the U.S. Dollar).

³⁸ Helen Partz, *Adviser to President of Russia Proposes Digital Currency in Crimea*, COINTELEGRAPH.COM (April 22, 2019), <https://cointelegraph.com/news/adviser-to-president-of-russia-proposes-digital-currency-in-crimea> (quoting Sergey Glazyev who opined that the cryptocurrency was to reduce "cross-border barriers" and attract foreign investors who "are afraid of sanctions").

³⁹ See generally, Lawrence J. Trautman & George P. Michaely, *The SEC & The Internet: Regulating the Web of Deceit*, 68 CONSUMER FIN. L. Q. REP. 262 (2014), <http://www.ssrn.com/abstract=1951148>.

⁴⁰ See Richard Milne and Daniel Winter, *Danske: anatomy of a money laundering scandal*, FIN.TIMES.COM (DEC. 19, 2018), <https://www.ft.com/content/519ad6ae-bcd8-11e8-94b2-17176fbf93f5> (mentioning Bank of America and JPMorgan Chase and reporting events from 2007 until 2015; JPMorgan Chase apparently exited correspondent banking for the Estonia branch in 2013 for dollar-denominated transactions, citing concerns with non-resident customers of the branch) [hereinafter "Milne and Winter"]; See Bradley Hope, Patricia Kowsmann, and Drew Hinshaw, *U.S. Probes Danish Bank Over Russia Money Flows*, WALL ST. J. at A8 (Sept. 15-16, 2018) (reporting that the SEC received a confidential whistleblower complaint about Danske Bank AS' involvement in laundering of \$150 billion through accounts of non-Estonian account holders at a tiny Danske Bank branch in Estonia, and implicating Deutsche Bank and Citigroup with transactions into and out of the Estonian branch) [hereinafter "Hope, Kowsmann, and Hinshaw"]. Both articles reveal how lax internal anti-money-laundering controls and management attitudes contributed to the duration of the behavior being investigated.

Money laundering is “the concealment of the existence, nature or illegal source of illicit funds in such a manner that the funds appear legitimate if discovered.”⁴¹ The deterrence-and-detection legal requirements and enforcement tools are aimed at three stages used to complete the laundering of funds and at the persons, enterprises, and methods involved:

- placement, “in which illicit proceeds are introduced into the financial system;”
- layering “in which the criminal attempts to separate the proceeds from the crime through a series of transactions”; and
- integration “where the illicit funds re-enter the economy disguised as legitimate funds.”⁴²

For any reader less familiar with these steps in money laundering, this Part includes a brief discussion of each stage. This essay also uses publicly available reports on the current probe of Danske Bank AS to demonstrate how these traditional means facilitate money laundering in a scandal in which other major international banks, including Deutsche Bank, Citigroup, Bank of America, and JPMorgan Chase may be implicated.⁴³

A. Placement of Funds or Assets into Vehicles That Enable Layering

The first task of money launderers, regardless of their reasons for seeking to obscure the origin of funds or assets, is to find a location or an asset in which to “place” them, initially -- preferably into a form of account or property that can be moved along quickly, repeatedly, and securely into the first “layering” transaction, described in the next section. Traditional choices for initial placements have included banks, broker-dealers in securities, insurance brokers, and a host of sellers of tangible property including real estate, motor vehicles, boats, jewelry, and art.

In the United States we apply the requirements mentioned in the first paragraph of this Part to most of the providers mentioned here, but the specific “customer identification” requirements of Section 326 of the USA Patriot Act⁴⁴ depend in some respects on the provider or seller chosen.

⁴¹ Statement of Michael J. Murphy, Senior Deputy Commissioner, Internal Revenue Service, *Business Community’s Compliance with Federal Money Laundering Statutes: Hearing Before the Subcomm. on Oversight of the House Comm. On Ways and Means*, 101st Cong., 2d Sess. 142 (1990).

⁴² U.S. Dep’t of Treasury, National Money Laundering Risk Assessment, at 2 n.1 (2015), <https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Money%20Laundering%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf> [hereinafter “NMLRA 2015”]. Note: the 2015 report does not address risks presented by virtual currencies or blockchain-based activity. See *id.* at 22-85 (discussion of specific financial and commercial activity used in money laundering). The Department also issues a U.S. Terrorist Financing Risk Assessment periodically.

⁴³ See Milne and Winter, *supra* note 40; Hope, Kowsmann, and Hinshar, *supra* note 40. Both articles reveal how lax internal anti-money-laundering controls and management attitudes contributed to the duration of the behavior being investigated. Both articles reveal how lax internal anti-money-laundering controls and management attitudes contributed to the duration of the behavior being investigated.

For additional discussion, see text accompanying note 40, *supra*, and notes 53-55, *infra*.

⁴⁴ The Uniting and Strengthening America by Providing Appropriate Tools required to Intercept and Obstruct Terrorism, tit. III (the International Money Laundering abatement and Anti-Terrorist Financing Act of 2001), Pub. L. 107-56, 107th Cong., 1st Sess. (October 26, 2001) (codified in various titles of the United States Code).

Nearly adult in the United States will have had to prove their identity when they seek to open a new account since the USA Patriot Act⁴⁵ became effective. This is true regardless of whether the “financial institution” at which they were seeking to open the account or obtain a loan or other financial service for the first time was an account at a bank, a nonbank financial services provider, a broker-dealer, or an insurance company.

If the person opening the account or conducting a transaction presents \$10,000 or more in cash, then US law requires that the recipient financial institution report that transaction to the Financial Crimes Enforcement Network (“FinCEN”) if the recipient is a bank or credit union, or a broker-dealer, or a dealer in precious metals, gemstones, or jewelry.⁴⁶ If the amount is less than \$10,000, a report might be required if (a) one or more transactions related to each other occurs in a brief period or in a “related transaction,”⁴⁷ (b) the customer made repeated transactions of smaller amounts that the recipient believes are intended to avoid the \$10,000 or more threshold and suggest that “structuring” to avoid being reported,⁴⁸ or (c) the buyer uses certain monetary instruments with face amounts of \$3,000 or more.⁴⁹ Such transactions also could be deemed “suspicious,” giving rise to obligations to file “Suspicious Activity Reports.”⁵⁰ “Persons engaged in trades or business” in the United States also must report transactions with customers in a \$10,000 or more-threshold basis with reports going to the Internal Revenue Service.⁵¹

Similar requirements do not exist in all countries. The U.S. Department of Treasury and FinCEN, and other intergovernmental organizations, publish reports on countries whose anti-money-laundering measures are perceived to be weaker than our requirements.⁵² Person seeking to obscure the origin of funds or assets or the beneficial ownership of those funds or assets traditionally may see benefit in making initial “placements” in banks or other intermediaries occur in a country with weaker customer-identification/account-opening, record-keeping, or transaction-reporting requirements.

Some entities involved in “placement” or “layering” outside of the United States are still subject to U.S laws because they are regulated by U.S. regulators. This was true in the investigation that led to the settlement with Rabobank National Association, a California-based subsidiary of Cooperative Rabobank, U.A. in the Netherlands, for engaging in money laundering.⁵³ This is true in the pending investigation of Danske Bank, as well as of Deutsche Bank and Citigroup offices abroad are regulated by

⁴⁵ 31 C.F.R. Part 1010 (2018).

⁴⁶ *Id.*

⁴⁷ 31 U.S.C. § 5318(g) (2018).

⁴⁸ *Id.*

⁴⁹ *Id.*

⁵⁰ *Id.*

⁵¹ 26 U.S.C. § 6050I (cash transaction reporting by persons engaged in a trade or business). For compliance information relating to this statute, see Internal Revenue Service, Form 8300, <https://www.irs.gov/pub/irs-pdf/f8300.pdf> (last updated Dec. 2018).

⁵² See, e.g., NMLRA 2015, *supra* note 16.

⁵³ U.S. Dept. of Justice, Press Release, *Rabobank NA Pleads Guilty, Agrees to Pay Over \$360 Million (February 7, 2018)*, <https://www.justice.gov> (guilty plea included conspiracy to defraud the United States, obstruction of examination of a financial institution, and concealing deficiencies in its AML program, which included taking “hundreds of millions of dollars in untraceable cash” into its branches in California, and later transferring them via wire transfers, checks, and cash without proper identification).

U.S. regulators.⁵⁴ Funds apparently given over to the Estonian branch of Danske Bank by non-Estonian customers of the branch and later moved into or from that branch in transactions involving dollar-denominated wire transfers handled by Deutsche Bank or in transactions from Citigroup's Moscow office to the Estonia branch of Danske Bank.⁵⁵

For cryptocurrencies, the source of "customer identification" requirements depends on whether there is a central manager of the currency or a service provider and whether that person qualifies as a "money service business" subject to FinCEN's registration requirements.⁵⁶ New York State's Department of Financial Services requires the holders of BitLicenses to record and maintain records of their customers.⁵⁷ The Uniform Regulation of Virtual-Currency Businesses Act ("URVCBA"), not yet enacted in any state, requires that licensees and registrants keep records of their customers and their customers' transactions.⁵⁸

B. "Layering" assets through multiple transfers or forms of property, banks, or banking systems

"Layering" is the stage during which funds or assets move away from their original placements toward the eventual, integration as clean money, bank credits, or other clean assets that money launderers' clients seek.

More than 20 years ago, the United States Department of the Treasury considered wire transfers to be "the arteries of the international financial system," and proclaimed that "use of wire transfers is a necessity for many large scale [sic] money laundering schemes. Wire transfers are used both to move funds out of (or into) the United States and to confuse the money trail."⁵⁹ Multiple wire transfers were used to repatriate to the United States funds originally derived from illicit drug sales in the United States but shipped or carried abroad and "placed" in banks there.⁶⁰ The value that these wire transfers represented would move through banks with offices in New York, for example, and then possibly move on inside the United States or wherever else the owner wished to have the funds available with the appearance of legitimacy in their ownership.

⁵⁴ Hope, Kowsmann, and Hinshaw, *supra* note 40.

⁵⁵ *Id.*

⁵⁶ 31 C.F.R. § 1010.

⁵⁷ 23 NYCRR § 200.12 (2015) (specifying "books and records" to be created and maintained by BitLicense holders).

⁵⁸ Uniform Law Comm'n, Uniform Regulation of Virtual-Currency Businesses Act, § 302 (2017), www.uniformlaws.org ("registrants" have alerted specific state regulators that they are engaging in "virtual-currency business activity" in their state but have volumes of business of less than \$35,000 annually; as they reach the dollar threshold, registrants must apply for licenses and may continue to do business in that state unless their application is denied). As noted in the Author's Note, I served as Reporter for this project.

⁵⁹ U.S. Dep't of Treasury, Press Release, The Treasury Department released two final rules Thursday that will for the first time require uniform recordkeeping for wire transfers under the Bank Secrecy Act (BSA), Dec. 22, 1994, <https://www.fincen.gov/news-releases/treasury-department-released-two-final-rules-thursday-will-first-time-require>.

⁶⁰ U.S. Dep't of Treasury, Bank Secrecy Act Regulations Relating to Recordkeeping for Funds Transfers by Banks and Transmittals of Funds by Other Financial Institutions, 54 Fed. Reg. 45,769 (Oct. 31, 1989) (proposed rule for international wire transfers or transmittals).

The Treasury Department originally proposed in 1990 to extend its Bank Secrecy Act record-keeping to domestic wire transfers and funds transmittals.⁶¹ This proposal specifically included among the non-bank transmitters to be covered currency exchanges, telegraph companies, and registered securities broker-dealers.⁶² The department eventually promulgated in 1994 an enhanced recordkeeping requirement for bank and nonbank financial institutions handling funds transfers and funds transmittals in amounts of \$3,000 or more.⁶³

A second proposed rule would require the “financial institution” to capture information about the originator or sender⁶⁴ of the first wire transfer in a sequence and keep that information “traveling along” through as many layers of wire transfers as happened until the funds arrived in the beneficiary’s bank.⁶⁵ This proposal had to overcome opposition based in the fact that the formats used for wire transfers at that time had limited “fields” for information, and the habit was only to pass along the information needed by the originating bank to reach the next bank in the sequence until the last “payment order”⁶⁶ in the wire transfer that ended with the beneficiary’s bank, and ultimately to reach the beneficiary. This effort culminated with what is known as “the travel rule” that required that the originator’s information flow through the payment orders to the end of the funds transfer or funds transmittal.⁶⁷

Similar regulations require maintenance of records in domestic funds transfers,⁶⁸ and for banks and nonbanks to maintain records of international funds transfers and transmittals of funds.⁶⁹ FinCEN’s “Travel Rule,” which applies only to funds transfers of \$3,000 or more and to the extent that a bank or “money transmitter” is involved does not apply to all cryptocurrency transactions. Still, because of a September 2010 amendment, the Travel Rule reaches many cross-border electronic transmittals of funds “denominated in any currency,”⁷⁰ and can serve as a powerful tool for law enforcement agencies

⁶¹ U.S. Dept’ of Treasury, Proposed Amendment to the Bank Secrecy Act Regulations Relating to Recordkeeping for Funds Transfers by Banks and Transmittals of Funds by Other Financial Institutions, 55 Fed. Reg. 41,696 (Oct. 15, 1990).

⁶² *Id.* at 41,704 (to be codified at 31 C.F.R. § 103.33(f), the precursor to current 31 C.F.R. § 1010.330).

⁶³ 12 C.F.R. Part 219 (2018) (Threshold for the Requirement to Collect, Retain, and Transmit Information on Funds Transfers and Transmittals of Funds) (Board of Governors of the Fed. Reserve System version of this regulation). For more information see, Fin. Crimes Enf. Net., Threshold for the Requirement to Collect, retain, and Transmit Information on Funds Transfers and Transmittals of Funds, 60 Fed. Reg. 220-21 (Jan. 3, 1995).

⁶⁴ 12 U.S.C. § 1829b(b)(3) (defining “funds transfer,” “originator,” “beneficiary,” and “payment order” for provisions related to banks, and “transmittal of funds” to include a funds transfer and the non-bank transmittal). For more information, see 31 C.F.R. §103.11(jj).

⁶⁵ Fin. Crimes Enf. Network, 60 Fed. Reg. 23401 (Jan. 3, 1995) (this rule was codified originally at 31 C.F.R. § 103.33(g)). FinCEN and the Board of Governors of the Federal Reserve System jointly promulgated a separate rule known colloquially as the “Funds Transfer Rule,” codified originally at 31 C.F.R. § 103.33(e) recordkeeping requirements for banks), 31 C.F.R. § 103.33(f) (recordkeeping for nonbank financial institutions).

⁶⁶ See Sarah Jane Hughes, *Policing Money Laundering Through Fund Transfers: A Critique of Regulation Under the Bank Secrecy Act*, 67 IND. L. J. 283 (1992) (describing how “payment orders” are comprised and how the combine to constitute a “funds transfer” on an end-to-end basis).

⁶⁷ 31 C.F.R. 31 C.F.R. § 1010 (2018) (definitions) (originally codified at 31 C.F.R. § 103.33(g)).

⁶⁸ 12 U.S.C. § 1829b(B)(2) (2018) (bank and nonbank financial institutions required to maintain records on transmittals of funds); 31 C.F.R. § 1010 (originally codified at 31 C.F.R. § 103.11(jj)).

⁶⁹ 12 U.S.C. § 1829b(b)(3) (2018).

⁷⁰ U.S. Dept. of Treasury, Financial Crimes Enforcement Network; Cross-Border Electronic Transmittals of Funds, 75 Fed. Reg. 60377, 60396 (September 2010), (including definitions originally codified at 103.14).

and regulators to observe the movements of funds through regulated “Four R’s” entities. These tools were useful in identifying funds flows, for example, from the Russian Federation and Estonia, that a whistleblower used to alert the Securities and Exchange Commission.⁷¹

C. Emergence of Funds or Assets in Forms That Look Legitimate or that Arrive

In the final phase of money laundering -- integration, funds finally emerge as funds or real or tangible assets that look legitimate to those around them. This is the goal of the cadres of bank and non-bank and other professionals that aid in the process.

Integration or emergence is the step that may leave the federal government’s focus on regulated entities as a viable tool in a blockchain-based future. This will be the case as long as money launderers and their clients will need to rely on regulated entities as they have in the past to use some proceeds in the mainstream economy.

IV. **Challenges and Opportunities that Cryptocurrencies or Other Crypto-Assets Present to Current AML Efforts and Remedies Currently Available to U.S. Law Enforcement Irrelevant**

Professors Vartanian and Ledig asked the interesting question -- whether permission-less blockchains will render AML detection and enforcement laws and protocols inadequate. *My answer to this question is “no” – or at least “not yet.”* Although most of the Bank Secrecy Act and FinCEN’s regulations enforcing the former’s many provisions have been focused on providers against whom the “Four R’s” were designed to work, at least for the immediate future those regulated providers will continue to be important to detection of money laundering through cryptocurrencies and other crypto assets. That information that FinCEN already requires these providers to have and to report can be augmented by reconstructions from public blockchains. Part of the reason for my answer is that many cryptocurrency transactions are not as anonymous as previously thought.⁷²

To evaluate why existing regulatory tools will remain useful, we should review what has happened since 2013 when, as described above, FinCEN published its first guidance on which cryptocurrency functions constituted “money services” and, accordingly, whose providers should register with FinCEN as “money services businesses.” Following that review, we need to look at specific requirements in force that serve AML deterrence, detection and enforcement purposes – assuming law enforcement agencies have suitable resources going forward. This Part also describes other tools available to detect money laundering through permission-less blockchains.

A. FinCEN’s Baseline Guidance on Administrators of and Exchanges dealing in “Convertible” Virtual Currencies as Subject to its “Money Services Businesses” Regulations

FinCEN’s March 2013 guidance on virtual currency⁷³ issued by a central management and third-party providers that offer comparable intermediary services to owners of cryptocurrencies expanded

⁷¹ Hope, Kowsmann, and Hinshaw, *supra* note 40.

⁷² See Emerging Tehcnology from the arXiv, *Bitcoin Transactions Aren’t as Anonymous as Everyone Hoped*, MIT TECH. REV. 1 (August 23, 2017), <https://www.technologyreview.com/s/608716/bitcoin-transactions-arent-as-anonymous-as-everyone-hoped/>.

⁷³ Fin. Crimes Enf. Net., U.S. Dep’t of Treasury, “Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN-2013-G001, at 1 (March 18, 2013), www.fincen.gov [hereinafter “FinCEN March 2013 Guidance”].

FinCEN's 2011 "prepaid access" provider regulations⁷⁴ to reach many products and providers in the cryptocurrency industry. The perimeter captured many provider-intermediaries of related products and services and required that they register with FinCEN as "money services businesses,"⁷⁵ even if no state law required them to be licensed as "money transmitters." Additionally, as noted above, FinCEN's customer-identification-program and "Travel Rule" requirements attached to these provider-intermediaries. Thus, for providers of convertible virtual currencies who do business in the United States, FinCEN's 2013 Guidance expanded the ability of regulators to oversee issuers, administrators, distributors, acceptors, transmitters and exchangers.⁷⁶

"Prepaid access" transactions, in turn, are subject to FinCEN's 2011 rules on anti-money-laundering compliance requirements.⁷⁷ The 2011 final rule imposed on persons offering "prepaid access" five types of duties – registration with FinCEN,⁷⁸ record-creation and keeping and reporting requirements,⁷⁹ anti-money-laundering compliance program creation and implementation,⁸⁰ currency-transaction reporting,⁸¹ and suspicious-activity reporting.⁸²

Failure to comply with the requirements FinCEN has imposed on prepaid access transactions include the array of AML criminal sanctions.⁸³ Failure to register as a "money services business" ("MSB") subjects the entity to prosecution under 18 U.S.C. § 1960, which penalizes MSBs that (1) fail to register themselves with FinCEN, (2) engage in unlicensed activity that state law prohibits to those not holding the appropriate license(s), or (3) knowingly receive the proceeds of illicit activity.⁸⁴ It is important to note that the first and second circumstances defined in Section 1960 are strict-liability, non-scienter criminal offenses for which courts impose substantial monetary penalties and prison sentences. Only the third is a scienter-based crime. Accordingly, participation or being and not intent is not required to establish liability.

The regulatory perimeter that FinCEN created in 2013 did not reach permission-less, public blockchains such as Bitcoin because it has no central management.⁸⁵ As a result, permission-less, blockchain-based transactions offer a competing avenue for moving value, including currency positions,

⁷⁴ Fin. Crimes Enf. Network, Bank Secrecy Act Regulations -Definitions and Other Regulations Relating to Prepaid Access, 76 Fed. Reg. 45403 (July 29, 2011) (renaming "stored value" as "prepaid access" and defining the term, imposing suspicious activity reporting, customer information and transaction information recordkeeping requirements on providers as well as sellers of prepaid access, requiring registration with FinCEN of providers, and exempting categories of prepaid access products and services "posing lower risks of money laundering and terrorist financing" from some requirements). The rule went into effect on September 27, 2011 with full compliance with 31 C.F.R. § 1022.380 required by January 29, 2012. *Id.* at 45403.

⁷⁵ 31 U.S.C. § 5330 (2018).

⁷⁶ FinCEN 2013 Guidance, *supra* note 73, at 1.

⁷⁷ 2011 Prepaid Access Regulations, *supra* note 60.

⁷⁸ 31 C.F.R. § 1022.380 (2018).

⁷⁹ 31 C.F.R. § 1022.420 (2018).

⁸⁰ 31 C.F.R. § 1022.210 (2018).

⁸¹ 31 C.F.R. § 1022.420 (2018).

⁸² See 31 C.F.R. § 1020.320 (2018) (requirements for banks, securities broker-dealers, and others).

⁸³ 31 C.F.R. § 1022.420 (2018).

⁸⁴ *Id.*

⁸⁵ *Id.*

outside of the regulatory perimeter previously established by FinCEN. These transactions also offer speedy and inexpensive, cross-border transactions⁸⁶ for trade and remittance purposes.

FinCEN has not yet extended its 2013 “prepaid access” guidance to transactions on permission-less blockchains where no intermediary is involved. As a result, there are no requirements enforced by the United States Treasury Department for permission-less blockchains *per se* or the individuals who participate in their consensus mechanisms to verify transfers in the United States to be registered as “money services businesses,” to keep records, to implement anti-money-laundering compliance programs, or to report “suspicious transactions” to the authorities.

Because of FinCEN’s designation of “money services businesses” to include persons administering or exchanging virtual currencies that can be converted to fiat currencies,⁸⁷ and the requirement of registration with FinCEN mentioned above, the failure of persons administering or offering exchange services operating inside the United States to register triggers criminal liability under 18 U.S.C. § 1960. Because permission-less blockchains often have no administrators within the scope of FIN-2013-G001, there may be no “person” with sufficient power over the blockchain governments can require to submit themselves to the Four R’s style requirements. This is one of the few features of public, permission-less blockchain technologies that Congress or Treasury might seek to address.

Unlike “wire transfers” and some other non-bank electronic transfers after Treasury’s “Travel Rule” became effective, blockchain-based transactions do not show information identifying the counter-parties (senders or recipients).⁸⁸ Transactions may take place on a peer-to-peer (“P2P”) basis with no traditional intermediary involved⁸⁹ or from one location to a recipient’s “personal wallet or another type of recipient unable to accept identifying information.”⁹⁰ In these environments, transactions may be used to obscure the identities to transactions through anonymity or pseudonymity, but reconstruction is possible, as noted above. To the extent a person subject to FinCEN’s 2013 Guidance is involved, that person’s separate customer-identification and record-keeping compliance obligations should be available to identify transaction participants in many current cryptocurrency offerings.

Blockchain-based transactions have been used for illicit transactions. Examples include the notorious dark-web bazaar for narcotics and weapons known as “Silk Road,” whose founder, Ross William Ulbricht, was identified, arrested and convicted of money laundering, using the pseudonymity of bitcoins.⁹¹ In 2018, Treasury’s Office of Foreign Assets Control (“OFAC”) identified two Iranian

⁸⁶ See Jeffrey Gogo, *Crypto-Based Transfers Can Cut Remittance Costs in Africa by 90%*, BITCOIN.COM (April 23, 2019), <https://news.bitcoin.com/crypto-based-transfers-can-cut-remittance-costs-in-africa-by-90/> (describing relative fees in percentages of dollars sent to Africa through banks and crypto systems); see also, *Bitcoin is Now Moving 11% of Venmo’s Yearly Total in One Day*, BITCOINIST.COM (April 11, 2019) (describing advantages in Bitcoin’s “scaling solutions” as causes of “headaches” for competitors).

⁸⁷ FinCEN 2013 Guidance, *supra* note 73, at 1-3 (“users” are exempt from “money services business” registration requirements under this guidance).

⁸⁸ See “‘Onerous’ FATF recommendations Harmful for Crypto Transparency: Chainalysis,” COINDESK.COM (April 12, 2019), <https://www.coindesk.com/chainalysis-onerous-fatf-recommendations-harmful-for-crypto-transparency> (commenting that the addresses used do not contain identification information and lack the capacity to carry it).

⁸⁹ Nakamoto, *supra* note 11, at 1.

⁹⁰ *Id.*

⁹¹ Sam Thielman, *Silk Road operator Ross Ulbricht sentenced to life in prison*, TheGuardian.com (May 29, 2015, 21.02 BST) (and imposition of a double-life sentence).

intermediaries by name who were laundering proceeds from the Sam-Sam ransomware attacks and placed them and their blockchain addresses on OFAC's "Specially Designated Nationals" list.⁹²

Cryptocurrency proponents note the value of public blockchains to help trace and reconstruct the value transfers and to identify the individuals involved.⁹³ The author of the Bitcoin white paper, Satoshi Nakamoto, hailed the ability of blockchains to enable transactions to be associated with others – by working back through the chain to the shortest entry on the chain and or identifying the transfers of assets in forward or reverse sequence as the length of the addresses lengthens or shortens, respectively.⁹⁴

B. The United States Has Other Tools to Deter and Help Detect Money Laundering Through Permission-less Blockchain-Based Transactions

The United States imposes a variety of obligations on depository institutions and a broad array of non-depository financial services providers designated as "financial institutions" collectively by the Bank Secrecy Act, including amendments since 1970, and by the USA Patriot Act of 2001.⁹⁵ The obligations include (1) establishment, monitoring, personnel training and re-retaining and revision of risk-based anti-money-laundering compliance programs required by Section 352 of the USA Patriot Act,⁹⁶ (2) transaction-record-keeping-and-retention requirements,⁹⁷ (3) threshold-based transaction reporting,⁹⁸ including "suspicious-activity" reports,⁹⁹ (4) requirements for customer-identification or beneficial ownership information to be obtained at account opening,¹⁰⁰ (5) rules prohibiting having "shell companies" as customers of banks,¹⁰¹ (6) special rules for certain correspondent-banking

⁹² U.S. Dep't. of Treasury, "Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses," Nov. 28, 2018, <https://home.treasury.gov/news/press-releases/sm556> (describing both actions taken against two Iranians, naming the Iranians, listing the individuals as "specially designated nationals," and warning individuals dealing with two Bitcoin addresses associated with these two "facilitators" that they might be subject to secondary sanctions for violations of OFAC regulations and Executive Orders) [hereinafter "Treasury Action Identifying Bitcoin Addresses"]. For more discussion of Treasury's action, see Alastair Marsh, *U.S. Exposes Bitcoin Addresses of Sanctioned Iranians*, BLOOMBERG.COM (Nov. 28, 2018, 1:10 PM EST), <https://www.bloomberg.com/news/articles/2018-11-28/u-s-exposes-bitcoin-users-addresses-in-iran-cyber-sanctions>.

⁹³ Jonathan Levin and Jesse Spiro, Chainalysis Letter to Secretariat, Financial Action Task Force, April 8, 2019, http://go.chainalysis.com/rs/503-FAP-074/images/Chainalysis_Input_7b_Public_Statement.pdf?mkt_tok=eyJpIjoiWW1abU1HVTF0VFPsT0RdyIsInQiOiIyRUIOcHE1c3NOTeHWRzArVW9uVWw4OGdTUSTYTXNDNVNRazRkTHFhMFBNMFPjbmNyRW1ha25ucplVms0RUNKdIwvTIZ0bWxFOGV0WDN1OHhPZm9mdTVPQjJmb2JHR09BRzFaR1UxNHU2dFhGdEQ4bUltZFh1UnJlMEJFYXErck0ifQ%3D%3D (offering comments on Interpretive Note to Recommendation 15, particularly paragraph 7(b) from a company that provides "commercial blockchain intelligence software" to "map blockchain transactions to real world entities") [hereinafter "Levin and Spiro"].

⁹⁴ See Nakamoto, *supra* note 3, at 2-3 (timestamp server and proof-of-work).

⁹⁵ 31 U.S.C. § 5318 (2018).

⁹⁶ 31 U.S.C. § 5318(h) (2018) (broker-dealers, banks, and others required to institute risk-based anti-money-laundering programs).

⁹⁷ 31 C.F.R. § 1022 (2018).

⁹⁸ 31 U.S.C. § 5318 (2018).

⁹⁹ 31 U.S.C. § 5318(g)(4) (2018) (requirements extend to broker-dealers as well).

¹⁰⁰ 31 U.S.C. § 5318(l) (2018) (provision designated "Verification and Identification of Customers").

¹⁰¹ 31 U.S.C. § 5318 (2018).

relationships,¹⁰² and (7) special rules for cross-border transmittals of funds.¹⁰³ These requirements apply to “money service businesses” and broker-dealers as well as banks.¹⁰⁴ Whistleblower complaints augment these record-and-reporting regimes.¹⁰⁵ The Supreme Court held that the Bank Secrecy Act was constitutional in a landmark decision in *California Bankers Association v. Shultz*,¹⁰⁶ with specific reasoning that Congress legally could delegate rulemaking authority to the Secretary of the Treasury for purposes encompassed by the original version of the Bank Secrecy Act.

In addition, under the wide-ranging statutes, Executive Orders, and regulations enforced by the Office of Asset Controls (“OFAC”) in the Department of the Treasury, “U.S. persons” are prohibited from doing business with entities and individuals on the OFAC’s published “Specially Designated Nationals” (“SDN”) list.¹⁰⁷ The prohibition applies unless an exemption exists or the U.S. person obtains a license specifically permitting the business or relationship to occur.

Section 311 of the USA Patriot Act¹⁰⁸ is among the most powerful tool for deterrence of money laundering. The Director of the Department of the Treasury’s Financial Crimes Enforcement Network (“FinCEN”) also has authority through a process including notice-and-comment rulemaking to designate jurisdictions of major money laundering concern¹⁰⁹ – with the result that specific entities will be banned from access to the U.S. financial system.¹¹⁰ These powers and practices have snared global banks, some in more than one investigation.¹¹¹

Remedies that may be imposed for violations include asset freezes and forfeitures, criminal penalties on individuals and organizations, designations of individuals, organizations, government

¹⁰² 31 U.S.C. § 5318(i)(2) (2018).

¹⁰³ 31 U.S.C. § 5318(n) (2018).

¹⁰⁴ 31 U.S.C. § 5318 (2018).

¹⁰⁵ See Bradley Hope, Patricia Kowsmann, and Drew Hinshaw, *supra* n. 40. Other reports put the amount that moved through the Estonian branch as high as \$234 billion. Frances Coppola, *The Banks That Helped Danske Bank Estonia Launder Russian Money*, FORBES.COM (Sept. 30, 2018, 5:42 pm) (also reporting that “much of the money was paid in U.S. dollars, ... and [the bank] needed help from other banks. Banks that had access to Fedwire).

¹⁰⁶ 416 U.S. 21 (1974) For a fascinating call for blockchain businesses to challenge to the constitutionality of the Bank Secrecy Act from a blockchain enthusiast, see Caitlin Long, *Supreme Court and Digital Privacy: Should Blockchain Companies Challenge the Bank Secrecy Act*, FORBES.COM (June 28, 2018 1:25 PM), <https://www.forbes.com/sites/caitlinlong/2018/06/28/supreme-court-and-digital-privacy-should-blockchain-companies-challenge-the-bank-secrecy-act/#4ee4bf0562fc> Ms. Long’s challenge is based on recent Fourth Amendment decisions by the Court. If Ms. Long proved to challenge the constitutionality of the BSA facially or as applied and prevailed, some of the conclusions in this essay could need revisiting.

¹⁰⁷ U.S. Dept. of Treasury, Office of Foreign Asset Controls, *Specially Designated Nationals and Blocked Persons List (SDN)*, (updated to April 26, 2019), www.treasury.gov/pages (list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries, or who are narcotics “kingpins”).

¹⁰⁸ 31 U.S.C. § 5318A (Special Measures for Jurisdictions, financial institutions, international transactions, or types of accounts of primary money laundering concern), Pub.L. 107-56, title III, § 311(a), Oct. 26, 2001, 115 Stat. 298.

¹⁰⁹ 31 U.S.C. § 5318A (2018),

¹¹⁰ *E.g.*, U.S. Dept. of Treasury, Fin. Crimes Enf. Network, *Imposition of Special Measures Against FBME Bank Ltd., Formerly Known as the Federal Bank of the Middle East Ltd., as a Financial Institution of Primary Money Laundering Concern*, 80 Fed. Reg. 45057 (July 29, 2015) (notice of finding and imposition of special measures using FinCEN’s authority under 31 C.F.R. Part 1010 against a bank with offices in Tanzania and Cyprus with alleged ties to Russia).

¹¹¹ *E.g.*, Standard Chartered Bank, HSBC, and others.

agencies, and property (particularly vessels) as prohibited for “U.S. persons” to engage with, and, using Section 311, loss of access to U.S. financial systems.¹¹²

Since Congress passed the Annunzio-Wylie Anti-Money Laundering Act of 1992,¹¹³ anti-money-laundering compliance requirements have increased significantly. Some of these new tools apply to banks and non-bank financial institutions, including some nonbank actors such as “money services businesses.”¹¹⁴ Others require record-keeping and threshold-based transaction reporting by persons engaged in trades or business,¹¹⁵ such as sellers of motor vehicles and luxury goods. FinCEN has issued guidance on the application to cryptocurrency products and industry participants since March 2013¹¹⁶ and working with other federal agencies has brought most of the enforcement actions since 2013 described in Subpart D of this Part and in the enforcement actions appendix to this essay.

These AML tools may seem old-fashioned in their reliance on information provided by financial intermediaries to ferret out money launderers and new methods. However, the Panama Papers¹¹⁷ and Paradise Papers¹¹⁸ investigations demonstrate that they remain powerful tools, for example, enabling New York State’s Department of Financial Services to demand from banks it supervises information on shell companies, customers, and transactions.¹¹⁹

C. Internal Revenue Service Guidance

¹¹² 31 U.S.C. § 5318A (2018).

¹¹³ 12 U.S.C. § 1829b(b)(2) (2018).

¹¹⁴ See 31 C.F.R. Parts 1010 (definitions of seller of prepaid access and “money services businesses”) and 1022 (rules for “Money Services Businesses”) (2018) [hereinafter “2011 Prepaid Access Regulations”]. For additional information on this 2011 final rule, see U.S. Dep’t of Treas., Fin/ Crimes Enf. Net., Bank Secrecy Act Regulations – Definitions and Other Regulations relating to Prepaid Access, 76 Fed. Reg. 45403 (July 29, 2011).

¹¹⁵ 26 U.S.C. § 6050I (2018) (requiring records of the receipt of cash or currency of \$10,000 or more in one or more “related transactions” in a calendar year, annual notices to customers whose use of cash exceeds the threshold, and annual reports to the U.S. Internal Revenue Service of personally identifiable information pertaining to those customers and of transaction details). Note that this requirement is codified in the revenue title, not the Bank Secrecy Act title of the U.S. Code. There is some overlap between the title 26 USC provisions and the title 31 USC provisions. For example, jewelers have record-keeping responsibilities to enable them to make title 26 reports and notices, and also to have title 31 anti-money-laundering compliance and customer-identification programs in place and up-to-date.

¹¹⁶ FinCEN March 2013 Guidance, *supra*, note 73, *passim*].

¹¹⁷ See Luke Harding, *What are the Panama Papers? A guide to history’s biggest data leak*, THEGUARDIAN.COM (April 5, 2016 10:42 BST), www.theguardian.com (reporting on a data breach affecting 11.5 million files from the offices of the world’s biggest offshore law firm, Mossack Fonseca, that highlighted the range of activities, assets, and identities of its clients, including those of government leaders in Russia, Pakistan, Ukraine, and Iceland, among others, leaked to investigative reporters).

¹¹⁸ Nick Hopkins and Helena Bengtsson, *What are the Paradise Papers and what do they tell us*, THEGUARDIAN.COM (November 5, 2017 18:00 GMT), www.theguardian.com (describing the leak of 13.4 million files, 6.8 million of which relate to Appleby, a law firm in Bermuda now called Estera, from 1993 to 2014 that detailed money flows into offshore centers on behalf of an exclusive clientele from the United States, United Kingdom, Hong Kong and China, also leaked to investigative journalists).

¹¹⁹ <https://www.icij.org/investigations/panama-papers/20160420-ny-banks-regulator/>.

In addition to FinCEN's regulations and guidance documents, the U.S. Internal Revenue Service declared in 2014 that virtual currencies were "property" not "currency."¹²⁰ This decision exposed virtual currency transactions to "capital gains" taxation under U.S. tax laws. Thus, persons who own virtual currencies and securities, for example, would have to report and pay tax on any gains they received on the later sale or use of the cryptocurrencies in transactions. IRS' position means that users of virtual currencies will need to track their bases in virtual currencies and the timing of transactions and ownership transfers. Records needed to mitigate capital gains liabilities should assist the IRS and law enforcement to the extent allowed by law.

D. U.S. Enforcement Actions before and after FinCEN's March 2013 Guidance

The final source of regulatory action is represented by enforcement actions. A handful of these actions illustrate the current capacity of U.S.-based law enforcement agencies and financial regulators to deal with cryptocurrency industry participants who are not licensed, not registered with FinCEN, or are name brands that had inadequate AML compliance programs. The online presence of many of the defendants in U.S. enforcement actions made their detection more likely, which is a benefit of public, permission-less blockchains. Currently, many blockchain-based transactions are, as Satoshi Nakamoto described them, open to view and traceable on the blockchain even if the parties – or the embedded "smart contracts" executing pre-arranged exchanges -- are anonymous or pseudonymous. The prospects that transactions may be executed via "smart contracts" following the occurrence of a predetermined, coded event or that more private cryptocurrencies, however, will make it more difficult to regulate them for many purposes.

To illustrate the array of law enforcement actions brought by the United States, Appendix 1 to this essay contains examples that demonstrate that law enforcement agencies have been able to detect the use of blockchain-based technologies by entities with weak AML compliance programs or entities accused to have engaged directly in money laundering. The examples in Appendix 1 show a range: they are (1) not all criminal actions, (2) not all federal actions, (3) not presented in chronological order, and (4) not presented in terms of the dollar amounts involved. The examples used in Appendix 1 are here primarily to help readers assess the types of activity that attracted law enforcement agencies' attention and the enforcement approaches being used. There is no explanation of how law enforcement agencies identified the targets or defendants: for such inside information, one needs a security clearance that I do not possess.

V. Cryptocurrency and Permission-less Blockchains Are Not the Major Issue in Tracing Placement and Laying of Illicit Proceeds – Locating the Entity to Regulate Is

As law enforcement agencies and financial regulators have succeeded in limiting access by money launderers to banks and other types of established financial services providers, the concern has been that professional money launderers will shift their efforts to other methods. These professionals may turn or already are turning to cryptocurrency and permission-less blockchain transactions for these

¹²⁰ Int. Rev. Serv., Notice 2014-21, Frequently Asked Questions (March 25, 2014), <https://www.irs.gov/pub/irs-drop>.

purposes.¹²¹ This part looks at the steps that money-laundering professionals take to launder money, the additional opportunities that permission-less blockchains offer these professionals and their clients and some barriers to ultimate movement away from all-blockchain, no-intermediary-involved commerce in goods or services, and tools that regulators and law enforcement agencies employ. Among the tools that U.S. regulators and law enforcement agencies have available is USA Patriot Act Section 311,¹²² available to deal with jurisdictions and actors that present special money-laundering concerns, which this Part also discusses.

A. Placement of Value

In the United States, we regulate those providers that can receive “deposits” of money as banks or credit unions, and those that can receive funds for prompt transmittal to others as “money transmitters” or “money services businesses.” States regulate the non-depository providers operating as “money transmitters” or “money services businesses.”¹²³ Bank regulators in two states recently opined that receiving cryptocurrencies as opposed to “fiat currency”¹²⁴ or “sovereign currency”¹²⁵ is not “money transmission” because the value being received is not “money.”¹²⁶ The guidance issued by Texas’ Banking Department, however, takes the position that “stable coins” such as Tether – cryptocurrencies issued by centralized entities with values pegged to and at least theoretically supported by designated fiat currencies¹²⁷ – as being within the definition of “money”¹²⁸ and, thus, confirmed that they are subject to licensure and prudential regulation in Texas.¹²⁹

Unlike bank deposits, cash, and monetary instruments whose use and flows through the hands of entities subject to the “Four 4’s,” once proceeds come in cryptocurrencies or are placed into cryptocurrencies, the ownership is harder to trace than the movements along permission-less blockchains. However, when the owner or controller of the cryptocurrency or other blockchain-based asset wants to convert it to fiat currency or use it to acquire other assets whose acquisition requires assistance from a “Four 4’s” regulated entity, the reason is that the persons using permission-less blockchains may not be subject to know-your-customer compliance, record-keeping, or threshold-based transaction reporting, including suspicious-activity reporting. Efforts to extend these AML and CTF

¹²¹ For additional information about prior cryptocurrencies and issues related to some of the more notorious, see Lawrence J. Trautman, *Virtual Currencies: Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox?*, 20 RICHMOND J.L. & TECH. 13 (2014), <http://www.ssrn.com/abstract=2393537>.

¹²² 31 U.S.C. § 5318A (2018).

¹²³ *E.g.*, Texas Finance Code Chapter 151 (2018).

¹²⁴ Texas Dept. of Banking, Supervisory Memorandum 1037, at 3 (January 2, 2019, revised April 1, 2019), <https://www.dob.texas.gov> (providing an excellent explanation of its reasoning why cryptocurrencies other than stable coins are not “money”) [hereinafter “Texas Supervisory Memorandum”]; Pennsylvania Dept. of Banking and Securities, “Money Transmitter Act Guidance for Virtual Currency Businesses,” at 1 (January 25, 2019), <https://www.dobs.pa.gov/Pages> (differentiating “money transmitters” subject to licensure from most virtual currency exchange platforms, kiosks, ATM, or vending machines) [hereinafter “Pennsylvania Revised Supervisory Guidance for Virtual Currency Businesses”].

¹²⁵ Texas Supervisory Memorandum, *supra* note 122, at 2 (explaining that sovereign-backed stable coins include rights allowing the coin holder to redeem the stable coin for for sovereign currency from the issuer).

¹²⁶ *E.g.*, Pennsylvania Revised Supervisory Guidance for Virtual Currency Businesses, *supra* note 122, at 1.

¹²⁷ Texas Supervisory Memorandum, *supra* note 122, at 2 (explaining that “one Tether coin is the equivalent value of one USD at all times”).

¹²⁸ *Id.*

¹²⁹ *Id.*

requirements to cryptocurrencies have begun – in the U.S., with FinCEN’s guidance since 2013, as described in Part IV, Section A of this essay, in New York State’s BitLicense regulations,¹³⁰ and under the EC’s AMLD5.¹³¹

B. Layering through Cryptocurrencies or Decentralized Ledgers

The speed at which transfers of value held in cryptocurrencies may occur and the degree of anonymity or pseudonymity users expect make permission-less blockchain transactions attractive means of “layering” illicit proceeds. Cryptocurrency transactions provide only pseudonymity.¹³² This pseudonymity “does not provide a user of blockchain technology with an absolute assurance that her identity will not be discovered” by “a determined party with access to certain information....”¹³³

We might perceive that it is easier to layer illicit proceeds through jurisdictions with stricter “bank secrecy” laws¹³⁴ than the U.S. or jurisdictions subject to the EU’s General Data Protection Regulation (“GDPR”) have.¹³⁵ A key feature of the GDPR, which went into effect in May 2018,¹³⁶ is the grant to individuals to have their personal data erased.¹³⁷ In contrast, a key feature of blockchain technologies is that there are no correction or deletion options.¹³⁸ Thus, the advantages of using certain weak-AML jurisdictions and blockchain technologies to layer illicit proceeds appear greater than they are likely to be in all jurisdictions.

C. Emergence of Layered Assets into Legitimate-Appearing Assets

The goal of placement and layering of illicit proceeds is to see them emerge as “clean assets.” Some of the methods that these professionals use were revealed when The Guardian and The New York Times, among other major newspapers, disclosed caches of transactions from the files of law firms in Panama and Bermuda, respectively known as “the Panama Papers”¹³⁹ and “the Paradise Papers.”¹⁴⁰

¹³⁰ 23 NYCRR Part 200, at § 200.15 (2015).

¹³¹ AMLD5, *supra* note 2.

¹³² See Christopher Escobedo Hart, *European Union: Blockchain and Data Privacy*, Foley Hoag Security, Privacy and the Law Blog, at 1, February 20, 2019, http://www.mondaq.com/article.asp?articleid=782988&email_access=on [hereinafter “Hart”].

¹³³ *Id.*

¹³⁴ See generally Lawrence J. Trautman, *Following the Money: Lessons from the “Panama Papers,” Part 1: Tip of the Iceberg*, 121 PENN. ST. L. REV. 807 (2017), <http://www.ssrn.com/abstract=2783503>.

¹³⁵ Eur. Comm’n, (EU) General Data Protection Regulation, https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en [hereinafter “GDPR Text”]. For more analysis, see <http://eugdpr.org>.

¹³⁶ *Id.*, at para. 53.

¹³⁷ *Id.* at Art. 17.

¹³⁸ See Hart, *supra* note 131, at 2.

¹³⁹ See Int’l Consortium of Investigative Journalists, *An ICIJ Investigation The Panama Papers: Exposing the Rogue Offshore Finance Industry, passim* (Jan. 31, 2017), <https://www.icij.org/investigations/panama-papers/> (a collection of separate reports focused on methods or individuals using the services of the defunct Panamanian law firm, Mossack Fonseca, to assist in hiding or protecting from taxes profits from many sources) [hereinafter “ICIJ Panama Papers Investigation”].

¹⁴⁰ See Int’l Consortium of Investigative Journalists, *An ICIJ Investigation Paradise Papers: Secrets of the Global Elite – The Long Twilight Struggle Against Offshore Secrecy, passim*, Nov. 5, 2017, <https://www.icij.org/investigations/paradise-papers/> (a collection of separate reports focused on persons using

These disclosures appear to have relied on whistleblowers, rather than original law enforcement investigations. The databases of records from each leak reveal a staggering global capacity to hide funds and other assets through placement and layering by professionals.¹⁴¹ There are no data of which I am aware that suggest what percentage may be conducted using some form of blockchain technology.

Where do permission-less blockchains fit into the three-stage schema employed by money-laundering professionals? Well, in many respects, they are available tools—but they are not yet fully operational for complete transformation into legitimate-appearing assets. Permission-less blockchains lack the centralized management or responsible parties that can be subjected to these “four R’s in themselves,” because the Four R’s regimes depend on having some personal or legal entity to regulate. However, in commerce, not all sellers of physical assets will accept cryptocurrencies or crypto assets for their goods or services. For this reason, unless we anticipate economies in which those who use permission-less blockchain transactions for the purpose of obscurity and never need access to fiat currency or current financial intermediaries to utilize or receive proceeds or other value transfers, we will not need to replace the Four R’s as central features of AML/CTF¹⁴² enforcement efforts.

D. OFAC’s Enforcement of U.S. Sanctions Laws and Executive Orders

OFAC designates nation states, commercial and financial organizations, such as banks, non-profit organizations and agencies of nation states, and individuals as persons with whom “U.S. persons” may not engage in any form of business and publishes lists of these “specially designated nationals.”¹⁴³

Of these tools for deterrence of involvement with perpetrators of money laundering, Section 311 of the USA Patriot Act¹⁴⁴ is among the most powerful. The Director of the Department of the Treasury’s Financial Crimes Enforcement Network (“FinCEN”) also has authority through a process including notice-and-comment rulemaking to designate jurisdictions of major money laundering concern¹⁴⁵ – with the result that specific entities will be banned from access to the U.S. financial system.¹⁴⁶ These powers and practices have snared global banks, some in more than one investigation.¹⁴⁷

services of the Bermudian law firm, Appleby, that reveal the offshoring habits of global elites) [hereinafter “ICI Paradise Papers”].

¹⁴¹ See Lawrence J. Trautman & Mason J. Molesky, *Bitcoin Versus Regulated Payment Systems: What Gives?* 38 CARDOZO L. REV. 1041, *passim* (2017), <http://ssrn.com/abstract=2730983>.

¹⁴² For ease of reference, the term AML in this essay will stand for all AML, CTF and anti-proliferation aspects that deal with the movements of proceeds or payments, including those related to economic sanctions imposed by the United States.

¹⁴³ U.S. Dept. of Treasury, Office of Foreign Asset Controls, *Specially Designated Nationals and Blocked Persons List (SDN)*, (updated to April 26, 2019), www.treasury.gov/pages (list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries, or who are narcotics “kingpins”).

¹⁴⁴ 31 U.S.C. § 5318A.

¹⁴⁵ *Id.*

¹⁴⁶ *E.g.*, U.S. Dept. of Treasury, Fin. Crimes Enf. Network, *Imposition of Special Measures Against FBME Bank Ltd., Formerly Known as the Federal Bank of the Middle East Ltd., as a Financial Institution of Primary Money Laundering Concern*, 80 Fed. Reg. 45057 (July 29, 2015) (notice of finding and imposition of special measures using FinCEN’s authority under 31 C.F.R. Part 1010 against a bank with offices in Tanzania and Cyprus with alleged ties to Russia).

¹⁴⁷ *E.g.*, Standard Chartered Bank, HSBC, and others.

Remedies that may be imposed for violations include asset freezes and forfeitures, criminal penalties on individuals and organizations, designations of individuals, organizations, government agencies, and property (particularly vessels) as prohibited for “U.S. persons” to engage with.

Since Congress passed the Annunzio-Wylie Anti-Money Laundering Act of 1992,¹⁴⁸ anti-money-laundering compliance requirements have increased significantly. Some of these new tools apply to banks and non-bank financial institutions, including some nonbank actors such as “money services businesses.”¹⁴⁹ Others require record-keeping and threshold-based transaction reporting by persons engaged in trades or business,¹⁵⁰ such as sellers of motor vehicles and luxury goods. FinCEN has issued guidance on the application to cryptocurrency products and industry participants since March 2013¹⁵¹ and working with other federal agencies has brought most of the enforcement actions since 2013 described in this part of this essay.

These AML tools may seem old-fashioned in their reliance on information provided by financial intermediaries to ferret out money launderers and new methods, but we found from the Panama Papers¹⁵² and Paradise Papers¹⁵³ investigations that they remain powerful tools, for example, enabling New York State’s Department of Financial Services to demand from banks it supervises information on shell companies, customers, and transactions.¹⁵⁴

E. Permission-less Blockchains Are Not the Major Issue in Tracing Placement and Laying of Illicit Proceeds – Identification of an Entity to Regulate Is

¹⁴⁸ 12 U.S.C. § 1829b(b)(2) (2018).

¹⁴⁹ See 31 C.F.R. Parts 1010 (definitions of seller of prepaid access and “money services businesses”) and 1022 (rules for “Money Services Businesses”) (2018) [hereinafter “2011 Prepaid Access Regulations”]. For additional information on this 2011 final rule, see U.S. Dep’t of Treas., Fin. Crimes Enf. Net., Bank Secrecy Act Regulations – Definitions and Other Regulations relating to Prepaid Access, 76 Fed. Reg. 45403 (July 29, 2011).

¹⁵⁰ 26 U.S.C. § 6050I (2018) (requiring records of the receipt of cash or currency of \$10,000 or more in one or more “related transactions” in a calendar year, annual notices to customers whose use of cash exceeds the threshold, and annual reports to the U.S. Internal Revenue Service of personally identifiable information pertaining to those customers and of transaction details). Note that this requirement is codified in the revenue title, not the Bank Secrecy Act title of the U.S. Code. There is some overlap between the title 26 USC provisions and the title 31 USC provisions. For example, jewelers have record-keeping responsibilities to enable them to make title 26 reports and notices, and also to have title 31 anti-money-laundering compliance and customer-identification programs in place and refreshed as any change in the business model, customers, or other risk factors may require.

¹⁵¹ Fin. Crimes Enf. Net., U.S. Dep’t of Treasury, “Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN-2013-G001, March 18, 2013, www.fincen.gov [hereinafter “FinCEN March 2013 Guidance”].

¹⁵² See Luke Harding, *What are the Panama Papers? A guide to history’s biggest data leak*, THEGUARDIAN.COM (April 5, 2016 10:42 BST), www.theguardian.com (reporting on a data breach affecting 11.5 million files from the offices of the world’s biggest offshore law firm, Mossack Fonseca, that highlighted the range of activities, assets, and identities of its clients, including those of government leaders in Russia, Pakistan, Ukraine, and Iceland, among others, leaked to investigative reporters).

¹⁵³ Nick Hopkins and Helena Bengtsson, *What are the Paradise Papers and what do they tell us*, THEGUARDIAN.COM (November 5, 2017 18:00 GMT), www.theguardian.com (describing the leak of 13.4 million files, 6.8 million of which relate to Appleby, a law firm in Bermuda now called Eterra, from 1993 to 2014 that detailed money flows into offshore centers on behalf of an exclusive clientele from the United States, United Kingdom, Hong Kong and China, also leaked to investigative journalists).

¹⁵⁴ <https://www.icij.org/investigations/panama-papers/20160420-ny-banks-regulator/>.

As law enforcement agencies and financial regulators have succeeded in limiting access by money launderers to banks and other types of regulated financial services providers, the concern has been that professional money launderers will shift their efforts to other methods. Among the obvious methods to which these professionals may turn or already are turning are cryptocurrency and permission-less blockchain transactions.¹⁵⁵

Many AML laws and international agreements and enforcement protocols rely on four legal cornerstones associated with traditional financial services “gatekeepers.” These four cornerstones are: registration (or licensure), regulation, record-keeping, and (transaction) reporting. This essay will refer to these four as “the Four Rs.” These four apply to regulated depository and non-depository providers of financial services. U.S. entities serving as financial services gatekeepers currently include banks, trust companies, credit unions, securities broker-dealers, money transmitters such as Western Union and other money services businesses. Some virtual-currency businesses are in this group themselves. Others, not yet subject to the Four Rs themselves, or their customers, likely will use services that gatekeepers provide when they seek to exchange virtual currency or other crypto or digital assets for fiat currency or need fiat currency to complete a transaction to purchase real- or digital-world goods or services.

VI. Global Anti-Money-Laundering Tools and Remedies; FATF’s 2018 and 2019 Guidance and Recommendations

This Part of this essay describes various global AML initiatives that have implications for cryptocurrencies and other crypto assets. These include policies developed by the Financial Action Task Force (“FATF”).

The FATF has defined “virtual currency” as:

Virtual currency is a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment in any jurisdiction. It is not issued or guaranteed by any jurisdiction, and fulfills the above functions only by agreement within the community of users of the virtual currency. Virtual currency is distinguished from **fiat currency** (a.k.a. “**real currency**,” “**real money**,” or “**national currency**”), which is the coin and paper money of a country that is designated as its legal tender; circulates; and is customarily used and accepted as a medium of exchange in the issuing country. It is distinct from **e-money**, which is a digital representation of fiat currency used to electronically transfer value denominated in fiat currency. E-money is a digital transfer mechanism to fiat currency – i.e., it electronically transfers value that has legal tender status. (bold font original; punctuation maintained; footnotes omitted)¹⁵⁶

¹⁵⁵ For additional information about prior cryptocurrencies and issues related to some of the more notorious problems with providers, see Lawrence J. Trautman, *Virtual Currencies: Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox?*, 20 RICHMOND J.L. & TECH. 13 (2014), <http://www.ssrn.com/abstract=2393537>.

¹⁵⁶ FATF, *Key Definitions and Potential AML/CTF Risks*, at 4 (2014), <http://www.fatf-gafi.org/publications/methodsandtrends/documents/virtual-currency-definitions-aml-cft-risk.html>.

Thus, if oil-backed or gold-backed, cryptocurrencies backed by sovereigns – Venezuela, Russia, or China – are deemed “legal tender” by their sponsors, they will cease to be “virtual currency” under FATF’s definition. However, they will become “property” subject to capital-gains-tax treatment under IRS’s 2014 guidance.¹⁵⁷

FATF has focused on enhancing global procedures for identifying and prosecuting persons and entities engaged in money laundering, terrorist finance, and weapons proliferation for some time. Over the past two years, FATF has amended its Recommendations including new provisions in its October 2018 amendments to Recommendation 15¹⁵⁸ and the February 2019 Draft Interpretive Note to FATF Recommendation 15,¹⁵⁹ and its February 2018 Guidance on Counter Proliferation Financing.¹⁶⁰ In April 2019, FATF published additional guidance on cryptocurrencies.¹⁶¹

FATF *should not abandon* efforts to obtain stronger detection and enforcement tools aimed at what this essay has called the “Four R’s” – registration or licensure, regulation, record-keeping, and transactional reporting – which are all features of its October 2018 Recommendations that urge member states to enact and use economic sanctions against persons committing or facilitating money laundering, terrorism finance, and WMD proliferation.¹⁶² These tools require a central management or responsible person or entity on which to focus this type of regulatory requirements – the very attributes that permission-less blockchains lack. Instead, FATF should continue to focus on entities already subject to the “Four R’s” to observe value flowing from public permission-less blockchains into the hands of regulated assets such as bank deposits, securities, commodities, or other tangible assets.

Demonstrating commitment to dealing with cryptocurrencies and intermediaries that those transferring cryptocurrencies to others or exchanging fiat currencies for cryptocurrencies or vice versa, in June 2019, FATF adopted and issued the February 2019 guidance mentioned above. This new guidance took the form of Interpretative Note to Recommendation 15 on New Technologies (also known as “INR. 15”). This Interpretative Note 15 is intended to bind FATF member nations and virtual currency asset providers (“VASPs”), as well as other entities that “engage in or provide virtual asset products and services,” to extend their AML/CTF “preventive measures” described under FATF

¹⁵⁷ See text accompanying and following note 119, *supra*. For additional perspective, see URVCBA, *supra* note 58, at § 103(a)(24) (relying on FATF’s definition, the URVCBA uses a similar method to distinguish between “virtual currency” and currency or foreign exchange). [Readers should recall my disclaimer that I served as the Reporter for this Uniform Law Commission project.]

¹⁵⁸ FATF Recommendation 15 October 2018, *supra* note 1.

¹⁵⁹ Fin. Action Task Force, Public Statement – Mitigating Risks from Virtual Assets, February 22, 2019, http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets-interpretive-note.html?mkt_tok=eyJpLjoiTm1Ka05EaGxaVEZqT1RJMSlInQioiKjVWV1JU1pwWEVGQmIGNXN3NXBzcitoMnh6VDFTY1hqXC9abUdhZGc4VXRYSERTNVA5XC94SXZWM1ZpWVZGRWpDRmgySVBFcUR5aXE4WVlk2ejBoRiJlOXdzRnJmamgzK0FtWDRrSStMTCs4Uyt5K3BnNVI4N3NHNNuVngxUXJ2dVZlIn0%3D (setting forth the specific recommendation and FATF’s interpretation of what they entail).

¹⁶⁰ Fin. Action Task Force, Guidance on Counter Proliferation Financing – The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction, 2018, www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-counter-proliferation-financing.html.

¹⁶¹ FATF April 2019 Recommendations, <https://www.fatf-gafi.org/fatf/publications/fatfgeneral>.

¹⁶² FATF 2018 Recommendations, *supra* note 159, *passim*.

Recommendations.¹⁶³ Among the “full range” of AML/CTF measures, FATF included in its June 2019 Interpretative Note 15 are:

... customer due diligence, record-keeping, suspicious transaction reporting, and screening all transactions for compliance with targeted financial sanctions, among other measures, just like other entities subject to AML/CTF regulation.¹⁶⁴

In addition, FATF’s full range of supervisory recommendations for nation state members includes ongoing risk-based assessments and mitigation of risks associated with virtual assets, licensure or registration requirements, and supervision or monitoring of VASP and other providers by “competent national authorities.”¹⁶⁵

Also, at its June 2019 Plenary Session, FATF published updated guidance entitled “Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers,” which FATF described as “building upon FATF’s ground-breaking 2015 guidance paper.”¹⁶⁶ The new guidance document may be found at fatf-gafi.org.

VII. Conclusions and Recommendations: Public Permission-less Blockchain Transactions Present New Challenges and Offer New Opportunities to Regulators and Law Enforcement Agencies

The themes I have used in this essay were aimed at finding ways to engage in “smart regulation,” as Professors Vartanian and Ledig framed their May 2019 Public Policy Conference. I have come to them though a longer journey than I expected when they first contacted me. Early on, I was concerned that public, permission-less blockchains and transactions recorded on them would damage AML efforts and enforcement tools that the United States and other nations with major money centers have enacted or implemented. Later, the fact that blockchains cannot be “corrected or erased” caused a change in my approach. I now view public permission-less blockchains as a valuable part of a robust AML enforcement toolkit, rather than an absolute obstacle to the achievement of AML goals.

This is not to say that domestic and global efforts of deterrence and detection will not need to be changed to meet new challenges arising from blockchain-based systems. This is likely, in part, because blockchain-based transactions are likely to displace traditional, centrally managed forms of value storage and execution of value transfers, with various depositories and transaction executors such as trust companies, safety-deposit companies, and banks or regulated/licensed non-bank providers of financial services. As these permission-less technologies continue to advance, they may enable value transfers more generally to move to spaces farther from the gatekeepers subject to the “Four R’s,” the term I have used in this essay to capture the four basic regulatory requirements that the United States, the European Union’s AMLD5, and FATF’s 2018 and 2019 Recommendations impose: regulation or licensure, regulation, record creation and maintenance requirements, and threshold-based transaction reporting, including of transactions that strike the provider or counter-party as “suspicious.”

¹⁶³ Fin. Action Task Force, Public Statement on Virtual Assets and Related Providers, at 1 (June 21, 2019), fatf-gafi.org [hereinafter “June 2019 FATF Public Statement”].

¹⁶⁴ *Id.* at 1.

¹⁶⁵ *Id.*

¹⁶⁶ *Id.*

This shift towards less transparent cryptocurrencies and away from longer-available cryptocurrencies that may be regulated similarly to legacy money transmitters can be seen in crypto products such as Monero.¹⁶⁷ Monero promises its users that its product is a “digital currency that is secure, private, and untraceable.”¹⁶⁸ Moreover, Monero advertises its crypto coins as “an obfuscated public ledger, meaning anybody can broadcast or send transactions, but no outside observer can tell the source, amount or destination.” Depending on how Monero is regulated—and under which government’s or governments’ authority it may be regulated—its product or service may fall into the second (low to low-middle level) or third (more serious) silos of concern I described at the outset of this essay. But it clearly signals that hybrid blockchains with some public and some private attributes will be in the marketplace and will require new AML approaches if they do not have a central administrator or offer services as “exchanges.”

The key observation in the last paragraph about Monero is the absence of the word “regulated.” In the U.S., if the provider is a “money services business” under FinCEN’s definition of that term, then specific AML requirements will be imposed on this provider and product and require it to obtain information from customers (in some states) and create and retain records of transactions. Thus, an outside may not “observe” the “source, amount, or destination,” but Monero will be accountable for having and keeping information about its customers and their transactions or instructions that Monero will execute on their behalf?

Public permission-less blockchains, in contrast, offer permanent, non-correctable, non-erasable records of transactions that are more *open to view*. Thus, these blockchains themselves may be seen as part of the toolkits that law enforcement authorities will use – rather than as an existential threat to law enforcement actions and governments’ AML priorities. Nevertheless, these blockchains operate without central managements on which to place the Four R’s requirements or to impose civil or criminal sanctions. In combination with newer investigatory methods, the integrity of blockchain-based transactions and the audit trails they rely on already offer much assistance to private entities including banks and securities firms to complete risk assessments on customers and fulfill their AML detection and deterrence responsibilities, and, based on the enforcement actions described in the appendix to this essay, to law enforcement agencies.

Recent actions against perpetrators of financial crimes and their facilitators suggest that governments show existing capacities to “follow the money” through cryptographic substitutes. Appendix 1 to this essay describes federal and state law enforcement actions addressing various types of crypto asset law violations. Two more recent actions by the federal government demonstrate that tools to “follow the money” are available to law enforcement agencies. The first of these actions is the late 2018 designation by OFAC of two Iranians that facilitated Sam-Sam ransomware-attack money laundering through bitcoins and, in a first, of the Iranians’ crypto-addresses as “specially designated nationals” list with whom “U.S. persons” are prohibited from dealing.¹⁶⁹

The second example of detection by law enforcement agencies in the United States involves the use of Executive Orders and implementing designations and regulations that the United States has used. These Executive Order 13827 of March 19, 2018 (“Executive Order 13827-Venezuela”) placing the “any

¹⁶⁷ <https://www.getmonero.org>.

¹⁶⁸ *Id.*

¹⁶⁹ See text accompanying note 92, *supra*.

digital currency, digital coin, or digital token, that was issued by, for, or on behalf of the Government of Venezuela on or after January 9, 2018, are prohibited as of the date of this order.”¹⁷⁰ Executive Order 13827-Venezuela demonstrates the same type of AML deterrence tool – ordering economic sanctions against a government and its cryptocurrency, prohibiting U.S. persons from transactions “related to, provid[ing] financing for, and other dealings in” digital currency, coins or tokens¹⁷¹ -- as OFAC used in the Sam-Sam ransomware case against the Iranians. In this case, the President can deny access to U.S. markets to cryptocurrencies whose purposes are declared “unlawful” by national legislatures such as Venezuela’s National Assembly.¹⁷²

It is important to think about the ramifications of actions such as that brought by Venezuela against the United States in the World Trade Organization for violations of the General Agreement on Tariffs and Trade of 1994 (“GATT”)¹⁷³ and General Agreement on Trade and Services (“GATS”) obligations in response to Executive Order 13827 and other actions taken.¹⁷⁴ Among other things, the Maduro Government charged that the United States is violating GATS Article II:1. That Article provides that no member will treat another member less favorably than any other nation.¹⁷⁵ Exceptions to WTO obligations arise if the member maintains that their actions relate to “essential security interests,”¹⁷⁶ and Executive Order 13827-Venezuela explicitly references a prior declaration of a national emergency by the United States against Venezuela in two Executive Orders, Executive Order 13692 of March 8, 2015¹⁷⁷ and Executive Order 13808 of August 24, 2017.¹⁷⁸

The Maduro government also complained that the United States was violating GATS Article XVII:1, which provides that member nations will not treat financial services and service suppliers of other nations less favorably than they treat similar providers in their own nations.¹⁷⁹ Although, as I note below, I plan to follow this action closely, at the moment the United States can make a strong argument based on the fact that this provision does not apply to government-sponsored currencies or securities. Rather, it protects private enterprises that provide financial services or who are “service providers.”

Additional economic sanctions offer tools more in the nature of foreign policy enforcement, rather than more traditional AML efforts. For example, since April 17, 2019, the Department of the

¹⁷⁰ Executive Order 13827-Venezuela, *supra* note 36.

¹⁷¹ *Id.*

¹⁷² *Id.*, at preamble.

¹⁷³ World Trade Organization, Final Agr. on Tariffs and Trade, 30 October 1947 (updated 1994) (applicable to trade in goods only) [hereinafter “GATT”]. For the 1994 updated agreement, see https://www.wto.org/english/docs_e/legal_e/ursum_e.htm#General.

¹⁷⁴ Complaint (filed Dec. 28, 2018). For more discussion of Venezuela’s complaint see Tom Miles, Venezuela launches WTO challenge to U.S. Sanctions, REUTERS.COM (Jan. 8, 2019 10:22 AM), <https://www.reuters.com/article/us-usa-venezuela-sanctions-wto/venezuela-launches-wto-challene-to-u-s-sanctions-idUSKCN1P21L6>.

¹⁷⁵ Gen. Agr. on Trade in Services, 33 I.L.M. 1167 (1994) [hereinafter “GATS”].

¹⁷⁶ GATT, Art. XXI (Security Exceptions), GATT-AI-2012-Art 21 at 599, https://www.wto.org/english/res_e/booksp_e/gatt_ai_e/art21_e.pdf. For discussion of how the WTO signatories expected Article 21 to be interpreted, see *Id.* at 600-608.

¹⁷⁷ President Barack Obama, Executive Order 13692 – Blocking Property and Suspending Entry of Certain Persons Contributing to the Situation in Venezuela, 80 Fed. Reg. 12747 (March 11, 2015).

¹⁷⁸ President Donald J. Trump, Executive Order 13808, 82 Fed. Reg. 41155 (August 29, 2017).

¹⁷⁹ GATT, *supra* note 172.

Treasury's Office of Foreign Assets Control has implemented additional sanctions relating to the Maduro government in Venezuela, or enterprises and individuals. Specifically, on April 17, OFAC added a designation of Banco Central de Venezuela pursuant to Executive Order 13850, as amended by Executive Order 13857, "for operating in the financial sector of the Venezuela economy."¹⁸⁰ OFAC also added Banco Central de Venezuela to its "Specially Designated Nationals" list and this addition makes any dealings with the Central Bank off-limits to all U.S. Persons unless OFAC issues a general or specific license allowing certain activities in the future.¹⁸¹ Citing Executive Order 13850, OFAC's designation also includes the Central Bank's SWIFT/BIC BCVEVECA, and Tax ID No. G200001100¹⁸² so that transactions with that SWIFT account or Tax ID Number also are prohibited in the absence of a license.

As nation states – particularly, the Russia Federation, China, and Venezuela – focus on issuing cryptocurrencies or tokens with the purpose of evading economic sanctions or of undermining the U.S. dollar's role in the global economy, we are likely to need new legal options. New legal options should go beyond the "Four R's" that I have described in this essay. These new options must be capable of being taken without violating nation states' obligations under international law or treaty obligations, but those obligations should not be interpreted as preventing legal remedies to thwart products or providers operating in my third silo, which includes fraudsters as well as rogue actors or rogue states. I plan to continue to work on how the United States might approach these state-sponsored cryptocurrencies.

Among the tools that might be ramped up to deter evasion of current or new AML/CTF efforts is the prospect that U.S. and other regulators will use their authority to send bad actors packing by imposition of special measures authorized by Section 311 of the USA Patriot Act and curtailing access by them to the payments systems in the United States and the trillions of USD of bank wire transfers and securities transactions managed by these payment systems on a daily basis.¹⁸³ Another (if seldom used) tool is the revocation of charters of U.S.-based banks, or of licenses by other non-bank providers who aid and abet placement, layering, and cleansing of domestic and global financial crimes, as current U.S. law allows for national banks.¹⁸⁴

¹⁸⁰ U.S. Dep't of Treas., Venezuela-related Designations; Issuance of Venezuela-related General Licenses, Issuance of Amended Venezuela-related General Licenses, and Publication of Venezuela-related Frequently Asked Question; Nicaragua-related Designations, April 17, 2019, <https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20190417.aspx>.

¹⁸¹ *Id.*

¹⁸² *Id.*

¹⁸³ Bd. of Gov. of the Fed. Res. Sys., Fedwire Funds Transfer -Monthly Statistics, updated through February 2019, <https://frbervices.org/resources/financial-services/wires/volume-value-stats/monthly-stats.html> (showing monthly statistics for transfers over Fedwire alone in the trillions of US dollars with the largest monthly volumes in 2018 of more than \$78 trillion USD).

¹⁸⁴ 12 U.S.C. § 93(d) (specifying process from the Department of Justice to the Office of the Comptroller of the Currency to consider revocation of charter revocation for depository institutions convicted of money laundering offenses). For discussion of one of the most recent calls for charter revocation, see *Public Citizen Calls on Comptroller of Currency to Revoke Rabobank Charter*, CORPORATECRIMEREPORTER.COM (Mar. 1, 2018 12:28 pm), <https://www.corporatecrimereporter.com/news/200/public-citizen-calls-for-comptroller-currency-revoke-rabobank-charter/> (call includes request to FDIC to terminate status as insured depository institution for Rabobank National Association, the U.S. affiliate of Rabobank, a Netherlands-based multinational financial conglomerate; Rabobank N.A.'s settlement of money-laundering charges for \$360 million avoided a conviction and, accordingly, avoided the mandatory referrals and hearings on revocation and termination, respectively, required of the Comptroller and FDIC under 12 U.S.C. § 93(d)).

Work by the United States, the EC, and FATF should continue to focus on known “high-risk money laundering jurisdictions” and to include jurisdictions that welcome blockchain-based businesses such as Malta or that permit blockchain businesses to operate with little accountability – those that do not impose licensure, regulation, record-keeping, or threshold-based reporting responsibilities. The European Commission’s February 13, 2019 “high-risk-jurisdiction” list -- those with lax AML regulations or enforcement.¹⁸⁵ FATF issued its recent list on February 22, 2019 and named 12 jurisdictions with “strategic deficiencies” in their AML/CFT programs – including The Bahamas, Botswana, Cambodia, Ethiopia, Ghana, Pakistan, Serbia, Sri Lanka, Syria, Trinidad and Tobago, Tunisia, and Yemen.¹⁸⁶ FATF issued a Public Statement (also on February 22, 2019) describing additional concerns.¹⁸⁷ FATF also issued an Interpretive Note on Recommendation 15 dealing specifically with virtual assets.¹⁸⁸

The following are some additional recommendations for new legal and cross-border collaborative steps that the U.S. and other nations might take, perhaps with particular focus on maintaining the Four R’s on the higher-risk products or providers I have assigned to the third silo, including:

- 1) retention by the U.S. of its current robust capacity and regulatory requirements to detect and deter global financial crimes and use by the providers and products in the third silo of U.S banking, securities, non-bank payment systems, and commodities trading capacities;
- 2) provision of appropriate resources for FinCEN, OFAC, and other law enforcement agencies including funding for artificial-intelligence tools and crypto-tracing-assets training;
- 3) retention by the U.S. of requirements for licensure as required by the States, and registration with FinCEN of certain providers of cryptocurrency services as “money services businesses;”
- 4) monitoring of stablecoins, which are “cryptocurrencies linked for pricing purposes to a real-world asset such as the United States Dollar”,¹⁸⁹

¹⁸⁵ E.g., https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/anti-money-laundering-and-counter-terrorist-financing_en (describing EC actions and policies to combat money laundering and terrorism finance); https://ec.europa.eu/info/files/commission-delegated-regulation-c-2019-1326-supplementing-directive-eu-2015-849-european-parliament-and-council-identifying-high-risk-third-countries-strategic-deficiencies_en (specifically designating jurisdictions of concern for lax anti-money-laundering or counter-terrorism-finance enforcement).

¹⁸⁶ Fin. Action Task Force, *Improving Global AML/CFT Compliance: On-going Progress – 22 February 2019*, 1 (Feb. 22, 2019), <http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/fatf-compliance-february-2019.html> (setting forth deficiencies in detail).

¹⁸⁷ Fin. Action Task Force, Public Statement – 22 February (February 22, 2019), <http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/public-statement-february-2019.html> (calling on members to apply measures to the Democratic People’s Republic of Korea and Iran).

¹⁸⁸ Fin. Action Task Force, Public Statement – Mitigating Risks from Virtual Assets (February 22, 2019), <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets-interpretive-note.html>.

¹⁸⁹ See *Crypto ‘stablecoins’ explained: What are they, how they work, and how they’re used*, WWW.BUSINESSINSIDER.COM (September 30, 2018).

- 5) supporting efforts by private operators of payments or payments-utilities systems such as SWIFT¹⁹⁰ to create more transparency for transactions using its telecommunications platform, including by using new technology to deliver unaltered remittance information when payments occur including a unique transaction “identifier” (the “UETR”), with trackable and traceable, end-to-end features and requirements that SWIFT participants commit to anti-crime compliance and security;
- 6) enhancing resources and legal tools available to foreign intelligence units – as the EC’s AMLD5 has proposed;¹⁹¹
- 7) granting explicit new statutory legal authority in the United States to require identification of owners of specified percentages of limited liability companies,¹⁹² including the beneficiaries of trusts,¹⁹³ and working with other governments that hold major financial centers and the United States’ major trading partners to do the same;¹⁹⁴
- 8) supporting new regulation like the EC’s new AMLD5¹⁹⁵ and prompt implementation of their requirements following enactment as the EC’s schedule for national enactments by January 10, 2020 requires;¹⁹⁶
- 9) using legal process in aid of criminal investigations across national borders via legal process directed at facilities globally and at cloud storage, as the U.S. achieved in its investigation of Liberty Reserve,¹⁹⁷ and German investigators achieved when they obtained documents held by law firms inside their jurisdiction;¹⁹⁸

¹⁹⁰ The acronym “SWIFT” stands for the Society of Worldwide Interbank Financial Telecommunications, which is headquartered in Belgium.

¹⁹¹ AMLD5, *supra* note 2.

¹⁹² Fin. Crimes Enf. Network, Customer Due Diligence Requirements for Financial Institutions, 81 Fed. Reg. 29398 (May 11, 2016) (codified at 31 C.F.R. Parts 1010 and 1024).

¹⁹³ AMLD5, *supra* note 2, at para. 27-35.

¹⁹⁴ See *e.g.*, Martha M. Hamilton and Will Fitzgibbon, *Swiss authorities propose major money-laundering law reforms*, ICIJ, June 11, 2018, <https://www.icij.org/investigations/panama-papers/swiss-authorities-propose-major-money-laundering-law-reforms/> (reforms include stricter fiduciary obligations on persons creating, managing or maintaining companies and trusts; disclosure of beneficial ownership; and establishment of a commercial registry). These steps, while important and uncommon for the privacy-strict Swiss, will not necessarily tackle permission-less blockchain activity as well as they may more traditional, bank-ledger-based activity.

¹⁹⁵ AMLD5, *supra* note 2, *passim*.

¹⁹⁶ *Id.* at para. 53.

¹⁹⁷ Declaration of Special Agent [redacted] in Support of Ex Parte Application for Post-Indictment Restraining Order, Seizure Warrant, and Injunction Pursuant to 21 U.S.C. § 853(e) and (f) ¶ 9, *United States v. Liberty reserve*, S.A., 13 Crim. 368 (S.D.N.Y. 2013), available at <http://goo.gl/ba29WV> (un-identified federal agent stated in an affidavit that investigative tools include “the first-ever ‘cloud’-based search warrants that had been directed to an Internet-service provider that Liberty Reserve had used to process the exchange’s Internet traffic.”). For additional discussion of the indictment of Liberty Reserve and the search warrants, see Sarah Jane Hughes and Stephen T. Middlebrook, “Virtual Uncertainty: Developments in the Law of Electronic Payments and Financial Services, 69 BUS. LAW. 263, 267-269 (2013).

¹⁹⁸ See Sarah Jane Hughes, *Above, Beyond and Around the ABA’s 2012 Model Rules of Professional Conduct: Growing On- and Off-shore and Low-Tech Challenges for U.S. Lawyers and Law Firms Using Cloud Computing*, in Lisa R. Lifshitz and John A. Rothchild, eds., *CLOUD 3.0: NEGOTIATING AND DRAFTING CLOUD COMPUTING AGREEMENTS*, (Am. Bar Ass’n., April, 2019) (describing different risks in using cloud storage and hard-copy storage in jurisdictions outside the United States, including access by German investigators to records of VW in the hands of Jones Day’s office in Munich, Germany).

- 10) deploying public-private partnerships to develop new tools to provide stronger end-of-end traceability of blockchain-based value transfers, such as the tracking solutions and AMK/KYC compliance tools being developed by commercial firms;¹⁹⁹
- 11) exploring methods to enjoin uses of cloud-based services, social media, or Internet Service Providers by blockchain-based enterprises that may be engaged in money laundering;²⁰⁰ and,
- 12) insisting that enterprises subject to the laws of the United States, European Union, and elsewhere comply with the Four R's continue to verify identify their customers; create and maintain records of owners/customers and of transactions, including initial coin offerings and coin/token trading in secondary markets, and strict compliance with U.S. requirements enforced by OFAC.

The ability of the United States and its major trading partners that host major money markets to contain money laundering will become more important as explained by Professor Eswar S. Prasad of Cornell University and the Brookings Institution at the point at which “decentralized nonofficial cryptocurrencies ... start playing a bigger role as mediums of exchange.”²⁰¹ This likelihood—that I cannot yet call an inevitability—makes reliance on enterprises or individuals subject to the Four R's even more important to future AML deterrence and detection.

To the extent that regulators and law enforcement agencies can continue to improve their investigatory tools, with proper funding, data from public permission-less blockchains will be valuable assets in AML detection and deterrence. Additionally, because traditional financial intermediaries such as banks, broker-dealers, and other regulated financial services providers will continue to be involved when the beneficiaries of illicit transactions want access to fiat currencies or traditional transaction-execution services from currently regulated entities, public permission-less blockchain transactions will not be the only sources of information available. To this end, we will need more widespread adoption of FATF's Recommendation, including those issued in April 2019, and robust enforcement of AML laws by G-20 members. Among the tools needed will be AML investigatory and enforcement authority where not currently in place, such as for the European Banking Authority (“EBA”).²⁰² We also need to be mindful of the costs of the compliance responsibilities that the gatekeepers I have described already bear.

As we proceed, I urge that Congress, regulatory agencies, law enforcement agencies, and others differentiate among the challenges presented by blockchain technologies generally (at the low end of concern from my perspective at this point), by crypto products and services including cryptocurrencies and tokens offered by entities in compliance with domestic laws where they do business (in the low-to-

¹⁹⁹ E.g., CipherTrace, Blockchain Security, Crypto AML Solutions, www.ciphertrace.com/AML/Solutions; Marie Huillet, *CipherTrace Detects Major Uptick in Cross-Border Payments to Offshore Crypto Exchanges*, COINTELEGRAPH.COM (April 29, 2019), www.cointelegraph.com.

²⁰⁰ Clarifying Lawful Use of Overseas Data Act, Pub. L. 115-141, 115th Cong., 2d Sess. (2018) (amending, among other things, section 2523 of the Wiretap Act codified 18 U.S.C. § 2523; known as the “CLOUD Act”).

²⁰¹ Prepared Statement, Hearing on “The Future of Money: Digital Currency,” U.S. House of Representatives, Committee on Financial Services, July 18, 2018, in Hearing Rept., Serial No. 115-111, at 62.

²⁰² <https://eba.europa.eu> (a regulatory agency of the European Union charged with prudential regulation and supervision of the EU's banking sector, increasing transparency in the European financial system and with identifying weaknesses in banks' capital structures).

low-middle middle ranges of concern depending on precisely how they are regulated now and the users who favor them), and bad actors and opportunists (at the high end of concern because of the potential for user/ consumer harm and the damage these actors can cause to other innovators as well). In this last category, I would include hackers and issuers of currencies and tokens that have no intention of allowing redemption of value exchanged or of providing any service to those who pay for it. This cautious approach follows a long-held view that maintains there is little reason to regulate the already sufficiently regulated. In other words, I see no reason to pile regulations actors, products and services that are subject to and in compliance with applicable federal and state laws in the United States and our major trading partners. The goal of future regulatory and law enforcement attention should be to maintain capacity to “follow the money” trails beyond that used with traditional gatekeepers (intermediaries, such as banks and securities-market participants) using the “smartest” approaches we can devise.

Issues for future research include both Venezuela’s 2019 challenge at the WTO relating to U.S. sanctions imposed on its Petro as violating other international law and global trade agreements²⁰³ and the proposals by the Russia Federation to create a sovereign cryptocurrency, as described briefly in Part II.B., above. Governments seeking to protect their own financial, commercial, and trade systems against government-sponsored cryptocurrencies designed to evade economic sanctions imposed by other nation states will have to consider their choice of methods in light of World Trade Organization responsibilities. Whether economic sanctions directed at a government-sponsored cryptocurrency can be deemed to violate WTO obligations is a topic that goes beyond the assignment given to me by the organizers of this George Mason Financial Services Roundtable, and so this issue is saved for future research. I also intend, at some point, to write about sovereign-issued cryptocurrencies and national security/cyber-warfare issues they may pose.

²⁰³ Nikhilesh De, *Venezuela Calls US Sanctions Against Its Petro Cryptocurrency “Discrimination,”* COINDESK.COM, Jan. 9, 2019 at 22:35 UTC, <https://www.coindesk.com/venezuela-us-sanctions-petro-world-trade-organization> (reporting on Venezuela’s complaint filed with the World Trade Organization against the United States for the latter’s actions against the Petro).

Appendix 1

Examples of Enforcement Actions Dealing with Providers of Cryptocurrencies or Other Crypto-Assets

The following are examples going back for more than ten years that demonstrate the ability of federal and state law enforcement agencies to detect and prosecute persons and entities whose activities violate federal or state laws relevant to registration or licensure, creation and maintenance of records of customers and their transactions, and threshold-based reporting to law enforcement agencies that I reviewed while pondering the central question in this essay. These are not the only examples, particularly of enterprises or persons who have faced scrutiny from securities and commodities regulatory agencies, but they provide a sense of how regulators and enforcement agencies view the seriousness of certain types of activities.

1. *Ripple Labs, Inc. and XRP II, LLC, its wholly owned subsidiary*

Ripple is the best-known of the examples of U.S. enforcement actions I have chosen to mention in this essay. FinCEN brought and settled its first civil enforcement action involving a virtual currency exchange, securing a \$700,000 civil penalty.²⁰⁴ FinCEN and the Department of Justice charged Ripple with willful violations of the Bank Secrecy Act,²⁰⁵ failure to register with FinCEN as a “money services business” (MSB), and failure to implement and maintain an anti-money-laundering compliance program as required for MSBs.²⁰⁶ The violation that FinCEN cited in its action reportedly occurred between March 6, 2013 through April 29, 2013, which I have noted in another essay bridges the date on which FinCEN issued its first guidance on virtual currency providers as “money services businesses.”

2. *BTC-e and Alexander Vinnik*

In July 2017, the Department of Justice announced the indictment of BTC-e, AKA Canton Business Corporation, and its alleged founder, a Russian national Alexander Vinnik, for operating an unlicensed money services business in violation of 18 U.S.C. § 1960, engaging in money laundering and a conspiracy to commit money laundering in violation of 18 U.S.C. §§ 1956(a)(1) and 1956(h), and additional unlawful monetary transactions in violation of 18 U.S.C. § 1957. The Department also sought criminal forfeiture pursuant to 18 U.S.C. § 982(a)(1).²⁰⁷ The Superseding Indictment alleged that BTC-e “was an international money-laundering scheme ... that facilitated crimes, including computer hacking and ransomware, fraud, identity theft, tax refund fraud schemes, public corruption, and drug trafficking.”²⁰⁸

Besides operating as an unlicensed money services business, the indictment charged that BTC-e “lacked basic anti-money laundering controls and policies and, as such was attractive to those who

²⁰⁴ Press Release, FinCEN Fines Ripple Labs, Inc. in First Civil Enforcement Action against a Virtual Currency Exchanger (May 5, 2015), http://www.fincen.gov/news_room/nr/pdf/20150505.pdf.

²⁰⁵ 31 U.S.C. § 5318 (2018).

²⁰⁶ Ripple Statements of Facts and Violations, at paras. 26-28, Attachment A to Ripple Press Release, *supra* note [46], http://www.fincen.gov/news_room/nr/pdf/Ripple_Facts.pdf.

²⁰⁷ United States v. BTC-e, Superseding Indictment, CR-16-0227 SI (Jul. 26, 2017) (unsealed indictment originally filed on Jan. 17, 2017), <https://www.justice.gov/usao-ndca/press-release/file/984661/download>.

²⁰⁸ *Id.* at para. 2.

desired to conceal criminal proceeds as it made it more difficult for law enforcement to trace and attribute funds.”²⁰⁹ BTC-e allegedly did not require basic identifying customer information (e.g., name, date of birth, address, or other identifiers) on account opening, and required only a user name, password, and an email address.²¹⁰

The indictment also charged that, although based abroad, BTC-e operated its servers inside the United States and did substantial amounts of business in the United States.²¹¹ In addition to potential criminal penalties, on July 26, 2017, FinCEN assessed a civil penalty of \$110 million against BTC-e, and a civil penalty of \$12 million against Vinnik.²¹²

3. *Liberty Reserve*

Liberty Reserve was an online, centralized digital-currency exchange²¹³ based in Costa Rica, alleged to have laundered approximately \$6 billion in criminal proceeds.²¹⁴ On May 28, 2013, the U.S. Attorney for the Southern District of New York unsealed a criminal indictment against Liberty Reserve and certain principals and employees for operating an unlicensed money transmission business and engaging in money laundering.²¹⁵ Liberty Reserve went out of business following this indictment and prior to the entry of a guilty plea by its founder, Arthur Budovsky.²¹⁶

This is the only one of two examples of federal enforcement actions against virtual-currency providers whose headquarters were outside the US at the time of the action. The other was against BTC-e, discussed above. For purposes of later discussion, the jurisdictional hooks with BTC-e and Liberty Reserve involved assets (servers) or customers inside the United States proper. A purely extraterritorial application of U.S. laws did not arise in either case. From these actions and settlements, we can see that the U.S. intends to apply its anti-money-laundering requirements to money services businesses that are located abroad but do business in the United States. Whether this will suffice to keep providers using

²⁰⁹ *Id.* at paras. 3, 6.

²¹⁰ *Id.* at para. 32.

²¹¹ *Id.* at paras. 20, 6, respectively.

²¹² Press Release, U.S. Attorney’s Office, Northern District of California, San Francisco Div., “Russian National and Bitcoin Exchange Charged in 21 Count Indictment For Operating Alleged International Money Laundering Scheme And Allegedly Laundering Funds from Hack of Mt. Gox, at 3 (July, 26, 2017), <https://www.justice.gov/usao-ndca/pr/russian-national-and-bitcoin-charged-21-count-indictment-operating-alleged-international-money-laundering-scheme-and-allegely-laundering-funds-from-hack-of-Mt.-Gox> (last visited December 28, 2018).

²¹³ United States. v. BTC-e, Superseding Indictment, CR-16-0227 SI, paras. 21-22 (Jul. 26, 2017) (unsealed indictment originally filed on Jan. 17, 2017), <https://www.justice.gov/usao-ndca/press-release/file/984661/download>.

²¹⁴ *Id.* at [from Liberty reserve indictment]; BTC-e Indictment, *supra* note [55], at paras. 21-22.

²¹⁵ Press Release, U.S. Attorney’s Office, Manhattan U.S. Attorney Announces Charges Against Liberty Reserve, One of World’s Largest Digital Currency Companies, and Seven of Its Principals and Employees for Allegedly Running A \$6 Billion Money Laundering Scheme (May 18, 2013), <http://www.justice.gov/usao/nys/pressreleases/May13/LibertyReservePR.php> (last visited December 28, 2018). For additional discussion of this and other virtual-currency developments in 2013, see generally Sarah Jane Hughes and Stephen T. Middlebrook, Virtual Uncertainty: Developments in the Law Affecting Electronic Payments and Financial Services, 69 BUS. LAW. 263 (2013).

²¹⁶ Press Release, U.S. Dep’t of Justice, Founder of Liberty Reserve Pleads Guilty to Laundering More Than \$250 million through His Digital Currency Business, (Jan. 29, 2016), <https://www.justice.gov/opa/founder-liberty-reserve-pleads-guilty-laudering-more-250-million-through-his-digital-currency-business>.

permission-less blockchain technologies with neither customers nor servers or agents in the United States is not yet clear.

Another important aspect of the prosecution of Liberty Reserve and Budovsky was the admission in the plea agreement that Liberty Reserve had 600,000 accounts associated with users in the United States and had laundered more than \$250 million on a worldwide basis.²¹⁷ This dollar value places Liberty Reserve's effect on global money laundering above the amount now known about Danske Bank's Estonia branch, as described above.

4. *E-Gold, Ltd.*

One of the earliest actions to involve a provider of virtual-assets products and services – one preceding both FinCEN's 2011 regulation on "prepaid access" and its March 2013 guidance on Virtual Currencies under the 2011 regulation -- was brought against an online provider known as e-Gold, Ltd. E-Gold was a digital currency backed by gold. The digital assets marketed by defendants preceded Bitcoin. E-Gold allowed its customers to open accounts anonymously and its services enabled fast cross-border transfers of value.²¹⁸ The action, filed in 2008, followed a return from a civil seizure warrant.²¹⁹ Defendant e-Gold, Ltd. challenged the seizure on grounds that it violated its Fifth and Sixth Amendment rights. A federal district court ruled in the government's favor. The United States Courts of Appeal for the D.C. Circuit, however, agreed with the e-Gold and individuals who were officers or shareholders in the firm that their rights had been violated.²²⁰ The methods that led investigators to e-Gold, Ltd. are described in the Complaint.²²¹

With a transaction volume that made it second to PayPal on a global basis at that time, e-Gold attracted bad actors and government investigators.²²² US regulators and the DOJ sought to force e-Gold, Ltd. to register with FinCEN as a "money transmitter" – a classification that, apparently, e-Gold thought was not applicable to its business model because it allowed customers to store value, in much the same manner as banks' customers store value with banks.²²³ E-Gold, it turned out, had become the vehicle for "carders" – enterprises that collected and sold information from stolen credit cards and extracted payments, much like ransomware attacks today, and was aiding the carders in moving significant amounts around the world.²²⁴

5. *Other Enforcement Actions Brought against Unlicensed Money Transmitters or Those Not Registered with FinCEN*

²¹⁷ *Id.*

²¹⁸ See Kim Zetter, *Bullion and Bandits: The Improbable Rise and Fall of e-Gold*, WIRED.COM (June 9, 2009 12:00 AM) (providing valuable insights into the operations of e-Gold, Ltd. Including the customer base and transaction volumes as well as its stores of gold and silver that backed the currency).

²¹⁹ Complaint, United States v. E-Gold, Ltd. (2005).

²²⁰ United States v. E-Gold, Ltd., No. 07-3704 (April 11, 2008), (vacating and remanding for further proceedings consistent with the order). The opinion contains an excellent summary of the facts leading law enforcement to e-Gold, Ltd., and to the seizure of the equivalent of more than \$1.4 million in e-Gold's assets.

²²¹

²²² *Id.* at 2.

²²³ *Id.*

²²⁴ *Id.* at 3.

There are numerous examples of enforcement actions brought against unlicensed money transmitters or those not registered with FinCEN as being engaged in “money services businesses.” For the purposes of this essay, however, I will offer only brief comments on a few of the earlier enforcement actions so that audience members get the flavor of the actions. These actions represent a combination of higher-tech and old-fashioned investigatory work, which is likely to remain the approach used to ferret out illicit proceeds on permission-less blockchains.

a. *Mutum Sigillum, LLC Account Seized from Dwolla*

Shortly before the Liberty Reserve indictment was unsealed, on May 14, 2013, the U.S. Department of Homeland Security (“DHS”) obtained a seizure warrant ordering the seizure and forfeiture of an account belonging to Mutum Sigillum, LLC.²²⁵ An affidavit filed in connection with the application for the seizure warrant stated that Mutum Sigillum LLC was a U.S.-based subsidiary of Mt. Gox, a large Bitcoin exchange based in Japan.²²⁶ Based on information allegedly from an informant, DHS alleged that Mutum Sigillum was engaged in “money transmission” without holding a license as a money transmitter and so should have been, but was not registered with FinCEN in violation of 31 U.S.C. § 5330, and that Mt. Gox, the parent company, was operating in violation of 18 U.S.C. § 1960.²²⁷ Following these actions, Mt. Gox announced that it would institute a new policy that required identity verification before it would allow currency withdrawals or deposits,²²⁸ a policy announcement that implies that no such identification information had been required previously.

b. *United States v. Murgio*

Another of the early enforcement actions was brought against Anthony Murgio for operating an unlicensed online currency exchange – a money transmitting business under FinCEN’s March 2013 guidance -- in violation of 18 U.S.C. § 1960.²²⁹ Additional charges included conspiracy, money laundering, and failure to file a suspicious activity report, which is required of providers of prepaid access and others engaged in activities that make them “financial institutions” for purposes of the AML requirements in U.S. laws.²³⁰ Moreover, the complaint charged that Murgio and co-conspirators were alleged to have knowingly facilitated “ransomware” attacks, for which the victim is asked to pay the ransom in a virtual currency such as bitcoins.²³¹ Victims approached Murgio’s exchange, known as coin.mx, to acquire the bitcoins used to pay ransoms, which the exchange provided. The exchange was

²²⁵ Seizure Warrant, at 1, *In re Contents of One Dwolla Account*, No. 13-1162 SKG (D. Md. May 14, 2013), <http://cdn.arstechnica.net/wp-content/uploads/2013/05/Mt-GOX-Dowlla-Warrant-5-14-13.pdf>.

²²⁶ Affidavit in Support of Seizure Warrant at 2, *In re Contents of One Dwolla Account*, No. 13-1162 SKG (D. Md. May 14, 2013), <http://cdn.arstechnica.net/wp-content/uploads/2013/05/Mt-GOX-Dowlla-Warrant-5-14-13.pdf>.

²²⁷ *Id.* at 1-2. Apparently, Mutum Sigillum also maintained an account at Wells Fargo, which received a separate seizure warrant for funds in that account. *Id.* at 4.

²²⁸ See David Gilson, *How to Get Verified at Mt. Gox*, June 6, 2013 at 12:38 UTC, <https://www.coindesk.com/how-to-get-verified-at-mt-gox> (includes screen shots of the steps necessary to verify one’s identity under the then-new Mt. Gox protocol), *still available on site as of February 23, 2019*.

²²⁹ Sealed Complaint, *United States v. Murgio*, No. 15-MAG-2508 (S.D.N.Y. July 17, 2015), <https://www.justice.gov/usao-sdny/file/632166/download>.

²³⁰ *Id.* at ¶¶ [complete this citation].

²³¹ *Id.* at 4.

accused to failing to file the suspicious activity report on the perpetrator or recipient of the bitcoins it provided to the victim.²³²

The complaint also alleged a more concerning fact about Murgio's scheme: that Murgio had acquired beneficial ownership of a small credit union in New Jersey and had used or planned to use the credit union to access electronic payments networks in order to support other illegal activities.²³³ The risks presented by direct access to payments networks makes this action against Murgio and co-conspirators unique among the U.S. enforcement actions of which I am aware.

c. State v. Espinoza

The third example does not involve federal law enforcement agencies, but rather state charges against a man accused in 2013 of selling bitcoins directly for cash in Florida.²³⁴ It also results from online surveillance by law enforcement agencies.²³⁵ This matter has current utility because, on January 30, 2019, the Third District Court of Appeals in Florida held²³⁶ that selling bitcoins directly to another person qualifies as "money transmission"²³⁷ under Florida's money transmitter statute.²³⁸ In addition to reviewing the basis for Florida's position that bitcoin is covered by the definition of "payment instrument,"²³⁹ the court explained its view that the two-party transactions in which Espinoza sold bitcoins for cash to individuals still constituted "money transmission" under the statute.²⁴⁰ This reasoning depends on the court's view that Espinoza received cash in order to transmit virtual currency to the person that paid the cash.²⁴¹ (In contrast, FinCEN's position has been that "money transmission" of virtual currencies occurs when an intermediary sends value from one person to another²⁴² or sends value owned by one person from one location to another location.²⁴³)

²³² *Id.* at 15-16.

²³³ *Id.* at 16-18.

²³⁴ *State v. Espinoza*, Crim. Div. Case No. F14-2913 (2014). Espinoza won at the trial court level and the state appealed. *The State of Florida v. Michell Abner Espinoza*, Order Granting Defendant's Motion to Dismiss the Information, Crim. Div. Case No. F14-2913, (Fla. 11th Cir. Ct. 2016). The Order describes how Miami detectives found Espinoza after online searches revealed a site, <https://localbitcoins.com>, that enabled sellers to advertise and buyers to respond. Order at 1. For an early discussion of the origins of this matter, see Stephen T. Middlebrook and Sarah Jane Hughes, *Development in the Law Affecting Electronic Payments and Financial Services*, 71 BUS. LAW. 361, 364 (2015-2016), <https://www.repository.law.indiana.edu/facpub/2041>.

²³⁵ See Judith Rinearson, Daniel S. Cohen, and Jeremy M. Laughlin, *Trouble in Paradise: Florida Court Rules that Selling bitcoin is Money Transmission*, at 1 (Feb. 13, 2019), <http://www.klgates.com/details/?pub=Trouble-in-Paradise-Florida-Court-Rules-that-Selling-Bitcoin-is-Money-Transmission-02-13-2019>.

²³⁶ *State v. Espinoza*, -- So. 3d --, 2019 WL 361893 (Fla. 3d DCA 2019).

²³⁷ *Id.*

²³⁸ *Id.*

²³⁹ *Id.*

²⁴⁰ *Id.*

²⁴¹ *Id.*

²⁴² 31 C.F.R. § 1010.100(ff)(5)(i)(A) (2018) (definition of "money transmission").

²⁴³ *Id.*