



2015

Advancing a Framework for Regulating Cryptocurrency Payments Intermediaries

Sarah Jane Hughes

Stephen T. Middlebrook

Follow this and additional works at: <http://digitalcommons.law.yale.edu/yjreg>



Part of the [Law Commons](#)

Recommended Citation

Sarah J. Hughes & Stephen T. Middlebrook, *Advancing a Framework for Regulating Cryptocurrency Payments Intermediaries*, 32 Yale J. on Reg. (2015).

Available at: <http://digitalcommons.law.yale.edu/yjreg/vol32/iss2/8>

This Article is brought to you for free and open access by Yale Law School Legal Scholarship Repository. It has been accepted for inclusion in Yale Journal on Regulation by an authorized administrator of Yale Law School Legal Scholarship Repository. For more information, please contact julian.aiken@yale.edu.

Feature

Advancing a Framework for Regulating
Cryptocurrency Payments Intermediaries

Sarah Jane Hughes & Stephen T. Middlebrook†

This Article looks at competing models for regulating providers of services to individuals and businesses that take cryptocurrencies in payment for goods and services, including operators of online wallets and exchanges, and other cryptocurrency market intermediaries whose functions resemble “money service businesses” or “money transmission.” We conclude that, in addition to whatever “money services” or “money transmission” prudential regulation the States or federal government may adopt, the operation of wallets and exchanges requires a new commercial law that lays out rights and liabilities of cryptocurrency users in a robust and transparent fashion. We use Article 4A of the Uniform Commercial Code as a model for regulating cryptocurrency transactions in which intermediaries play a role.

Introduction..... 496

I. What Are Cryptocurrencies? 503

II. How Are Cryptocurrencies Regulated Today? 507

 A. Regulation by the United States Federal Government and the States 507

 B. Actions by the Federal Government..... 507

 C. Actions by the States 511

 D. Regulation in Other Nations 512

III. Which Existing Regulatory Schemes Might Help Us Model a Regulatory Approach to Cryptocurrency Intermediaries?..... 516

 A. Regulatory Models that Apply to Products and Services with Which Cryptocurrencies May Compete 517

 1. Payment Systems 517

 2. Money Services Businesses and Money Transmission..... 521

 a. Federal Laws that Apply to Money Services Businesses and Money Transmission..... 522

 b. State Laws Regulating Money Transmitters, Money Service Businesses, and their Receipt and Transfers of Money..... 523

 3. Deposit Taking and Deposit Insurance 525

4. SEC Broker-Dealer Registration and Compliance Requirements	527
5. CFTC Commodities Trading Regulation	529
6. Anti-Money Laundering and Counter-Terrorism Financing....	530
7. Taxation	532
8. Remittance Transfers	533
<i>B. New York State Department of Financial Services' Final BitLicense Regulations and its 2014 Proposal.....</i>	<i>536</i>
1. BitLicense Final Definition of "Virtual Currency".....	538
2. BitLicense's Definition of "Virtual Currency Business Activity"	539
3. BitLicense's Licensing Requirements	541
4. BitLicense's Anti-Money-Laundering and Customer Identification Requirements	542
5. BitLicense's Consumer Disclosures	544
6. BitLicense's Requirements Related to Engaging in Fraudulent Activity and to Detecting and Deterring Fraud	545
IV. What Other Factors Should We Consider in Deciding Whether and How to Regulate Cryptocurrencies Generally or Cryptocurrency Intermediaries?	546
V. A Proposed Framework for Regulating Cryptocurrency Payments Intermediaries who Execute Payments for Goods and Services from U.C.C. Article 4A	549
A. <i>The Subject Matter and Covered Participants</i>	551
B. <i>Requirements for Cryptocurrency Payment Instructions to Operators of Wallets and Exchanges</i>	552
C. <i>Fees and Fee Disclosures</i>	554
D. <i>Rules Governing Unauthorized Transfers, including Counterfeits and Replicates, and Providing Error-Resolution or Reversibility Rights</i>	554
E. <i>Miscellaneous Issues Arising from Custom or Otherwise from Article 4A</i>	556
Conclusion	556

Introduction

The time has come to regulate the transfer of cryptocurrencies such as Bitcoin by intermediaries facilitating these transfers, including operators of online wallets, exchanges, and gateways. Transaction-execution rules for cryptocurrency payments are the missing link in the regulation of cryptocurrency transactions in the United States. "Default rules," such as those commonly provided in commercial laws, obviate the necessity of negotiating terms for each transaction and provide users of cryptocurrency payment

services with basic transactional rights and responsibilities, particularly in multi-party transactions.

In the simplest, peer-to-peer bitcoin transaction,¹ the sender's cryptographic credentials are used to sign the transfer, which is recorded on the master public ledger and can be verified by other users.² Such transactions are referred to as taking place "on the block chain."³ A growing percentage of transactions, however, take place through one or more intermediaries. Intermediaries act as custodians of cryptocurrency or cryptocurrency credentials originally belonging to their clients and may facilitate and clear transactions for clients without updating the public ledger. Such transactions are referred to as taking place "off the block chain." Off the block chain transactions may not appear in the public ledger at all, or, if they do, they

† Sarah Jane Hughes is the University Scholar and Fellow in Commercial Law at the Maurer School of Law, Indiana University. Ms. Hughes has served as the Reporter for the Uniform Law Commission's ("ULC") Study Committee on Alternative and Mobile Payments since March, 2014 and now serves as the Reporter for the ULC's Drafting Committee on Alternative Payments. Her research since the early 1990's has involved electronic payments, anti-money-laundering efforts, privacy and data security. She served as the American Bar Association's Advisor to the ULC's Money Services Business Drafting Committee. Prior to joining the Maurer School in 1989, Ms. Hughes served for 14 years at the Federal Trade Commission focusing on consumer credit and payments issues. The views expressed in this article do not necessarily reflect those of the Trustees of Indiana University or of the Uniform Law Commission. She can be reached at sjhughes@indiana.edu.

Mr. Middlebrook is the General Counsel of Unirush LLC, a prepaid card program manager, and formerly served as General Counsel of FSV Payment Systems, Inc., a prepaid processor and program manager that was acquired by U.S. Bank in 2012. He also served as Senior Counsel, Financial Management Service, U.S. Department of the Treasury, and as an American Bar Association Advisor to the ULC's Study Committee. The views expressed in this article do not necessarily reflect the views of his current or former employers or of the American Bar Association. He can be reached at stm@aol.com.

Neither Ms. Hughes nor Mr. Middlebrook has a financial interest in any cryptocurrency company. Instead, they express their interest in the smooth functioning of e-payments markets and appropriate protections for counterparties in e-payments transactions, as their scholarship over the last decade and more suggests.

Ms. Hughes and Mr. Middlebrook appreciate the invitation from the editors to prepare this article and the quality of their comments on it. Over the course of the past year, we have others to thank for help with this article, including Von Welch who is the Director of the Center for Applied Cybersecurity Research at Indiana University for assistance with technical questions and for pointing us to scholarly works outside the law field that pertain to cryptocurrencies, and Ms. Michelle Botek Troumbo and Ms. Jennifer B. Morgan of the Maurer School Library for their amazing support. Much of the research for this article was completed in 2014; any cut-off date for research in a field moving as fast as this one is risky, but, with the few exceptions that readers will see, we have chosen to leave the date of the publication of the final BitLicense Regulation, June 24, 2015, as the end-point for this research. Despite help received, we remain solely responsible for errors.

1. CRAIG K. ELWELL, M. MAUREEN MURPHY, & MICHAEL V. SEITZINGER, CONG. RESEARCH SERV., R 43339, BITCOIN QUESTIONS, ANSWERS AND ANALYSIS OF LEGAL ISSUES, at SUMMARY (2015), <https://fas.org/sgp/crs/misc/R43339.pdf>.

2. See François R. Velde, *Bitcoin: A Primer*, CHI. FED. LETTER, no. 317, Dec. 2013, at 2-3 [hereinafter *Bitcoin Primer*]. For additional insights into how Bitcoin works, see Sarah Meiklejohn et al., *A Fistful of Bitcoins: Characterizing Payments Among Men with No Names*, IMC '13 PROCEEDINGS OF THE 2013 CONFERENCE ON INTERNET MEASUREMENT 10-13 (2013), available at <http://dl.acm.org/citation.cfm?doid=2504730.2504747> [hereinafter *Fistful of Bitcoins*].

3. *Bitcoin Primer*, supra note 2, at 2-3.

appear as transactions involving not the sender and receiver, but the intermediaries.

Intermediaries to cryptocurrency transactions act much like intermediaries to transactions in traditional payment systems. They pose similar types of credit and liquidity risks to consumers, market participants, and national economies. The increasing prevalence of intermediaries in cryptocurrency transactions necessitates regulation of these new market participants. In contemplating that regulation, it seems logical to look at regulations governing existing payment mechanisms to start a discussion of when and how to regulate cryptocurrencies.

This Feature article reviews the existing forms of regulations in the United States (and to a limited extent in other nations) that could be adapted to regulate the rights and duties of third-party market participants such as online wallets and exchanges engaging in transfers of cryptocurrencies. It then describes the features that any framework for regulating market participants using cryptocurrencies to make payments should include.

Crafting the right, first-stage regulation of any new technology is a daunting task. It will be unclear, possibly for some time, whether it is worth spending public and private resources on a technology that may never gain widespread acceptance. This difficulty may explain our legislators' and regulators' habits of allowing new technologies, particularly those involving financial innovations, to operate in unregulated spaces until a significant problem arises.

In the universe of virtual currencies and cryptocurrencies, a significant problem with a new technology hit the headlines in early 2014. The Mt. Gox Bitcoin exchange in Japan suspended transactions in February 2014⁴ and subsequently filed for bankruptcy protection in Japan.⁵ Approximately \$650 million of Bitcoin value allegedly vanished.⁶

In the United States, individual states became more actively engaged in efforts to regulate cryptocurrencies around that time.⁷ These efforts, however, have been primarily reactive to whatever crisis is in the news and the immediate costs associated with it. As such, legislators and regulators may fail

4. See Alex Hern, *Bitcoin Exchange MtGox Offline Amid Rumors of Theft*, GUARDIAN (Feb. 25, 2014, 5:06 PM), <http://www.theguardian.com/technology/2014/feb/25/bitcoin-exchange-mtgox-offline-amid-rumours-of-theft> [hereinafter Hern, *Mt. Gox Offline*].

5. See Alex Hern, *MtGox Files for Bankruptcy in Japan After Collapse of Bitcoin Exchange*, GUARDIAN (Feb. 28, 2014, 8:30 AM), <http://www.theguardian.com/technology/2014/feb/28/bitcoin-mtgox-bankruptcy-japan> [hereinafter Hern, *Mt. Gox Bankruptcy Filing*].

6. Shivam Srivastava & Marja Novak, *Bitcoin Exchange Bitstamp Suspends Service After Security Breach*, REUTERS (Jan. 6, 2015, 8:58 AM), <http://www.reuters.com/article/2015/01/06/us-bitstamp-cybersecurity-idUSKBN0KF0UH20150106> (reporting that Bitstamp, based in Slovenia, announced that the breach would affect a "small fraction of its total Bitcoin" holdings and that it would honor its Bitcoin account holders in full) [hereinafter *Bitstamp Breach*].

7. For discussion of state efforts responding to virtual currencies, see text accompanying notes 89 to 98, *infra*.

to regulate new technologies in a manner that protects users, preserves utility, and enables future innovation.

On the other hand, by offering basic rules, early regulation can aid those innovators by removing complex questions about whether a certain law applies to a new product as well as the risk of law enforcement actions if the innovator fails to comply with a law that is applicable. It also can reduce transactional costs among counterparties and externalities. In setting forth a vision for governing cryptocurrency payment transactions by intermediaries, our goals are to foster innovation and, accordingly, to encourage adoption of these technologies by adding to transactional certainty.

We are not alone in suggesting that regulation of new payments technologies may add to those technologies' perceived legitimacy and spur faster adoption for some purposes. For example, one commentator argued that Coinbase's opening as the first licensed exchange in the United States could bring "needed legitimacy to [Bitcoin], which isn't backed by a central government and is traded over virtual exchanges, primarily overseas."⁸ Other proponents of (some) regulation have voiced their views.⁹

One can argue that, in the infancy of three-party credit cards in the 1970s (and subsequently of debit cards), federal regulation provided transparent protections for users and may have aided consumer adoption of innovative new services and products.¹⁰ Regulation also can provide signals of legitimacy for bankers and investors whose attention is required both to get products and services to market and to reap the rewards that new technologies offer.¹¹ It enables these actors to measure the new product against a standard of behavior.

This being said, promoters of new technologies have expressed concerns that inappropriate government constraints could destroy nascent industries. These views are common among commentators on cryptocurrencies.¹²

When regulation comes early in the development of a new technology, missteps may occur. Too much regulation can cause regulatory arbitrage—

8. See Greg Bensinger, *Bitcoin Exchange to Open in U.S.*, WALL ST. J., Jan. 26, 2015, at C5 (reporting on receipt by the Coinbase exchange of financial support from USAA Bank, the New York Stock Exchange and others) [hereinafter Bensinger].

9. E.g., Kevin V. Tu & Michael W. Meredith, *Rethinking Virtual Currency Regulation in the Bitcoin Age*, 90 WASH. L. REV. 271 (2015) (urging a focus on policy goals in development of comprehensive, cohesive and scaled virtual currency regulation); Daniela Sonderegger, Note, *A Regulatory and Economic Perplexity: Bitcoin Needs Just a Bit of Regulation*, 47 WASH. U. J.L. POL'Y 175 (2015); Patrick Kirby, *Virtually Possible: How to Strengthen Bitcoin Regulation Within the Current Regulatory Framework*, 93 N.C. L. REV. 189, 220 (2014) (arguing that regulators can add certainty and legitimacy to the use of bitcoins).

10. E.g., Truth in Lending Act, 15 U.S.C. §§ 1666-1666j (2013) (provisions also known as the Fair Credit Billing Act), and Electronic Fund Transfer Act, 15 U.S.C. §§ 1693-1693r (2013).

11. Bensinger, *supra* note 8.

12. See, e.g., Robert McMillan, *New York's New Bitcoin Rules Are Going to Kill Its Startups*, WIRED (July 17, 2014), http://www.wired.com/2014/07/ny_bitcoin/; Tim Worstall, *It Could Be the Bureaucrats That Kill Bitcoin*, FORBES (May 16, 2013), <http://www.forbes.com/sites/timworstall/2013/05/16/it-could-be-the-bureaucrats-that-kill-bitcoin/>.

movements of developers to less regulated channels or jurisdictions,¹³ which may not be the optimal spaces for the technology to prosper. On the other hand, failure to regulate technology that is designed to compete with existing products and services may cause other market distortions. Failure to regulate prudentially or to offer rules for multi-party transfers also may delay adoption of the new technology by a significant number of users. Adoptions are key to producing revenue streams from those users whose transactions generate revenue streams and attract investments needed to finance the next generation of developments.

The regulation of cryptocurrencies up through late 2014 in the United States focused on public purposes such as tax collection, the deterrence of money laundering, economic sanctions laws, unregistered securities offerings, and commodities transactions with cryptocurrencies as the underlying asset. One example is the U.S. Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN") guidance on the threshold requirements for certain intermediaries in cryptocurrency transactions to register as "money service businesses."¹⁴ In another example of this type of public-purposes regulation, the Internal Revenue Service ("IRS") stated that the receipt of convertible cryptocurrencies through a process known as "mining,"¹⁵ and subsequent transfers of cryptocurrencies in payment for goods and services give rise to gains or losses depending on whether the property "received in exchange exceeds the taxpayer's adjusted basis of the virtual currency."¹⁶ The IRS's designation of cryptocurrencies as "property" instead of as "currency" deprives the trader/user of favorable tax treatment afforded to foreign currency transactions and forces the taxpayer to track his or her "basis" in each unit of currency upon the sale or exchange and, to calculate any net gain or loss realized.¹⁷

Part I of this Article briefly explains what "cryptocurrencies" (also known as math-based currencies) are and how they operate.

13. See Frank Partnoy, *Financial Derivatives and the Costs of Regulatory Arbitrage*, 22 J. CORP. L. 211, 227 (1997) (defining regulatory arbitrage as "those financial transactions designed specifically to reduce costs or capture profit opportunities created by different regulations or laws"). For a more recent discussion of regulatory arbitrage in a somewhat broader context, see Annelise Riles, *Managing Regulatory Arbitrage: A Conflict of Laws Approach*, 47 CORNELL L. REV. 63 (2014).

14. FIN. CRIMES ENFORCEMENT NETWORK, DEP'T OF THE TREASURY, FIN-2013-G001, APPLICATION OF FINCEN'S REGULATIONS TO PERSONS ADMINISTERING, EXCHANGING, OR USING VIRTUAL CURRENCIES (2013), http://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf [hereinafter 2013 FinCEN Guidance] (clarifying the coverage of regulations that implement the federal Bank Secrecy Act to persons engaged, among other things, in the receipt, distribution, exchange, and transmittal of virtual currencies).

15. Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN.ORG 4, <https://bitcoin.org/bitcoin.pdf> (last accessed Sept. 9, 2015) [hereinafter Nakamoto] (explaining the analogy to "gold miners"). For additional discussion of the process and rewards of "mining" of Bitcoin, see *Bitcoin Primer*, *supra* note 2, at 2.

16. I.R.S. Notice 2014-21 (Apr. 14, 2014), at Frequently Asked Questions 3, 4 & 6, <http://www.irs.gov/pub/irs-drop/n-14-21.pdf> [hereinafter 2014 IRS Guidance].

17. *Id.* at Frequently Asked Questions 1, 2 & 3.

Part II's first sub-part provides background on the regulation of virtual currencies in the United States up through the end of 2014, focusing on the five major developments over the past two years that demonstrate the types of regulatory actions being taken. These developments include the two mentioned above: the March 2013 guidance by FinCEN on virtual currencies issued,¹⁸ and the IRS' position that virtual currencies are taxable as property, not currency.¹⁹ The remaining three include: (1) the first comprehensive licensing and supervision scheme for regulating virtual currency businesses and market participants—originally proposed by the New York State Department of Financial Services in July 2014 (the “BitLicense” proposal)²⁰ and adopted in June 2015 with minor changes (the “BitLicense Final Regulations”);²¹ (2) the December 2014 Conference of State Bank Supervisors' Policy on Virtual Currency Regulation and Draft Model Regulatory Framework;²² and (3) the December 2014 Report from the Uniform Law Commission's Study Committee on Alternative and Mobile Payments.²³ These documents will frame the first steps in cryptocurrency regulation in the United States.

The second sub-part of Part II describes steps taken by other national governments relating to the regulation of virtual currencies. No other nation has yet moved towards regulating cryptocurrency transaction execution, a vital step toward growth of cryptocurrencies in payments and toward maintaining level playing fields between traditional payments systems operators and their cryptocurrency competitors.

In Part III, we review existing regulation schemes in the United States that could be brought to bear upon cryptocurrency payments or on cryptocurrencies as commodities. We look at various rationales for regulation, including the aforementioned regulation for primarily public-law purposes such as collecting taxes or deterring money laundering. A second rationale for regulations such as those applicable to commodities and securities markets is that these types of

18. 2013 FinCEN Guidance, *supra* note 14.

19. 2014 IRS Guidance, *supra* note 16, at 2.

20. Regulation of the Conduct of Virtual Currency Businesses, 36 N.Y. Reg. 14 (July 23, 2014), <http://docs.dos.ny.gov/info/register/2014/july23/pdf/rulemaking.pdf> [hereinafter BitLicense Proposal]. For additional information on the 2014 proposal, see Press Release, N.Y. Dep't of Fin. Serv., NY DFS Releases Proposed BitLicense Regulatory Framework for Virtual Currency Firms (July 17, 2014), <http://www.dfs.ny.gov/about/press2014/pr1407171.html> [hereinafter BitLicense Press Release].

21. Regulation of the Conduct of Virtual Currency Businesses, 37 N.Y. Reg. 7 (June 24, 2015) (to be codified at N.Y. COMP. CODES R. & REGS. tit. 23, pt. 200), <http://docs.dos.ny.gov/info/register/2015/june24/pdf/rulemaking.pdf> [hereinafter BitLicense Final Regulation].

22. CSBS Policy on Virtual Currency Regulation, CONF. OF ST. BANK SUPERVISORS (Dec. 16, 2014), <http://www.csbs.org/regulatory/ep/Documents/CSBS%20Policy%20on%20State%20Virtual%20Currency%20Regulation%20--%20Dec.%2016%202014.pdf> [hereinafter CSBS Framework]. The Policy document focuses on areas such as consumer protection, market stability, and law enforcement goals, and also makes recommendations on covered activities, policy implementation, and possible exclusions. *Id.* at 2-3.

23. UNIF. LAW COMM'N, FINAL STUDY COMMITTEE ON ALTERNATIVE AND MOBILE PAYMENTS REPORT, Dec. 19, 2014 (copy on file with authors and with the editors of the Yale Journal on Regulation) [hereinafter ULC STUDY COMMITTEE FINAL REPORT].

regulations contribute to transparent and well-functioning marketplaces. They enhance the accountability of market participants and market-makers and protect users. Market-enhancing regulation may include mandatory licensure or registration, prudential requirements such as minimum capital standards and periodic inspections, and other types of supervision. One of the potential benefits from this type of regulation is that users can identify entities that have passed muster with regulators. This creates a kind of trust for these entities.²⁴ Trust diminishes issuers' and market-makers' costs to attract new customers, and also reduces users' search costs.

Other forms of regulation more specifically serve private-law purposes by, for example, establishing default rules among counterparties to certain kinds of transactions. Default rules apply in the absence of negotiated contracts or when negotiated contracts are silent on the issue in question. This type of regulation allocates risks, rights, and duties to counterparties. Although many of the provisions in such sets of default rules may be modifiable by the parties, default rules also reduce transaction costs and externalities and contribute some trust effects to marketplaces, which enable counterparties to know what to expect from each other. This is true even absent separately negotiated contracts. In the United States, we have varied levels of these default rules, including provisions of the Uniform Commercial Code.²⁵

We submit that cryptocurrency payment intermediaries should be subject to this last type of regulation: private-law, default-rule regulations available to other payment transaction-execution participants. As cryptocurrency wallets, exchanges, and gateways proliferate inside the United States and position themselves as substitutes for legacy intermediaries in the banking and non-bank money transmitter industries, these intermediaries place themselves in competition with traditional "trusted intermediaries" that cryptocurrencies were designed to do away with, at least in part.²⁶ As *intermediaries*, the terms and conditions on which they offer transaction execution and value-storage services to others should be transparent and enforceable. Such intermediaries are accountable to their customers for performing the payments instructions sent by customers faithfully and in a timely manner. Transparent and enforceable rules for counterparties in cryptocurrency payments and storage services will contribute to trust in the entity, which will enable it to compete with other providers of similar transaction-execution and value-storage services. This trusted status, in turn, should allow the market for these services to grow.

Other classes of regulation combine features of the public-law, private-law, or market-enhancing purposes we have mentioned above. For example, the

24. CSBS Framework, *supra* note 22.

25. See, e.g., U.C.C. arts. 3, 4, 4A *passim*; Collection of Checks and Other Items by Federal Reserve Banks and Funds Transfers through Fedwire (Regulation J), 12 C.F.R. pt. 210 (2013).

26. See Nakamoto, *supra* note 15, at 1 (observing that Bitcoin could replace trusted intermediaries in payments). For additional information about the trusted intermediary in payments transactions, see CSBS Framework, *supra* note 22.

requirements that certain cryptocurrency market participants register with FinCEN as “money services businesses”²⁷ or obtain licenses from states as “money transmitters” and remain in compliance with state requirements serve, respectively, some public-law and some market-enhancing purposes.

In Part III, we also offer some analysis of the New York State Department of Financial Services BitLicense regulation that will require licensure in order to engage in New York or with a “New York Resident” in what the BitLicense defines as “virtual-currency business activity.”²⁸

Parts IV and V outline a framework for regulating payment transaction execution by cryptocurrency intermediaries in both consumer- and merchant-side transactions, as well as rules applicable to executing instructions to intermediaries to exchange cryptocurrency for fiat currency. Our framework proceeds from Article 4A of the Uniform Commercial Code, which regulates wholesale wire transfers, for basic concepts of verifying transactions and allocating risks and responsibilities, and from the federal Electronic Fund Transfer Act for some “consumer protection” concepts.

The Conclusion offers a few principles that we hope will guide the development of the various new regulations that will be developed for cryptocurrency market participants.

I. What Are Cryptocurrencies?

Discussions of emerging payment mechanisms are frequently hampered by ambiguities in terminology that can lead to confusion. For purposes of this article, we will use the term “currency” to mean the legal tender of a particular nation or group of nations. Examples of currencies include the U.S. dollar, Australian dollar, euro, Philippine peso and Russian ruble. “Legal tender,” in turn, refers to a form of national money lawfully established by the government to serve as a medium of payment of taxes and used for commercial exchange.²⁹ Counterparties are required by law to take the legal tender of their jurisdiction as payment for the discharge of debts or releases of securities, and, more commonly today, as modes of payment for transactions in goods and services. It is no surprise that disputes over a sovereign’s ability to designate new forms of “legal tender” have occurred throughout history—from the days of Queen Elizabeth’s rule over Ireland,³⁰ to the question of President Lincoln’s ability to

27. 2013 FinCEN Guidance, *supra* note 14.

28. BitLicense Final regulation, *supra* note 21, § 200.2(g), (h), (q).

29. BLACK’S LAW DICTIONARY 1035 (10th ed. 2014).

30. See *The Case of Mixed Money* (1605) 80 Eng. Rep. 507 (P.C.) (upholding the right of Elizabeth I of England to devalue the currency, as she had in 1601, even if it caused great suffering among the people of Ireland), translated in JOHN DAVIES, A REPORT OF CASES AND MATTERS IN LAW: RESOLVED AND ADJUDGED IN THE KING’S COURTS OF IRELAND [1604-1612], at 48 (1762). The most famous sentence in the opinion proclaimed: “[I]t appertaineth only to the [K]ing of England, to make or coin money within his dominions . . .” *Id.* at 51. Since *The Case of Mixed Money*, three attributes of “money” and of “legal tender” that distinguish them from other forms of exchange have

introduce paper legal tender in the United States during the Civil War,³¹ to the recent debate over the use of Scottish banknotes in England and Wales.³² Indeed, frustration with government control of and perceived manipulation of existing fiat currency values was one of the drivers for the creation of Bitcoin.³³

We use the term “virtual currency” to refer to a medium of exchange existing entirely in intangible form that is not legal tender but which can substitute for legal tender. Older forms of “currency” that are not “legal tender” include paper-based currency substitutes, such as military scrip and depression scrip.³⁴ In recent times, the term “virtual currency” has developed an added connotation that it exists only in an electronic or digital form and is used only as a medium of exchange between members of an online or virtual currency community.³⁵ Virtual currencies may be used for online games, social media, or corporate loyalty programs to purchase virtual goods or redeem prizes.³⁶

A subset of virtual currency is “cryptocurrency,” by which we mean an internet-based virtual currency in which the ownership of a particular unit of value is validated using cryptography.³⁷ Cryptocurrencies are not legal tender³⁸ and, thus, their use requires the consent of both parties to a transaction. They

been acknowledged: “the authority of the prince, the stamp, and the value”—that is, the sovereign, its stamp designating the “thing” as money or legal tender, and the sovereign’s power to set the value for purposes of commerce and foreign exchange. *Id.* at 52.

31. See The Legal Tender Acts, 12 Stat. 345 (Feb. 25, 1862), 12 Stat. 532 (July 11, 1862), 12 Stat. 709 (Mar. 3, 1863). The constitutionality of these acts, which authorized the federal government to issue paper currency called “treasury notes” or “greenbacks” was the subject of numerous decisions of the Supreme Court. Among them were *Knox v. Lee & Parker v. Davis* (“The Legal Tender Cases”), 79 U.S. (12 Wall.) 457 (1870) (overruling *Hepburn v. Griswold*, 75 U.S. (8 Wall.) 603 (1869) (finding no express authority in the Constitution to make notes or bills of credit as opposed to coining “legal tender” for payment of debts).

32. See Severin Carrell, *Scottish Banknotes: the Treasury’s Symbolic Hostage in the Independence Debate*, GUARDIAN (Apr. 22, 2013, 9:37 AM), <http://www.theguardian.com/politics/scottish-independence-blog/2013/apr/22/scottish-independence-banknotes> (last visited Jan. 20, 2015).

33. The economic theory underlying cryptocurrency stems from the Austrian school of economics and its critique of central bank intervention in support of government issued fiat currency. See EUR. CENT. BANK, VIRTUAL CURRENCY SCHEMES 22-23 (2012) [hereinafter ECB REPORT]. Keynesian economists question whether cryptocurrency can serve as a long-term store of value or whether it is merely a bubble. See Paul Krugman, *Bitcoin is Evil*, N.Y. TIMES, Dec. 28, 2013, <http://krugman.blogs.nytimes.com/2013/12/28/bitcoin-is-evil/>.

34. See generally Loren Gatch, *Local Money in the United States During the Great Depression*, 26 ESSAYS IN ECONOMIC AND BUSINESS HISTORY 47 (2008). For additional discussion, see Stephen T. Middlebrook & Sarah Jane Hughes, *A Historical Analysis of Substitutes for Legal Tender and Their Implications for the Regulation of Virtual Currency*, in RESEARCH HANDBOOK ON ELECTRONIC COMMERCE LAW (John A. Rothchild ed., Edward Elgar Publishing, forthcoming 2016).

35. See, e.g., ECB REPORT, *supra* note 33, at 13 (defining virtual currency as “a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community”).

36. *Id.* at 13-16.

37. See *Bitcoin Primer*, *supra* note 2, at 2.

38. The Canadian government experimented with but abandoned the idea of issuing a cryptocurrency that would have “legal tender” status. See David George-Cosh, *Canada Puts Halt to MintChip Plans*, WALL ST. J., Apr. 4, 2014, <http://blogs.wsj.com/canadarealtime/2014/04/04/canada-puts-halt-to-mintchip-plans-could-sell-digital-currency-program/>.

are not denominated in or backed by gold or silver. Economists call currencies backed by precious metals and the like “commodity-based currencies.”³⁹ We note that a cryptocurrency given the status of “legal tender” by a government would qualify as “fiat currency” under the BitLicense Final Regulation⁴⁰ and would appear to fall outside its definition of “Virtual Currency.”⁴¹ That would send persons who transmit cryptocurrency back to the realm of more traditional “money transmitter” regulation.

Bitcoin is the best-known cryptocurrency. Bitcoin have no physical presence and their ownership is verified not by possession but by entries in a massive database known as the “block chain,” which is maintained over a peer-to-peer network.⁴² Transactions between a sender and receiver are “signed” using the participants’ cryptographic credentials (“keys”) and sent to the network for validation.⁴³ If the network validates the key “signatures,” then the block chain is updated to reflect the transaction.⁴⁴ There is no central authority that validates the transactions; instead, the block chain is maintained by a group of volunteers referred to as “miners” who are periodically rewarded for their service by receiving newly created bitcoin.⁴⁵ The Bitcoin protocol allows the supply of the cryptocurrency to expand slowly over time until it reaches a limit of 21 million bitcoin.⁴⁶ A senior Federal Reserve Bank economist refers to bitcoin as a “fiduciary currency,” because bitcoin have “no intrinsic value, and they derive their value in exchanges either from government fiat or from the belief that they may be accepted by someone else.”⁴⁷

A number of variations on the Bitcoin protocol, referred to as “altcoins,” have been implemented, each trying to improve on the protocol by changing how coins are generated, modifying the size of the money supply, or fixing other perceived flaws.⁴⁸ As a June 2014 report issued by the Clearing House and Independent Community Bankers of America noted, “establishing firm definitions is a challenge” as these new altcoin variations continue to emerge.⁴⁹

39. *Bitcoin Primer*, *supra* note 2, at 2-3.

40. Compare BitLicense Final Regulation, *supra* note 21, § 200.2(d) (definition of “fiat currency”), with § 200.2(m) (definition of “virtual currency”). As defined, it appears that the two terms are intended to be mutually exclusive.

41. BitLicense Final Regulation, *supra* note 21, § 200.2(p).

42. See ECB REPORT, *supra* note 33, at 21. For additional information, see *Bitcoin Primer*, *supra* note 2 at 2-3.

43. ECB REPORT, *supra* note 33, at 23. For additional discussion of the validation process, see *Bitcoin Primer*, *supra* note 2, at 2.

44. *Id.* at 23-24.

45. *Id.* at 24.

46. *Id.* at 24-25.

47. *Bitcoin Primer*, *supra* note 2, at 2-3.

48. See *Comparison of Cryptocurrencies*, BITCOIN WIKI (updated as of Sept. 2, 2014 at 22:53), https://en.bitcoin.it/wiki/List_of_alternative_cryptocurrencies (listing “altcoins” that have market caps of more than \$1 million or that have become notorious for some reason).

49. The Clearing House & Independent Cmty. of Bankers of America, *Virtual Currency: Risks and Regulation*, ICBA.ORG, June 23, 2014, <http://www.icba.org/files/ICBASites/PDFs/virtualcurrencywhitePaperJune2014.pdf> [hereinafter Clearing House/ICBA Report].

Although the virtual currencies in the market place each have unique characteristics, there remain ways of categorizing these products intelligibly for the purposes of regulation. The first attribute relates to whether a virtual currency has a centralized or decentralized administrative structure. As noted above, Bitcoin is a decentralized scheme lacking a single authority and instead relying on the “miners” to maintain its administrative records.⁵⁰ Because there is no entity issuing or backing bitcoin, there is no place a holder of bitcoin may turn to redeem his or her holdings.⁵¹ This is in contrast to underlying virtual currencies in online games like World of Warcraft or Second Life for which the company that provides the game administers the virtual currency, sets the rules for when and how it may be purchased and at what price.⁵²

The second attribute relates to whether a virtual currency can be exchanged for legal tender either with the issuer or on a virtual currency exchange. Bitcoin and other cryptocurrencies can be bought and sold in return for legal tender currencies on a number of exchanges.⁵³ This “convertibility” contrasts with virtual currencies in most on-line games where the system is “closed” and the virtual currency may be spent within the game, but cannot be “converted” back to dollars or other legal tender currencies.⁵⁴ The one exception, however, is Second Life, which allows users to sell their in-game currency for real money.⁵⁵

These attributes are summarized below:

Taxonomy of Virtual Currencies

	Centralized	Decentralized
Convertible	e-Gold, Liberty Reserve, Second Life Linden Dollars	Bitcoin, altcoins
Non-convertible	World of Warcraft Gold and other in-game currencies, loyalty rewards, airline reward points	No examples currently exist

This taxonomy that divides virtual currencies into centralized/ decentralized and convertible/nonconvertible is a fundamental tool in how

50. ECB REPORT, *supra* note 33, at 24-25.
51. *Id.*
52. *Id.* at 13-14.
53. *Id.* at 25-6.
54. *Id.* at 13.
55. *Id.* at 29.

regulators decide to treat individual financial products. The distinctions played a key role in FinCEN's 2013 Guidance on Bank Secrecy Act compliance for virtual currency market participants, which defined and focused on "convertible" virtual currencies.⁵⁶ The distinctions were also instrumental in the Financial Action Task Force's 2013 assessment of the money laundering risks posed by virtual currencies, which set forth definitions of "convertible" and non-convertible" virtual currencies.⁵⁷

II. How Are Cryptocurrencies Regulated Today?

A. Regulation by the United States Federal Government and the States

Before 2013, neither the federal government nor the states had issued regulatory guidance over cryptocurrencies, their issuers, or the exchanges that facilitate their transfer. Since March 2013, the U.S. Department of the Treasury (through FinCEN and the IRS) and several States have taken or begun actions to regulate cryptocurrencies. By the spring of 2013, they also took other actions against cryptocurrency market participants that we discuss below.

B. Actions by the Federal Government

The first federal regulatory guidance dealing with cryptocurrencies was FinCEN's March 2013 Guidance describing compliance obligations under the federal Bank Secrecy Act ("BSA")⁵⁸ for certain participants in cryptocurrency transactions.⁵⁹ That Guidance distinguished between "convertible" and "non-

56. 2013 FinCEN Guidance, *supra* note 14, at 1, 4-5. This guidance proceeds from prior FinCEN guidance and regulations involving "money transmitters" and the issuance and sale of "prepaid access." See Bank Secrecy Act Regulations—Definitions and Other Regulations Relating to Money Services Businesses (the "MSB Rule"), 76 Fed. Reg. 43,585 (July 21, 2011); Final Rule—Definitions and Other Regulations Relating to Prepaid Access, 76 Fed. Reg. 45,403 (July 29, 2011).

57. For a comprehensive discussion of distinctions among types of crypto- and virtual currencies, see FIN. ACTION TASK FORCE, VIRTUAL CURRENCIES: KEY DEFINITIONS AND POTENTIAL AML/CFT RISKS 4-8 (June 2014), <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>. The report explains that "convertible" virtual currencies need not enjoy an "ex officio convertibility (e.g. in the case of a gold standard), but rather a de facto convertibility (e.g. because a market exists)." *Id.* at 4. Non-convertible currencies "cannot be exchanged for fiat currency." *Id.*

58. Bank Secrecy Act, tit. I-II, Pub. L. No. 91-508, 84 Stat. 1114, 1114-24 (1970) (codified as amended at 12 U.S.C. §§ 1829b, 1951-59; 31 U.S.C. §§ 5311-14, 5316-32 (2012)) (authorizing the Secretary of the Treasury to issue regulations requiring organizations deemed to be "financial institutions" to keep records and file certain reports as the Secretary of the Treasury deems to have a "high degree of usefulness in criminal, tax, or regulatory investigations or proceedings, . . . or in the conduct of intelligence or counterintelligence analysis, including analysis to protect against terrorism" (quoting 12 U.S.C. § 1829b(a)(1)(A) (2012); 31 C.F.R. §§ 1000-1099 (2013))) [hereinafter FinCEN's BSA regulations].

59. 2013 FinCEN Guidance, *supra* note 14.

convertible” virtual currencies⁶⁰ and between those with a central administrator and those without one.⁶¹

After that guidance, the Department of Homeland Security in May 2013 seized assets owned by a Bitcoin exchange based in Japan and one of its subsidiaries.⁶² The Department’s seizure warrant was directed at Dwolla, an Iowa-based Internet payments company, ordering the seizure and forfeiture of an account held in the name of Mutum Sigillum, LLC.⁶³ The federal agent’s affidavit that the Department filed in support of the seizure warrant described Mutum Sigillum as a U.S.-based subsidiary of the Mt. Gox Bitcoin exchange.⁶⁴ The affidavit cited transactions in which a confidential informant had used U.S. dollars to purchase and exchange Bitcoin for U.S. dollars through Mutum Sigillum and Dwolla accounts.⁶⁵ These transactions supported the Department’s claim that Mutum Sigillum was engaged in money transfers but had failed to register with FinCEN pursuant to the March 2013 Guidance and 31 U.S.C. § 5330.⁶⁶

Following these developments, the question arose of whether or when Congress or federal government agencies might regulate virtual currencies for other purposes, including in connection with securities offerings and commodities transactions, and in consumer transactions. In November 2013, the Senate Committees on Homeland Security and Banking and Urban Affairs held hearings, respectively on national security and terrorist-financing concerns,⁶⁷ and on the need for regulation of cryptocurrencies with some attention to consumer protection and anti-money-laundering concerns.⁶⁸

60. *Id.* at 1.

61. *Id.* at 4.

62. See Joe Mullin, *Feds Seize Money from Dwolla Account Belonging to Top Bitcoin Exchange Mt. Gox*, ARS TECHNICA (May 14, 2013, 5:55 PM), <http://arstechnica.com/tech-policy/2013/05/feds-seize-money-from-top-bitcoin-exchange-mt-gox/> [hereinafter Mullin]. For more discussion, see Stephen T. Middlebrook & Sarah Jane Hughes, *Virtual Uncertainty: Developments in the Law of Electronic Payments and Financial Services*, 69 BUS. LAW. 263, 264 (2013).

63. Seizure Warrant at 1, *In re Seizure of the Contents of One Dwolla Account*, No. 13-1162-SKG (D. Md. May 14, 2014), <http://cdn.arstechnica.net/wp-content/uploads/2013/05/Mt-Gox-Dwolla-Warrant-5-14-13.pdf> [hereinafter Seizure Warrant]. For additional information, see Mullin, *supra* note 62.

64. Jordan Maglich, *Bitcoin Exchange Mt. Gox files for bankruptcy*, FORBES (Feb. 28, 2014), <http://www.forbes.com/sites/jordanmaglich/2014/02/28/bitcoin-exchange-mt-gox-files-for-bankruptcy> [hereinafter Maglich].

65. Seizure Warrant, *supra* note 63, at 1. Affidavit in Support of Seizure Warrant at 3, *In re Seizure of the Contents of One Dwolla Account*, No. 13-1162-SKG (D. Md. May 14, 2013), available at <http://cdn.arstechnica.net/wp-content/uploads/2013/05/Mt-Gox-Dwolla-Warrant-5-14-13.pdf> [hereinafter Affidavit in Support of Seizure Warrant]. For additional information, see Mullin, *supra* note 62.

66. Affidavit in Support of Seizure Warrant, *supra* note 65, at 2.

67. *Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies*, Hearing before the S. Comm. on Homeland Sec., 113th Cong. (2013), <http://www.hsgac.senate.gov/hearings/beyond-silk-road-potential-risks-threats-and-promises-of-virtual-currencies>.

68. *The Present and Future Impact of Virtual Currency: National Security and International Trade and Finance*, Hearing before the S. Comm. on Banking, Hous. & Urban Affairs,

In February 2014, the Mt. Gox Bitcoin exchange suspended operations and subsequently collapsed.⁶⁹ Mt. Gox later filed for bankruptcy protection in Japan⁷⁰ and commenced an ancillary proceeding in Texas under the U.S. Bankruptcy Code's Chapter 15.⁷¹ A class action lawsuit was filed against Mt. Gox in the Northern District of Illinois.⁷²

At roughly the same time, states began to determine whether and how to regulate cryptocurrencies when the Conference of State Bank Supervisors⁷³ and the Uniform Law Commission⁷⁴ created new projects aimed at studying the need for forms of cryptocurrency regulations.

Federal agencies moved cautiously with no plans to embark on a systematic regulatory scheme for cryptocurrencies. In late February 2014, the chair of the Board of Governors of the Federal Reserve System testified that the Board "lacked authority to supervise or regulate Bitcoin in any way."⁷⁵ Other federal agencies were not silent on or shy about how cryptocurrencies fit into various regulations in force. For example, in January 2014, FinCEN issued additional regulatory guidance on virtual currencies, clarifying that "mining" itself—that is the receipt of cryptocurrency as a reward for maintaining the block chain⁷⁶—was not "money transmission"⁷⁷ and, thus, clarified its own 2013 Guidance.⁷⁸ In April 2014, the IRS announced it would treat Bitcoin as "property" (not as foreign currency) for purposes of recognizing ordinary income and capital gains under the Internal Revenue Code.⁷⁹ In May 2014, the

113th Cong. (2013), http://www.banking.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_ID=955322cc-d648-4a00-a41f-c23be8ff4cad. One of the authors was a witness at this hearing.

69. See Maglich, *supra* note 64, at 1.

70. See *Herm, Mt. Gox Bankruptcy Filing*, *supra* note 5.

71. See *In re Mt. Gox Co.*, No. 14-31229 (Bankr. N.D. Tex. filed Mar. 10, 2014).

72. Class Action Complaint at ¶¶ 47, 81, 128, 135, *Greene v. Mt. Gox Inc.*, No. 14-01437 (N.D. Ill. Feb. 27, 2014).

73. CSBS Framework, *supra* note 22.

74. Press Release, Unif. Law Comm'n, New ULC Study and Drafting Committees to be Appointed (Jan. 28, 2014).

75. See Dominic Rushe, *Federal Reserve has no authority to regulate Bitcoin*, GUARDIAN, Feb. 27, 2014, www.theguardian.com/business/2014/feb/27/janet-yellen-federal-reserve-no-authority-regulate-bitcoin (reporting on the Semiannual Monetary Policy Report to the Congress by the Hon. Janet L. Yellen, Chair of the Board of Governors of the Federal Reserve System, before the United States Senate Committee on Banking, Housing, and Urban Affairs, and particularly her answers to questions on the Board's authority to regulate Bitcoin).

76. See *Bitcoin Primer*, *supra* note 2, at 2-3.

77. FIN. CRIMES ENFORCEMENT NETWORK, DEP'T OF THE TREASURY, FIN-2014-R01, APPLICATION OF FINCEN'S REGULATIONS TO VIRTUAL CURRENCY MINING OPERATIONS (2014), http://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R001.pdf [hereinafter *Fin-2014-R001*]; FIN. CRIMES ENFORCEMENT NETWORK, DEP'T OF THE TREASURY, FIN-2014-R002, APPLICATION OF FINCEN'S REGULATIONS TO VIRTUAL CURRENCY SOFTWARE DEVELOPMENT AND CERTAIN INVESTMENT ACTIVITY (2014), http://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R002.pdf [hereinafter "*Fin-2014-R002*"]. For more discussion of how a Bitcoin is mined, see generally *Bitcoin Primer*, *supra* note 6 at 2.

78. See 2013 FinCEN Guidance, *supra* note 14, at 2.

79. 2014 IRS Guidance, *supra* note 16.

Securities and Exchange Commission issued an investor alert⁸⁰ and announced an enforcement action against an offeror of unregistered Bitcoin-related securities.⁸¹

The calls for regulation increased. On June 23, 2014, the Clearing House Association and Independent Community Bankers Association published a study entitled “Virtual Currency: Risks and Regulation,” which was designed to “promote consideration of how existing regulatory regimes in the United States may be applied to virtual currency, virtual currency system participants and products, and virtual currency transactions.”⁸² On June 26, 2014, the Government Accountability Office released a report responding to a request from Senator Tom Carper, Chair, Senate Committee on Homeland Security and Governmental Affairs.⁸³ That report called for, among other things, more involvement by the Consumer Financial Protection Bureau (“CFPB”).⁸⁴ It also offered a useful précis of actions taken by other federal agencies related to cryptocurrencies generally.⁸⁵ Then, in August 2014, the CFPB issued a consumer alert describing various risks posed by virtual currencies.⁸⁶ In December 2014 the CFPB issued a proposed rule modifying the regulation of prepaid accounts which the Bureau acknowledged “may have potential application to virtual currency.”⁸⁷

On December 10, 2014, the Chair of the Commodity Futures Trading Commission (“CFTC”) testified before the U.S. Senate Committee on Agriculture, Nutrition, and Forestry that the CFTC considered virtual currencies trading as commodities to be covered by its jurisdiction. He further

80. U.S. SEC. & EXCH. COMM’N, INVESTOR ALERT: BITCOIN AND OTHER VIRTUAL CURRENCY-RELATED INVESTMENTS (May 7, 2014), <http://investor.gov/print/4536>.

81. U.S. SEC. & EXCH. COMM’N, SEC-2014-111, SEC CHARGES BITCOIN ENTREPRENEUR WITH OFFERING UNREGISTERED SECURITIES, (Jun. 3, 2014), <http://www.sec.gov/News/PressRelease/Detail/PressRelease/1370541972520>. A prior SEC enforcement action alleging violations of the antifraud and registration requirements occurred in 2013. *Sec. & Exch. Comm’n v. Shavers*, No. 413-CV-418 (E.D. Texas Aug. 6, 2013). Charges included operating a Ponzi scheme.

82. Clearing House/ICBA Report, *supra* note 49, at 4.

83. U.S. GOV’T ACCOUNTABILITY OFFICE, GAO-14-496, VIRTUAL CURRENCIES EMERGING REGULATORY, LAW ENFORCEMENT, AND CONSUMER PROTECTION CHALLENGES 1 (2014) [hereinafter GAO-14-496]. This report also compares the operations and tax consequences of virtual currencies such as Bitcoin that can be used outside virtual economies with those such as Linden dollars that can be used only within virtual economies, such as Second Life. *Id.* at 9. It also follows the GAO’s 2013 study of virtual economy and currency taxation issues. U.S. GOV’T. ACCOUNTABILITY OFFICE, GAO-13-516, VIRTUAL ECONOMIES AND CURRENCIES: ADDITIONAL IRS GUIDANCE COULD REDUCE TAX COMPLIANCE RISKS (2013), <http://www.gao.gov/assets/660/654620.pdf> [hereinafter GAO-13-516].

84. GAO-14-496, *supra* note 83, at 37-40 (describing interagency task forces working on virtual currency issues, but noting the absence or limited involvement of the CFPB on those task forces).

85. *Id.* at 24-37.

86. CONSUMER FIN. PROT. BUREAU, RISKS TO CONSUMER POSED BY VIRTUAL CURRENCIES (Aug. 2014), http://files.consumerfinance.gov/f/201408_cfpb_consumer-advisory_virtual-currencies.pdf [hereinafter CFPB 2014 Virtual Currency Advisory].

87. Prepaid Accounts Under the Electronic Fund Transfer Act (Regulation E) and the Truth in Lending Act (Regulation Z), 79 Fed. Reg. 77,102, 77,121 (proposed Dec. 23, 2014) (noting that CFPB’s review of virtual currencies and related products is “ongoing”).

testified that the CFTC had approved a registration to trade virtual currencies as commodities.⁸⁸ In other words, the CFTC's authority to regulate cryptocurrencies relates to the trading of cryptocurrencies as commodities, and does not extend to regulation of cryptocurrency market participants whose business involves execution of payments transactions, such as through online wallets and exchanges.

C. Actions by the States

Most states have now taken positions on virtual currencies by issuing consumer and investor alerts based on or reiterating work by the Conference of State Bank Supervisors and the North American Securities Administrators Association.⁸⁹ State regulators are actively policing investment schemes related to virtual currencies, taking action against a company that solicited oil and gas investments in bitcoin,⁹⁰ and sanctioning a deceptive investment pool seeking investors to fund the development of new bitcoin mining equipment.⁹¹

On July 17, 2014, the New York State Department of Financial Services jolted the virtual currency community by proposing a comprehensive regulation that would require virtual currency participants to obtain what the state called a "BitLicense."⁹² The proposed regulations unleashed a fury of commentary, both informal postings⁹³ and formal public comments.⁹⁴ As noted above, the

88. *The Commodity Futures Trading Comm'n—Effective Enforcement and the Future of Derivatives Regulation: Hearing Before the S. Comm. on Agric., Nutrition & Forestry*, 113th Cong. 62 (2014) (statement of Timothy Massad, Chairman, Commodity Futures Trading Comm'n) [hereinafter Massad 2014 Senate Testimony], <http://www.gpo.gov/fdsys/pkg/CHRG-113shrg94366/pdf/CHRG-113shrg94366.pdf>.

89. Conference of State Bank Supervisors & N. Am. Sec. Admin. Ass'n, *Model State Consumer and Investor Guidance on Virtual Currency*, CSBS.ORG (Apr. 23, 2014), <http://www.csbs.org/legislative/testimony/documents/modelconsumerguidance--virtual%20currencies.pdf>.

90. *In re* Balanced Energy, LLC, ENF-14-CDO-1731 (Tex. Sec. Bd., 2014); see also Joe Mont, *Texas Becomes First State to Halt a Bitcoin Investment Deal*, COMPLIANCE WEEK (Mar. 12, 2014), <http://www.complianceweek.com/blogs/enforcement-action/texas-becomes-first-state-to-halt-a-bitcoin-investment-deal>.

91. *In re* Virtual Mining Corp., Case No. AP-14-09 (Mo. Sec'y of State 2014), <http://www.sos.mo.gov/securities/orders/ap-14-09.pdf>; see also Press Release, Mo. Sec'y of State, Kander Halts Deceptive Bitcoin Scheme in Springfield (June 2, 2014), <http://www.sos.mo.gov/securities/mipc/newsrelease.asp?nID=1394>.

92. Bitlicense Proposal, *supra* note 20.

93. See, e.g., Erik Voorhees, *Reflection on the NYDFS BitLicense Proposal and the Right of Privacy*, MONEY AND STATE, (July 18, 2014), <http://moneyandstate.com/reflections-right-privacy-response-nydfs-bitcoin-proposal/>; Tone Vays, *Top 5 Issues with the NYDFS BitLicense Proposal*, COINTELEGRAPH (July 24, 2014 11:18 PM) (containing links to three additional commentaries on the BitLicense proposal); Ryan Selkis, *Bitcoin at a Crossroads - tackling the BitLicense*, COINTELEGRAPH (July 20, 2014 4:15 PM), <http://cointelegraph.com/news/112104/bitcoin-at-a-crossroads-tackling-the-bitlicense> (dividing aspects of the proposed BitLicense into "the good, the bad, and the ugly").

94. For a complete listing of the 3,746 public comments on the BitLicense proposal, see Comments Regarding the Proposed Virtual Currency Regulatory Framework, N.Y. DEP'T FIN. SERV (2014), dfs.ny.gov/legal/vcrf_comments.htm (last visited Dec. 4, 2014).

final BitLicense regulations were published on June 24, 2015.⁹⁵ We discuss key features of the final BitLicense regulation in Part III of the article.

Between July 2014 and June 2015, both California and North Carolina considered changes to their money transmission licensing requirements to bring virtual currencies under their respective regimes.⁹⁶ Because both states' legislation was pending as we completed editing of this article, we do not discuss these bills in depth in this article. New York State also granted in May 2015 what appears to be the first trust company charter in the nation to the itBit Trust Company.⁹⁷ The charter allows itBit to offer custodian services for customers' assets, including bitcoin and U.S. dollars, but it does not allow itBit to function as a full-fledged commercial bank.⁹⁸

D. Regulation in Other Nations

When one looks outside the United States, one finds only limited regulation of cryptocurrencies. Some countries—China,⁹⁹ Iceland,¹⁰⁰ the Russian Federation,¹⁰¹ and Thailand¹⁰²—have issued edicts effectively prohibiting the use of Bitcoin for payment purposes in their domestic markets. Other nations have focused on regulating cryptocurrencies only for limited purposes.¹⁰³ For example, some countries have dealt with the taxation issues associated with virtual currencies,¹⁰⁴ and some have announced their plans to

95. BitLicense Final Regulation, *supra* note 21.

96. H.R. 289, 2015 Sess. (N.C. 2015) (defining “money transmission” to include “maintaining control of virtual currency on behalf of others” and allowing licensees to hold as “permissible investments . . . [v]irtual currency owned by the licensee, but only to the extent of outstanding transmission obligations received by the licensee in like-kind virtual currency”), available at <http://www.ncleg.net/Sessions/2015/Bills/House/PDF/H289v1.pdf>. For analysis of this bill, see *North Carolina Bill Defines Bitcoin as “Permissible Investment,”* COINFOX.COM (May 22, 2015), <http://www.coinfox.info/news/2085-north-carolina-bill-defines-bitcoin-as-permissible-investment>. See also A.B. 1326, 2015-16 Leg., Reg. Sess. (Cal. 2015) (last amended Jun. 1, 2015) (extending licensing requirements to persons or entities developing virtual currency network software or providing data storage or cyber security services for licensed businesses), https://leginfo.ca.gov/faces/billNavClient.xhtml?bill_id=201520160AB1326.

97. See *Questions from the Community: itBit's Trust Charter*, ITBIT.COM (May 18, 2015 1:30 PM), www.itbit.com/blog/questions-from-the-community-itbits-trust-charter (providing a splendid chart comparing the operational differences between the trust company charter, the BitLicense, and a traditional money transmitter license).

98. See *id.*

99. *Virtual Currencies: International Actions and Regulations*, PERKINS COIE, <http://www.perkinscoie.com/virtual-currencies-international-actions-and-regulations> [hereinafter Perkins Coie Virtual Currencies Report] (last updated June 2015) (containing a chart showing actions by many national governments). The report is updated periodically.

100. *Id.*

101. *Id.*

102. *Id.*

103. See GLOBAL LEGAL RES. DIRECTORATE STAFF, REGULATION OF BITCOIN IN SELECTED JURISDICTIONS (2014), <http://www.loc.gov/law/help/bitcoin-survey/> (hereinafter Global Research Center 2014 Report); Perkins Coie Virtual Currency Report, *supra* note 99.

104. Perkins Coie Virtual Currency Report, *supra* note 99 (e.g. Australia, Canada, and Germany).

regulate virtual currencies as commodities,¹⁰⁵ or as exchange.¹⁰⁶ Governments have issued warnings about the risks of using virtual currencies,¹⁰⁷ and have announced their intentions to apply existing anti-money-laundering laws and reporting to virtual currency transactions.¹⁰⁸ The predominant existing regulations around the world, however, focus on taxation and frameworks to thwart the use of cryptocurrencies.¹⁰⁹ As far as we have been able to find, only the Swiss government has announced its intention not to regulate Bitcoin.¹¹⁰

Canada's federal government is the exception to this pattern of limited regulation of cryptocurrencies. Canada is the only national government so far to amend its anti-money-laundering and terrorist financing *statute* specifically to cover cryptocurrencies.¹¹¹ The June 19, 2014 amendments to Canada's Proceeds of Crime (Money Laundering) and Terrorist Financing Act cover four main subject areas: (1) regulating those dealing in digital currencies as money service businesses, so that they are subject to record keeping, verification procedures, suspicious transaction reporting, and registration requirements; (2) requiring registration with the Financial Transactions and Reports Analysis Centre of Canada ("FINTRAC," which is Canada's equivalent to the U.S. Department of the Treasury's FinCEN) and implementation of a full-dress anti-money laundering compliance program; (3) covering all foreign digital currency money service businesses that market to Canada as well as those inside Canada (but exempting businesses providing services only outside Canada for external services only); and (4) prohibiting banks from opening accounts for digital currency money services businesses if they are not registered with FINTRAC.¹¹² The term "dealing in virtual currencies" was not defined. As recently as June 2015, a report prepared for the Senate Committee

105. *Id.* (e.g. Finland and Germany).

106. *Id.* (e.g. Netherlands).

107. *Id.* (e.g. Argentina, Belgium, and Brazil).

108. See, e.g., Proceeds of Crime (Money Laundering) and Terrorist Financing Act, S.C. 2000, c. 17 (Can.), amended by S.C. 2014, c. C-31 (Can.), <http://laws-lois.justice.gc.ca/PDF/P-24.501.pdf>; Perkins Coie Virtual Currency Report, *supra* note 99 (Czech Republic).

109. See Global Research Center 2014 Report, *supra* note 103 *passim*; Perkins Coie Virtual Currency Report, *supra* note 99.

110. *Swiss Government to Refrain from Bitcoin Regulation*, COINBRIEF (June 13, 2015), <http://coinbrief.net/swiss-bitcoin-regulation> (describing study conducted by Swiss National Bank and the government's Federal Council that led to the conclusion not to regulate Bitcoin "for the present," and noting that any victims of Bitcoin problems were "already protected by Swiss law")

111. Proceeds of Crime (Money Laundering) and Terrorist Financing Act, S.C. 2000, c. 17 (Can.), amended by S.C. 2014, c. C-31 (Can.). See Christine Duhaime, *Canada Implements World's First National Digital Currency Law; Regulates New Financial Technology Transactions*, DUHAIME LAW (July 2014), <http://www.duhaime.com/2014/06/22/canada-implements-worlds-first-national-bitcoin-law>.

112. See FIN. TRANSACTIONS & REPORTS ANALYSIS CTR. OF CAN., FINTRAC ADVISORY REGARDING MONEY SERVICES BUSINESSES DEALING IN VIRTUAL CURRENCY (July 30, 2014), <http://www.canafe-fintrac.gc.ca/new-neuf/avs/2014-07-30-eng.asp>. See also Duhaime, *supra* note 111.

on Banking, Trade and Commerce recommended both monitoring and “a light regulatory touch—almost a *hands off* approach.”¹¹³

As of the mid-point of 2015, it remains unclear whether other national governments outside the United States and Canada will see a need to take additional steps to regulate cryptocurrencies or regulate cryptocurrency market participants engaged in commodities or securities brokering or intermediaries engaged in transaction execution of value storage. Not all national governments apparently are persuaded that cryptocurrencies will mature into full-fledged competitors for existing legal tender or payment systems,¹¹⁴ or that they will survive future price volatility,¹¹⁵ operations suspensions,¹¹⁶ or losses.¹¹⁷

Beyond individual nation-states, other groups are working on assessing the risks and benefits of cryptocurrencies. In what is perhaps the most extensive report on the regulatory risks and needs of virtual currencies to date outside the United States and Canada, the European Banking Authority (“EBA”) published its “Opinion on ‘virtual currencies’” in July 2014.¹¹⁸ The Opinion identifies multiple risk factors that may affect virtual currency market participants¹¹⁹ and lays out a “proposed regulatory approach,”¹²⁰ including an “immediate regulatory response for the short term,”¹²¹ and a “rationale for a consistent regulatory response across the EU.”¹²² The Opinion specifies risks to users, non-user market participants, financial integrity, payments systems and providers whose businesses involve fiat currencies, and risks to regulatory

113. STANDING S. COMM. ON BANKING, TRADE & COMMERCE, DIGITAL CURRENCY: YOU CAN'T FLIP THIS COIN (Can. 2015), <http://www.parl.gc.ca/Content/SEN/Committee/412/banc/rep/rep12jun15-e.pdf>.

114. See, e.g., Jerin Mathew, *Japan's Finance Minister Taro Aso Says He Thought Bitcoin 'Won't Last Long'*, INT'L BUS. TIMES (Feb. 28, 2014, 10:53 AM), <http://www.ibtimes.co.uk/japans-finance-minister-taro-aso-says-he-thought-bitcoin-wont-last-long-1438312>.

115. BITCOIN PRICE INDEX CHART, COINDESK.COM, <http://coindesk.com> (last visited May 31, 2015) (showing price fluctuations since May 31, 2014 from more than \$600 per bitcoin to less than \$200 briefly in January 2015 to \$232.60 at 1 pm on May 31, 2015; trading over week prior to May 31, 2015 ranged from \$232.60 to \$241.19).

116. E.g., Kim LaChance Sandrow, *Bitcoin Exchange Bitstamp Suspends Operations Following Hack*, ENTREPRENEUR.COM (Jan. 5, 2015, 5:15 PM), <http://www.entrepreneur.com/article/241432> (last visited May 31, 2015); Louis Goddard, *Bitcoin Exchange BitFloor Suspends Operations After \$250,000 Theft*, THEVERGE.COM (Sept. 5, 2012, 07:12 AM), [http://www.theverge.com/2012/9/5/3293375/bitfloor-bitcoin-exchange-suspends-operations-after-\\$250,000-theft](http://www.theverge.com/2012/9/5/3293375/bitfloor-bitcoin-exchange-suspends-operations-after-$250,000-theft) (last visited May 29, 2015) [hereinafter Goddard].

117. Cameron Keng, *Bitcoin's Mt. Gox Goes Offline, Loses \$409 Million -- Recovery Steps and Taking Your Tax Losses*, FORBES (Feb. 25, 2014, 4:46 AM), <http://www.forbes.com/sites/cameronkeng/2014/02/25/bitcoins-mt-gox-shuts-down-loses-409200000-dollars-recovery-steps-and-taking-your-tax-losses/>; Goddard, *supra* note 116 at 1.

118. EUR. BANKING AUTH., EBA OPINION ON ‘VIRTUAL CURRENCIES,’ (Jul. 4, 2014), [hereinafter EBA 2014 Opinion], <https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf>.

119. *Id.* at 5-6, 21-37.

120. *Id.* at 38-45.

121. *Id.* at 43-44.

122. *Id.* at 45-46.

authorities.¹²³ It also articulates features of both the “immediate regulatory response” and some longer-term goals.¹²⁴

Focusing on the EBA’s recommendations for the intermediate response, the Opinion advances a series of specific goals that have much in common with the state of regulatory play in the United States and uses regulatory models similar to those we use to explain our own thoughts on what needs to be addressed inside the United States in the near-term. Among the risks addressed by the Opinion are:

- Losses and theft of virtual currencies,
- Large-scale money laundering or criminal activity facilitated by virtual currency exchanges,
- Damage to conventional payment systems and payment system operators, and
- Risks to individual users of virtual currencies.¹²⁵

The intermediate solutions to these issues involve (1) creating a requirement that any entity participating in the virtual currency market be “a legal person”¹²⁶ and be “responsible for maintaining the integrity of the central transaction ledger, the protocol, and any other core functional component of the scheme,” and meet “regulatory and supervisory requirements” imposed by the overall regulatory system created;¹²⁷ (2) recommending that virtual currency exchanges be subjected to the anti-money laundering and counter-terrorist financing provisions of the 2005 EU Anti Money Laundering Directive,¹²⁸ which would make them “subject to its anti-money laundering and counter terrorist financing requirements”¹²⁹ and impose requirements like the “customer-identification-program requirements”¹³⁰ of FinCEN’s AML regulations;¹³¹ (3) “shielding regulated financial services from” virtual currency schemes and “mitigat[ing]... risks that arise from the interaction between [virtual currency] schemes and regulated financial services”;¹³² and (4)

123. *Id.* at 21-37.

124. *Id.* at 44-46.

125. *Id.* ¶ 177, at 44.

126. *Id.* ¶ 159, at 40.

127. *Id.* ¶ 154, at 39.

128. Directive 2005/60, of the European Parliament and of the Council of 26 October 2005 on the Prevention of the Use of the Financial System for the Purpose of Money Laundering and Terrorist Financing, <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32005L0060>. Readers should note that the EBA 2014 Opinion uses the term “obliged entities,” which does not appear in this Directive.

129. EBA 2014 Opinion, *supra* note 118, at 6, ¶178, at 44.

130. *Id.* ¶ 156, at 40.

131. Financial Crimes Enforcement Network, Department of the Treasury, 31 C.F.R. ch. X (2015).

132. EBA 2014 Opinion, *supra* note 118, ¶177, at 44.

adopting measures that are designed to protect individual users, including liquidity requirements,¹³³ accountability to regulators,¹³⁴ and documentation requirements.¹³⁵

The mixture of public and private legal purposes, along with measures that can be used to maintain the functions of virtual currency market participants (through transparency, corporate governance, sufficient capital reserves and liquidity for the scope of the entity's operations), effectively align with the regulatory models we discuss in Part III of this article. In Part III.A, we look at other regulatory regimes in the United States whose coverage bears on cryptocurrency market participants in one form or another. The 2014 BitLicense proposal described in Part III.B of this article and the final 2015 BitLicense regulation focus on the prudential regulatory needs we mention throughout this article.

We move beyond other regulatory regimes in Part V to suggest a framework of "commercial law" rules. Among the reasons we recommend development of commercial law "default rules" is the goal of promoting uniformity and certainty in transactions among counterparties and in interpretations by courts. In our view, commercial law rules mitigate risks to individual users that are different from those addressed by prudential regulation and corporation laws. Commercial laws set forth rights and duties of persons who use intermediaries in payments or value-conversion transactions. Part V outlines some key features we would consider appropriate for a commercial law to cover.

III. Which Existing Regulatory Schemes Might Help Us Model a Regulatory Approach to Cryptocurrency Intermediaries?

Financial products that share at least some attributes with cryptocurrencies already exist and are already regulated. Policymakers considering whether and how to regulate a new industry may start by looking at how current law treats analogous products. In this Part, we describe the regulatory models that we think are more likely to influence regulators looking at cryptocurrency. These descriptions are not meant to convey a complete synopsis of each model, but rather to focus on high-level policy objectives of each and highlight salient differences among the models.

In Part III.A, we look at the regulatory models that already apply to some products and services with which cryptocurrencies might compete. These models, which we described briefly in the Introduction, address: (1) public-law purposes (such as prevention and detection of money laundering or of tax

133. *Id.* ¶ 164, at 41.

134. *Id.* ¶ 153, at 39.

135. *Id.* ¶ 161, at 41, ¶ 159, at 40.

evasion); (2) purposes related to market-efficiency, transparency and accountability; and (3) default rules for transaction-execution purposes.

In Part III.B, we look in somewhat greater depth at the New York State Department of Financial Services' BitLicense regulation and the 2014 proposal from which it emerged. The Final Regulation employs components of several of the models we have suggested in Part III.A. We explain our concerns about New York's approach. Among these are our concerns that the BitLicense imposes more onerous prudential regulatory requirements on cryptocurrency intermediaries than New York State imposes on legacy providers whose e-payment products and services are provided via the internet (including those that states license and supervise as "money transmitters").

A. Regulatory Models that Apply to Products and Services with Which Cryptocurrencies May Compete

1. Payment Systems

The most obvious model for regulating cryptocurrency market participants—including miners managing the block chain but also all of the users and intermediaries who facilitate payments using cryptocurrencies—is as a payment system. The term "payment system" refers to an operational network that is governed by laws, rules and standards and that links bank accounts, providing the functionality for monetary exchange using bank deposits.¹³⁶ The term also includes "the infrastructure (comprised of institutions, instruments, rules, procedures, standards, and technical means) established to effect the transfer of monetary value between parties discharging mutual obligations." Its technical efficiency determines the efficiency with which transaction money is used in the economy and the risk associated with its use.¹³⁷

Payment systems are highly regulated in the United States because they typically involve more than two participants and also involve both credit and liquidity risks of intermediaries whose participation is required to complete the payment transaction from end to end. Beyond the prospect of a consumer user of cryptocurrencies in payments for goods and services having no transparent, end-to-end regulatory scheme by which to measure the execution of the payment transaction, we submit that it is an error to allow some participants in payments transactions to operate with no transparency and little accountability. The difference in operating costs between a regulated payments system

136. See PAYMENT SYSTEMS: DESIGN, GOVERNANCE AND OVERSIGHT 3 (Bruce J. Summers, ed., Central Banking Publications Ltd, London, 2012).

137. See Biago Bossone & Massimo Cirasino, *The Oversight of the Payment Systems: A Framework for the Development and Governance of Payment Systems in Emerging Economies*, WORLD BANK 7 (July 2001), http://www-wds.worldbank.org/external/default/WDSPContentServer/WDSP/IB/2007/03/02/000310607_20070302132738/Rendered/PDF/388270Oversight0of0payments01PUBLIC1.pdf.

provider and an unregulated provider would give a substantial cost advantage to the unregulated provider. Consumer users may or may not appreciate the divergence in the risks to their own transactions. Participants in the larger field of payment systems should not have to compete with unregulated actors while being burdened with the costs of being regulated entities. This view is not motivated by a desire to protect legacy payment systems (a field in which one of us works) from unregulated competition but to ensure that lay users enjoy protections comparable to protections that other payment systems are required to offer.

Despite the fact that participants in Bitcoin-denominated transactions follow the Bitcoin protocol and that the protocol has a small number of basic rules, Bitcoin itself is not a payment system.¹³⁸ A bitcoin holder, or a person having both the public and private keys for a bitcoin or fraction of a bitcoin, may be able to make a person-to-person (“P2P”) or person-to-business (“P2B”) transfer of the bitcoin’s value without the assistance of a trusted intermediary, including a financial institution.¹³⁹ This transfer of ownership rights to a new owner is the equivalent of handing cash or a chattel to another in payment of an obligation or as a gift. Bitcoin are units of value storage or of account, and the systems of drawing against “deposits” of Bitcoin in the various online wallets, competing exchanges, and merchant processing service providers are closer to “payment systems.” On the other hand, some cryptocurrency systems are intended to operate as payment systems, that is, they are operational networks governed by rules and standards that link accounts to use and transfer value between those accounts.¹⁴⁰ For example, Ripple is a payment system.¹⁴¹

Payment system “rules” and operating standards in the United States are found in: (1) statutes such as the federal Electronic Fund Transfer Act¹⁴² and Article 4A of the Uniform Commercial Code enacted by the states,¹⁴³ which govern wholesale and retail electronic transfers involving bank accounts, (2) federal regulations such as the Federal Reserve Regulation E¹⁴⁴ that governs consumer electronic transfers involving bank accounts and prepaid cards, or (3) system rules such as those developed by organizations such as NACHA, the

138. See, e.g., Nakamoto, *supra* note 15, at 1-2 (explaining how the block chain works without a trusted intermediary).

139. *Id.* at 1 (Abstract); Bitcoin Primer, *supra* note 2, at 2-3.

140. Nakamoto, *supra* note 15, at 1; Bitcoin Primer, *supra* note 2, at 2-3.

141. *How Ripple Works*, RIPLE.COM (Oct. 14, 2014), https://ripple.com/knowledge_center/how-ripple-works [hereinafter “How Ripple Works”]. Of particular note is discussion of how Ripple helps users avoid counterparty risk otherwise present when intermediaries such as banks participate in transactions.

142. 15 U.S.C. §§ 1693-1693r (2012).

143. U.C.C. § 4A-101 to -507 (AM. LAW INST. & UNIF. LAW COMM’N 2012).

144. 12 C.F.R. pt. 1005 (2014).

Clearing House Interbank Payments System (“CHIPS”),¹⁴⁵ Visa¹⁴⁶ and MasterCard.¹⁴⁷

Statutory schemes and the regulations that implement them—such as the Electronic Fund Transfer Act and its companion Regulation E mentioned above—and some payment system rules in the United States may provide for consumer protections against fraud and error. Visa¹⁴⁸ and MasterCard,¹⁴⁹ for example, both have policies that protect cardholders from liability for most unauthorized transactions. The Visa and MasterCard system rules supplement the longstanding federal Regulation E’s consumer protection requirements for disclosures,¹⁵⁰ procedures for error resolution,¹⁵¹ and limitations on consumer liability for unauthorized transfers.¹⁵² The Bitcoin protocol does not address these issues.

Statutes and system rules also prescribe rules for payment transactions to assist counterparty and particularly multiple-party transactions. For example, the U.C.C.’s Article 4A, enacted in every state,¹⁵³ contains provisions that spell out when payments occur,¹⁵⁴ when obligations are discharged by payment,¹⁵⁵ and the consequences of payments made late or otherwise improperly executed.¹⁵⁶ Article 4A established a set of private-law default rules that govern all or part of transactions not specifically covered by contract or system rules. Default rules facilitate transactions and establish trust for transaction participants. Most of the default rules can be varied by agreement of the parties to the transaction or by system rules that apply to some or all of the parties to the transaction.

Regulation of electronic consumer payment systems at the federal level in the United States requires, for example, upfront disclosure of costs, as both the Truth in Lending Act¹⁵⁷ and Regulation E’s provisions on cross-border

145. *Clearing House Interbank Payments System Rules and Administrative Procedures*, THE CLEARING HOUSE (Mar. 2013), <https://www.chips.org/financials/operations/rulesDocs/073219.pdf>.

146. *Visa International Operating Regulations*, VISA (2013), <https://usa.visa.com/download/merchants/visa-international-operating-regulations-main.pdf>.

147. *MasterCard Rules*, MASTERCARD (2014), http://www.mastercard.com/us/merchant/pdf/BM-Entire_Manual_public.pdf.

148. *Zero Liability*, VISA U.S.A., <http://usa.visa.com/personal/security/zero-liability.jsp> (last visited on Oct. 8, 2014).

149. *MasterCard Zero Liability Protection*, MASTERCARD, <http://www.mastercard.us/zero-liability.html> (last visited on Oct. 8, 2014).

150. 12 C.F.R. §§ 1005.4 & 1005.7 (2014).

151. *Id.* § 1005.11.

152. *Id.* § 1005.6.

153. *See UCC Article 4A, Funds Transfers* (1989), UNIF. LAW COMM’N, [http://www.uniformlaws.org/Act.aspx?title=UCC%20Article%204A,%20Funds%20Transfers%20\(1989\)](http://www.uniformlaws.org/Act.aspx?title=UCC%20Article%204A,%20Funds%20Transfers%20(1989)) (last visited Aug. 30, 2015).

154. U.C.C. § 4A-401 (AM. LAW INST. & UNIF. LAW COMM’N 2012).

155. *Id.* § 4A-406(b).

156. *Id.* §§ 4A-303 to -305.

157. 15 U.S.C. §§ 1631(a), 1632(a) & (c) (2012 & Supp. 2013).

remittance transfers do.¹⁵⁸ Federal laws also set forth minimum procedures for making claims of execution errors (delays, delivery to a recipient not intended by the initiator of the payment, duplicate payments, and the like).

Other important features of traditional payment system regulation, whether based on statutes or system rules, relate to transaction execution and implied warranties that persons or institutions participating in the payments flow either meet certain behavioral standards or will be responsible for the consequences of their failure to do so. These implied warranties favor other participants in the transaction—or series of transactions—that may be required to complete the transfer. For example, U.C.C. Article 4A prescribes liability for certain transaction execution errors, such as delivery to the wrong beneficiary¹⁵⁹ or late delivery of the funds.¹⁶⁰ U.C.C. Articles 3 and 4 impose implied warranties on transferors of notes, drafts and checks,¹⁶¹ and on those who present them for payment.¹⁶² At the federal level, subpart C of Federal Reserve Board Regulation “CC,”¹⁶³ which implements the Check Clearing for the 21st Century Act,¹⁶⁴ imposes implied warranty obligations on counterparties otherwise subject to their provisions.¹⁶⁵ Rules allocating liability for transmission errors and imposing warranty obligations would be similarly useful for cryptocurrencies.

A set of rules for cryptocurrency payment transactions need not cover every transaction to be effective generally. For example, payment methods can benefit from the establishment of clear parameters for when the particular set of rules applies and does not apply. Certain payment rules provide exemptions for *de minimis* activities or players. For instance, Regulation E does not apply to those cross-border remittance transfers under \$15¹⁶⁶ or to entities that provide one hundred or fewer remittance transfers a year.¹⁶⁷ Persons or entities operating below these levels are not expected to comply with the regulation.¹⁶⁸ Given that hefty compliance costs may attend participation in regulated payment systems, a *de minimis* exemption for similarly low-volume or low-value transactions might make sense for online wallet or exchange operations. The U.C.C. payments provisions—Articles 3, 4 and 4A—each have provisions

158. *Id.* § 1693o-1(a)(2) (disclosure required).

159. U.C.C. § 4A-303 to -304.

160. *Id.* § 4A-305.

161. *Id.* §§ 3-416, 4-207.

162. *Id.* §§ 3-417, 4-208.

163. 12 C.F.R. pt. 229 (2014).

164. 12 U.S.C. §§ 5001-5018 (2012).

165. 12 C.F.R. § 229.34, .38, .52 (2014).

166. *Id.* § 1005.30(e)(2)(i) (definition of “remittance transfer”).

167. *Id.* § 1005.30(f)(2)(i) (definition of “remittance transfer provider”).

168. See Electronic Fund Transfers (Regulation E), 77 Fed. Reg. 50,244 (Aug. 20, 2012) (discussion of “safe harbor” created by sections 1005.30(e)(2)(i) and 1005.30(f)(2)(1)).

explaining the nature of the transactions they govern.¹⁶⁹ In the case of Article 4A, coverage depends on whether the bank that has received an instruction to pay (called a “payment order”) has agreed to handle it, a status referred to as “acceptance.” Before executing the payment order, the bank will have verified it using security procedures adopted by agreement with its customer as required by the provisions of Section 4A-201,¹⁷⁰ and will have agreed to handle the payment order, which is signified by “acceptance” of the customer’s payment order.¹⁷¹

No existing or proposed regulation of cryptocurrencies in the United States so far offers rules that are comparable to these more established *payment system rules* in terms of determining their coverage, requiring disclosures, managing transaction execution, or dealing with errors or disputes in transactions or transfers. Thus, they do not provide rules that make cryptocurrency market participants function with the same degree of transparency and accountability to their counterparties or provide users with means of obtaining remedies when the transaction is not completed pursuant to instructions that traditional payment system statutes, regulations, or rules do. A comparable situation existed prior to the enactment by the states of U.C.C. Article 4A when wholesale wire transfers were governed by bilateral contracts for the most part and participants lacked end-to-end rules governing transfers.¹⁷²

2. Money Services Businesses and Money Transmission

Non-depository providers of services that receive and/or transmit money on behalf of customers are regulated by the states,¹⁷³ with additional federal regulations dealing with specified actors and their respective anti-money-laundering measures,¹⁷⁴ economic sanctions compliance,¹⁷⁵ and record keeping

169. U.C.C. §§ 3-102, 4-102 (AM. LAW INST. & UNIF. LAW COMM’N 2002); U.C.C. §§ 4A-102, -104(a), -108 (AM. LAW INST. & UNIF. LAW COMM’N 2012).

170. U.C.C. § 4A-201.

171. *Id.* § 4A-209.

172. U.C.C. Art. 4A, Pref. Note, iii and § 4A-507 (2012). For additional information on the operation of wholesale wire transfers and the rights and duties of participants, see Raj Bhala, *Legal Foundations of Large Value-Transfer Systems*, in *THE PAYMENT SYSTEM: DESIGN, MANAGEMENT AND SUPERVISION* 53, 63 & n. 52-53 (Bruce J. Summers, ed., 1998).

173. See State-by-State Regulation, THE NAT’L MONEY TRANSMITTERS ASS’N, <http://www.nmta.us/state-by-state-regulation> (last visited Dec. 27, 2014) (useful summary of manner in which states regulate licensing and operation of money services businesses and money transmitters as businesses).

174. See generally 31 C.F.R. ch. X (2014) (setting out anti-money-laundering requirements for various entities that meet the definition of “financial institution” under 31 U.S.C. §§ 5311-5330 (2012 & Supp. 2013)).

175. See, e.g., *id.* § 560.530(a)(3) (requirements for special licenses for transactions with Iran). For a comprehensive listing of OFAC regulations and guidance pertinent to Iran, see Iran Sanctions, U.S. DEP’T OF THE TREASURY, www.treasury.gov/resources-center/sanctions/Programs?pages/Iran.aspx (last visited May 28, 2015).

and reporting requirements.¹⁷⁶ In this subsection, we briefly discuss the most significant federal and state statutes and regulations that currently apply to cryptocurrency market participants such as online wallets and exchanges. We do not take positions on whether existing federal or state laws are good laws; we instead present them as illustrations of the various means by which the federal government and the states have regulated aspects of these types of businesses and operators to date.

Money-service-business and money-transmitter prudential regulatory schemes straddle the public-law and market-enhancing models we outlined above. Crafting prudential regulations of cryptocurrency intermediaries as money service businesses or money transmitters is part of the larger scheme of regulations needed to create the trust that we think cryptocurrencies will need to gain wider acceptance, but it is not the focus of this Article.

a. Federal Laws that Apply to Money Services Businesses and Money Transmission.

The Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN") requires entities operating as "money services businesses" ("MSBs"), including currency exchanges and money transmitters, to register with FinCEN,¹⁷⁷ establish a risk-based anti-money laundering program,¹⁷⁸ and maintain certain records and file certain reports.¹⁷⁹ FinCEN's MSB registration regulations do not have prudential supervision or other prescriptive provisions. MSB regulations apply to traditional, brick-and-mortar check cashers, remittance transfer companies such as Western Union and MoneyGram, and others.¹⁸⁰

FinCEN's 2013 Guidance identifies participants in certain cryptocurrency schemes as "money transmitters" for purposes of its MSB regulations and requires their compliance with its MSB registration requirements.¹⁸¹ The agency explained that the regulatory definition of "money transmission" includes the transmission of "currency, funds, or *other value that substitutes for*

176. See Agency Collection Activities; Comment Request; Renewal without Change of Bank Secrecy Act Recordkeeping Requirements, 79 Fed. Reg. 30,928 (May 29, 2014) (summary of record-keeping and recording requirements imposed under 31 C.F.R. ch. X).

177. 31 C.F.R. § 1022.380 (2014).

178. *Id.* § 1022.210(a), (b), (d) (describing, respectively, requirements to develop, implement and maintain AML programs, to ensure that the program is "commensurate with the risks posed by the location and size of, and the nature and volume of the financial services" provided by the MSB, and to set forth minimum elements of the AML program).

179. See generally *id.* §§ 1022.300-.380 (reports to be made by money service businesses), .400-.410 (records to be maintained by money service businesses).

180. See *id.* § 1010.100(d) (exclusion of banks and persons regulated by the Securities and Exchange Commission or the Commodities Futures Trading Commission), .100(ff) (coverage only if "activity threshold" for money service business greater than \$1,000 per day in one or more transfers; no threshold for money transmitters' coverage), .100(t) (definition of "financial institution").

181. 2013 FinCEN Guidance, *supra* note 14, at 1.

currency” and thus reaches the transfer of money substitutes such as cryptocurrencies.¹⁸²

FinCEN later limited the reach of its 2013 Guidance by clarifying that an entity is not an MSB if it merely “mines” Bitcoin by solving the algorithms for which the Bitcoin protocol offers Bitcoins, pays for goods and services with it, or converts Bitcoin into legal tender.¹⁸³ The agency also has advised that the production and distribution of software to manage Bitcoin holdings is not “money transmission,” even if the software facilitates the purchase and sale of crypto-currency.¹⁸⁴ It is possible that a market participant in cryptocurrencies will have registration requirements under FinCEN’s guidance, a circumstance that would allow FinCEN to track the participant’s compliance with federal anti-money laundering, tax reporting and economic sanctions statutes and regulations, but might not have to obtain a license from any state as a “money transmitter” or “money service business,” a situation we describe below. As the states decide how they want to regulate cryptocurrency wallets and exchanges, more wallet and exchange providers may have to comply with state as well as federal requirements.

b. State Laws Regulating Money Transmitters, Money Service Businesses, and their Receipt and Transfers of Money

Prudential regulation of money transmitters and other MSBs remains the province of the states. States have established robust licensure programs,¹⁸⁵ require background checks on principal owners and officers, set bonding/security and minimum capitalization requirements,¹⁸⁶ dictate or require regulations on the types of permissible investments,¹⁸⁷ and authorize on-going review of financial statements.¹⁸⁸ Generally, money transmitters are required to maintain the amount of funds they are holding for senders based on transaction volume.¹⁸⁹ Like provisions that underlie federal bank “deposit insurance”

182. *Id.* at 2-3 (citing 31 C.F.R. § 1010.100(ff)(5)(i)(A) (2014)) (emphasis added).

183. *Application of FinCEN’s Regulations to Virtual Currency Mining Operations*, FIN. CRIMES ENF’T NETWORK 2-3 (Jan. 30, 2014), http://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R001.pdf. For additional information on how Bitcoin, for example, are mined, see Bitcoin Primer, *supra* note 2, at 2.

184. FIN-2014-R002, *supra* note 77, at 2.

185. *E.g.*, WASH. REV. CODE § 19.230.030 (2013).

186. *E.g.*, *id.* § 19.230.050, .060 (surety bond/security requirements; net worth requirements).

187. *E.g.*, *id.* § 19.230.200-210.

188. *See, e.g.*, VA. CODE ANN. § 6.2-1900 (2014) (defining “money transmission” and “money transmitter”); WASH. REV. CODE § 19.230.010(17)-(19) (2013) (defining “money services,” “money transmission,” and “money transmitter”). For a comprehensive listing of state “money transmission” and “money services” statutes compiled by the National Conference of State Legislatures, see NAT’ CONF. OF STATE LEGISLATURES, www.ncsl.org (last visited Dec. 28, 2014).

189. *See, e.g.*, WASH. REV. CODE § 19.230.200(1)(a)-(b) (2013); VA. CODE ANN. § 6.2-1912.A (2014) (licensee liable for “all funds collected for transmission”); *id.* § 6.2-1918.A(ii) (requirement to hold permissible investments equal to at least the aggregate market value of all

offered by the Federal Deposit Insurance Corporation (“FDIC”),¹⁹⁰ these reserve requirements ensure the depositor’s ability to redeem (or recover) the same value that he or she placed with the third-party money transmitter.¹⁹¹ Some state regulators have described how their states’ money transmission or money service business statutes apply to cryptocurrencies and the entities offering services as exchanges, as well as how statutes apply to individuals transacting with peers.¹⁹² Compared to the FinCEN provisions described in the previous section, which are focused on registration of entities offering types of products and services and establishing their anti-money-laundering compliance responsibilities, state money-transmitter and money-service-business regulations, in our view, are more oriented towards prudential and market-enhancing purposes.

One example showing the need for prudential regulation is the case of the Mt. Gox Bitcoin exchange in Japan, which suspended operations in February 2014.¹⁹³ Shortly before that event, commentators began to call for cryptocurrency depositories (wallets and exchanges) to protect depositors’ rights to redeem their deposits by reserves, a trust, or some form of “deposit” insurance.¹⁹⁴ However, deposit insurance in the United States would not necessarily cover bitcoin held by a bank outside the United States for a

outstanding money transmission transactions and sales of money orders from operations in all states in which the licensee does business).

190. Federal Deposit Insurance Act of 1950, Pub. L. No. 81-797, 64 Stat. 873 (codified as amended at 12 U.S.C. §§ 1811-1835a (2012)).

191. See THE OXFORD UNIVERSAL DICTIONARY 1680-81 (3d ed. 1955) (definitions of “redeem” and “redemption” with origins from Middle English related to deposits of funds or property (particularly in the latter case when the deposit is for the purpose of securing an obligation)). Deposit insurance, for example, protects the depositor’s ability to redeem at par the funds deposited with a bank or credit union or the holder of a prepaid card’s ability to access the underlying funds, subject to whatever notice the depositor and depository may have agreed upon by contract. See *Insurability of Funds Underlying Stored Value Cards and Other Nontraditional Access Mechanisms*, 73 Fed. Reg. 67,155-01 (Nov. 13, 2008) (revising requirements for “pass-through” deposit insurance for certain pooled deposit accounts); *Stored Value Cards and Other Nontraditional Access Mechanisms*, New General Counsel’s Op. No. 8, FIL-129-2008, FED. DEPOSIT INS. CORP., <https://www.fdic.gov/news/news/financial/2008/fil08129.pdf> (Nov. 17, 2008) (replacing original Fed. Deposit Ins. Corp. General Counsel Opinion No. 8 issued in 1996) [hereinafter “FIL-129-2008”].

192. E.g., *Supervisory Memorandum 1037, Regulation of Virtual Currencies under the Texas Money Services Act*, TEX. DEP’T OF BANKING 2-3 (Apr. 3, 2014), <http://www.dob.texas.gov/public/uploads/files/consumer-information/sm1037.pdf> (distinguishing between exchanges of cryptocurrencies into “sovereign currencies” via third-party providers as money transmission, and movements from one cryptocurrency to another cryptocurrency as not constituting money transmission regardless of the number of participants in the transactions); *Guidance Document MT 2014-01*, KAN. OFF. OF THE ST. BANKING COMM’R (June 6, 2014), http://www.osbckansas.org/mt/guidance/mt2014_01_virtual_currency.pdf; Press Release, N.Y. Dep’t of Fin. Serv., New York Requires Foreign-Located Money Transmitters including Bitcoin Exchanges and Administrators to Obtain Money Transmitter Licenses (Mar. 31, 2011), (announcing abandonment of “physical presence” in the state as a prerequisite for money transmitter licensure).

193. See Hern, *Mt. Gox Offline*, *supra* note 4.

194. See, e.g., Joe Adler, *Bitcoin Backers Seek FDIC-Style Insurance*, AM. BANKER (Jan. 22, 2014 12:14 ET), http://www.americanbanker.com/issues/179_15/bitcoin-backers-seek-fdic-style-insurance-1065089-1.html (mentioning insurance prospects through Lloyd’s of London and derivatives trading).

customer or held by a bank or other depository or actor outside the United States.¹⁹⁵ For example, U.S. deposit insurance covers depositors whose deposits are in banks insured by the FDIC, even if the depositor is not a citizen or resident of the United States.¹⁹⁶ However, price fluctuations of bitcoin could complicate deposit insurance because of the extra burden of determining the value on initial deposit and the value at failure with the need possibly to cover a decline in value at failure over the value at deposit. The suit brought by U.S. persons against Mt. Gox seeking to recover for the losses of Bitcoin they had sustained demonstrates the importance of prudential regulation and adequate insurance or other forms of deposit protection for customers of domestic and foreign wallets or exchange operators.¹⁹⁷

Although it is very important, it is *insufficient* for the states to regulate cryptocurrency market participants merely on a prudential basis. States also should enact laws that assign rights and responsibilities to crypto-payments intermediaries regarding commercial aspects of these payments transactions. Without rules defining a participant's potential liabilities, it is not possible to determine or guarantee that entity's safe and sound operations vis-à-vis its customers.

3. Deposit Taking and Deposit Insurance

Taking deposits is a highly regulated business in the United States. It also is a fundamental aspect of the highly regulated business of banking under the National Bank Act.¹⁹⁸ The United States, however, has no general “law of deposit” that would reach deposits of value made in units such as cryptocurrencies. The United States does have a more limited-scope scheme known as “deposit insurance.” Deposit insurance provides the guarantees that the depositor will be able to redeem—that is, to retrieve from the depository—the same value that the depositor placed with the depository on the basis of their original agreement up to any limit prescribed by their agreement or by any applicable program of insurance, whether public or private. Deposit insurance systems serve as “redeemers of last resort” for depositors in the event the depository to which they entrusted value fails or is unable to perform.¹⁹⁹ Deposit insurance has public- and market-enhancing purposes.

195. See 12 U.S.C. §§ 1813(l)(1) (definition of “deposit”), (m) (definition of “insured deposit”) (2012). The key requirement in the definition of “deposit” is the receipt of “money or its equivalent” by a bank or other insured financial institution. *Id.* § 1813(l)(1).

196. See *When a Bank Fails - Facts for Depositors, Creditors, and Borrowers*, FED. DEPOSIT INS. CORP. (July 28, 2014), <https://www.fdic.gov/consumers/banking/facts/>.

197. See Class Action Complaint *passim*, *Greene v. Mt. Gox Inc.*, No. 14-01437 (N.D. Ill. Feb. 27, 2014).

198. National Bank Act, 12 U.S.C. § 24 (Seventh) (2012) (granting general powers to national banks, including the power to take deposits of money, as well).

199. See EBA 2014 Opinion, *supra* note 118, at 43 ¶ 174 (discussing special risks associated with virtual currencies because there is no “redeemer of last resort”).

Congress has defined the term “deposit” for purposes of Federal Deposit Insurance Corporation (FDIC) insurance to mean “the unpaid balance of money or its equivalent” received by a bank that meets certain other requirements.²⁰⁰ Whether holdings of cryptocurrencies can or should constitute deposits is an interesting policy question. “Deposit”-taking institutions currently are required to obtain and hold a banking or similar charter, and to be approved for deposit insurance. In sharp contrast to money transmitters, which must maintain reserves or “permissible investments” equal to their average daily transmission liabilities in the equivalent of one-to-one reserves,²⁰¹ depository institutions operate a system of fractional reserves,²⁰² loan out a portion of their deposits, and thus are able to expand the supply of money in circulation. Indeed, the ability of banks to increase the money supply by operating on fractional reserves—not keeping enough money on hand to repay all of the depositors at one time—is one of the reasons proponents believe virtual, non-fiat currencies are superior to government-controlled currencies.²⁰³

One could argue that treating cryptocurrencies as “deposits” for regulatory purposes is a logical next step given the capacity for technology to blur the line between traditional “deposits” in insured depository institutions and the proliferating numbers of “access devices” (such as payroll or other prepaid cards or mobile wallets) that reach pooled assets.²⁰⁴ Treating cryptocurrency “deposits” as deposits for federal deposit insurance purposes would not

200. Federal Deposit Insurance Act, 12 U.S.C. § 1813(l) (2012).

The term “deposit” is defined for the purposes of determining eligibility for federal deposit insurance, in part, as:

(1) the unpaid balance of money or its equivalent received or held by a bank or savings association in the usual course of business and for which it has given or is obligated to give credit, either conditionally or unconditionally, to a commercial, checking, savings, time, or thrift account, or which is evidenced by its certificate of deposit, thrift certificate, investment certificate, certificate of indebtedness, or other similar name, or a check or draft drawn against a deposit account and certified by the bank or savings association, or a letter of credit or a traveler’s check on which the bank or savings association is primarily liable: *Provided*, That, without limiting the generality of the term “money or its equivalent”, any such account or instrument must be regarded as evidencing the receipt of the equivalent of money when credited or issued in exchange for checks or drafts or for a promissory note upon which the person obtaining any such credit or instrument is primarily or secondarily liable, or for a charge against a deposit account, or in settlement of checks, drafts, or other instruments forwarded to such bank or savings association for collection.

201. *E.g.*, WASH. REV. CODE § 19.230.200(1)(a)-(b) (2013). Additional examples of these types of prudential requirements for money service businesses include surety bond and security requirements, *id.* § 19.230.050, and provisions on the character and fitness of applicants for licenses, *id.* § 19.230.070(b).

202. JONATHAN R. MACEY, GEOFFREY P. MILLER & RICHARD SCOTT CARNELL, *BANKING LAW AND REGULATION* 55-56 (3d ed. 2001).

203. F.A. HAYEK, *DENATIONALISATION OF MONEY: THE ARGUMENT REFINED* 24 (3d ed. 1990). For additional discussion of fractional reserve systems, see Joshua N. Feinman, *Reserve Requirements: History, Current Practices, and Potential Reform*, 1993 FED. RES. BULL. 569, 573 (explaining that a fractional reserve system is “one with reserve requirements of less than 100 percent”).

204. *See generally* FIL-129-2008, *supra* note 191 (revising requirements for “pass-through” deposit insurance for certain pooled deposit accounts).

Regulating Cryptocurrency Payments Intermediaries

necessarily require cryptocurrencies to become “money” or “legal tender.” But it would require a legal framework—a more generalized law of deposit—that we do not have in the United States. Our existing federal statutory deposit-insurance programs focus on certain deposits in commercial banks and federal savings institutions.²⁰⁵ Moreover, apart from the likely objections of other insured depository institutions, the costs of a publicly backed deposit insurance system—even if it were possible to insure only “domestic” deposits with cryptocurrency wallet and exchange operators—likely would be a significant obstacle to the “deposit” and “deposit insurance” models extending to non-bank, non-“currency” products such as cryptocurrencies.

4. SEC Broker-Dealer Registration and Compliance Requirements

Broker-dealer registration and compliance requirements form one of the possible frameworks for regulating persons who facilitate exchanges of cryptocurrencies. Broker-dealers execute instructions on behalf of clients and may transfer assets from clients to third parties. But, these transaction-execution functions are primarily connected with assets held as investments. With regard to cryptocurrencies, the security—whether interests in pools or cryptocurrencies held separately for investment purposes or under the custody of a broker-dealer in an entitlement account, or in cryptocurrency exchanges or instruments based on cryptocurrencies—may need to be registered with the Securities and Exchange Commission or one or more state blue-sky regulators.

Broker-dealer registration and compliance requirements primarily serve market-enhancing purposes, namely efficiency, transparency and accountability. They also deter insider abuses and market manipulation.

Broker-dealers are heavily regulated at the federal level.²⁰⁶ Similar to other financial service providers, persons subject to broker-dealer regulations have to meet requirements related to registration, record keeping, disclosure, and investor protection.²⁰⁷ They also have responsibilities to maintain robust customer-identification programs,²⁰⁸ anti-money laundering compliance programs,²⁰⁹ and economic sanctions compliance requirements.²¹⁰

205. See 12 U.S.C. § 1813(h), (l), (m) (2012). For a discussion of the limits of the “deposit” and “insured deposit” definitions, see *Fed. Deposit Ins. Corp. v. Phila. Gear Corp.*, 476 U.S. 426 (1986).

206. Securities Exchange Act of 1934, Pub. L. No. 73-291, 48 Stat. 881 (also called the Exchange Act, the ‘34 Act, or the 1934 Act) [hereinafter “Exchange Act”]. The full text of the Exchange Act is available at <http://www.sec.gov/about/laws/sea34.pdf>.

207. 17 C.F.R. § 240 (2014). For comprehensive guidance on requirements imposed on broker-dealers, including numerous exclusions and exemptions, see Div. of Trading & Mkts., *Guide to Broker-Dealer Registration*, U.S. SEC. & EXCH. COMM’N (Apr. 2008), <http://www.sec.gov/divisions/marketreg/bdguide.htm>. For some additional discussion of these requirements as applied to cryptocurrencies, see GAO-14-496, *supra* note 83, at 16-17.

208. 31 C.F.R. § 1023.220 (2014).

209. *Id.* § 1023.210.

210. *Id.* § 501.606.

Since 1999, banks that trade in securities must also register as broker-dealers.²¹¹ Non-bank broker-dealers are required to be a member of a self-regulatory organization²¹² as well as of the Securities Investor Protection Corporation (“SIPC”) that insures investors against losses associated with the failure of a broker-dealer and provides other user protections.²¹³ SIPC compensates customers who suffer losses.²¹⁴ Broker-dealer operations are subject to both public and self-regulatory scrutiny; these regulatory systems includes specific enforcement provisions to ensure compliance as well as remedies for investors. These regulations do not set forth the rights and liabilities of parties to transactions in the manner of a commercial law, which is what we recommend be developed for cryptocurrency intermediaries.

Online wallet operators and exchanges in the cryptocurrency industry do not have comparable regulatory requirements and, as a result, their customers are exposed to higher credit and liquidity risks of cryptocurrency wallets and exchanges than are customers of traditional money service businesses or money transmitters or depository institutions. This was an issue following the failure of the Mt. Gox exchange in 2014.²¹⁵ It also is a concern raised by the January 2015 suspension of certain accounts and loss of around 19,000 Bitcoin by the BitStamp exchange; despite the security breach, Bitstamp claims it can refund all affected account holders “in full.”²¹⁶

The broker-dealer and securities regulation models are possible means by which the federal government could regulate cryptocurrency market participants engaged in securities transactions and cryptocurrency assets that qualify as “securities,” such as a unit of cryptocurrency or a right to units held by a broker in a form of entitlement account, although cryptocurrencies themselves are not “securities” (just as they are not “currency” or “legal tender”). Regardless, a “securities regulation” framework would not address the rights and duties of parties using cryptocurrencies in payment of goods or services or the exchange of units of cryptocurrency for legal tender. Thus, although it is highly desirable for the Securities and Exchange Commission (SEC) to continue to regulate and supervise those who would offer securities based on cryptocurrencies, such as it did in *Securities and Exchange*

211. Definition of Terms in and Specific Exemptions for Banks, Savings Associations, and Savings Banks Under Sections 3(a)(4) and 3(a)(5) of the Securities Exchange Act of 1934, 66 Fed. Reg. 27,760 (May 18, 2001); Order Extending Temporary Exemption of Banks, Savings Associations, and Savings Banks from the Definition of “Broker” under Section 3(a)(4) of the Securities Exchange Act of 1934; Notice of Intent to Amend Rules, Exchange Act Release No. 34-47649 (Apr. 8, 2003).

212. Securities and Exchange Act, 15 U.S.C. § 78e (2012).

213. 15 U.S.C. § 78ccc(a)(2)(A) (2012).

214. *Securities Investor Protection Corporation (SIPC)*, U.S. SEC. & EXCH. COMM’N, <http://www.sec.gov/answers/sipc.htm> (last accessed Sept. 3, 2015) (explaining \$500,000 limit on insurance protection for failed broker-dealers).

215. See Hern, *Mt. Gox Bankruptcy Filing*, *supra* note 5.

216. See *Bitstamp Breach*, *supra* note 6.

Commission v. Shavers,²¹⁷ any role played by securities regulators, including the SEC, would not resolve all of the issues involved with the use of cryptocurrencies in payment transactions. These models would not be on par with commercial-law, payments-execution models, such as we propose in Part V.

5. CFTC Commodities Trading Regulation

As Part II explained, many nations have classified cryptocurrencies including Bitcoin as “commodities” and not as “foreign currencies.” As we also have noted, the U.S. Internal Revenue Service has classified cryptocurrencies as commodities.

Commodities trading regulation is similar to securities broker-dealer and trading regulation in terms of the models it offers for the regulation of cryptocurrencies and market participants. Commodities trading regulation focuses on the market-efficiency, transparency, and accountability models we have been discussing above, but it shares some of characteristics of the public-law models being employed by FinCEN or the IRS, for example, for money-laundering prevention and detection.

Trading cryptocurrencies as futures contracts will trigger the Commodities Exchange Act of 1936 (CEA), as amended,²¹⁸ and the jurisdiction of the Commodities Futures Trading Commission (CFTC).²¹⁹ Despite the IRS’s declaration that convertible cryptocurrencies are “commodities” and thus “property” rather than “currencies,” that declaration does not automatically trigger the provisions of the Commodities Exchange Act of 1936. CEA Section 5(b) is triggered by the trading of a commodity. If trading is occurring or about to occur, Section 5(b) imposes both obligations to have facilities and clearing systems cover market participants, and obligations to have market professionals under the oversight of the CFTC. The CFTC deters price manipulation or other market disruptions, in order to ensure financial integrity of all transactions and to avoid systemic risk.²²⁰

For the purposes of the CEA’s coverage, the key definition is the definition of the term “commodity,” which provides, following a listing of specific tangible items, the catch-all phrase “and all services, rights, and interests (except motion picture box office receipts, or any index, measure, value or data related to such receipts) in which contracts for future delivery are

217. No. 4:13-CV-416, 201 WL 4652121 (E.D. Tex. Sept. 18, 2014); Press Release, Sec. and Exch. Comm’n, Litigation Press Release No. 23090: Final Judgment Entered Against Trendon T. Shavers, A/K/A “Pirateat40” - Operator of Bitcoin Ponzi Scheme Ordered to Pay More than \$40 Million in Disgorgement and Penalties (Sept. 22, 2014).

218. 7 U.S.C. §§ 1-27f (2012).

219. Commodity Futures Trading Commission Act of 1974, Pub. L. No. 93-463, 88 Stat. 1389 (codified as amended at 7 U.S.C. § 4a (2012)) (amending the Commodity Exchange Act of 1936 and creating the CFTC).

220. 7 U.S.C. § 5(a) (2012).

presently or in the future dealt in.”²²¹ In September, 2014, the CFTC authorized a New Jersey-based Bitcoin exchange, TeraExchange, to execute swaps, thus suggesting that the CFTC is indeed ready to regulate commodities *trading* in Bitcoin.²²²

Like our previous observations about securities offerings and trading in cryptocurrency assets and the role that securities regulators could play in those transactions, the CFTC’s jurisdiction would be limited to oversight of commodities and trading transactions—it would not extend to regulation or oversight of cryptocurrencies as *methods of payment*.

However, as a model for defining complex roles that market participants might play, the CEA’s definitions of market participants such as “commodity pools” and “commodity pool operators,”²²³ “derivatives clearing organization,”²²⁴ and “electronic trading facility”²²⁵ offer templates that may be adopted to help define different roles among market intermediaries in cryptocurrency payments transactions. From the perspective available in mid-2015, it may be that securities or commodities transactions in cryptocurrency holdings may be more significant commercially than payments transactions in cryptocurrency. But it is important to recall that the asserted purpose of cryptocurrencies is to substitute for payments made in fiat currency and through legacy payment providers such as banks.²²⁶ But, in keeping with our observations about securities regulation not being a substitute for commercial laws governing the rights and duties of third-party participants in cryptocurrency payment transaction execution, we do not see the regulation of cryptocurrencies using the commodities trading regulatory scheme as the answer to regulating third-party payment participants. In Part V, below, we propose basic outlines for a more comprehensive payments-execution regulatory approach that could supplement such securities or commodities regulatory compliance requirements.

6. Anti-Money Laundering and Counter-Terrorism Financing

Regulation to identify and prevent money laundering and terrorism financing, and to enforce other economic sanctions and anti-proliferation

221. *Id.* § 1a(9).

222. See Douwe Miedema, *Bitcoin Gets Boost as U.S. Watchdog Approves First Swap*, REUTERS (Sept. 12, 2014, 8:49 EDT), <http://www.reuters.com/article/2014/09/12/us-usa-bitcoin-cftc-idUSKBN0H71FU20140912>.

223. 7 U.S.C. § 1a(10)-(11) (2012).

224. *Id.* § 1a(15).

225. *Id.* § 1a(16).

226. See FRIEDRICH A. VON HAYEK, *DENATIONALIZATION OF MONEY: THE ARGUMENT* (1976) (arguing that government provision of currency threatens liberty and financial stability because governments undermine the value of currency to reap revenues through inflation, and that therefore sound money needs competition from privately issued currencies).

purposes is primarily a federal, and sometimes international, affair. Regulations in this category can serve important public-law purposes.

As mentioned earlier, FinCEN has promulgated and enforces detailed anti-money-laundering regulations.²²⁷ The regulations prescribe general risk-based assessment requirements for specific industries that the federal Bank Secrecy Act (BSA) governs²²⁸ and impose certain additional responsibility for maintaining customer-identification programs²²⁹ and anti-money-laundering compliance programs²³⁰ for certain sub-industries otherwise identified as “financial institutions.”²³¹ FinCEN’s 2013 and 2014 Guidances brought operators of virtual-currency “wallets” and “exchanges” into the scope of the term “money services” and, accordingly, into the term “financial institutions” for BSA purposes.²³²

Under FinCEN’s 2013 Guidance, certain participants in “virtual currency” programs became obligated to comply with regulations governing the operations of MSBs.²³³ These obligations include establishment of an anti-money laundering (AML) program, the details of which will depend on the risks posed by the location, size, nature and volume of the business, and designation of a compliance officer.²³⁴ Because FinCEN’s AML program requirements are risk-based, money service businesses can tailor their compliance programs to individual business models.

Additionally, two international organizations have been studying the risks associated with the use of cryptocurrencies, including for AML purposes. The first is the European Banking Authority.²³⁵ The second is the Financial Action Task Force (FATF), an independent inter-governmental body. The FATF describes its own role as “develop[ing] and promot[ing] policies to protect the global financial system against money laundering, terrorist financing, and the financing of proliferation of weapons of mass destruction.”²³⁶ Both studies explain from pan-European and OECD perspectives, respectively, the perceived risks that cryptocurrencies may enable money laundering, terrorism financing and (in the case of the FATF study) trafficking in weapons of mass destruction.²³⁷

227. See 31 C.F.R. ch. X (2013).

228. Bank Secrecy Act, Pub. L. 91-508, tit. I-II, 84 Stat. 1114 (1970) (codified as amended at 12 U.S.C. § 1829(b) (2012), 12 U.S.C. § 1951-59 (2012), and 31 U.S.C. § 5318(h) (2012)).

229. 31 C.F.R. § 1010.220 (2013).

230. *Id.* § 1010.210.

231. *Id.* § 1010.100(f).

232. See 2013 FinCEN Guidance, *supra* note 14; Fin-2014-R001, *supra* note 77.

233. See FinCEN 2013 Guidance, *supra* note 14.

234. 31 C.F.R. § 1022.210(b) (2011).

235. EBA 2014 Opinion, *supra* note 118, at 21-37.

236. *Virtual Currencies: Key Definitions and Potential AML/CFT Risks*, FIN. ACTION TASK FORCE 3 (June 2014), <http://www.fatf-gafi.org/media/fatf/documents/reports/virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>.

237. *Id.* at 3, 9-12.

Finally, regulations promulgated by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) already prohibit transactions with certain countries and with designated entities, unless the U.S. person participating in the transaction has obtained one or more "licenses" to engage in the transaction.²³⁸ These OFAC regulations apply to transactions in goods or services as well as to payments made in connection with these transactions.²³⁹ Payments in cryptocurrencies—or, for that matter, barter exchanges involving cattle or oil—would be covered by these OFAC restrictions on transactions. We see no reason for additional laws or regulations in the spaces already occupied by FinCEN and OFAC regulations.

7. Taxation

Whether and how to tax value transfers, either in the form of ordinary income for sellers of goods or services, or as capital gains from the sale of commodities or securities, or under some kind of "financial transaction fee" scheme, is another regulatory issue that governments may confront in relation to cryptocurrencies. As described in Part II above, other governments as well as the Internal Revenue Service (IRS) have begun to regulate cryptocurrencies for taxation purposes. In taxonomy, tax regulation is for public-law purposes.

In the United States, for example, the IRS has issued guidance on the tax consequences of virtual economy transactions, stating that transactions based in virtual currencies should be treated as exchanges of "property" for federal tax purposes.²⁴⁰ Under the IRS's guidance, "if the fair market value of property received in exchange for virtual currency exceeds the taxpayer's adjusted basis of the virtual currency," the user's gain may be taxable.²⁴¹

Commentators expressed concern about the IRS's guidance, one arguing that the IRS's guidance destroys the fungible nature of virtual currency, rendering it less useful for online commerce.²⁴² The Government

238. See, e.g., 31 C.F.R. § 560.530(a)(3) (2013) (codifications of sanctions programs enforced by OFAC) (updated to July 25, 2013 and containing information pertinent to general licenses for transactions with Iran). For a comprehensive listing of OFAC regulations and guidance pertinent to Iran, see *Iran Sanctions*, U.S. DEP'T OF THE TREASURY, www.treasury.gov/resources-center/sanctions/Programs/pages/iran.aspx (last visited May 28, 2015); *Statement of Licensing Policy*, U.S. DEP'T OF THE TREASURY, www.treasury.gov/resource-center/Sanctions/Documents/licenses-pol.pdf (last visited May 28, 2015).

239. See Office of Foreign Assets Control, *What You Need To Know About U.S. Economic Sanctions*, U.S. DEP'T OF THE TREASURY, <http://www.treasury.gov/resource-center/sanctions/Programs/Documents/iran.pdf> (last visited Jan. 5, 2015) (explaining coverage of imports from and exports to Iran involving, with exceptions, goods, technology, or services).

240. 2014 IRS Guidance, *supra* note 16.

241. *Id.* at Q-6.

242. Adam Levitin, *Bitcoin Tax Ruling*, CREDIT SLIPS (Mar. 26, 2014, 9:56 am), <http://www.creditslips.org/creditslips/2014/03/bitcoin-tax-ruling.html>; see also Robinson Meyer, *Why Bitcoin Can No Longer Work as a Virtual Currency*, THE ATLANTIC (Mar. 26, 2014, 12:49 pm), <http://www.theatlantic.com/technology/archive/2014/03/why-bitcoin-can-no-longer-work-as-a-virtual-currency-in-1-paragraph/359648/>.

Accountability Office (GAO), however, praised the IRS's approach as a "low-cost step to potentially mitigate some of the noncompliance risks associated with [virtual economy transactions]." ²⁴³ We believe that the IRS's acknowledgement that virtual currencies are property and not foreign currency is correct under current law and is consistent with other governments' views, as we described them above. ²⁴⁴ We note, however, that the record-keeping burden placed on users is onerous and urge the IRS and tax experts to devise a more user-friendly solution, if feasible.

Taxation principles and governments' exercise of jurisdiction to tax property or transactions, however important to governments and market participants, do not resolve the need for rules otherwise governing the use of cryptocurrencies to make payments. That is, they do not address the need for a private-law regime that allocates rights and duties to intermediaries representing the counterparties in payments transactions. As we explain below in more detail, a private-law regime would cover issues such as protection of the rights to redeem units of cryptocurrencies from wallets and exchanges, timely execution of payment or transfer instructions, error resolution rights and procedures, and inter-participant implied warranties.

8. Remittance Transfers

The last form of regulation currently in effect in the United States that applies to some transactions by cryptocurrency payment transaction executors is the CFPB's 2013 consumer protection regulation of remittance transfers. ²⁴⁵ These regulations serve a dual purpose in our schema: they create transparency and accountability for consumers who send remittance payments abroad, and they also establish certain transaction-execution norms for remittance market participants.

The CFPB's rules define "remittance transfer" as:

(e) *Remittance transfer*—(1) *General definition*. A "remittance transfer" means the electronic transfer of funds requested by a sender to a designated recipient that is sent by a remittance transfer provider. The term applies regardless of whether the sender holds an account with the remittance transfer provider, and regardless of whether the transaction is also an electronic fund transfer, as defined in [12 C.F.R. § 1005.3(b)].

(2) *Exclusions from coverage*. The term "remittance transfer" does not include:

(i) *Small value transactions*. Transfer amounts, as described in [12 C.F.R. § 1005.31(b)(1)(i)], of \$15 or less. (ii) *Securities and commodities transfers*. Any

243. GAO-13-516, *supra* note 83, at 17.

244. See discussion *supra* Part II.B.

245. 12 C.F.R. pt. 1005 subpart B (2014).

transfer that is excluded from the definition of electronic fund transfer under [12 C.F.R. § 1005.3(c)(4)].²⁴⁶

The rule also applies when a sender in the United States sends funds to a person or business located outside the United States.²⁴⁷

The rule only covers “remittance transfer provider[s]” who act for consumers in the United States. The rule defines the terms “remittance transfer provider” and “provider” as “. . . any person that provides remittance transfers for a consumer in the normal course of its business, regardless of whether the consumer holds an account with such person.”²⁴⁸ Additionally, the “sender” of the remittance transfer whose transactions trigger the regulation’s requirements must be engaged in a transaction “primarily for personal, family, or household purposes” and must have requested a remittance transfer provider to send a remittance transfer to a designated recipient.²⁴⁹

Two of the rule’s provisions seem particularly helpful in framing payment transaction execution rules for cryptocurrency payments. The first is the rule on the timing of receipts.²⁵⁰ The second is the clear definition of an “error” for the rule’s purposes,²⁵¹ the timing and content requirements for error notices from senders,²⁵² and the timing and scope of the remedies available to consumer senders if the remittance transfer provider concludes that an error has occurred.²⁵³

In conclusion, the existing federal and state approaches to regulating cryptocurrencies focus primarily on public-purpose goals such as the deterrence of money laundering or of terrorist support regulations enforced by FinCEN,²⁵⁴ the economic sanctions regimes enforced by the Department of the Treasury’s Office of Foreign Assets Control,²⁵⁵ and the tax-collection purposes of IRS’s 2014 Guidance.²⁵⁶ In our opinion, they serve their organic purposes well.

The Consumer Financial Protection Bureau’s proposed “prepaid card” rule has defined the term “prepaid account” in a manner that it acknowledges may cover virtual currency products.²⁵⁷ Although Regulation E provides for

246. 12 C.F.R. § 1005.30(e) (2014).

247. See Electronic Fund Transfers (Regulation E), 78 Fed. Reg. 30,662, 30,662 (May 22, 2013) (explaining the scope of Section 1073 of the Dodd-Frank Act of 2010 and its mandate to regulate cross-border remittance transfers where the sender is a consumer in the United States).

248. 12 C.F.R. § 1005.30(f) (2014).

249. *Id.* § 1005.30(g).

250. *Id.* § 1005.31(e)(2).

251. *Id.* § 1005.33(a).

252. *Id.* § 1005.33(b).

253. *Id.* § 1005.33(d).

254. See generally 31 C.F.R. ch. X (2013).

255. See generally 31 C.F.R. §§ 501.101-596.901 (2013).

256. See Fin-2014-R001, *supra* note 77, at 2-3; Fin-2014-R002, *supra* note 77.

257. Prepaid Accounts under the Electronic Fund Transfers Act (Regulation E) and the Truth in Lending Act (Regulation Z), 79 Fed. Reg. 77,112, 77,112-13, 77,128 (Dec. 23, 2014) (describing the scope of the term in the proposed regulation’s subsections 1005.2(b)(1), 1005.2(b)(3)).

disclosures and error-resolution procedures, the scope of the proposed rule will continue Regulation E's longstanding limitation to accounts held for "personal, family, or household purposes,"²⁵⁸ so that it will not protect non-consumer users.

Existing state "money transmitter" and "money services businesses" licensing and prudential supervision regimes²⁵⁹ are focused primarily on safety and soundness. They do not govern transaction execution or allocate rights and duties among counterparties to sales, services or financial transaction. Those tasks are normally the province of "private" or "commercial law," such as provisions of the Uniform Commercial Code, or of federal "consumer protection laws," such as the Electronic Fund Transfer Act ("EFTA").

When evaluating different regulations as models for future regulations, it is important to consider that individual features that might look attractive on their own are generally intertwined with and potentially inseparable from other aspects of the single regulatory model from which they came. Some features may be usable on a stand-alone or borrowed basis. Others may not. In other words, if policymakers want to borrow a hat from one of these models to put atop cryptocurrencies, they may be obligated to take the shoes—or the entire outfit. And, perhaps, regulators should exercise caution in borrowing the whole outfit head to toe without careful consideration of the costs as well as benefits of the whole for the purposes under consideration.

We submit that licensure and prudential regulation of innovative products and services, such as cryptocurrencies, or of the intermediaries that process transactions on their clients' behalf do not always require the crafting of a separate regulatory scheme. Often, it will be preferable to amend the existing regulation or even to issue tailored guidance that—like FinCEN's 2013 Guidance—situates the new product or service within an existing regulatory regime, as states such as Texas and Kansas have decided to do for now.

As we explain in our analysis of the New York State Department of Financial Services ("NYDFS") BitLicense Final Regulation below, for some of the proposed provisions, the Department has borrowed a hat (from their own general "money transmitter" regulations), but also borrowed shoes from other outfits that do not quite suit the ensemble being created, such as highly prescriptive instead of risk-based anti-money-laundering requirements or a cross-reference to FinCEN's requirements. We think the BitLicense Regulation failed to take the right shoes—those that make the complete "outfit." We submit that a wiser choice might have been to situate the licensing and prudential supervision of cryptocurrency market participants inside the state's existing "money services business" licensing and prudential regulatory scheme and to leave certain proposals beyond the border of that scheme for more general application. In other cases, such as their highly prescriptive state anti-

258. *Id.* at 77,128 (describing subsection 1005.2(b)(1)).

259. *See* 2014 IRS Guidance, *supra* note 16.

money-laundering requirements, described below, we think that the NYDFS did too much. Thus, in proposing to regulate cryptocurrency intermediaries performing payment transaction execution services for owners of cryptocurrencies, we recommend that regulators proceed to the extent feasible within the frameworks that exist and craft new regulations only where significant regulatory gaps exist, such as in transaction-execution services. Moreover, absent solid reasons, regulators should not impose more stringent requirements on cryptocurrency providers in the “money transmitter” or “money-service-business” markets than they do on more traditional money transmitters or money-service businesses.

B. New York State Department of Financial Services' Final BitLicense Regulations and its 2014 Proposal

On July 23, 2014, the New York State Department of Financial Services (“NYDFS”) issued for public comment a proposed framework for regulating cryptocurrency businesses, which it dubbed the “BitLicense.”²⁶⁰ On June 3, 2015, the NYDFS announced the promulgation of the final BitLicense regulation.²⁶¹ A proceeding commenced in 2013,²⁶² the BitLicense regulations are intended to provide a prudential licensing and regulations for cryptocurrency market participants and consumer protection, anti-money laundering and cyber security issues surrounding the use of Bitcoin and other cryptocurrencies.²⁶³ The final and proposed BitLicense regulations²⁶⁴ contain provisions on subjects common to existing state money transmitter regulations, such as licensure, examination, permissible investments, and capital requirements. They also set forth obligations, such as suspicious activity reporting and cybersecurity program requirements that borrow from several other models to create an amalgam that, while at times inspired, suffers from some weaknesses that appear to stem from the tensions and inconsistencies between the underlying models. As explained above, the BitLicense regulation and proposal also go beyond the requirements applicable to traditional brick-

260. BitLicense Proposal, *supra* note 20. For additional background, see Press Release, NY DFS Releases Proposed BitLicense Regulatory Framework for Virtual Currency Firms (July 17, 2014), <http://www.dfs.ny.gov/about/press2014/pr1407171.html> (hereinafter “BitLicense 2014 Press Release”).

261. Benjamin Lawsky, Superintendent, N.Y. Dep’t. of Fin. Servs., Remarks at the BITS Emerging Payments Forum, (June 3, 2015) (transcript available at <http://www.dfs.ny.gov/about/speeches/sp1506031.htm>). For the text of the regulation announced, see BitLicense Final Regulation, *supra* note 21.

262. N.Y. DEP’T. OF FIN. SERV., Notice of Inquiry on Virtual Currencies (Aug. 12, 2013), <http://www.dfs.ny.gov/about/press2013/memo1308121.pdf>. For commentary on the commencement of this proceeding, see Kashmir Hill, *Every Important Person in Bitcoin Just Got Subpoenaed by New York’s Financial Regulator*, FORBES.COM (Aug. 12, 2013 1:43 PM), <http://www.forbes.com/sites/kashmirhill/013/08/12/every-important-person-in-bitcoin-just-got-subpoenaed-by-new-york-s-financial-regulator> (listing recipients).

263. BitLicense 2014 Press Release, *supra* note 260.

264. BitLicense Final Regulation, *supra* note 21.

and-mortar money transmitters and money services businesses. These proposals seem, one could argue, designed to discourage applications for BitLicenses. On the other hand, rules such as cyber-security compliance requirements and designations of cyber compliance officers and basic anti-money laundering provisions should apply generally to non-depository providers providing intermediary services that are money transmission or are comparable to money transmission – not only to virtual currency market participants.

Because it is the first comprehensive cryptocurrency-specific “money services” licensing and regulatory framework for cryptocurrencies both in the United States and worldwide, the BitLicense is positioned to be the platform against which other cryptocurrency-specific “money services” regulations are likely to be measured. However, the BitLicense, despite its breadth, does not tackle important payments transaction-execution needs that we address in Part III of this article. Still, given its lead in the race to regulate cryptocurrency market participants, it would be an error not to examine its key features and to evaluate the tradeoffs and limitations in regulatory choice that it presents.

In the following analysis, we focus primarily on the June 2015 final regulation, highlighting the significant differences between the July 2014 proposed regulation and the final regulation. In this subpart, we also note those provisions that illustrate tradeoffs and limitations in regulatory choice.

The BitLicense Final Regulation draws authority from existing New York State laws relating to non-depository providers of “money transmission” or “money services.”²⁶⁵ The regulation has features that are similar to other states’ “money transmission” or “money services business” licensure and supervision regimes. For example, the BitLicense requires anyone who engages in “Virtual Currency Business Activity” to obtain a license,²⁶⁶ meet certain capital requirements,²⁶⁷ maintain books and records,²⁶⁸ file financial reports,²⁶⁹ and subject themselves to examination.²⁷⁰ Those who obtain licenses, who we will refer to as “BitLicensees,” are required to protect customers by three means: (1) maintenance of basic capital in the form of permissible investments,²⁷¹ (2) maintenance of “a bond or trust account in United States for the benefit of its customers”, virtual currency of the “same type and amount as that which is owed or obligated to” a third person,²⁷² and (3) observance of the prohibition on selling, transferring, lending, hypothecating, pledging, or otherwise using or

265. *Id.* (citing authority for the provisions under Financial Services Law, sections 102, 104, 201, 206, 301, 302, 309, and 408).

266. BitLicense Final Regulation, *supra* note 21, § 200.3(a).

267. *Id.* § 200.8.

268. *Id.* § 200.12.

269. *Id.* § 200.14.

270. *Id.* § 200.13.

271. *Id.* § 200.8(a), (b). Permissible investments for this basic requirement do not include any form of virtual currency. *Id.* § 200.8(b).

272. *Id.* § 200.9(a), (b).

encumbering assets . . . held, stored, or maintained by, or under the custody or control of, [the] Licensee on behalf of another Person.”²⁷³

Additionally, the BitLicensees must appoint a compliance officer and establish compliance policies,²⁷⁴ and implement separate, not risk-based anti-money laundering programs,²⁷⁵ cyber-security programs,²⁷⁶ and business continuity plans.²⁷⁷ Licensees’ advertising and marketing materials are subject to review.²⁷⁸ These proposals are substantially more onerous than those applicable to other, non-depository providers under the DFS’ jurisdiction, because they impose separate state anti-money laundering program requirements²⁷⁹ not imposed on other providers and differ from those imposed by FinCEN on “money services businesses.”²⁸⁰

A BitLicensee is required to make a detailed set of disclosures to customers before a transaction,²⁸¹ obtain acknowledgement of each disclosure,²⁸² provide a receipt for each transaction,²⁸³ and establish a complaint resolution procedure.²⁸⁴ These requirements are more burdensome than those applicable to other, non-depository “money services” providers under the DFS’ jurisdiction.

BitLicensees also must implement an anti-fraud policy.²⁸⁵ In addition, the NYDFS must pre-approve all material changes to its products and services.²⁸⁶

1. BitLicense Final Definition of “Virtual Currency”

The BitLicense defines virtual currency as “any type of digital unit that is used as a medium of exchange or form of digitally stored value or that is incorporated into payment system technology.”²⁸⁷ The term is to be “broadly construed” but does not include digital units used solely as part of customer affinity or rewards that can only be redeemed by designated merchants and not converted to cash, or currencies used only within online gaming platforms.²⁸⁸

273. *Id.* §§ 200.8; 200.9((a), (c).

274. *Id.* § 200.7(b).

275. *Id.* §§ 200.7(c); 200.15; 200.16; 200.17.

276. *Id.* § 200.16.

277. *Id.* § 200.17.

278. *Id.* § 200.18.

279. *Id.* § 200.15.

280. FINCEN 2013 Guidance, *supra* note 14, at 1-2.

281. BitLicense Final Regulation, *supra* note 21, § 200.19(a), (b) and (c).

282. *Id.* § 200.19(d).

283. *Id.* § 200.19(e).

284. *Id.* § 200.20.

285. *Id.* § 200.19(g).

286. *Id.* § 200.10(a). The BitLicense Final Regulation defines “material change” as well. *Id.* § 200.10(b). It also specifies how a BitLicensee’s plan for proposed material changes must be explained to the NYDFS with specificity. *Id.* § 200.10(c).

287. *Id.* § 200.2(p).

288. *Id.* § 200.2(p)(1).

The definition does not require that a virtual currency be a substitute for legal tender, which was a cornerstone of FinCEN's conclusion that some virtual currency activities constitute "money transmission."²⁸⁹ Without this limitation in the definition, it is unclear what prevents the BitLicense Final Regulation from applying to electronic forms of legal tender²⁹⁰ or dollar-denominated demand deposit accounts, which we discuss in more detail below. The BitLicense defines the term "Fiat Currency"²⁹¹ to mean "government-issued currency that is designated as legal tender in its country of issuance through government decree, regulation or law."²⁹²

2. BitLicense's Definition of "Virtual Currency Business Activity"

A BitLicense is required for anyone who engages in "Virtual Currency Business Activity."²⁹³ The latter term is defined to include the following types of activities involving New York or a New York Resident:

- receiving Virtual Currency for transmission or transmitting the same;
- securing, storing, holding or maintaining custody or control of Virtual Currency" on behalf of others;
- buying and selling Virtual Currency as a customer business;
- performing retail conversion services, including the conversion or exchange of Fiat Currency or other value into Virtual Currency, the conversion or exchange of Virtual Currency into Fiat Currency or other value, or the conversion or exchange of one form of Virtual Currency into another form of Virtual Currency; or
- controlling, administering, or issuing a Virtual Currency."²⁹⁴

The scope of activities included here is significantly broader than that traditionally covered by the money transmitter statutes upon which these regulations are based. However, it is narrower than provided in the 2014 BitLicense proposal. The 2014 BitLicense proposal was unclear as to whether merely providing software services, which enable some cryptocurrency exchanges or administrators to operate but do not involve the receipt of funds or cryptocurrencies for transmission from individuals, investors, or other

289. Compare *id.* with FinCEN 2013 Guidance, *supra* note 14. For more information, see Clearing House/ICBA Report, *supra* note 41, at 6. The gap between the approaches taken by FinCEN and the NYDFS leaves room for confusion, particularly among new entrants and innovators.

290. BitLicense Final Regulation, *supra* note 21, § 200.2(e).

291. See *id.* § 200.2(d). We find that the term "fiat currency" carries with it unhelpful connotations that may obscure legal and policy discussions about virtual currency. We would have preferred that the BitLicense regulation had used the term "legal tender" instead of "fiat currency" in its Virtual Currency definition. See *id.* § 200.2(m).

292. BitLicense Final Regulation, *supra* note 21, § 200.2(e).

293. *Id.* § 200.3(a).

294. *Id.* § 200.2(q).

exchanges, might trigger a licensing obligation.²⁹⁵ Other states' money services and money transmitter statutes cover receipt of funds or substitutes for transmission, but not the software services that are for internal functioning purposes, not for transmission to third parties.²⁹⁶ The BitLicense Final Regulation is now in harmony with FinCEN's 2014 determination that the production and distribution of software, even if that software facilitates transmission of virtual currency, do not constitute money transmission.²⁹⁷

The proposed BitLicense regulations also might apply to depository institutions that are generally exempt from similar money transmitter regulations.²⁹⁸ Banks other than those chartered under New York Banking Law and approved by the superintendent to engage in Virtual Currency Business Activity" are exempt from the BitLicense requirements.²⁹⁹ Banks not chartered by New York State or not also approved to engage in Virtual Currency Business Activity will require BitLicenses.³⁰⁰ We think that is unnecessary. Merchants and consumers that use Virtual Currency "solely for the purchase or sale of goods or services" do not require BitLicenses to proceed with transactions.³⁰¹

The "Virtual Currency Business Activity" definition is limited to activities "involving New York or a New York resident."³⁰² For most internet-based businesses, which presumably include all virtual market currency participants, it will be extremely difficult to prevent one's business activities from involving New York or a "New York Resident."³⁰³ For those market participants using money-center banks, this may be even harder. The scope of this provision highlights the need for a more general resolution of jurisdictional questions involving internet-based transactions.

There is no fail-safe way to determine where an internet user is located geographically. There is no way to guarantee that one's internet traffic will not touch a server in New York. It is impossible to prevent a New York resident from travelling to another state and interacting with a service provider;

295. BitLicense Proposal, *supra* note 20, § 200.2.

296. *See, e.g.*, WASH. REV. CODE § 19.230.010(17)-(19) (2013).

297. *See* Fin-2014-R002, *supra* note 77, at 2.

298. *Compare* BitLicense Final Regulation, *supra* note 21, § 200.3(c) (exemption from licensing requirements limited to persons chartered under the New York Banking Law and approved to engage in Virtual Currency Business Activity), *with* WASH. REV. CODE § 19.230.20(4) (2013) (chapter not applicable to financial institutions as defined in § 19.230.010(12) (2013)); VA. STAT. ANN. § 6.2-1902.3 (2014) (chapter not applicable to banks and persons operating as agents of banks).

299. BitLicense Final Regulation, *supra* note 21, § 200.2(q) (definition of "Virtual Currency Business Activity").

300. *Id.* § 200.3(c)(1).

301. *Id.* § 200.3(c)(2).

302. *Id.* § 200.2(g), (h).

303. *Id.* § 200.2(g) (New York Resident includes "any Person that resides, is located, has a place of business, or is conducting business in New York"). There appears to be no limitation or requirement on what type of business triggers this "conducting business in" status, though perhaps regulations will offer more specificity on this test.

however, there may be some limits on jurisdiction in cases in which the resident travels to another state to transact business.³⁰⁴ If there is no practical way for a virtual currency business to avoid engaging in activity that involves New York, there is no true limitation on New York's jurisdictional reach or on its BitLicense requirements.

Extraterritorial application of New York law appears to be the exception, not the rule. Indeed, the (general) presumption appears to be against extraterritorial application.³⁰⁵ We suggest that it would be beneficial for NYDFS to create a jurisdictional "safe harbor," delineating what steps a virtual currency business would need to take in order to be assured that it was not engaged in activity involving New York. Adoption of guidelines that virtual currency market participants could employ to filter out customers who are residents of New York and reject their business would be one option. Another would involve creating a *de minimis* rule that would not require a BitLicense until the virtual currency market participant has a defined number of transactions or transactions exceeding a specific dollar-equivalent threshold.³⁰⁶ Additionally, a virtual currency market participant should be able itself to assure depository institutions with which they may deal that they are (or are not) New York citizens or do (or do not do) sufficient business in the state to meet its nexus tests without being required to obtain a BitLicense.

3. BitLicense's Licensing Requirements

In addition to eligibility requirements, the BitLicense requires that entities holding funds on behalf of another person must hold the same type and amount of virtual currency.³⁰⁷ With respect to amount, this provision follows the "money transmission" model and not the "deposit" model, as described above. The requirement to hold the same type of cryptocurrency as the transaction instructs be paid or exchanged makes sense because third-party intermediaries could offer to execute transactions in more than one cryptocurrency and the counterparties in cryptocurrency transactions – whether used in payments or for other purposes – may have contractual rights to receive payment in specific cryptocurrencies, as opposed to receiving cryptocurrencies of a comparable value on a given date.

304. See, e.g., *Midwest Title Loans Inc. v. Mills*, 593 F.3d 660 (7th Cir. 2010), *cert denied* 131 S. Ct. 83 (2010) (denying jurisdiction of Indiana law to consumer transaction in which the consumer had to cross over into Illinois physically to sign the loan agreement and receive the loan proceeds).

305. *Global Reinsurance Corp.-U.S. Branch v. Equitas Ltd.*, 18 N.Y.3d 722, 735 (2012) ("The established presumption is, of course, against the extraterritorial operation of New York law.")

306. See, e.g., 12 C.F.R. § 1005.30(e)(1)(i) (2012) (defining small remittances as outside the rule's coverage).

307. *Id.* § 200.9(b).

4. BitLicense's Anti-Money-Laundering and Customer Identification Requirements

U.S. anti-money-laundering laws generally allow entities to make their own risk-based assessments or the money-laundering risks to which they are exposed, and to implement, monitor, and adjust their programs and retrain personnel to ensure compliance.³⁰⁸ They are otherwise not prescriptive of the steps that must be taken by licensees. For example, FinCEN regulations require a money services business to establish an anti-money laundering program that is “reasonably designed to prevent money laundering and the financing of terrorist activities” and that is “commensurate with the risks posed by the location and size of, and the nature and volume of the financial services provided.”³⁰⁹ Likewise, the BSA examination process for MSBs takes a risk-based approach.³¹⁰

In contrast, the BitLicense regulation is prescriptive, not risk-based. For example, BitLicense requires customer identification including name and physical location.³¹¹ Collection or maintenance of customer identification information is not a general requirement under state Money Service Business or Money Transmitter acts. However, the USA Patriot Act imposed section 326 “customer identification program” requirements on entities that were required to adopt section 352 “anti-money-laundering-compliance programs.”³¹² The federal “customer-identification-program” requirement does not require capture or retention of the customer’s “physical location.”³¹³ Rather, FinCEN’s regulations – like its Joint Final Rule with the SEC in 2003 – allow entities such as the broker-dealers in that Joint Final Rule – to satisfy this requirement by any one of several means.³¹⁴ The Section-by-Section Analysis of the 2003 Joint Final Rule implementing the customer-identification-program requirements offers more flexible means of satisfying the “address” requirement in the Rule and is not limited to a home address.³¹⁵ The

308. 31 C.F.R. §§ 1010.210, 1022.210(d)(2)(ii), 1022.210(d)(3)-(4) (2012); 31 U.S.C. 5318(h)(1) (2013).

309. 31 C.F.R. § 1022.210(a) and (b) (2013).

310. Financial Crimes Enforcement Network, Bank Secrecy Act/Anti-Money Laundering Examination Manual for Money Services Businesses 26-29 (2009), http://www.fincen.gov/news_room/rp/files/MSB_Exam_Manual.pdf.

311. BitLicense Final Regulation, *supra* note 21, § 200.15(l)(1).

312. USA Patriot Act, Pub. L. 107-56, 115 Stat. 272 (2001) (codified at 31 U.S.C. §§ 5311 et seq.). The interagency rule implementing the customer-identification program was codified originally at 31 C.F.R. §§ 103.121 et seq. (2003).

313. 31 C.F.R. § 1010.312 (2013) (requirement to record and verify customers’ names, addresses and identities, account numbers, and federal tax identification (SSN or EIN) numbers if the transaction is being conducted on behalf of another person or entity).

314. See Joint Final Rule—Customer Identification Programs for Broker-Dealers, 31 C.F.R. § 103.122(b) (2003), subsequently re-codified at 31 C.F.R. § 1023.220(a), 75 Fed. Reg. 65806, 65809 (Oct. 26, 2011).

315. See 31 C.F.R. § 1020.220(a)(2)(i)(A)(3) (2012) (recodified from 31 C.F.R. § 103.122(b) (2003)).

BitLicense's requirement to collect and maintain the physical location for the customer raises issues about the feasibility of a requirement to record the customer's physical location at a particular time because of the ease of adopting a situs different from an actual situs, and attendant enforcement issues for a wallet or exchange that collected information that later proved inaccurate.³¹⁶ The BitLicense's "physical location" requirement perhaps could be associated with the jurisdictional "hook" that the BitLicense Final Regulation will utilize,³¹⁷ rather than with its customer-identification provisions.

In addition to other new AML and customer identification requirements in the proposed New York State regulations, the New York regulations will require licensees to file suspicious activity reports with the State of New York, even if FinCEN's regulations would not require a filing.³¹⁸ The BitLicense Final Regulation requires that BitLicensees report, in cases in which transactions are not subject to currency transaction reporting under federal law, transactions in aggregate amounts exceeding U.S.D. \$10,000 in one day, within 24 hours,³¹⁹ as opposed to the longer period allowed by FinCEN.³²⁰ The virtual currency community likely will see these requirements as problematic because they exceed applicable FinCEN requirements.

Three final issues arise from the BitLicense Final Regulation, which tends in these respects to be an improvement over the Proposed Regulation. First, the responsibility to report suspicious activity affects only BitLicensees, not including certain vendors and software developers.³²¹ These categories of participants may have no direct dealings with the day-to-day operations of the licensees or their customers, but they may see activities by licensees that should be brought to the attention of the Department of Financial Services, including vulnerabilities such as those that allegedly caused Mt. Gox to suspend its operations in 2014.³²² Second, the record-retention period for transactions will be seven years,³²³ as compared with the five years under FinCEN's regulations.³²⁴ We are not certain that the Regulation's longer records retention period is justified. Third, the Regulation has a Suspicious Activity Report ("SAR") requirement that in many cases will duplicate the FinCEN regime.

316. BitLicense Final Regulation, *supra* note 21, § 200.15(d)(1).

317. *Id.* § 200.2(q) (limiting to holders of BitLicensees "Virtual Currency Business Activity" involving New York or a New York Resident), (h) (defining New York Resident).

318. *Id.* §§ 200.15(e)(3)(i). FinCEN's regulations require a filing if a transaction is suspicious or if it involves a transfer of \$2,000 or more. 31 C.F.R. § 1022.320(a)-(f) (2011).

319. BitLicense Final Regulation, *supra* note 21, § 200.15(e)(2).

320. 31 C.F.R. § 1022.320(a)-(f) (2011) (money services businesses have 30 days to file suspicious activity reports).

321. BitLicense Final Regulation, *supra* note 21, § 200.15(d)(3).

322. Hern, *Mt. Gox Offline*, *supra* note 4; Hern, *Mt. Gox Bankruptcy Filing*, *supra* note 5.

323. BitLicense Final Regulation, *supra* note 21, § 200.12(a). The Regulation provides for a five-year retention of records of "non-completed, outstanding, or inactive accounts or transactions" to be treated as abandoned property after the five-period expires. *Id.* § 200.12(c).

324. 31 C.F.R. § 306(a)(2).

We are not certain that it is fair to require reports duplicative of federal filings. Final questions about transaction and SAR reporting under Section 200.12 relate to two subjects: (1) what is New York going to do with these data? and (2) will the data enjoy the same protections, such as under the Right to Financial Privacy Act of 1978³²⁵ and the Fair Credit Reporting Act³²⁶ that they currently have under federal law? The Final Regulation answers neither of these questions.

5. BitLicense's Consumer Disclosures

The BitLicense Final Regulation includes highly prescriptive consumer disclosure requirements³²⁷ that exceed those imposed under many of the models for analogous products. For example, the BitLicense Final Regulation requires licensees to inform customers of a long list of "material risks" associated with cryptocurrency, including the fact that (1) it is not legal tender, is not FDIC insured, and may be adversely affected by legislative and regulatory change, (2) that payment/ transfer transactions are generally irreversible, and (3) that there is no assurance that other parties will continue to accept virtual currency.³²⁸ In contrast, Regulation E has nothing like the "material risk" disclosures and its required initial disclosures focus on product features and limitations, liability and fees.³²⁹ Generally, in the United States, the obligation to disclose material facts is frequently limited to relationships in which the provider owes a fiduciary duty to the customer, such as broker-dealer and investment advisor relationships.³³⁰ BitLicensees also must disclose "general terms and conditions" such as the customer's liability for unauthorized

325. Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401-3422 (2011) (creating with exceptions statutory rights to replace the Fourth Amendment protection for bank records following the Supreme Court's ruling in *United States v. Miller*, 425 U.S. 435 (1976)).

326. Fair Credit Reporting Act, 15 U.S.C. § 1681-1681(a) (2011) (containing limitations on sharing of information from consumers' credit histories with law enforcement agencies and others).

327. BitLicense Final Regulation, *supra* note 21, § 200.19.

328. *Id.* § 200.19(a)(1)-(10).

329. 12 C.F.R. § 1005.7 (2012).

330. Investment advisors are considered to have fiduciary responsibilities to clients. See Duties of Brokers, Dealers, and Investment Advisors, Exchange Act Release No. 69,013, Investment Advisers Act Release No. 3558, at 3 (Mar. 1, 2013), <http://www.sec.gov/rules/other/2013/34-69013.pdf>. [hereinafter SEC Release 34-69013]. Broker-dealers are not normally treated as fiduciaries to their clients. *Id.*; see also *supra* note 3. State common law normally defines the instances in which broker-dealers owe duties to their customers, including when the broker-dealer exercises "discretion or control over customer assets, or has a relationship of trust and confidence with their customers" that is "similar to that of investment advisors." Staff of the U.S. Sec. & Exch. Comm'n, *Study on Investment Advisers and Broker-Dealers as Required by Section 913 of the Dodd-Frank Wall Street Reform and Consumer Protection Act*, SEC. & EXCH. COMM'N viii, 101, 109, 166 (Jan. 2011), www.sec.gov/news/studies/2011/913studyfinal.pdf. In the Study, the SEC's staff made recommendations for "enhanced consumer protections" and also to "decrease retail customers' confusion about the standard of conduct owed to them when their financial professional provides them with personal advice." SEC Release 34-69013, *supra* note 330, at 6 & note 10. See also *supra* note 3 (citing *United States v. Skelly*, 442 F. 3d 94, 98 (2d Cir. 2006)).

transactions, privacy policies and the customer's right to receive periodic statements, receipts and prior notice of changes.³³¹ A final provision that may prove hard to implement is the requirement to give consumers receipts.³³² Moreover, the DFS may request the form of the BitLicensees' receipts.³³³

In addition, disclosures must be made prior to each transaction, detailing the type and amount of the transaction and any fees to be assessed along with a warning that the transaction may not be undone.³³⁴ This disclosure scheme is far more rigid and detailed than that imposed on money transmitters and electronic payment providers, but it is similar to disclosures required of entities engaged in cross-border remittance transfers under Regulation E.³³⁵

6. BitLicense's Requirements Related to Engaging in Fraudulent Activity and to Detecting and Deterring Fraud

The BitLicense regulation prohibits BitLicensees from engaging in fraudulent activity.³³⁶ The Regulation does not define "fraud."³³⁷ The

331. BitLicense Final Regulation, *supra* note 21, § 200.19(b)(1)-(7) (general terms and conditions), 200.19(c) (terms of specific transactions).

332. *Id.* § 200.19(e). In connection with the requirement to give receipts, we note that questions will arise about the content requirements for receipts. Consumers in the United States are accustomed to receipts that truncate all but the last four digits of credit card numbers, for example. Whether truncation of the "addresses" associated with the initiator and recipient of the crypto-payment will be required is one of the issues to be resolved. For discussion of the issue of truncation of account numbers in other electronic payments systems, see Patricia J. Allouisie, Stephen T. Middlebrook, & Sarah Jane Hughes, *Developments in the Laws Affecting Electronic Payments and Stored Value Products: A Year of Stored-Value Bankruptcies, Significant Legislative Proposals, and Federal Enforcement Actions*, 64 BUS. LAW. 219, 229-233 (2008) (discussing litigation involving the failure to truncate card numbers on some receipts pursuant to 15 U.S.C. § 1681(c) (2013)). The article explains the split of federal district courts on the application of this subsection to internet transactions. *Id.* at 231-233.

333. *Id.* § 200.19(f).

334. *Id.* § 200.19(c).

335. 12 C.F.R. § 1005 (2012).

336. BitLicense Final Regulation, *supra* note 21, § 200.19(g). The 2014 draft regulation also had reached fraud perpetrated by third parties, providing that "customers of Licensees that are victims of fraud shall be entitled to claim compensation from any trust account, bond, or insurance policy maintained by the Licensee." BitLicense Proposal, *supra* note 20, § 200.19(g). The Proposal failed to limit customer's fraud rights under the proposal to fraud committed by the BitLicensee. It provided no claims process or deadline. Deletion of the compensation provision no doubt will be a welcome change for BitLicensees, and a disappointment for some users and user advocates.

337. See James A. Deeken, *Choice of Law in Contract-Fraud Claims – New York v. Delaware*, AKIN GUMP 1 (Jan. 10, 2014), <http://www.akingump.com/en/experience/practices/corporate/ag-deal-diary/choice-of-law-in-contractual-fraud-claims-new-york-vs-delaware.html> (last visited Dec. 5, 2014) (brief discussion of elements of contract-fraud causes of action in New York State).

The author points out that the elements include:

1. Representation was made of a material fact.
2. Representation was untrue.
3. Party making the representation knew it was untrue.
4. Representation was made with the intent to deceive and for the purpose of inducing the recipient to act upon it.
5. Recipient justifiably relied on the representation.
6. By relying on the untrue statement, the recipient suffered damages.

BitLicense also requires BitLicensees to detect and deter fraud being committed by third parties. This duty raises the question of whether the courts will recognize a private right of action for consumers, and, if so, whether the BitLicensee's liability would be limited to the value of its trust account, bond or insurance policy. In the former connection, implied private rights of action are not always recognized.³³⁸ In the latter, a disclosure of any applicable cap on recovery would help users decide whether to risk the loss of their assets or to be limited in their potential recoveries.

On balance, the BitLicense Final Regulation addresses many concerns that we had about the 2014 Proposal, but it does not answer questions that we have noted above that are likely to require answers.

IV. What Other Factors Should We Consider in Deciding Whether and How to Regulate Cryptocurrencies Generally or Cryptocurrency Intermediaries?

The progress of e-payments in the 50 years since e-payments first emerged suggests that first system rules and eventually formal regulations follow initial periods of non-regulation. System rules and regulations mature and then afford protections of counterparties to transactions.

A prime example of maturation in payment methods to the point of regulation is found in the regulatory history of "wire transfers" or "fund transfers." The ability to transfer funds by wire arose shortly after the advent of the telegraph in the 19th century³³⁹ to move funds speedily (by the standards of the day), and arguably more securely than transportation of money, drafts, or even letters of credit. Then, the Uniform Law Commission study committee known as the "3-4-8 Committee" reported out a proposal that addressed issues relative to consequential damages for delays of wire transfers, funds sent to the wrong recipient, and other errors, and offered protections beyond bilateral contracts and some system rules.³⁴⁰ Their work led to Article 4A of the Uniform Commercial Code, which all the states have adopted.³⁴¹ The issue has

Id. (citing *e.g.*, *DynCorp v. GTE Corp.*, 215 F. Supp. 2d 308, 326 (S.D.N.Y. 2002); *Brown v. Lockwood*, 76 A.D.2d 721, 730 (2d Dep't 1980); *Banque Arabe et Internationale D'Investissement v. Maryland Nat'l Bank*, 57 F.3d 146, 153 (2d Cir. 1995)).

338. See *Janus Capital Group, Inc. v. First Derivative Traders*, 564 U.S.—(June 13, 2011) (No. 09-525) (expanding on the ruling in *Stoneridge Inc. Partners v. Scientific-Atlanta, Inc.*, 552 U.S. 148 (2007)).

339. U.C.C. art. 4A, pref. note (1989), <http://www.uniformlaws.org/Act.aspx?title=UCC%20Article%204A,%20Funds%20Transfers%20%281989%29>. For a useful overview of Article 4A and the specific issues it was drafted to address, see Robert G. Ballen & Natalie H. Diana, *The Need for Article 4A*, 45 BUS. LAW. 1399 (1989-1990).

340. See Uniform Law Comm'n., UCC Article 4A, Funds Transfers (2012), <http://www.uniformlaws.org/Act.aspx?title=UCC%20Article%204A,%20Funds%20Transfers%20%281989%29> (last visited May 29, 2015) (reflecting amendments made in 2012 of the original 1989 uniform law).

341. See Fred H. Miller & Sarah Jane Hughes, *Interim Report of the Study Comm. on Alt. & Mobile Payment Sys.* (2014) (copy on file with the authors).

been raised whether Article 4A could serve as a model for – or the home of – regulation of transactions involving virtual currencies.³⁴²

Specific events, such as FinCEN’s 2013 Guidance, the collapse of the Mt. Gox Bitcoin exchange in February 2014, and the BitLicense proposal have ended the wait-and-see approach that many states and Congress followed in 2013. Thus, in contrast to the slow development of wire-transfer regulations over a century, and even of e-commerce over the last 20 years, the moment for regulation of cryptocurrencies is upon us.

Proponents of cryptocurrencies maintain that early regulation could hamper development in this space, particularly as innovations may proceed from the underlying distributed computing technologies – those that go beyond making payments or storing value. The risk here is that we might miss uses of the distributed computing technology that underlies the block chain in Bitcoin for tracking intangibles – particularly intangible financial assets such as e-mortgages or e-notes or copyrighted intangibles. Such uses could be as revolutionary as barcodes once were for the tracking of physical objects in space. One commentator has referred to Bitcoin as an “Internet-for-value exchange.”³⁴³ The distributed computing technology that underlies the block-chain could be used to restrict or at least serve as a check against unauthorized transfers or uses.³⁴⁴ We should not regulate cryptocurrencies in such a manner that investments in potential future applications and resulting technologies will not be made.

The second risk relates to the prospects of adopting the wrong regulation, for example by over-regulating or under-regulating the most pressing regulatory issues. The degree of “regulatory risk” from the first actor to regulate could depend on the purpose for which the regulations were designed. As noted above,³⁴⁵ the BitLicense appears to be a regulate-for-many-purposes proposal covering subjects beyond the existing money transmission and money services regulations. The BitLicense duplicates subjects – particularly related to anti-money laundering issues – that are fully covered by existing federal requirements such as FinCEN’s requirements discussed elsewhere in this Feature.³⁴⁶ Regulatory overlap such as the anti-money laundering requirements in the BitLicense and FinCEN regulations will be costly for participants and possibly confusing.

342. *Id.*

343. See Andrew Barnes, *Digging Deeper with Ripple: The Internet of Money*, PAYMENT WEEK (Apr. 14, 2014), <http://paymentweek.com/2014-4-14-digging-deeper-with-ripple-the-internet-of-money-4534> (comments of Chris Larsen, founder and CEO of Ripple, mentioning that Bitcoin shows the world “how to confirm financial transactions without a central operator”).

344. See Nakamoto, *supra* note 15, at 1, 2, 5 & 8; Fistful of Bitcoins, *supra* note 2, at 11-12.

345. For more discussion, see Part III.B *supra* and text accompanying notes 260-86.

346. *Supra* notes 241 to 249.

A third set of questions relates to whether regulators should segregate the regulation of new technologies from regulation of products with which they may compete. For example, should we regulate cryptocurrencies as payments mechanisms separately from existing payments or should regulations affecting existing mechanisms be amended to take cryptocurrency transactions into their scope? In addition to the prospect of using Uniform Commercial Code Article 4A or a model based on it, other regulatory frameworks that exist at least for consumer payments include the federal Electronic Fund Transfer Act. In a recent proposal to amend the regulations that implement the EFTA, the CFPB states that its review of virtual currencies is “ongoing.”³⁴⁷ A representative of the Bitcoin Foundation recently asked whether Bitcoin could be “integrated . . . into existing financial regulations.”³⁴⁸

Was the Foundation’s suggestion unrealistic? We do not think so. Rules that exist for physical-world transactions can apply to new technologies and avoid unfair competition from them vis-à-vis older-style systems that the new technologies may disrupt. Adaptation of an existing framework to include emerging products can avoid uncertainties and delays attendant to the regulatory process and the risk of slower adoptions by end-users in unregulated space.

The Bitcoin Foundation’s question suggests that cryptocurrencies may follow the path that disruptors such as PayPal followed more than a decade ago. PayPal buckled down and obtained money transmitter licenses from all the states that require them.³⁴⁹ Keeping cryptocurrencies in the money transmitter framework also offers a benefit of greater interstate consistency that the BitLicense does not offer.

Beyond those questions, the choice of regulatory approach could be made in terms of whether regulators see the innovation in cryptocurrencies primarily as a storage of value useful primarily to make payments or whether regulators see them as commodities, securities, or some combination of stored-value, payments technologies, commodities and securities. Each of these regulatory schemes has merit, and, as we have explained in this Part, each may be needed to achieve a fully functioning marketplace for cryptocurrencies innovations to grow. Despite the normative value of some regulatory schemes, some are more

347. CFPB Prepaid Accounts Proposal, *supra* note 79, at 77121.

348. See Michael Virtanen, *New York Regulators Propose Regulations for Bitcoin, Other Virtual Currencies*, GUARDIAN (July 18, 2014), reprinted in *New York Regulators Propose Regulations For Bitcoin*, COLUMBUS DISPATCH (July 21, 2014), <http://www.dispatch.com/content/stories/business/2014/07/21/new-york-proposing-regulations-for-bitcoin.html>.

349. For 10-Q disclosures showing the progress of PayPal’s licensure as a money transmitter and compliance with the EFTA, see eBay Inc., Quarterly Report (Form 10-Q) 44 (Apr. 25, 2007); eBay Inc., Quarterly Report (Form 10-Q) 46 (July 27, 2007); eBay Inc., Quarterly Report (Form 10-Q) 50 (Oct. 29, 2007). For an insider’s view of money transmitter licensing, see Sean Sposito, *PayPal Veterans Share State Licensing War Stories*, AM. BANKER (Aug. 6, 2013 6:25pm ET), http://www.americanbanker.com/issues/178_151/paypal-veterans-share-state-licensing-war-stories-1061148-1.html (remarks attributed to John Muller, [then] General Counsel of PayPal).

likely to contribute to this growth potential than others. For example, as we have noted, cryptocurrencies in themselves are not “currency” for all purposes, and also are not commodities or securities.

As the regulation of cryptocurrency payments or of commodities transactions in which cryptocurrencies are the underlying assets proceeds, we submit that policy makers should assign regulatory responsibilities to those with the most experience regulating the functionalities that are causing the issues requiring regulation and with the greatest available resources to engage in the effort (effectively, a boots-on-the-ground approach to allocating responsibility).

If we follow this approach, then states should regulate the payment-execution aspects because they have the greatest experience with regulating non-depository providers of payments and stored-value products, money transmitter licensing and supervision regimes and supervisory personnel in place, and the deepest experience licensing emerging entities in this space such as PayPal.

Regulation for certain purposes such as income recognition and tax collection, anti-money-laundering and anti-terrorist financing, economic sanctions, and the regulation of securities and derivatives based on market values of cryptocurrencies such as Bitcoin should be handled at the federal level.

V. A Proposed Framework for Regulating Cryptocurrency Payments

Intermediaries who Execute Payments for Goods and Services from U.C.C.
Article 4A

Readers already know that we propose that a commercial law regulating the terms and conditions of transfers of cryptocurrencies in payment of goods and services. This subject is a step not so far addressed by ongoing work by the States or the Federal Government. We explained that commercial-law rules contribute to uniformity and predictability for counterparties and may lead to greater numbers of adoptions of – and investments in – these new payments technologies. This is not an alternative to ongoing regulatory work. Rather, it is the missing link, if you will, in the progress of cryptocurrencies as payment methods.

Your authors have had special opportunities to consider the usefulness of a commercial law for cryptocurrencies over the past 18 months. In December 2014, the ULC’s Study Committee on Alternative and Mobile Payments (in which we both participated in one capacity or other) issued its final report recommending that the ULC authorize a drafting committee to regulate cryptocurrency market participants offering transaction-execution services and users of cryptocurrencies to make payments.³⁵⁰ The report does not set forth the

350. ULC STUDY COMMITTEE FINAL REPORT, *supra* note 23.

specifics of such regulation, but speaks in terms of regulating the rights and duties of cryptocurrency-payment participants with roles in transaction execution, among other things, primarily from a commercial law perspective.³⁵¹

This Part of this Article outlines key topics that should be considered in a framework for regulating the rights and duties of cryptocurrency payments users, including the intermediaries that operate depositories and execute transactions as providers of “wallets”³⁵² and “exchanges.”³⁵³ It does not contain draft language for the purposes of dealing with those topics.

In making the following recommendations for subjects that a regulation of cryptocurrency payments intermediaries— wallet and exchange operators for the most part— should take into account, we have looked to provisions of Uniform Commercial Code Article 4A. Article 4A serves as the basis for state laws regulating “funds transfers” also known as “wholesale wire transfers” in which commercial banks act for the originator and beneficiary and also serve as intermediaries in the series of transfers needed to push funds into the beneficiary’s account.³⁵⁴

Any framework regulating transaction-execution intermediaries should cover all of the following issues, relationships, and miscellaneous issues that Article 4A covers to the extent that they arise in cryptocurrency transactions:

- defining the framework’s subject matter and covered participants,
- giving cryptocurrency payment instructions to their respective intermediaries,
- executing senders’ cryptocurrency payments instructions,
- fixing the Timing and Effect of Payments; Obligations to the Initiator of the Payment Instruction; Obligations of Intermediaries to Complete Transaction; Discharge of Underlying Obligations, and,
- addressing miscellaneous Issues that include provisions related to creditor service of process.

We do not build on provisions of Article 4A that, in our view, are not needed for cryptocurrency transaction intermediaries. This Part of this Article also discusses the reasons why each of these subjects should be included in any cryptocurrency-intermediary payment regulatory framework.

351. *See id.*

352. *See Fistful of Bitcoins*, *supra* note 2, at 10-12 (describing how Bitcoin works and the third-party providers known as “wallets” or “exchanges” that users use to store their bitcoin). The BitLicense Final Regulation uses neither of these terms in its definition of “virtual currency business activity” but its language would encompass both terms. BitLicense Final Regulation, *supra* note 21, § 200.2(n).

353. *See id.*

354. U.C.C. § 4A-104(a) (2012) (definition of “funds transfer”).

A. The Subject Matter and Covered Participants

Unless amendments to a federal consumer financial protection law such as the Electronic Fund Transfer Act³⁵⁵ cover transactions in which the initiator and obligor of an underlying transaction is a consumer, a new law governing cryptocurrency payments should govern the rights of consumers and persons and entities to which they owe payments for goods or services, the operators of cryptocurrency wallets and exchanges, and any other entity whose services are required to complete a cryptocurrency payment transaction. The new Regulation E provisions would cover only transactions in which a consumer is the initiator or sender of the payment or transactions in which a consumer's account is debited or credited regardless of whether the consumer involved is the initiator or the recipient of the payment.

The provisions of any new payments law governing cryptocurrency payments, as the Official Comment to U.C.C. § 4A-102 proposed,³⁵⁶ should cover many subjects. These will include provisions to assign responsibilities, define key behavioral norms, allocate risks, and (perhaps) assign limits on liability so that cryptocurrency payments participants can predict risks, insure against them, adjust transaction-specific as well as generic security procedures, and price their services according to the risks they have identified and the costs of providing those services.

The participants and the roles they perform should also be defined in any statute or regulation that may be enacted or adopted. Although much of the terminology that Article 4A uses could be used in the cryptocurrency payments laws, the risk of confusing some participants would be greater if the same terms were used, particularly because Article 4A does not apply to consumer transactions governed by federal law.³⁵⁷ For this reason, and only for the purposes of this Article and not for drafting of legislation, we propose that the person issuing the instruction to a wallet, exchange, or other intermediary to make a payment for goods or services, as well as to [convert] cryptocurrency to fiat currency, be known as the initiator. The operator of a public wallet in which owners may store cryptocurrencies should be known as the wallet operator. The operator of an exchange that offers transaction execution services to the public should be known as the exchange operator. The beneficiary of a payment for goods and services can be known as the recipient, and if the transaction involves the conversion of cryptocurrency for fiat currency or vice versa, the party requesting the conversion can be known as the conversion-requester. The transactions will be called payment instructions if they pertain to payments for goods and services or conversion instructions if they pertain only

355. Electronic Fund Transfer Act, 15 U.S.C. §§ 1693-1693r (2013).

356. U.C.C. § 4A-102 cmt. (1989).

357. U.C.C. § 4A-108 (2012) (reflecting an amendment necessitated by amendments to 15 U.S.C. § 1693-1693r (2013)).

to conversion between one cryptocurrency and a different cryptocurrency, or a conversion to legal tender.

B. Requirements for Cryptocurrency Payment Instructions to Operators of Wallets and Exchanges

Aside from the operational requirements that banks offering wholesale wire transfers may specify in contracts with their customers, U.C.C. Article 4A sets forth specific requirements for the issuance and acceptance of payment orders.³⁵⁸ Operators of public wallets and exchanges should be required to have transparency on each of the following types of subjects:

(1) Security Procedures. Wallets and exchange operators should require agreement with their customers on the scope and details of any security procedure needed to verify the rights of an initiator to give a payment instruction to the wallet or exchange. The wallet or exchange operator will need to use the security procedure to detect unauthorized payment instructions or conversion instructions or errors in the transmission or content of the payment or conversion instruction.

(2) Provisions for the duty of the recipients of payment instructions to execute them, including the prospect of additional contractual provision requirements related to security of the transaction, amendments and cancellations of payment instructions, and other operational concerns. This group of provisions could look much like those in Part 2 of Article 4A (“Issue and Acceptance of Payment Orders”). They would relate to the operator’s ability to rely on the security procedure, rules (if appropriate) for amending or cancelling payment instructions before the operator acts on them, enforceability or unenforceability of certain payment instructions, duty of the initiator to report lost cryptocurrency or unauthorized payment instructions, handling of payment instructions that are erroneous (including possible misidentification of the recipient’s account or account to which converted cryptocurrency should be sent or of the operator to which cryptocurrency should be sent), and the ability of the operator to reject a payment instruction that does not comply with any security requirements added by contract.

(3) Execution of Cryptocurrency Payment Instructions. Like Part 3 of U.C.C. Article 4A (“Execution of Sender’s Payment Order by Receiving Bank”), new laws or regulations related to execution of cryptocurrency payments instructions or conversion instructions should deal with:

- The date of the execution of the transaction requested,
- The operator’s obligations in executing the payment instruction, errors in the execution of payment instructions, and

358. U.C.C. art. 4A, Part 2 (Issue and Acceptance of Payment Order) (1989).

- The duty of the initiator to report errors in the execution of payment instructions.

(4) Timing and Effect of Cryptocurrency Payments Instructions; Discharge of Underlying Obligation of the “Sender” of the Payment Instruction. Like section 4A-406 (“Payment by Originator to Beneficiary; Discharge of Underlying Obligation”) generally, rules setting both the timing of payments made through the intermediary and the amount of the payment made should be in any commercial law that governs cryptocurrency payments intermediaries.³⁵⁹ In addition, like section 4A-406(b), payments made to satisfy obligations should discharge those obligations “to the extent discharge would result from payment to the beneficiary of the same amount in money”³⁶⁰ with exceptions comparable to those stated in this subsection. Those exceptions include cases in which (i) the payment was made by a means prohibited in the contract between initiator and beneficiary,³⁶¹ (ii) the recipient refused the payment within a reasonable time after receiving notice of the payment,³⁶² (iii) the recipient never withdrew the cryptocurrency or applied it to the debt,³⁶³ or (iv) the recipient would suffer a loss that “could reasonably have been avoided if payment had been made by a means complying with the contract.”³⁶⁴

(5) Right of the initiator to be subrogated to the rights the recipient to receive payment from the recipient’s agent in the event that the payment does not result in a discharge under the discharge rules.³⁶⁵

(6) Amount of payment and resulting discharge if intermediaries for the initiator and recipient, or other intermediaries, deduct charges from the amount of the payment instruction sent, comparable to the rule in section 4A-406(c).³⁶⁶ Section 4A-406(c) also deems the payment to the beneficiary to be an amount equal to the amount of the originator’s payment order unless the beneficiary makes a demand on the originator to pay over the deducted charges and the originator does not pay them.³⁶⁷ Although one of the values of using current cryptocurrencies in payments is lower transaction-execution charges, as crypto-payments intermediaries develop their markets or add value by offering the equivalent of deposit insurance, pricing could rise. Thus, the issue of fee deductions along the path from initiator to recipient could arise as the market matures and should be considered.

359. *Id.* § 4A-406(a).

360. *Id.* § 4A-406(b).

361. *Id.* § 4A-406(b)(i). Such a requirement protects a counterparty that expects legal tender, not cryptocurrencies, in payment of the obligation.

362. *Id.* § 4A-406(b)(ii).

363. *Id.* § 4A-406(b)(iii).

364. *Id.* § 4A-406(b)(iv).

365. *Id.* § 4A-406(b) (last sentence).

366. *Id.* § 4A-406(c).

367. *Id.* § 4A-406(c).

(7) Like section 4A-406(d), the rules for cryptocurrency intermediaries should provide that no agreement except one made by the initiator and recipient of the crypto-payment should affect the rights and obligations to the cryptocurrency payment instruction.³⁶⁸ Such a provision would protect the initiator and recipient from terms of agreements that might arise between intermediaries, while also preserving the rights of initiator and recipient to vary the terms of the regulation by their own agreement.³⁶⁹

These types of provisions are needed to balance the interests of expert providers (including online wallet and exchange providers) with those of the general public who may acquire or use cryptocurrencies through purchase or receive them in payment for goods and services, but who are not expert cryptocurrency market participants.

C. Fees and Fee Disclosures

The Uniform Commercial Code does not address issues such as fees or fee disclosures made by banks under Article 4A. But federal consumer financial protection statutes and the regulations that implement them do. Crypto-payment intermediaries will operate more like providers of remittance transfers under the EFTA³⁷⁰ and Regulation E³⁷¹ and, when consumers are the initiators of crypto-payments instructions, it is not unthinkable that fee disclosures of the types and at times required by Regulation E's remittance transfer provisions could be appropriate. Section 1005.31(b) requires pre-payment disclosures of fees imposed by the provider of the remittance transfer and the recipient's provider, and of taxes that the provider will collect on behalf of a state or other governmental body including by someone in the chain needed to complete the transaction, such as a foreign provider, to the extent the provider in the United States collects them up-front from the sender of the payment.³⁷² Pre-transaction fee disclosures are one of the potential rules in a crypto-payments transaction execution regulation that would apply primarily to consumers.

D. Rules Governing Unauthorized Transfers, including Counterfeits and Replicates, and Providing Error-Resolution or Reversibility Rights

Bitcoin was designed to overcome some of the problems with payments systems. Among these was the absence, as Satoshi Nakamoto explained, of a "mechanism . . . to make payments over a communications channel without a trusted party."³⁷³ Instead Nakamoto suggested "cryptographic proof" could

368. *Id.* § 4A-406(d).

369. *Id.* § 4A-501(a).

370. 15 U.S.C. §§ 1693-1693r (2013).

371. See 15 C.F.R. Part 1005, Subpart B (2014).

372. 12 C.F.R. § 1005.31(b) (2013).

373. Nakamoto, *supra* note 15, at 1.

substitute for trust and “[allow] any two parties to transact directly with each other without the need for a trusted third party.”³⁷⁴ Nakamoto further explained that the “peer-to-peer electronic cash system” proposed would involve “[t]ransactions that are computationally impractical to reverse” and that feature would “protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers.”³⁷⁵ Additionally, Nakamoto proposed to solve the problem of “double-spending” by “using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions.”³⁷⁶ These provisions serve to protect participants making transactions on the block chain, but they do not provide equal protection to participants using payments intermediaries to execute their transactions.

Payment transaction-execution rules normally contain provisions to allocate risks of unauthorized transfers, counterfeits, and double-spending or replicates. Despite protections that the cryptographic proof of the timestamp chronology is designed to provide, state regulation of cryptocurrency payments transaction-execution should include protections of these types. This is because the instructions sent by the initiator of a crypto-payment to an intermediary payment provider may not involve all of the proof and timestamp features required for this level of protection. We say that they may not protect the intermediary or the initiator sufficiently because wallets and exchanges have reported the loss of cryptocurrencies.³⁷⁷

Regulation E’s remittance transfer rules also establish rules for error-resolution and call for providers to investigate and resolve claimed errors if the consumer sender has made his or her claim within 180 days of the promised date of delivery of the payment.³⁷⁸ The error-resolution procedures apply to the three types of errors specified in section 1005.33(a)(1): incorrect amount paid to the recipient, failure to make the funds available to the recipient on the date stated on the receipt given to the consumer sender of the payment in the United States, and provider errors that result in the payment being sent to the wrong recipient.³⁷⁹

U.C.C. Article 4A provides rules for the unenforceability of certain verified payment orders,³⁸⁰ and rules governing refunds of payments and imposing a duty on the customer to report unauthorized payment orders.³⁸¹

374. *Id.*

375. *Id.*

376. *Id.* For additional perspective on this issue, see *Fistful of Bitcoins*, *supra* note 2, at 11 (explaining that in peer-to-peer transactions, double-spending is prevented by giving every peer “access to the entire transaction history (or at least to the transactions in which the received bitcoins have not been spent).”).

377. *E.g.*, *Hern, Mt. Gox Bankruptcy Filing*, *supra* note 5.

378. 12 C.F.R. § 1005.33 (2014).

379. *Id.*

380. U.C.C. § 4A-203 (2012).

381. *Id.* § 4A-204.

Rules comparable to these Article 4A rules would be suitable for non-consumer initiators of payments instructions.

E. Miscellaneous Issues Arising from Custom or Otherwise from Article 4A

A few miscellaneous provisions that come from custom or from U.C.C. Article 4A could be considered. Examples of such provisions include:

(1) Notices to initiators and recipients. For example, beneficiaries in Article 4A transactions get “advice of credit” notices from the bank that serves as their depository bank. Advices of credit inform beneficiaries that the bank has “accepted” a “payment order” intended for their accounts; because “acceptance” makes the fund transfer final as to a particular beneficiary. This is the last event in the chain of transfers needed to move funds from the originator to the beneficiary’s bank. Advices, thus, reflect final payments and discharge any underlying obligation of the originator to pay the beneficiary. The initiator of a cryptocurrency payment may need to get a notice of receipt or other form of receipt from the wallet or exchange operator who serves as the intermediary.

(2) Rules governing special issues when creditor process is served on the recipient’s agent³⁸² and agents’ rights of setoff against credits to the recipient’s account with the agent (for example, for payment instructions made by the same customer or for fees owed by the customer to the agent).³⁸³ Inclusion of a rule similar to section 4A-502(d) that limits the effect of service of creditor process to service on the recipient’s agent in the particular crypto-payment transaction should be considered.³⁸⁴ Of course, in a crypto-payment transaction, the exchange operator is likely to be able to receive the payment instruction from the initiator and credit the account of the recipient, but we envision a stage in the progress of crypto-payments in which multiple intermediary wallets or exchange operators might be engaged in completing a single payment instruction through to the recipient.

Conclusion

This article has described what cryptocurrencies are, how cryptocurrencies are distinct in our view from “virtual currencies,” and what efforts to regulate them so far have produced both here and abroad. It also has reviewed public-law regulatory models – for purposes such as deterring and detecting money laundering or violations of economic sanctions, collecting taxes and identifying those avoiding taxes, regulation of the issuance of securities and of those who trade in them as a business, and regulation of commodities and those who trade in them as a business—that, so far, seem to be the predominant models abroad.

382. See U.C.C. § 4A-502(a)-(b) (1989).

383. See *id.* § 4A-502(c).

384. *Id.* § 4A-502(d).

We have suggested that some of these models also serve to enhance markets and may even offer some private-facing provisions that replace the need for dickered contracts. We have identified provisions of the New York State BitLicense Final Regulation that, as a case study of licensure and prudential regulation regimes for cryptocurrencies, may not represent the rules that other States are likely to adopt. We have looked beyond the steps taken to seek the last link in a more robust and mature complex of regulations for cryptocurrency payments transactions conducted by intermediaries.

It is clear that New York State's 2015 BitLicense Regulation³⁸⁵ and its 2014 BitLicense Proposal,³⁸⁶ and the reports from the Conference of State Bank Supervisor's Emerging Payments Task Force³⁸⁷ and the Final Study Committee on Alternative and Mobile Payments³⁸⁸ have fundamentally changed the debate about cryptocurrency regulation. Although a few ideological partisans may hold out, the consensus view is shifting from a discussion of whether cryptocurrency should be regulated to more pointed questions regarding when, how and by whom such actions should be taken.³⁸⁹

The movement to a more interventionist approach by governments is in part a reaction to two class action lawsuits in the United States,³⁹⁰ the January 2015 hacking of Bitstamp's online storage depository³⁹¹ and the Mt. Gox bankruptcy proceedings in Japan³⁹² and ancillary Chapter 15 action in Texas.³⁹³

As it appears that reluctance to regulate cryptocurrencies has been overcome at both the State and Federal levels, as evidenced by the BitLicense Final Regulation and the work of the CSBS and ULC, we have proposed that

385. BitLicense Final Regulation, *supra* note 21.

386. BitLicense Proposal, *supra* note 20.

387. CSBS Framework, *supra* note 22.

388. ULC STUDY COMMITTEE FINAL REPORT, *supra* note 23.

389. See Fred H. Miller & Sarah Jane Hughes, Preliminary Report to the [Uniform Law Commission] Study Committee – Alternative and Mobile Payment Systems, UNIF. L. COMM'N (June 30, 2014), www.uniformlaws.org/shared/docs/Alternative%20and%20Mobile%20Payments/AMPS%20Preliminary%20Report%20063014.pdf (additional discussion of regulation of virtual currencies); Lawrence Trautman, *Virtual Currencies: Bitcoin & What Now after Liberty Reserve, Silk Road, and Mt. Gox?*, 20 RICH. J. L. & TECH. 13 (2014); Nicholas Plassaras, *Regulating Digital Currencies: Bringing Bitcoin within the Reach of the IMF*, 14 U. CHIC. J. OF INT'L L. 377 (2013); Omri Y. Marian, *Are Cryptocurrencies Super Tax Havens?*, 112 MICH. L. REV. FIRST IMPRESSIONS 38 (2013); Aleksandra Bal, *Stateless Virtual Money in the Tax System*, 53 EUR. TAXATION 351 (2013).

390. *Hussein v. Coinabul*, No. 1:14cv5735 (N.D. Ill. July 25, 2014) (alleging that defendant Coinabul, LLC, an online marketplace based in Cheyenne, Wyoming, defrauded its customers who had been offered a vehicle for exchanging bitcoins into silver or gold); *Greene v. Mt. Gox*, *supra* note 72.

391. See Michael J. Casey & Amir Mizroch, *Bitcoin Exchange Bitstamp Suspends Services After Breach*, WALL ST. J. (Jan. 6, 201, 3:21 p.m. ET), <http://www.wsj.com/articles/bitcoin-exchange-bitstamp-temporarily-suspends-services-1420575704>.

392. See Alex Hern, *Mt. Gox Files for Bankruptcy in Japan After Collapse of Bitcoin Exchange*, GUARDIAN (Feb. 28, 2014), <http://www.theguardian.com/technology/2014/feb/28/bitcoin-mtgox-bankruptcy-japan>; *Tokyo Court Orders Bankruptcy Trustee to Begin Mt. Gox Liquidation*, REUTERS (Apr. 24, 2014), <http://www.reuters.com/article/2014/04/24/us-bitcoin-mtgox-bankruptcy-idUSBREA3N0KM20140424>.

393. *In re Mt. Gox Co Ltd.*, No. 14-31229 (Bankr. N.D. Tex. Mar. 10, 2014).

now is the time to begin writing a commercial law that would regulate the rights and duties of counterparties to the transfers of cryptocurrency transactions – those engaged in “money transmission” as FinCEN has defined it. That said, we think that other applications of the distributed computing technology that underlies cryptocurrencies – such as using the block chain to manage intangibles like mortgages – are not ripe for regulation at this time.

We have suggested a framework for the commercial law we believe is needed. We built our framework on Article 4A of the Uniform Commercial Code because it offers the closest analogy to rules for multi-party transfers of credits in the United States. Minor variations, which we have suggested above, may be needed to make an Article 4A model such as we propose work for cryptocurrency payments intermediaries. In Part IV of this article, we have suggested topics for inclusion in a commercial law for cryptocurrency payments intermediaries that are found in other payments and e-payments commercial or consumer protection laws. These include error-resolution, rules regulating redemption of value by persons who deliver value into the custody of others, and rules establishing the liabilities of counterparties to each other. We have not suggested where this new commercial law should be housed – that is, whether a new subpart of Article 4A or a new model or uniform law outside the Uniform Commercial Code should emerge to deal with cryptocurrency payment intermediaries’ business dealing on behalf of others. We remain persuaded that Article 4A offers useful points of comparison with legacy systems and may enhance opportunities for new entrants and legacy providers to innovate.

In connection with our proposal, we also attempted to observe the following principles:

- (1) Cryptocurrency providers should be regulated by the agency, whether of the federal or state governments, with the most experience supervising similar entities for similar purposes. In the United States, for example, for prudential purposes and for private-law purposes related to transaction execution, state regulators with the greatest familiarity with non-depository supervision and private law regulation of transaction execution should take the lead. Other public-law purposes such as taxation, securities registration and broker-dealer conduct, commodities trading and dealer transactions, deterrence of money laundering and of terrorist finance, and enforcement of economic sanctions regimes seem more properly the province of the federal government.
- (2) Regulation should be designed to increase comfort levels for market participants that, we suggest, will spur earlier and more widespread adoption of regulated technologies. This trust or trusted entity factor should not be overlooked in debate about regulating cryptocurrency payment intermediaries.

Regulating Cryptocurrency Payments Intermediaries

- (3) Clarity in the scope of regulations and guidance is essential. Clarity that exposes loopholes that innovators can exploit is not bad in itself. The exploitation of loopholes is in the nature of innovation in financial services and financial services technologies.
- (4) A risk-based approach, such as U.C.C. Article 4A, is more likely to allow innovation than a prescriptive approach such as the BitLicense Final Regulation. Risk-based regulation also may reduce the need for frequent revisions to regulations that are costly for all market participants. A final benefit of a risk-based approach is that it can suit specific applications – with greater and lesser risks – better than a prescriptive, one-size-fits-all approach, and, accordingly, can lower costs while preserving the allocations of rights and responsibilities intended.

We believe that these principles are suitable to guide other forms of future regulation of cryptocurrencies and the persons that use or trade in them.

The different potential uses of the algorithms underlying Bitcoin and other cryptocurrencies make the task of getting their early regulation right all the more important. But as the potential exists for more uses of cryptocurrencies in payments transactions, it is important that we begin to draft a basic scheme for regulating the obligations of the parties to such transactions – initiators, and particularly all classes of intermediaries including wallet providers, exchanges and other service providers. We also recommend that it be developed at roughly the same time as prudential regulation of those offering payments execution and value-storage services. Finally, we encourage that both a commercial law and prudential regulations be adopted soon enough to allow these payment options to flourish.

