

[forthcoming in 87:2 of LAW AND CONTEMPORARY PROBLEMS  
(2024 symposium issue on “Regulating Digital Currencies”)]

## *De-Mystifying Digital Currencies*

*Steven L. Schwarcz*<sup>1</sup>  
*with assistance from David N. Ord*<sup>2</sup>

### I. INTRODUCTION

The potential of digital currencies—monetary currencies that are evidenced electronically and not in physically tangible form—to improve the speed and efficiency of payments and to broaden financial inclusion makes such currencies an important part of our future.<sup>3</sup> Large payments among businesses and financial institutions (“wholesale” payments) already occur digitally,<sup>4</sup> and Bitcoin has been with us for more than a decade.<sup>5</sup> Recent events, including turmoil in digital asset markets and growing doubt about the status of the U.S. Dollar as the global reserve currency, have increased the importance of studying digital currencies.

Three approaches to digital currency have emerged with varying levels of governmental and private sector support: generic cryptocurrencies, stablecoins, and central bank digital currencies (CBDC).<sup>6</sup> Generic cryptocurrencies refer to digital currencies that are electronically evidenced using secure cryptography. Stablecoins are a subset of cryptocurrencies that are backed by assets having intrinsic value. CBDC may be either a type of central bank sponsored

---

<sup>1</sup> Stanley A. Star Distinguished Professor of Law & Business, Duke University School of Law; Senior Fellow, the Centre for International Governance Innovation (CIGI); Founding Director, Duke Global Financial Markets Center.

<sup>2</sup> Duke University School of Law, J.D. 2025.

<sup>3</sup> See U.S. DEP’T OF TREASURY, PRESIDENT’S WORKING GROUP ON FINANCIAL MARKETS STATEMENT ON KEY REGULATORY AND SUPERVISORY ISSUES RELEVANT TO CERTAIN STABLECOINS 1 (2020) [hereinafter PRESIDENT’S WORKING GROUP STATEMENT], <https://home.treasury.gov/system/files/136/PWG-Stablecoin-Statement-12-23-2020-CLEAN.pdf> (finding that “[d]igital payments . . . have the potential to improve efficiencies, increase competition, lower costs, and foster broader financial inclusion”).

<sup>4</sup> See, e.g., FED. RSRV. SYS., FEDWIRE FUNDS SERVICE <https://www.frbservices.org/assets/financial-services/wires/funds.pdf> (last visited Dec. 2, 2021). Wholesale digital payments operate through electronic funds transfers.

<sup>5</sup> See Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN PROJECT (2008), <https://bitcoin.org/bitcoin.pdf> (outlining the concept of bitcoin).

<sup>6</sup> Although the terms “digital currency” and “cryptocurrency” are often used in similar contexts, digital currencies encompass any digital asset that can be used as a currency, which may include certain cryptocurrencies but may also include non-cryptocurrency assets.

cryptocurrency or a central bank sponsored digital currency issued under account-based models (utilizing electronic funds transfer systems such as FedWire or FedNow).

This Article discusses each approach and briefly comments on the suitability of each to fulfill the three primary functions of currency: as a medium of exchange, as a store of value, and as a unit of account. The Article then considers regulatory concerns with the adoption of retail digital currencies and evaluates potential solutions. The Article's discussion and analysis are based on and draw heavily from the Author's previous works.<sup>7</sup>

### A. Generic Cryptocurrencies

The most popular generic cryptocurrency is Bitcoin. The motivation behind Bitcoin was to create a secure currency that has no centralized control.<sup>8</sup> As such a “decentralized” currency, Bitcoin is not subject to government control.<sup>9</sup> Bitcoin itself functions—and likewise, other generic cryptocurrencies are intended to function—as a medium of exchange. This means, for example, that parties can use Bitcoin to pay for goods or services. Bitcoin and other generic cryptocurrencies are also intended to serve as a store of value for their holders, although the market value of such currencies can fluctuate widely. In general, though, generic currencies are not intended to be used as a unit of account.

Cryptocurrencies become secure by using cryptography<sup>10</sup> to record ownership, to verify transfers and other transactions, and to facilitate the creation of digitally evidenced units of currency.<sup>11</sup> Sometimes called digital coins or tokens,<sup>12</sup> these units of currency are comparable to cash—other than being physically evidenced by paper or metal. They are recorded on a blockchain, which is a database (typically called a “ledger,” as in accounting) spread across multiple computers that connect via the internet.<sup>13</sup> Once the computers set the order of specific transactions,<sup>14</sup> that order becomes fixed.<sup>15</sup>

---

<sup>7</sup> See Steven L. Schwarcz, *Regulating Global Stablecoins: A Model-Law Strategy*, 75 VAND. L. REV. 1729 (2022), and Steven L. Schwarcz, *Regulating Digital Currencies: Towards an Analytical Framework*, 102 B.U. L. REV. 1037 (2022).

<sup>8</sup> Ittay Eyal, *Blockchain Technology: Transforming Libertarian Cryptocurrency Dreams to Finance and Banking Realities*, COMPUTER, Sept. 2017, at 38-39 (stating that Bitcoin started “as a means for creating a secure currency that had no centralized control”).

<sup>9</sup> *Id.*

<sup>10</sup> “Cryptography” generally refers to the use of algorithms or codes to obfuscate or secure information and communications.

<sup>11</sup> Wolfgang K. Härdle et al., *Understanding Cryptocurrencies*, 18 J. FIN. ECON. 181, 182 (2020) (stating that cryptocurrencies use cryptography “to secure transactions, to control the creation of additional value units, and to verify the transfer of assets”).

<sup>12</sup> The technical differences between those terms are arcane and not well defined.

<sup>13</sup> Lindsay Sain Jones, *Beyond the Hype: A Practical Approach to Cryptoreg*, 25 VA. J.L. & TECH. 175, 186 (2022). The term “blockchain” refers to the ledger that represents all transactions on the network. The ledger, or database, is organized as a chain of “blocks”, where each block contains one or more transactions.

<sup>14</sup> Eyal, *supra* note 8, at 40 (stating that nodes work to “agree on the order of all transactions placed in the system by grouping transactions into blocks and forming a chain of blocks”).

<sup>15</sup> Härdle et al., *supra* note 11, at 185. This immutability eliminates any double-spending problem because if a unit of cryptocurrency appears in two conflicting transactions, only one of

Cryptocurrency users agree on the order of transactions through a “consensus mechanism.”<sup>16</sup> That mechanism is intended to provide trust in the absence of a centralized authority.<sup>17</sup> Different generic cryptocurrencies rely on different consensus mechanisms.

Bitcoin, for example, relies on a Proof-of-Work (PoW) consensus mechanism, in which participants reach consensus by solving a cryptographic puzzle designed by the developers. In the case of Bitcoin, the puzzle consists of finding a value, which, when input to a mathematical function produces a result within a pre-determined range.<sup>18</sup> Users in the network compete by attempting to be the first to guess the solution. The user that solves the puzzle first creates adds a set of transactions to the database, which is then added to the network. This user is rewarded with an amount of Bitcoin set by the developers, which incentivizes network participation. The most frequent critique leveled at PoW consensus mechanisms is their relative high energy costs, resulting from users attempting to increase their Bitcoin rewards by utilizing an ever-higher quantity of computational resources.<sup>19</sup>

While many other consensus mechanisms exist, the most popular alternative to PoW is called Proof-of-Stakes (PoS). Cryptocurrencies such as Cardano, which use PoS consensus mechanisms, select which user will add the next set of transactions to the database based on the amount of cryptocurrency held. That is, if a user holds more Cardano, that user will more frequently be chosen to add transactions.<sup>20</sup> The stake-based block production leads to significantly lower energy costs compared to PoW blockchains.<sup>21</sup>

Cryptocurrencies have potential to provide high accessibility and low costs. Because cryptocurrencies operate without a centralized authority and without intermediaries, many of the costs and inefficiencies associated with multiple transfers between financial institutions can be avoided.<sup>22</sup> This benefit compounds in the case of cross-border payments which may also include multiple currency exchanges.<sup>23</sup> Additionally, anyone with access to the internet can use

---

those units will be placed on the blockchain with no ability to add the second. Eyal, *supra* note 8, at 40.

<sup>16</sup> Cong T. Nguyen et al., *Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities*, IEEE Access, June 26, 2019, at 85729.

<sup>17</sup> *Id.* (stating that the consensus mechanism “ensures that every participant agrees on the state of the network in such trustless environments ... [and] governs other operations of the network, such as transaction adding and incentivizing the participants to behave properly”).

<sup>18</sup> Eyal, *supra* note 8, at 40. The puzzle consists of “a solution searching process, where each node must find a nonce for its new block.” Nguyen, *supra* note 16, at 85729. When the nonce, the hash of the previous block, and the transactions in the new block produce a hash within an acceptable range, the block may be added to the chain. *Id.* “A hash function is a one-way mathematical algorithm that takes an input and transforms it into an output, known as the hash.” Härdle et al., *supra* note 11, at 183. Nodes in the network, or miners, attempt to guess the nonce before other nodes.

<sup>19</sup> See Nguyen, *supra* note 16, at 85730.

<sup>20</sup> See *id.*

<sup>21</sup> Nguyen, *supra* note 16, at 85731.

<sup>22</sup> Sain Jones, *supra* note 13, at 190.

<sup>23</sup> *Id.*

cryptocurrencies; that can provide broader access to financial services, particularly in nations in which distrust in financial institutions is high.<sup>24</sup>

However, because of their fluctuating market value, the utility of Bitcoin and other generic cryptocurrencies to serve as a retail medium of exchange and store of value is in question. Like fiat currencies, cryptocurrencies have no intrinsic value. They can only function if “sufficient market acceptance is present and if the belief exists that the currency has the value attributed to it.”<sup>25</sup> Unless and until a generic cryptocurrency obtains widespread adoption, and its users perceive a more stable value, price volatility limits the practical retail use of generic cryptocurrencies.<sup>26</sup> It is notable, however, that at least one nation, El Salvador, has already adopted Bitcoin as legal tender.<sup>27</sup>

The price volatility of generic cryptocurrencies has sparked the development of another approach to non-government-issued cryptocurrencies: stablecoins.

## B. Stablecoins

Although cryptocurrencies, stablecoins are designed to maintain a stable target price.<sup>28</sup> To the extent they hold a constant value, they can more effectively serve as a retail medium of exchange and as a store of value.<sup>29</sup>

As with any other retail currency, the main developmental challenges to using stablecoins as retail currencies include increasing accessibility (the ability of consumers to transfer and have day-to-day access to the currency) and reducing cost (the ability of consumers to achieve that access and transferability on a cost-effective basis).<sup>30</sup>

Like all other cryptocurrencies, stablecoins are digitally evidenced units of currency issued on a blockchain and protected by cryptography.<sup>31</sup> In general, therefore, stablecoins should have the same high accessibility and low transaction costs of generic cryptocurrencies.<sup>32</sup> However, the

---

<sup>24</sup> See *id.* at 192-93.

<sup>25</sup> Härdle et al., *supra* note 11, at 185.

<sup>26</sup> Mary E. Burke, Comment, *From Tether to Terra: The Current Stablecoin Ecosystem and the Failure of Regulators*, 28 *FORDHAM J. CORP. & FIN. L.* 99, 107 (2023).

<sup>27</sup> HENRI ARSLANIAN ET AL., *EL SALVADOR’S LAW: A MEANINGFUL TEST FOR BITCOIN*, 1, (2021)

<sup>28</sup> JOACHIM ZAHNENTFERNER ET AL., *DJED: A FORMALLY VERIFIED CRYPTO-BACKED PEGGED ALGORITHMIC STABLECOIN 1* (2021) (stating that stablecoins provide “mechanisms to maintain a low deviation of its price from a target price”).

<sup>29</sup> Burke, *supra* note 26, at 107.

<sup>30</sup> See BANK FOR INT’L SETTLEMENTS, *CENTRAL BANK DIGITAL CURRENCIES: FOUNDATIONAL PRINCIPLES AND CORE FEATURES* (2020), <https://www.bis.org/publ/othp33.pdf>, [hereinafter *BIS CBDC REPORT*], at 16; Tommaso Mancini-Griffol, Maria Soledad Martinez Peria, Itai Agur, Anil Ari, John Kiff, Adina Popescu & Celine Rochon, IMF Staff Discussion Note, *Casting Light on Central Bank Digital Currencies* 7, 29, *SDN/18/08* (Nov. 12, 2018), <https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2018/11/13/Casting-Light-on-Central-Bank-Digital-Currencies-46233>, at 29.

<sup>31</sup> Jake Frankenfield, *Cryptocurrency*, *INVESTOPEDIA* (Jan. 11, 2022), <https://www.investopedia.com/terms/c/cryptocurrency.asp>.

<sup>32</sup> See, e.g., Nakamoto, *supra* note 5, at 1; GAVIN WOOD, *ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER: BERLIN VERSION* (2022), <https://ethereum.github.io/yellowpaper/paper.pdf> (providing official document of Ethereum).

adoption of stablecoins depends on an additional factor: the ability or inability to maintain a stable value.

Stablecoins are redeemable, meaning exchangeable, for reference assets such as government fiat currencies or commodities like gold.<sup>33</sup> The stablecoin issuer may then hold assets in reserve to help ensure its ability to perform the exchanges. Those reserve assets may be the reference asset itself (e.g., a fiat currency) or may include other liquid assets such as interest-bearing securities.

A stablecoin's value depends on the ability of its holders to redeem their currency for the reference assets upon demand made to the relevant stablecoin issuer, which may be a financial institution or, in many cases, a tech company or similar organization.<sup>34</sup> Any failure of the issuer to satisfy such redemption rights, or even the perception that such a failure might occur, would likely lead to a loss of confidence in the stablecoin and a collapse in its value.<sup>35</sup> As later discussed, this could resemble a classic bank run, especially if the issuer is unable to obtain sufficient reference assets to satisfy correlated demands by stablecoin holders.<sup>36</sup>

Because of their prevalence, the regulatory issues discussed in this Article will focus on fiat-backed, centralized stablecoins.

### C. Central Bank Digital Currencies

The third approach to digital currencies is for governmental central banks to issue the currency. Such "CBDC" currencies would function similar to a nation's fiat currency but in digital form. Because wholesale fiat-currency payments are already settled digitally, the implementation of a retail CBDC may be straightforward. The utility of a CBDC as a medium of exchange, a store of value, and a unit of account is clear; it would mirror that of the physical fiat currency. The CBDC's digital form could improve accessibility and reduce transaction costs, thereby promoting widespread usability. Two digital formats have emerged: account-based CBDC and token-based CBDC.<sup>37</sup>

---

<sup>33</sup> Burke, *supra* note 26, at 112-13; Härdle et al., *supra* note 11, at 187.

<sup>34</sup> See FIN. STABILITY BD., REGULATION, SUPERVISION AND OVERSIGHT OF "GLOBAL STABLECOIN" ARRANGEMENTS 9 (2020) [hereinafter FSB STABLECOIN REPORT], <https://www.fsb.org/wp-content/uploads/P131020-3.pdf>, at 10 (identifying redemption as core function of stablecoin arrangement).

<sup>35</sup> *Id.* at 15. The FSB itself recognizes this distinction between operational factors and value. When discussing the impact of global stablecoins on financial stability, it differentiates "operational disruption" which "might have significant impacts on economic activity and financial system functioning," and variations in "value" of global stablecoins which "might cause significant fluctuations in users' wealth" that are "sizeable enough to affect spending decisions and economic activity." *Id.* at 13.

<sup>36</sup> See *infra* Section II.C.2. Some argue that even an apparently fully reserved stablecoin issuer might pose redemption risk because there is no uniform transparency policy with respect to reserve assets. ZAHNENTFERNER ET AL., *supra* note 28, at 2. Decentralized alternatives, such as so-called "algorithmic" stablecoins, potentially might help to mitigate that risk. Discussion of these alternatives is beyond this Article's scope.

<sup>37</sup> A token-based currency model is sometimes referred to as coin-based.

### 1. Account-based vs. Token-based CBDC

In an account-based CBDC, the currency would represent an electronically registered claim against—that is, a deposit at<sup>38</sup>—the central bank or its agent bank (for example, a commercial bank).<sup>39</sup> A currency transfer would involve debiting all or part of the transferor’s (i.e., the payor’s) claim and crediting that amount to the transferee’s (i.e., the payee’s) account with the central bank or its agent bank.<sup>40</sup> These would simply be book entries in accounts that are held and managed by banks.<sup>41</sup> An account-based CBDC could be implemented by extending the current wholesale digital payment capability to the retail space. For example, the FedWire or FedNow digital wire transfer systems could be extended to retail customers because, at least technologically, there do not appear to be significant differences between retail and wholesale digital funds transfers.

In a token-based CBDC, the units of currency would be issued by the central bank but recorded on a blockchain.<sup>42</sup> In contrast to an account-based CBDC, in which the recordkeeping is maintained through the transferor and transferee deposit accounts, the recordkeeping for a token-based CBDC could be maintained through other central-bank-specified forms of identifying currency transfers.<sup>43</sup>

---

<sup>38</sup> A deposit at a bank is the term generally used for a customer making a loan to the bank. Technically, the deposit evidences the customer’s claim against the bank for repayment. *Citizens Bank of Md. v. Strumpf*, 516 U.S. 16, 21 (1995).

<sup>39</sup> See, e.g., Michael D. Bordo & Andrew T. Levine, *Central Bank Digital Currency and the Future of Monetary Policy* 6 (Nat’l Bureau of Econ. Rsch., Working Paper No. 23711, 2017), [https://www.nber.org/system/files/working\\_papers/w23711/w23711.pdf](https://www.nber.org/system/files/working_papers/w23711/w23711.pdf) (stating that “individuals and firms would hold funds electronically in CBDC accounts at the central bank or in specially designated accounts at supervised depository institutions” (emphasis omitted)); CENT. BANK OF ICE., *RAFKRÓNA? CENTRAL BANK DIGITAL CURRENCY INTERIM REPORT* 12, at 11 (2018), [https://www.cb.is/library/Skraarsafn---EN/Reports/Special\\_Publication\\_12.pdf](https://www.cb.is/library/Skraarsafn---EN/Reports/Special_Publication_12.pdf) (noting that CBDC can be issued “as a registered, traceable deposit to a payment account”); see also *supra* note 4 (observing that wholesale digital payments operate through electronic funds transfers).

<sup>40</sup> See BANK OF ENG., *CENTRAL BANK DIGITAL CURRENCY OPPORTUNITIES, CHALLENGES AND DESIGN* 47 (2020), <https://www.bankofengland.co.uk/-/media/boe/files/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design.pdf>.

<sup>41</sup> See, e.g., Alexander Lee, Brendan Malone & Paul Wong, *Tokens and Accounts in the Context of Digital Currencies*, BD. OF GOVERNORS OF THE FED. RSRV. SYS. (Dec. 23, 2020), <https://www.federalreserve.gov/econres/notes/feds-notes/tokens-and-accounts-in-the-context-of-digital-currencies-122320.htm>.

<sup>42</sup> BANK OF ENG., *supra* note 40, at 47.

<sup>43</sup> See *id.* Such forms might involve the use of smart contracts, for example, to serve as an algorithmic trusted third party to execute and record transactions. Sarah Allen et al., *Design Choices for Central Bank Digital Currency: Policy and Technical Considerations* 9 (Nat’l Bureau of Econ. Rsch., Working Paper No. 27634, 2020), [https://www.nber.org/system/files/working\\_papers/w27634/w27634.pdf](https://www.nber.org/system/files/working_papers/w27634/w27634.pdf) (discussing the three primary functions of money: as a medium of exchange, a store of value, and a unit of account), at 47-48. A currency transfer could involve the transferor (i.e., the payor) producing a digital “signature” that verifies the transfer of token ownership to the transferee (i.e., the payee). BANK OF ENG., *supra* note 40, at 47.

Different jurisdictions are taking different approaches to developing a retail CBDC. The European System of Central Banks has engaged in a proof-of-concept for a token-based CBDC, designed to preserve cash-like privacy for CBDC transactions.<sup>44</sup> The digital yuan being developed by the People's Bank of China appears to combine account-based and token-based features,<sup>45</sup> involving a cash-like liability that is distributed to the public through accounts at commercial banks and other trusted payment-system intermediaries.<sup>46</sup>

In the United States, a retail CBDC is likely to be account-based, at least initially.<sup>47</sup> Much of the existing U.S. infrastructure of both central and commercial banks<sup>48</sup>—as well as the widespread application of that infrastructure to wholesale digital funds transfers among businesses

---

<sup>44</sup> EUR. CENT. BANK, EXPLORING ANONYMITY IN CENTRAL BANK DIGITAL CURRENCIES 1-2 (2019), <https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.mipinfocus191217.en.pdf>.

<sup>45</sup> Raphael Auer, Giulio Cornelli & Jon Frost, *Rise of the Central Bank Digital Currencies: Drivers, Approaches and Technologies* 22-23 (Bank for Int'l Settlements, Working Paper No. 880, 2020), <https://www.bis.org/publ/work880.pdf>; Anton N. Didenko, Dirk A. Zetzsche, Douglas W. Arner & Ross P. Buckley, *After Libra, Digital Yuan and COVID-19: Central Bank Digital Currencies and the New World of Money and Payment Systems* 37 (Eur. Banking Inst., Working Paper No. 65, 2020), [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3622311](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3622311) (discussing how China's digital currency will be transferred). Although some claim that consumers lacking a bank account will be able to use China's digital currency, the details are sparse. See Karen Yeung, *What Is China's Sovereign Digital Currency?*, S. CHINA MORNING POST (May 13, 2020, 10:35 AM), <https://www.scmp.com/economy/china-economy/article/3083952/what-chinas-cryptocurrency-sovereign-digital-currency-and-why> (claiming digital wallets can be used without linking to a bank account).

<sup>46</sup> See, e.g., Lulu Yilun Chen, Heng Xie & Xize Kang, *China Enlists Ant-backed Mybank in Expanding Digital Yuan Trial*, BLOOMBERG (Feb. 22, 2021, 2:00 AM), <https://www.bloomberg.com/news/articles/2021-02-22/china-enlists-ant-backed-mybank-in-expanding-digital-yuan-trial>; Auer et al., *supra* note 45, at 22; Allen et al., *supra* note 43, at 82-83.

<sup>47</sup> See generally John Crawford, Lev Menand & Morgan Ricks, *FedAccounts: Digital Dollars*, 89 GEO. WASH. L. REV. 113 (2021) (focusing on a Federal Reserve Bank account-based system); Michael D. Bordo & Andrew T. Levine, *Central Bank Digital Currency and the Future of Monetary Policy* 6 (Nat'l Bureau of Econ. Rsch., Working Paper No. 23711, 2017), [https://www.nber.org/system/files/working\\_papers/w23711/w23711.pdf](https://www.nber.org/system/files/working_papers/w23711/w23711.pdf), at 6-7 (favoring the account-based CBDC design because of its payment verification and transaction efficiency); Auer et al., *supra* note 45, at 20-21 (finding account-based CBDC designs to be most common among ongoing retail CBDC projects). Recently, for example, two bills were introduced in the U.S. Congress—the Banking for All Act in the Senate, and the Automatic BOOST to Communities Act in the House of Representatives—that call for creating an account-based CBDC. S. 3571, 116<sup>th</sup> Cong. § 2 (2020); H.R. 6553, 116<sup>th</sup> Cong. § 2 (2020).

<sup>48</sup> For convenience, this Article refers to commercial banks broadly, as including all nongovernmental banks.

and financial institutions<sup>49</sup>—is already account-based.<sup>50</sup> Because an account-based retail digital currency also could operate through electronic funds transfers,<sup>51</sup> the United States should be able to use technologies largely already in place at commercial banks and merely extend their access to a wider user base.<sup>52</sup>

Similarly, an account-based retail CBDC may have lower operating costs and should be less disruptive to commercial borrowing than a token-based system. An account-based retail CBDC may have lower operating costs because currency transfers are made simply through book entries. That avoids the need to design and continuously update the security of cryptographic record keeping. It also should be less disruptive to commercial borrowing because consumers would maintain deposit accounts, thereby assuring the continuance of deposits as a relatively low-cost source of funds from which banks can make business loans.<sup>53</sup> Additionally, although, a token-based CBDC may have stronger privacy protections, a central bank normally wants to maintain surveillance and control over its national monetary system.<sup>54</sup> For these reasons, this Article hereinafter will focus on an account-based retail CBDC.<sup>55</sup>

---

<sup>49</sup> See U.C.C. § 4A, Prefatory Note (AM. L. INST. & UNIF. L. COMM'N 2020) (discussing centrality of digital payments in banking system).

<sup>50</sup> Financial institutions in the United States, for example, hold accounts at the Federal Reserve and use Fedwire to transfer money between these accounts. See FED. RSRV. SYS., *supra* note 4, at 1.

<sup>51</sup> See Charles M. Kahn & William Roberds, *The Design of Wholesale Payments Networks: The Importance of Incentives*, 1999 FED. RSRV. BANK ATLANTA ECON. REV. 30, 30; BANK FOR INT'L SETTLEMENTS COMM. ON PAYMENT & SETTLEMENT SYS., *THE ROLE OF CENTRAL BANK MONEY IN PAYMENT SYSTEMS* 8 (2003), <https://www.bis.org/cpmi/publ/d55.pdf> (observing that wholesale funds transfers between banks are already settled digitally).

<sup>52</sup> Following path dependence implicitly assumes that the cost of switching to a new path—in this case, to a token-based retail digital currency—would exceed its efficiency gains. Whether that assumption is valid ultimately will be an empirical question.

<sup>53</sup> *But see* Benjamin Geva, *Virtual Currencies and the State*, JUST MONEY (Apr. 22, 2020), <https://justmoney.org/b-geva-payment-in-virtual-currency/> (contending that a token-based CBDC could achieve efficiency gains by reducing level of retail deposits—although with concomitant risks).

<sup>54</sup> See, e.g., Aleksander Berentsen & Fabian Schär, *The Case for Central Bank Electronic Money and the Non-case for Central Bank Cryptocurrencies*, 100 FED. RSRV. BANK ST. LOUIS REV. 97, 104 (2018).

<sup>55</sup> This Article assumes the feasibility—now or in the near future—of technology required to manage an account-based retail CBDC. This assumption appears to be realistic. The Clearing House, a banking association and payments company that is owned by large commercial banks, has created its Real Time Payments (RTP) network to facilitate real-time digital retail funds transfers. *Real Time Payments for All Financial Institutions*, CLEARING HOUSE, <https://www.theclearinghouse.org/payment-systems/rtp> (last visited Dec. 4, 2021). The Federal Reserve is developing FedNow, an interbank real-time funds transfer service that is faster than FedWire. FedNow follows the lead of the Federal Reserve's Faster Payments Task Force, whose objective was to investigate and support faster payments in the United States. See *Mission and Objectives*, FASTER PAYMENTS TASK FORCE, <https://fasterpaymentstaskforce.org/meet-the-task-force/mission-and-objectives/> (last visited Dec. 4, 2021). The Task Force's goals included

## II. REGULATORY OVERVIEW

The Bank for International Settlements (an international body that acts “as a bank for central banks”),<sup>56</sup> the U.S. Federal Reserve (“the Fed”), and other prominent governmental institutions have observed that it is critical to provide a comprehensive and robust regulatory framework covering retail digital currencies.<sup>57</sup> When used for making cross-border payments, these currencies will generate high costs if multiple, and potentially conflicting, legal frameworks govern their use. Indeed, key jurisdictions are already pursuing different regulatory approaches.<sup>58</sup> Requiring compliance with a multitude of laws would be exceptionally expensive, both legally and operationally.<sup>59</sup> Furthermore, the interaction of conflicting legal frameworks could create “uncertainty about the enforceability of contractual obligations.”<sup>60</sup>

Additionally, in a 2020 joint statement on digital payments, the G7’s finance ministers and central bank governors suggested that stablecoins should be regulated and supervised to ensure

---

facilitating “identify[ing] and evaluat[ing] alternative approaches for implementing safe, ubiquitous, faster payments capabilities in the United States.” *Id.* And China is already testing a retail CBDC in four cities. *See* Jonathan Cheng, *China Rolls Out Pilot Test of Digital Currency*, WALL ST. J. (Apr. 20, 2020, 8:22 A), <https://www.wsj.com/articles/china-rolls-out-pilot-test-of-digital-currency-11587385339>.

<sup>56</sup> *See About BIS - Overview*, BANK FOR INT’L SETTLEMENTS, <https://www.bis.org/about/index.htm?m=1> (last visited Sept. 18, 2022) (“Our mission is to support central banks’ pursuit of monetary and financial stability through international cooperation, and to act as a bank for central banks.”).

<sup>57</sup> BIS CBDC REPORT, *supra* note 30, at 11 (focusing on CBDC, though expressing principles equally applicable to stablecoins); *cf.* Christian Catalini & Jai Massari, *Stablecoins and the Future of Money*, HARV. BUS. REV. (Aug. 10, 2021), <https://hbr.org/2021/08/stablecoins-and-the-future-of-money> (arguing that without “robust legal and economic frameworks, there’s a real risk stablecoins would be anything but stable”).

<sup>58</sup> Dave Michaels, Caitlin Ostroff & Elaine Yu, *Cryptocurrency’s Surge Leaves Global Watchdogs Trying to Catch Up*, WALL ST. J. (Aug. 23, 2021, 9:53 AM), <https://www.wsj.com/articles/cryptocurrencys-surge-leaves-global-watchdogs-trying-to-catch-up-11629720000>.

<sup>59</sup> COMM. ON PAYMENT & MKT. INFRASTRUCTURES, G7 WORKING GROUP ON STABLECOINS: INVESTIGATING THE IMPACT OF GLOBAL STABLECOINS 4 (2019), <https://www.bis.org/cpmi/publ/d187.pdf> (attributing the exceptionally high cost of making cross-border payments to several factors, including the need to coordinate and to comply with the laws of multiple jurisdictions); *cf.* Morten Bech & Jenny Hancock, *Innovations in Payments*, BIS Q. REV., Mar. 2020, at 21, 28 (discussing the high costs and inefficiency of cross-border payments); Keith E. Maskus, Tsunehiro Otsuki & John S. Wilson, *The Cost of Compliance with Product Standards for Firms in Developing Countries: An Econometric Study* 3 (World Bank, Policy Research Working Paper No. 3590, 2005), <https://openknowledge.worldbank.org/handle/10986/8961> (“At the firm level, complying with differing standards in such major export markets as the European Union (EU), the United States, and Japan can add costs.”).

<sup>60</sup> COMM. ON PAYMENT & MKT. INFRASTRUCTURES, *supra* note 59, at 4.

consumer protection and privacy.<sup>61</sup> Similarly, the G7 finance ministers and central bank governors suggest that regulations should also address factors that could undermine financial stability<sup>62</sup> and monetary integrity, including money laundering and terrorist (including proliferation)<sup>63</sup> financing, breaches of cybersecurity, and failures of operational resilience.<sup>64</sup>

The following discusses general regulatory considerations with respect to digital currencies, including protecting against financial crimes, protecting consumers and privacy, and protecting monetary integrity and financial stability.

#### A. Protecting Against Financial Crimes

The risk of financial crimes associated with the use of digital currencies is dependent, at least in part, on the underlying technology. As such, different digital currencies may be associated with different levels or risk for different crimes.

##### 1. Counterfeiting

Counterfeiting refers to the fraudulent replication or production of a financial instrument, typically a currency.<sup>65</sup> Traditionally, the counterfeiting risk for money has been concerned with illicit production of physical representations of the money, such as the unauthorized reproduction

---

<sup>61</sup> *G7 Finance Ministers and Central Bank Governors' Statement on Digital Payments*, U.S. DEP'T OF THE TREASURY (Oct. 13, 2020) [hereinafter *G7/Central Bank Statement*], <https://home.treasury.gov/news/press-releases/sm1152>.

<sup>62</sup> *Id.*; see PRESIDENT'S WORKING GRP. ON FIN. MKTS., FED. DEPOSIT INS. CORP. & OFF. OF THE COMPTROLLER OF THE CURRENCY, REPORT ON STABLECOINS 3 (2021), [https://home.treasury.gov/system/files/136/StableCoinReport\\_Nov1\\_508.pdf](https://home.treasury.gov/system/files/136/StableCoinReport_Nov1_508.pdf) [hereinafter PRESIDENT'S WORKING GRP.], at 1, 3 (discussing the risk of stablecoin activities "to the broader financial system"). Some critics have argued that the very nature of stablecoins invites financial instability. Lee Reiners, formerly with the Federal Reserve Bank of New York, has noted how stablecoins "are effectively treated by users as bank deposits," but the risk of a bank run is greater due to the coins not being "insured by the F.D.I.C." Eric Lipton & Ephrat Livni, *Crypto's Rapid Move into Banking Elicits Alarm in Washington*, N.Y. TIMES, [https://www.nytimes.com/2021/09/05/us/politics/cryptocurrency-banking-regulation.html?campaign\\_id=2&emc=edit\\_th\\_20210905&instance\\_id=39687&nl=todaysheadlines&regi\\_id=31966400&segment\\_id=68166&user\\_id=00d678ef49ea59edc7006d16f3b4a163](https://www.nytimes.com/2021/09/05/us/politics/cryptocurrency-banking-regulation.html?campaign_id=2&emc=edit_th_20210905&instance_id=39687&nl=todaysheadlines&regi_id=31966400&segment_id=68166&user_id=00d678ef49ea59edc7006d16f3b4a163) (last updated Nov. 1, 2021). Senator Elizabeth Warren would "ban banks in the United States from holding cash deposits backing up [the] stablecoins . . ." *Id.* Federal Reserve Chair Jerome Powell observes that "[y]ou wouldn't need stablecoins, you wouldn't need cryptocurrencies if you had a digital U.S. currency." *Id.* Whether or not that is true, the United States still has no viable digital currency.

<sup>63</sup> Proliferation financing refers to financing the illegal development or distribution of weapons that threaten national security. See FIN. ACTION TASK FORCE, COMBATING PROLIFERATION FINANCING 11 (2010), <https://www.fatf-gafi.org/media/fatf/documents/reports/Status-report-proliferation-financing.pdf>.

<sup>64</sup> *G7/Central Bank Statement*, *supra* note 61.

<sup>65</sup> Ralph E. McKinney, Jr., Lawrence P. Shao, Dale H. Shao & Duane C. Rosenlieb, Jr., *The Evolution of Financial Instruments and the Legal Protection Against Counterfeiting: A Look at Coin, Paper, and Virtual Currencies*, 2015 U. ILL. J.L. TECH. & POL'Y 273, 299.

of U.S. dollar bills. The protections involve increasing the complexity and markings of bills.<sup>66</sup> These concerns have no obvious parallel digital currencies.

Counterfeiting risk may vary depending on whether a digital currency is token-based or account-based, or whether the currency is issued on a decentralized blockchain or by a central authority. There are two possible ways to counterfeit an account-based CBDC, although both also could be classified as fraud: by double spending, and by making transfers involving an unverified account.<sup>67</sup> Double spending can occur when a payor uses the same money in an account to make two purchases before the transactions clear in the payment system.<sup>68</sup> Transfers involving an unverified account can occur when a payee causes the bank to credit money from a phantom account, which only appears to exist, to the payee's account and then quickly withdraws the money.<sup>69</sup>

To the extent an account-based CBDC makes use of existing banking technology and systems,<sup>70</sup> these counterfeiting risks should be comparable to counterfeiting risks in current wholesale digital banking.<sup>71</sup> On the other hand, a digital currency recorded through a decentralized blockchain, such as a cryptocurrency, may have a lower risk of counterfeiting depending on the associated consensus mechanism. For example, a proof-of-work consensus mechanism ensures each transaction is verified and prevents double-spending.<sup>72</sup> In a large, distributed network such as Bitcoin, double-spending is virtually impossible because of the immutability of the blockchain and the difficulty of manipulating transactions; a user would need to control a majority of the computer power in the network to manipulate transactions and double-spend currency. In practice, manipulation might be a greater risk in smaller networks because having a smaller number of computers in total means that a smaller number of computers is needed to gain control.<sup>73</sup> Cybersecurity also involves the risk of making transfers involving unverified accounts.<sup>74</sup> As with double spending, the unverified accounts risk could be minimized by using a centralized

---

<sup>66</sup> *Id.* at 302-03.

<sup>67</sup> See MKTS. COMM., BANK FOR INT'L SETTLEMENTS, CENTRAL BANK DIGITAL CURRENCIES 4 (2018), <https://www.bis.org/cpmi/publ/d174.pdf> (observing that form of verification needed differs between token-based and account-based money).

<sup>68</sup> See *id.* at 4 n.5 (observing double spending problem for digital tokens). This Article's reference to double spending includes, of course, any multiple spending of the same money in an account.

<sup>69</sup> See, e.g., Lily Hay Newman, *How Hackers Pulled Off a \$20 Million Mexican Bank Heist*, WIRED (Mar. 15, 2019, 7:00 AM), <https://www.wired.com/story/mexico-bank-hack/> (discussing transfer initiated by hackers from phantom account to real account within bank).

<sup>70</sup> Crawford et al., *supra* note 47, at 138-39.

<sup>71</sup> The security threat caused by a possible centralization of accounts in the central bank would still need to be considered.

<sup>72</sup> Kelly Mahoney, Comment, *Cryptocurrency: Regulate or Facilitate? How States' Approaches to Cryptocurrency Can Be Applied on a Federal Level*, 43 J. Nat'l Ass'n Admin. L. Judiciary C (2023). In such a system, a bad actor would need to control greater than 51% of the network's computing power to successfully manipulate a transaction. See Nguyen, *supra* note 16, at [].

<sup>73</sup> *Id.*

<sup>74</sup> See G7/Central Bank Statement, *supra* note 61 and accompanying text.

clearinghouse that logs all cryptocurrency transfers.<sup>75</sup> Similarly, blockchain technology could reduce the double-spending risk by improving account verification.<sup>76</sup>

Accordingly, while regulation of an account-based CBDC may resemble existing monetary regulation, regulating cryptocurrencies more broadly may be tied to the currency's underlying technology.

## 2. *Fraud*

The decentralized nature of cryptocurrencies may provide new means of committing fraud.<sup>77</sup> For example, fraudulent schemes may include tricking people into sending funds to an incorrect address. Because cryptocurrencies operate without intermediaries, there may be no way to cover the loss.<sup>78</sup> Similarly, cryptocurrency transactions are irreversible by definition, making it impossible to recover lost funds.<sup>79</sup> On the other hand, fraud risk associated with an account-based CBDC would closely resemble the existing currency-fraud risks. As such, current legal protections against fraud should be generally applicable.

## 3. *Money Laundering*

Globally, anti-money-laundering (“AML”) laws generally follow the Financial Action Task Force’s (FATF) recommendations.<sup>80</sup> The FATF seeks “to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system.”<sup>81</sup> To this end, the FATF makes recommendations for an AML legal framework in member countries.<sup>82</sup>

If the introduction of an account-based CBDC leaves the commercial banking sector as the retail depository institutions, no change should be needed, in principle, to AML laws. If the CBDC scheme contemplates that retail CBDC account holders have accounts directly with the central bank, that would raise questions whether the central bank or commercial banks should be obligated to comply with the AML laws.

The risk of money-laundering is likely to be greater with cryptocurrencies, which provide for instant payments with at least some level of anonymity.<sup>83</sup> Although anonymity is inherent to

---

<sup>75</sup> See Kevin V. Tu & Michael W. Meredith, *Rethinking Virtual Currency Regulation in the Bitcoin Age*, 90 WASH. L. REV. 271, 280 (2015).

<sup>76</sup> ORI JACOBOWITZ, BLOCKCHAIN FOR IDENTITY MANAGEMENT 2 (2016), <https://www.cs.bgu.ac.il/~frankel/TechnicalReports/2016/16-02.pdf> (discussing using digital IDs stored on a blockchain and attached to every stablecoin transaction).

<sup>77</sup> Sain Jones, *supra* note 13, at 6-8; see also Kelly Mahoney, *supra* note 72, at 6.

<sup>78</sup> *Id.*

<sup>79</sup> *Id.*

<sup>80</sup> FIN. ACTION TASK FORCE, INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION 7 (2021) [hereinafter FATF RECOMMENDATIONS], <https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf>.

<sup>81</sup> *What Do We Do*, FIN. ACTION TASK FORCE, <https://www.fatf-gafi.org/about/whatwedo/> (last visited Dec. 5, 2021).

<sup>82</sup> FATF RECOMMENDATIONS, *supra* note 80, at 10-11.

<sup>83</sup> Sain Jones, *supra* note 13, at 8.

cryptocurrency networks, it is still possible to track transactions across the network, particularly when a company can associate a network address to an individual. Some cryptocurrency applications, such as “mixers” or “tumblers,” are designed to make it difficult to trace transfers of such currencies back to their source and so would further elevate money laundering risk.<sup>84</sup> However, the benefits of increased privacy protections may arguably offset the risk of money laundering.

The FATF is considering how it should expand its recommendations to include cryptocurrencies and other virtual assets.<sup>85</sup> Prior to any widespread launch of stablecoins, for example, it recommends that stablecoin issuers be regulated and subject to monitoring systems that ensure AML and similar compliance.<sup>86</sup> The FATF also recommends that such regulation and monitoring should include institutions that conduct stablecoin exchange, transfer, or safekeeping services.<sup>87</sup> However, if stablecoin exchanges and transfers evolve to include large numbers of anonymous users—such as in peer-to-peer exchanges that do not involve institutional intermediaries—such exchanges and transfers could avoid regulation.<sup>88</sup> In theory at least, that threat should be no greater than is posed by today’s large numbers of cash transactions.<sup>89</sup>

One of the central approaches to address money laundering is the requirement to conduct customer due diligence (also known as Know-Your-Customer (“KYC”) laws).<sup>90</sup> Many institutions involved with providing cryptocurrency services, such as centralized exchanges, have begun to implement KYC requirements.<sup>91</sup> However, KYC requirements nullify the primary privacy and anonymity motivation behind cryptocurrencies. Additionally, if KYC obligations require every retail transaction to be scrutinized, it would impose high transaction costs due to

---

<sup>84</sup> *Id.*

<sup>85</sup> FATF RECOMMENDATIONS, *supra* note 80, at 17.

<sup>86</sup> *Id.*

<sup>87</sup> *Id.* at 76; *see also Money Laundering Risks from “Stablecoins” and Other Emerging Assets*, FIN. ACTION TASK FORCE (Oct. 18, 2019), <http://www.fatf-gafi.org/publications/fatfgeneral/documents/statement-virtual-assets-global-stablecoins.html> (FATF statement clarifying that “global ‘stablecoins’ and their service providers would be subject to the FATF standards”).

<sup>88</sup> *Id.* at 7–8 (“If unmediated peer-to-peer transactions become easier and more secure, this could prompt a shift away from the use of VASPs. This could increase the number and value of payments not subject to AML/CFT controls and could present a material ML/TF vulnerability if mass-adopted.”).

<sup>89</sup> *Cf. id.* (observing that like cash transactions that fall out of the scope of the FATF standards, there is a risk that some peer-to-peer stablecoin transactions that occur with no financial intermediary would avoid regulations).

<sup>90</sup> *Id.* at 14-15.

<sup>91</sup> Simon Dyson et al., *The Challenges of Investigating Cryptocurrencies and Blockchain Related Crime*, J. Brit. Blockchain Ass’n, Nov. 20, 2018 at 1-6.

the sheer volume of those transactions.<sup>92</sup> To reduce these costs, AML laws could place a floor on the value of transfers that would trigger the need to conduct customer due diligence.<sup>93</sup>

## B. Protecting Consumers and Privacy

Although decentralized cryptocurrencies have intrinsic anonymity, some privacy concerns remain. Because blockchain security relies on a public ledger and public verification of each transaction,<sup>94</sup> each user can freely inspect all transactions.<sup>95</sup> From a privacy standpoint, this can become problematic if an institution can view its competitors' transactions.<sup>96</sup> For example, two banks may want to conceal their transactions from other banks both for competitive reasons and for their client's privacy.<sup>97</sup> To mitigate this concern, some cryptocurrencies, such as Monero, have implemented technologies to hide amounts, addresses, or other information associated with transactions to specifically increase user privacy.<sup>98</sup>

Privacy concerns might also arise if a stablecoin issuer is a powerful social network or other type of data-information or data-sharing firm.<sup>99</sup> Those types of firms are historically poor at maintaining consumer privacy.<sup>100</sup> Indeed, they often profit from user data by sharing, selling, or

---

<sup>92</sup> FATF Recommendation 17 allows financial institutions to outsource their customer due diligence requirements to third parties; however, liability remains with the delegating party. FATF RECOMMENDATIONS, *supra* note 80, at 18. For a retail CBDC this could mean central banks are outsourcing customer due diligence to commercial banks. It may be preferable to have commercial banks responsible to the central bank for failed due diligence. *Contra id.* at 35 (allowing financial institutions to outsource due diligence in Recommendation 17).

<sup>93</sup> See 31 C.F.R. § 1010.311 (2020) (setting U.S. reporting practices requiring financial institutions only to report “each deposit, withdrawal, exchange of currency or other payment or transfer, by, through, or to such financial institution which involves a transaction in currency of more than \$10,000”).

<sup>94</sup> See *infra* Section I.A

<sup>95</sup> Eyal, *supra* note 8, at 46.

<sup>96</sup> *Id.*

<sup>97</sup> *Id.*

<sup>98</sup> Dyson et al., *supra* note 91, at 1-6.

<sup>99</sup> See *FTC Imposes \$5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, FED. TRADE COMM'N (July 24, 2019), <https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions> (reporting that Facebook agreed to pay a penalty of \$5 billion to settle charges that it “violated a 2012 FTC order by deceiving users about their ability to control the privacy of their personal information”); Spencer Bokak-Lindell, Opinion, *Can We Trust Facebook to Run a Bank?*, N.Y. TIMES (Oct. 24, 2019), <https://www.nytimes.com/2019/10/24/opinion/facebook-libra-zuckerberg.html> (discussing privacy concerns over Libra).

<sup>100</sup> See Taylor Telford, *Why Governments Around the World are Afraid of Libra, Facebook's Cryptocurrency*, WASH. POST (July 12, 2019, 1:11 PM), <https://www.washingtonpost.com/business/2019/07/12/why-governments-around-world-are-afraid-libra-facebooks-cryptocurrency/>.

otherwise misusing that data.<sup>101</sup> Regulation should at least require issuers to be transparent about how they protect stablecoin users' privacy.<sup>102</sup> Furthermore, any information about stablecoin users should be kept confidential; there is a long-established interest, for example, in protecting financial records from government access.<sup>103</sup>

Similarly, the use of CBDCs may further centralize data about the money supply. With the help of KYC or other identification requirements, a central bank could connect an individual to every transaction that they or someone close to them makes, while also connecting additional information such as demographic, geographic, or personal identifying information.<sup>104</sup> To the extent an account-based CBDC makes funds transfers easier to trace,<sup>105</sup> how should privacy and access to capital be balanced? Governments have a poor track record when it comes to protecting consumer privacy. In the United States, the government has long been using the PATRIOT Act to justify widespread surveillance of citizens.<sup>106</sup> A CBDC could lead to further government surveillance and control.<sup>107</sup> Such privacy concerns would need to be addressed through regulation before widespread adoption of any CBDC.

To address these concerns, regulators should consider the advantages of decentralizing accounts at commercial banks rather than requiring central bank accounts. That would also increase security. If an account-based CBDC is totally centralized, then any security vulnerability could be systemic, and everyone could be affected.<sup>108</sup> However, if the account-based CBDC makes use of infrastructure and security measures at commercial banks, then a vulnerability at one bank

---

<sup>101</sup> See Karla Valdés Posada, *Diem, Facebook's New Cryptocurrency. Does it Keep Data Private?*, MIRANDA PARTNERS (Jan. 21, 2021, 3:08 PM), <https://miranda-partners.com/diem-facebooks-new-cryptocurrency-does-it-keep-data-private/>.

<sup>102</sup> Cf. Natasha Lomas, *Libra, Facebook's Global Digital Currency Plan, Is Fuzzy on Privacy, Watchdogs Warn*, TECHCRUNCH (Aug. 5, 2019, 1:47), <https://techcrunch.com/2019/08/05/libra-facebooks-global-digital-currency-plan-is-fuzzy-on-privacy-watchdogs-warn/> (noting the lack of detailed information on Libra's privacy protections and describing the concerns of international privacy watchdogs).

<sup>103</sup> Congress enacted the Right to Financial Privacy Act of 1978, for example, to prevent banks and other financial institutions from disclosing a person's financial information to the government unless the records are disclosed pursuant to subpoena or search warrant. See 12 U.S.C. §§ 3401-3422.

<sup>104</sup> Thompson J. Hangen, Note, *We Know What's in Your Wallet: Data Privacy Risks of a Central Bank Digital Currency*, 75 FED. COMM. L.J. 81 (2022).

<sup>105</sup> BIS CBDC REPORT, *supra* note 26, at 10-11, 13-14.

<sup>106</sup> See Patrick G. Eddington, *The PATRIOT Act Has Threatened Freedom for 20 Years*, CATO INSTITUTE, (Oct. 21, 2021), <https://www.cato.org/commentary/patriot-act-has-threatened-freedom-20-years> (last visited Nov. 16, 2023).

<sup>107</sup> See Norbert Michel, *Central Bank Digital Currencies and Freedom Are Incompatible*, CATO INSTITUTE (July 18, 2022), <https://www.cato.org/commentary/central-bank-digital-currencies-freedom-are-incompatible> (last visited Nov. 16, 2023); and James A. Dorn, *China's Digital Yuan: A Threat to Freedom*, CATO INSTITUTE (Aug. 25, 2021), <https://www.cato.org/blog/chinas-digital-yuan-threat-freedom> (last visited Nov. 16, 2023).

<sup>108</sup> Allen et al., *supra* note 43 at 19.

would not necessarily be present at other commercial banks (because of the variability of security measures in place).<sup>109</sup>

### C. Protecting Monetary Integrity and Financial Stability

Subsection C.1 next addresses protecting monetary integrity, and subsection C.2 addresses protecting financial stability. The discussions in these subsections overlap insofar as the factors that could undermine monetary integrity also could undermine financial stability if they cause consumers to lose confidence in a widely used digital currency.<sup>110</sup> Also, because these protections for a CBDC would largely mirror the protections for physical central-bank-issued currencies, the discussion focuses on stablecoins, the private-sector digital currency that is most likely to be widely used.

#### 1. Monetary Integrity

Factors that could undermine monetary integrity include money laundering and terrorist financing, breaches of cybersecurity, and failures of operational resilience. Money laundering and terrorist financing already threaten the integrity of domestic payments.<sup>111</sup> The added complications of cross-border global stablecoin payments would increase the threat.<sup>112</sup>

Breaches of stablecoin cybersecurity and failures of operational resilience could also undermine monetary integrity.<sup>113</sup> Cybersecurity involves several risks. One such cybersecurity risk is that the cryptology used to secure the networks on which stablecoins are issued may be compromised, enabling cyberattacks.<sup>114</sup> Cyberattacks can heavily affect the financial sector.<sup>115</sup> For

---

<sup>109</sup> *Id.* at 21-22.

<sup>110</sup> *See, e.g.*, COMM. ON PAYMENT & MKT. INFRASTRUCTURES, *supra* note 59, at 4 & 12–16 (attributing the exceptionally high cost of making cross-border payments to several factors, including the need to coordinate and to comply with the laws of multiple jurisdictions); FIN. STABILITY BD., DECENTRALISED FINANCIAL TECHNOLOGIES: REPORT OF FINANCIAL STABILITY, REGULATORY AND GOVERNANCE IMPLICATIONS 6–7 (2019), <https://www.fsb.org/wp-content/uploads/P060619.pdf> (discussing operational risks to financial stability); *cf.* Schwarcz, *supra* note 7, at 1076 (observing that “[i]f [a global stablecoin is] widely used for payments, ‘any operational disruption in the [global stablecoin] arrangement might have significant impacts on economic activity and financial system functioning,’ ” in which case “[h]olders relying on the stablecoin to make regular payments would face ‘significant operational disruptions,’ which ‘could quickly affect real economic activity, e.g. by blocking remittances and other payments.’ ” (quoting FSB STABLECOIN REPORT, *supra* note 34, at 13)).

<sup>111</sup> U.S. DEP’T OF THE TREASURY, 2015 NATIONAL MONEY LAUNDERING RISK ASSESSMENT 6 (2015), <https://home.treasury.gov/system/files/246/National-Money-Laundering-Risk-Assessment-06-12-2015.pdf>; DEP’T OF THE TREASURY, 2015 NATIONAL TERRORIST FINANCING RISK ASSESSMENT 4 (2015), <https://home.treasury.gov/system/files/246/National-Terrorist-Financing-Risk-Assessment-06-12-2015.pdf>.

<sup>112</sup> COMM. ON PAYMENT & MKT INFRASTRUCTURES, *supra* note 59, at 4.

<sup>113</sup> *See G7/Central Bank Statement, supra* note 61 and accompanying text.

<sup>114</sup> Schwarcz, *supra* note 7, at 1067.

<sup>115</sup> *See, e.g.*, Danny Brando, Antonis Kotidis, Anna Kovner, Michael Lee & Stacey L. Schreft, *Implications of Cyber Risk for Financial Stability*, BD. OF GOVERNORS OF THE FED. RSRV. SYS.: FEDS NOTES (May 12, 2022), <https://www.federalreserve.gov/econres/notes/feds->

example, PolyNetwork briefly lost \$600 million, much of which was only returned after the thieves relented.<sup>116</sup>

Failures of operational resilience could also undermine monetary integrity by disrupting a payment system that relies on stablecoins.<sup>117</sup> Regulation could help to protect against this threat of disruption by requiring the stablecoin infrastructure to include secure hardware technology as well as further security mechanisms in addition to cryptographic protections.<sup>118</sup> Regulation also could require stablecoin issuers to back up their cryptology through separate networks. The most likely failure might occur, for example, if certain validator nodes are compromised or stop operating.<sup>119</sup> For example, a cryptocurrency network may include computers with varying reliability based on the technical ability of the user (i.e., an individual may operate a computer less reliably or securely than a financial institution). Regulators might be able to protect against that risk by requiring the issuer to maintain, as a disaster recovery failsafe, a backup validation plan to help assure recoverability of computerized files after a data-loss event. Any regulatory scheme may include governmental study of these alternative ways to prevent failures of operational resilience.

Stablecoins also can pose externalities to governments. The primary externality is the risk that a stablecoin could become so widely used that it would undermine the ability of a government to use its currency to affect monetary, and thus economic, policy. At least where the reference asset for the stablecoin is a government's fiat currency, the government might consider mandating a strategic public-private partnership to protect against this risk. As part of this partnership, the government might offer the stablecoin issuer some protection against the redemption risk. For example, the partnership could permit the government to use the stablecoin to affect monetary policy, such as by controlling the issuance of new stablecoins (and hence the money supply).<sup>120</sup> In

---

notes/implications-of-cyber-risk-for-financial-stability-20220512.html (“Cyber events, especially cyberattacks, are among the top risks cited in financial stability surveys in the United States and globally.”); Anton N. Didenko, *Cybersecurity Regulation in the Financial Sector: Prospects of Legal Harmonization in the European Union and Beyond*, 25 UNIF. L. REV. 125, 129 (2020).

<sup>116</sup> Lipton & Livni, *supra* note 62.

<sup>117</sup> See *G7/Central Bank Statement*, *supra* note 61 and accompanying text; *cf.* PRESIDENT'S WORKING GRP., *supra* note 62, at 3 & 13 (observing that operational risks can include transaction processing errors that delay or otherwise “disrupt the ability of users to make payments”).

<sup>118</sup> See Allen et al., *supra* note 43, at 54–61.

<sup>119</sup> *Addressing the Regulatory, Supervisory, and Oversight Challenges Raised by “Global Stablecoin” Arrangements*, FIN. STABILITY BD. 13 (Apr. 14, 2020), <https://www.fsb.org/wp-content/uploads/P140420-1.pdf>. In the event of validator failure, transaction processing could be delayed with “large volumes of transactions [that] might amplify users’ loss of confidence, and trigger further redemption requests.” *Id.* It is notable that operational resilience may be of greater concern in the case of a centralized CBDC. Lacking the benefits of decentralization, a CBDC would provide a single point of failure for a nation’s financial system. See Norbert Michel & Nicholas Anthony, *The Risks of CBDCs: Why Central Bank Digital Currencies Shouldn’t be Adopted*, CATO INSTITUTE (Feb. 22, 2023), <https://www.cato.org/study/risks-of-cbdcs> (last visited Nov. 16, 2023).

<sup>120</sup> See Scott A. Wolla, *A New Frontier: Monetary Policy with Ample Reserves*, PAGE ONE ECON., May 2019, at 1, 1-2, [https://files.stlouisfed.org/files/htdocs/publications/page1-econ/2019/05/03/a-new-frontier-monetary-policy-with-ample-reserves\\_SE.pdf](https://files.stlouisfed.org/files/htdocs/publications/page1-econ/2019/05/03/a-new-frontier-monetary-policy-with-ample-reserves_SE.pdf) (discussing how Federal Reserve affects monetary policy by conducting open market operations to manage the

return, possibly for a fee,<sup>121</sup> the government could guarantee the issuer's ability to redeem its stablecoins, potentially reducing the issuer's cost of collateralizing or hedging its redemption obligation by effectively making the stablecoins insured deposits.

To facilitate stablecoin development, a government and a private-sector stablecoin issuer could partner by creating, for example, a special purpose vehicle (SPV) that issues the stablecoin pegged to the government's fiat currency. The partnership arrangement could give the government control of the stablecoin to the extent needed to manage monetary policy.

## 2. *Financial Stability*

Although the factors discussed above could impair monetary integrity, they also could undermine financial stability if they cause consumers to lose confidence in a widely used stablecoin. The primary reason that consumers could lose that confidence would be the issuer's inability to redeem the stablecoin for its underlying reference asset.<sup>122</sup> That inability would resemble a classic bank run if, for example, the issuer is unable to obtain sufficient reference assets to satisfy correlated demands by stablecoin holders.<sup>123</sup>

Consumers also could lose confidence in a widely used stablecoin if they merely question the issuer's ability to satisfy its redemption obligations. That loss of confidence could reduce the stablecoin's value. If the stablecoin is widely used as a common store of value—which might be especially likely to occur in emerging markets and developing economies<sup>124</sup>—even a moderate variation in its value might cause significant fluctuations in holders' wealth.<sup>125</sup> If that fluctuation is sizeable enough to affect spending decisions and economic activity,<sup>126</sup> it could impair the real economy.

One way to assure the issuer's ability to satisfy its redemption obligations would be to make stablecoins the equivalent of insured deposits. For example, a stablecoin issuer could

---

money supply); Team Circle, *Circle Partners with Bolivarian Republic of Venezuela and Airtm to Deliver Aid to Venezuelans Using USDC*, CIRCLE (July 16, 2021), <https://www.circle.com/blog/circle-partners-with-bolivarian-republic-of-venezuela-and-airtm-to-deliver-aid-to-venezuelans-using-usdc> (discussing how government used stablecoin to carry out financial intervention).

<sup>121</sup> The U.S. Federal Deposit Insurance Corporation (“FDIC”) charges banks for providing deposit insurance, which a stablecoin-redemption guarantee would resemble. Charging an appropriate fee would help to internalize costs and reduce moral hazard.

<sup>122</sup> Schwarcz, *supra* note 7, at 1067; *cf.* FSB STABLECOIN REPORT, *supra* note 34, at 1 (expressing concern that a widely adopted global stablecoin “could become systemically important in and across one or many jurisdictions, including as a means of making payments”).

<sup>123</sup> *See* Schwarcz, *supra* note 7, at 1063 (explaining that a failure to satisfy redemption rights would “expose the issuer and stablecoin holder[s] to default risk, similar to the liquidity ‘run’ risk of a bank run . . .”). In a bank run, the bank's depositors panic, converging on the bank to quickly withdraw their monies. Because banks keep only a small fraction of their deposits on hand as cash reserves, a bank may have insufficient cash to pay all withdrawal demands, causing it to default and ultimately fail. R. W. HAFER, *THE FEDERAL RESERVE SYSTEM: AN ENCYCLOPEDIA* 25, 145 (2005) (observing that a bank's cash reserves are often less than 5% of its deposits).

<sup>124</sup> Allen et al., *supra* note 43, at 12–13.

<sup>125</sup> *See id.* at 13.

<sup>126</sup> *See id.*

collateralize or otherwise maintain reserves against its redemption obligation,<sup>127</sup> or it could hedge the risk with derivatives or other guarantees.<sup>128</sup>

Other than by making stablecoins the equivalent of insured deposits, these redemption protections could be expensive and difficult to implement. Because collateral would need to be liquid, collateralizing the redemption obligation would be expensive and inefficient.<sup>129</sup> Maintaining reserves against the redemption obligation also could be costly. Some recommend, for example, that stablecoin issuers be required to hold 100% reserves, plus an additional cushion, in cash or high-quality cash equivalents such as U.S. treasuries.<sup>130</sup>

Other potential concerns about holding reserves against the redemption obligation include that stablecoin issuers may hold their reserves in various currencies, creating exchange risk, or in non-liquid assets, creating liquidity risk.<sup>131</sup> Whether it would be feasible to hedge the redemption risk with derivatives or other guarantees would depend on market factors; in another context, for example, the derivatives market was not deep enough to provide a sufficient hedge for an affordable price.<sup>132</sup>

Regulation may require a supervisory agency to monitor, supervise, and regulate against any potential systemic impacts or monetary policy implications regarding stablecoins or any persons issuing or trading stablecoins or otherwise engaging in any stablecoin-related services or other activities. In the United States, for example, the Financial Stability Oversight Council (“FSOC”) is tasked with overseeing financial stability by coordinating with various other agencies

---

<sup>127</sup> Cf. Mario Bellia & Sebastian Schich, What Makes Private Stablecoins Stable? (Oct. 26, 2020) (unpublished manuscript), <https://ssrn.com/abstract=3718954> (arguing that nongovernment issued stablecoins can have stable value by being collateralized by fiat currency).

<sup>128</sup> Facebook’s Libra Dollars, now Diem, are expected to be backed by a managed reserve of U.S. dollars, its reference asset. See Libra Ass’n Members, *White Paper v2.0*, LIBRA 2 (Apr. 2020), [https://wp.diem.com/en-US/wp-content/uploads/sites/23/2020/04/Libra\\_WhitePaperV2\\_April2020.pdf](https://wp.diem.com/en-US/wp-content/uploads/sites/23/2020/04/Libra_WhitePaperV2_April2020.pdf), at 12 (noting that the Libra reserve will consist of eighty percent short-term, low-credit risk government securities and twenty percent cash). Libra also claims that the Libra reserve “will be further endowed with a capital buffer.” *Id.* at 12–13.

<sup>129</sup> Craig Calcaterra, Wulf A. Kaal & Vadhindran Rao, *Stable Cryptocurrencies: First Order Principles*, 3 STAN. J. BLOCKCHAIN L. & POL’Y 62, 64 (2020), <https://stanford-jblp.pubpub.org/pub/stable-cryptocurrencies-principles/release/1>.

<sup>130</sup> Catalini & Massari, *supra* note 57.

<sup>131</sup> Randal K. Quarles, Vice Chair for Supervision, Fed. Rsrv. Bd., Remarks at the 113th Annual Utah Bankers Association Convention: Parachute Pants and Central Bank Money 8 (June 28, 2021), <https://www.federalreserve.gov/newsevents/speech/files/quarles20210628a.pdf>.

<sup>132</sup> See Steven L. Schwarcz, *Enron and the Use and Abuse of Special Purpose Entities in Corporate Structures*, 70 U. CIN. L. REV. 1309, 1310 (2002) (“Where the value of Enron’s investment and Enron’s stock price simultaneously fell, the SPE would lack sufficient assets to perform its hedge.”). Failing to find an affordable hedge in the derivatives market, Enron hedged the value of its “merchant assets” through structured finance, which through an unexpected confluence of falls in market value led to its default. Enron created “independent” SPVs, capitalized with Enron publicly traded stock, to guarantee (i.e., hedge) the value of its merchant assets; but Enron did not anticipate a concurrent collapse of both the merchant-asset values and its stock value. See *id.*

and addressing systemic risk.<sup>133</sup> FSOC could designate a stablecoin issuer as a systematically important financial institution, thereby subjecting it to enhanced prudential oversight by the Federal Reserve in addition to any monitoring, supervision, and regulation imposed on that issuer by the supervisory agency.<sup>134</sup>

To additionally protect financial stability, central banks could provide emergency short-term liquidity to stablecoin issuers to help ensure the timely performance of their redemption obligations and to mitigate the adverse confidence effects of a “run,” in which many stablecoin holders attempt to exercise redemption rights in a short period of time. This would somewhat parallel the short-term liquidity funding often provided by central banks to deposit-taking banks,<sup>135</sup> to provide emergency liquidity and maintain reserve requirements<sup>136</sup> as well as to discourage bank runs.<sup>137</sup> That funding reflects the traditional role of central banks in supporting liquidity and stability,<sup>138</sup> by helping depository institutions manage liquidity risk and discouraging actions with negative consequences, “such as withdrawing credit during times of market stress.”<sup>139</sup>

---

<sup>133</sup> George W. Madison, Michael E. Borden & David A. Miller, *FSOC Designation Treasury Report: A Fundamental Shift*, HARV. L. SCH. F. ON CORP. GOVERNANCE (Feb. 4, 2018), <https://corpgov.law.harvard.edu/2018/02/04/fsoc-designation-treasury-report-a-fundamental-shift/>; see also *About FSOC*, U.S. DEP’T OF THE TREASURY, <https://home.treasury.gov/policy-issues/financial-markets-financial-institutions-and-fiscal-service/fsoc/about-fsoc> (last visited Aug. 18, 2022) (describing the FSOC’s function and how it helps maintain the United States’ financial stability).

<sup>134</sup> Cf. Andrew Ackerman & Anna Maria Andriotis, *Biden Administration Seeks to Regulate Stablecoin Issuers as Banks*, WALL ST. J. (Oct. 1, 2021), [www.wsj.com/articles/biden-administration-seeks-to-regulate-stablecoin-issuers-as-banks-11633103156](http://www.wsj.com/articles/biden-administration-seeks-to-regulate-stablecoin-issuers-as-banks-11633103156) (reporting that the U.S. Treasury is discussing whether the FSOC should “designate stablecoin activities as systemically important,” which “could ultimately lead to the Federal Reserve writing more-stringent risk-management standards for” stablecoin issuers). In its recent annual report, the FSOC recommended that U.S. regulators adopt a “comprehensive regulatory framework” for stablecoins and other digital assets. FIN. STABILITY OVERSIGHT COUNCIL, 2021 ANNUAL REPORT § 3.6.2.1, at 123 (2021), <https://home.treasury.gov/system/files/261/FSOC2021AnnualReport.pdf> [hereinafter FSOC ANNUAL REPORT], at 173–74.

<sup>135</sup> Primary liquidity advances made by the Fed have ninety-day maturities, see, for example, *The Primary & Secondary Lending Programs*, FED. RSRV., <https://www.frbdiscountwindow.org/Pages/General-Information/Primary-and-Secondary-Lending-Programs.aspx> (last visited Aug. 19, 2022).

<sup>136</sup> Julia Kagan, *Lending Facility*, INVESTOPEDIA, <https://www.investopedia.com/terms/l/lending-facility.asp> (last updated Dec. 31, 2020). The Federal Reserve, for example, may extend credit to banks under certain emergency circumstances. 12 U.S.C. § 343(3)(A).

<sup>137</sup> See Chris B. Murphy, *Definition of Liquidity Coverage Ratio*, INVESTOPEDIA, <https://www.investopedia.com/terms/l/liquidity-coverage-ratio.asp> (last updated June 20, 2022) (“The liquidity coverage ratio (LCR) refers to the proportion of highly liquid assets held by financial institutions, to ensure their ongoing ability to meet short-term obligations.”).

<sup>138</sup> *The Discount Window*, FED. RSRV., <https://www.frbdiscountwindow.org/pages/general-information/the%20discount%20window#introduction> (last updated Dec. 14, 2021).

<sup>139</sup> *Id.* (observing that “[p]roviding liquidity in this way is one of the original purposes of the Federal Reserve System and other central banks around the world”).

In order to access central bank liquidity funding, central banks typically require borrowers to provide adequate collateral. This requirement reflects the widespread view that central banks should support solvent but temporarily illiquid banks, thereby taking no credit risk (and thus not imposing a cost on taxpayers).<sup>140</sup> The collateral ensures repayment in the event the borrower is not merely illiquid but also turns out to be insolvent. It also should reduce the risk of moral hazard.<sup>141</sup> Regulation may require that all collateral must be acceptable to the supervisory agency and the central bank.<sup>142</sup>

Regulation may allow the supervisory agency to protect financial stability by imposing capital requirements or ring-fencing measures on persons that issue or trade stablecoins or otherwise engage in any stablecoin-related services or other activities. Capital requirements effectively require firms to maintain certain levels of equity that are designed to buffer them against a financial crisis by absorbing losses.<sup>143</sup> Ring-fencing requirements are designed primarily to protect firms against becoming subject to liabilities.<sup>144</sup> In the context of banking, ring-fencing

---

<sup>140</sup> Cf. Joao A.C. Santos & Stavros Peristianis, *Why Do Central Banks Have Discount Windows?*, FED. RSRV. BANK OF N.Y. (Mar. 30, 2011), <https://libertystreeteconomics.newyorkfed.org/2011/03/why-do-central-banks-have-discount-windows/> (observing that the dictum “that central banks should lend only to illiquid but solvent banks, has been challenged” because of a debate over whether “central bankers are . . . better equipped to distinguish illiquid but solvent banks than are private investors,” but noting that the Fed “should lend freely but at a high rate . . . to any borrower with good collateral”).

<sup>141</sup> Cf. David Rowell & Luke B. Connelly, *A History of the Term “Moral Hazard,”* 79 J. RISK & INS. 1051 (2012) (discussing moral hazard in the context of whether to issue government stablecoin insurance); Jakob Vestergaard & Daniela Gabor, *Should Central Bank Liquidity Provision Be a Vehicle for Fiscal Discipline?*, INST. FOR NEW ECON. THINKING (Dec. 8, 2021), <https://www.ineteconomics.org/perspectives/blog/should-central-bank-liquidity-provision-be-a-vehicle-for-fiscal-discipline> (discussing the moral hazard risk of extending central bank liquidity).

<sup>142</sup> Cf. *Pledging Collateral*, FED. RSRV., <https://www.frbdiscountwindow.org/rightnavpages/pledging-collateral> (last modified Dec. 14, 2021) (requiring Fed discount-window advances to “be secured by collateral acceptable to the Reserve Bank,” including government securities, collateralized mortgage obligations, asset-backed securities, corporate bonds, etc.).

<sup>143</sup> Steven L. Schwarcz, *Systemic Risk*, 97 GEO. L. REV. 193, 210 (2008) (“[C]apital adequacy requires banks to hold minimum levels of capital, a requirement intended to limit excessive risk taking and buffer against financial crisis.”); *What Is the Difference Between a Bank’s Liquidity and Its Capital?*, BD. OF GOVERNORS OF FED. RSRV. SYS. [https://www.federalreserve.gov/faqs/cat\\_21427.htm#:~:text=Liquidity%20is%20a%20measure%20of,banks%20have%20to%20absorb%20losses](https://www.federalreserve.gov/faqs/cat_21427.htm#:~:text=Liquidity%20is%20a%20measure%20of,banks%20have%20to%20absorb%20losses) (last modified Dec. 31, 2019) (“Capital is the difference between all of a firm’s assets and its liabilities. Capital acts as a financial cushion to absorb losses.”).

<sup>144</sup> Steven L. Schwarcz, *Ring-Fencing*, 87 S. CAL. L. REV. 69, 81–82 (2013) (“[R]ing-fencing has at least four uses: to protect a firm from becoming subject to liabilities and other risks associated with bankruptcy; to help ensure that a firm is able to operate on a standalone basis even if its affiliated firms fail; to protect a firm from being taken advantage of by affiliated firms, thereby preserving the firm’s business and assets; and to limit a firm from engaging in risky activities.”).

means limiting a bank's ability to engage in risky behavior.<sup>145</sup> In a stablecoin context, ring-fencing might include similar requirements. It might also focus on lowering the risk of cyberattacks by separating, for example, stablecoin issuers from affiliates or parent companies engaging in other activities, thereby narrowing the breadth of data available to cyberattackers.<sup>146</sup> Ring-fencing also could help to protect redemption rights. For example, creating a bankruptcy-remote legal entity for funds related to stablecoin issuance could protect those funds and, therefore, holders' redemption rights from the issuer's creditors.<sup>147</sup>

The widespread use of stablecoins additionally could threaten financial stability by significantly reducing bank deposits—thereby causing commercial banks to rely on more expensive sources of funding, in turn increasing the cost of business loans.<sup>148</sup> This so-called “disintermediation”<sup>149</sup> is especially likely to occur in countries whose fiat currencies are less stable than accessible stablecoins.<sup>150</sup> Regulators could help to protect against disintermediation by

---

<sup>145</sup> *Id.* at 78.

<sup>146</sup> As stablecoin issuers become more competitive, that aspect of ring-fencing may become less important. In a competitive market, if cyberattacks drive up the cost of services for one stablecoin issuer, other issuers with stronger security measures, and thus lower costs, could serve as substitutes. *Cf. id.* at 109 (arguing that it is less certain for ring-fencing to be beneficial in banking than in public utilities because the banking market is more competitive, and therefore banks could substitute for others that become unable to provide services due to risky behavior).

<sup>147</sup> *Cf.* Dan Awrey & Kristin van Zwieten, *The Shadow Payment System*, 43 J. CORP. L. 775, 815 (2018) (describing how ring-fencing could protect customer funds for companies offering electronic payment systems); Catalini & Massari, *supra* note 57 (suggesting that it might be prudent to “isolate reserve assets from their other assets, so that in insolvency or bankruptcy [of the stablecoin issuer], coin holders can be prioritized over other creditors”). But creating a bankruptcy-remote legal entity for funds related to stablecoin issuance might limit the ability of stablecoin issuers to use proceeds from securities issuances to fund lending activities, thereby inadvertently increasing disintermediation. *See infra* notes 234-236 and accompanying text; Awrey & van Zwieten, *supra*, at 816 (“[T]he ring-fencing of customer funds envisioned by structural separation necessarily limits the ability of institutions to engage in other socially useful forms of financial intermediation.”).

<sup>148</sup> Alexander Kriwoluzky & Chi Hyun Kim, *Public or Private? The Future of Money*, EUR. PARLIAMENT 15 (Dec. 2019), <https://www.europarl.europa.eu/cmsdata/207653/13.%20PE%20642.356%20DIW%20final%20publication-original.pdf>.

<sup>149</sup> *See, e.g.*, Nitin Gaur, *Blockchain – A Platform for Disintermediation*, INFOCAST, <https://infocastinc.com/market-insights/technology/blockchain-a-platform-for-disintermediation/#:~:text=Disintermediation%20is%20defined%20as%20reduction,rather%20than%20through%20a%20bank> (last visited Oct. 24, 2022) (defining “disintermediation” as “reduction in the use of intermediaries between producers and consumers, for example by investing directly in the securities market rather than through a bank”).

<sup>150</sup> *Id.* Stablecoin-motivated disintermediation could cause a secondary externality if a stablecoin issuer is required to invest in safe assets to collateralize its redemption obligation. That could increase the demand for—and thus the price of—those safe assets, which the country's banks might be required to hold. Katrin Assenmacher, *Monetary Policy Implications of Digital Currencies*, SOCIÉTÉ UNIVERSITAIRE EUROPÉENNE DE RECHERCHES FINANCIÈRE 5 (May 2020), [https://www.suerf.org/docx/f\\_ec9b954aefd15bc4fffe92f5683d1dd2\\_13537\\_suerf.pdf](https://www.suerf.org/docx/f_ec9b954aefd15bc4fffe92f5683d1dd2_13537_suerf.pdf).

limiting stablecoin issuance to banks and classifying monies received from stablecoin purchasers as “deposits.”<sup>151</sup> Limiting issuance to banks would help maintain the relationship between customers and banks and, more importantly, dissuade the transfer of capital from bank accounts to nonbank stablecoin issuers, thus preserving banks’ supply of lendable funds.<sup>152</sup> Further, by classifying monies received from selling stablecoins as “deposits,” regulators could utilize reserve requirements to influence interest rates, similar to how some central banks already have the ability to change reserve requirements to influence the supply of funds for lending.<sup>153</sup>

Alternatively, if disintermediation occurs, regulators could take steps to alleviate its effects, such as by encouraging the emergence of other platforms to support low-cost business lending. “Unbundled” FinTech firms that specialize in lending—without engaging in other banking-related

---

That in turn would increase bank costs, thereby potentially increasing interest rates. Fabio Panetta, Member of the Exec. Bd. of the Eur. Cent. Bank, Speech at Il Salone dei Pagamenti: The Two Sides of the (Stable)coin (Nov. 2020), <https://www.ecb.europa.eu/press/key/date/2020/html/ecb.sp201104~7908460f0d.en.html>. Increased interest rates would increase the cost of capital, which could reduce economic activity. ECB Crypto-Assets Task Force, *Stablecoins: Implications for Monetary Policy, Financial Stability, Market Infrastructure and Payments, and Banking Supervision in the Euro Area*, EUR. CENT. BANK 20 (Sept. 2020), <https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op247~fe3df92991.en.pdf>.

<sup>151</sup> Cf. Stablecoin Classification and Regulation Act of 2020, H.R. 8827, 116th Cong. §§ 3(a)(5), 3(aa)(2)(D)(i), 52(a)(1) (2020) (proposing similar changes by adding “stablecoins issued by such bank or savings association” to the definition of the term “deposit” in the Federal Deposit Insurance Act (12 U.S.C. § 1813) and amending § 1811 of that Act to limit stablecoin issuance to “insured depository institution[s] that [are] member[s] of the Federal Reserve System”).

<sup>152</sup> Cf. Tomasso Mancini-Griffoli, Maria Soledad Martinez Peria, Itai Agur, Anil Ari, John Kiff, Adina Popescu & Celine Rochon, *IMF Staff Discussion Note: Casting Light on Central Bank Digital Currency*, INT’L MONETARY FUND 24 (Nov. 2018), <https://www.imf.org/-/media/Files/Publications/SDN/2018/SDN1808.ashx> (suggesting that regulators could address disintermediation related to CBDCs by allowing banks to offer wallets for consumers to store their cryptocurrency).

<sup>153</sup> For example, the U.S. Federal Reserve determines the percentage of the amounts on deposit that banks must hold as reserves to reduce the risk that a bank could fail to meet the demands of a run. Will Kenton, *Reserve Ratios Definition*, INVESTOPEDIA, <https://www.investopedia.com/terms/r/reserveratio.asp> (last updated Jan. 17, 2022). Such reserve requirements recognize that deposits are loans by customers (aka depositors) to their bank, creating, effectively, short-term liabilities of the bank to repay those loans on demand. *See id.* The logic of classifying monies received from selling stablecoins as deposits is that the stablecoin redemption requirements similarly create, effectively, short-term liabilities of the bank to redeem those stablecoins on demand. *See* Charles W. Calomiris, *Chartering the FinTech Future*, 42 CATO J. 1, 20 (2021) (arguing that stablecoin-issuing banks could protect against this redemption risk by maintaining lines of credit covering any shortfall—adjusted by the amount of expected future fees—in the amount of cash on hand). By increasing or decreasing the reserve requirements—whether those requirements apply to ordinary deposits or to stablecoin-sale proceeds that are classified as deposits—the Federal Reserve could contract or expand the supply of funds that banks have available to lend. Kenton, *supra*.

activities—are likely to gain market share from traditional banks because of lower overhead costs and technological advantages.<sup>154</sup> The effects of disintermediation may also be alleviated by the increased prevalence of decentralized finance (“DeFi”) protocols.<sup>155</sup> Such applications rely on a blockchain’s security and decentralization to implement protocols that allow users to earn interest by lending out their currency or by investing it in a type of savings account.<sup>156</sup> As such, though disintermediation may reduce the role of commercial banks, alternatives may allow a more widespread access to capital to meet the needs of the market.

Any new regulatory approaches should, of course, carefully balance innovation with financial stability, and regulators should closely cooperate with issuers and other appropriate market participants.

### III. IMPLEMENTATION CONSIDERATIONS

This Article so far has addressed how digital currencies should be regulated. This Part III next addresses who should perform that regulation. For a CBDC, the answer is clear: the Fed and other governmental central banks that issue the CBDC. Central banks have long been working together to try to harmonize banking regulations to minimize cross-border costs due to conflicting laws. In the same way, they should be expected to work together to try to harmonize CBDC regulation to minimize cross-border costs due to conflicting laws. Recently, for example, the Bank for International Settlements proposed that one of CBDC’s advantages is its potential to provide standards and design consistency as well as interoperability, which should lower cost and increase speed, access, and transparency.<sup>157</sup>

For non-governmental cryptocurrencies, implementation costs are likely to be high. Those currencies could become subject to numerous laws and supervised by a multiplicity of government agencies, some of which may lack the precedent and tradition of working together domestically, much less internationally.<sup>158</sup> In the United States, for example, international coordination could involve the Fed, the Office of the Comptroller of the Currency (“OCC”),<sup>159</sup> the Securities and

---

<sup>154</sup> See Calomiris, *supra* note 153, at 390 (“Unbundled FinTech enterprises that can customize loan portfolios to meet the specific preferences of loan funders, that can take advantage of state-of-the-art information processing when screening and monitoring borrowers, and that can avoid the physical costs of maintaining branch networks, will increasingly win the competitive struggle to serve customers.”).

<sup>155</sup> For a more detailed discussion and analysis of DeFi and financial technology (FinTech) generally, see Steven L. Schwarcz, “Regulating Financial Innovation: FinTech, Crypto-assets, DeFI, and Beyond” (draft on file with author).

<sup>156</sup> Burke, *supra* note 22, at 128.

<sup>157</sup> BANK FOR INT’L SETTLEMENTS, CENTRAL BANK DIGITAL CURRENCIES FOR CROSS-BORDER PAYMENTS: REPORT TO THE G20, at 2–3 (2021) (citations omitted), <https://www.bis.org/publ/othp38.pdf>.

<sup>158</sup> Even U.S. federal agencies do not always work well together. See, e.g., Yin Wilczek, *Trouble Ahead for SEC, CFTC Rulemaking Under Reform Act as Group Urges Oversight*, BLOOMBERG L.: SEC. REGUL. & L. REP. (Dec. 22, 2010, 1:26 PM), <https://www.bloomberglaw.com/document/MI9XWB3H0JK0>:

<sup>159</sup> A stablecoin issuer holding reserves in a bank would need to comply with OCC regulations. See *OCC Chief Counsel’s Interpretation on National Bank and Federal Savings Association Authority to Hold Stablecoin Reserves*, OFF. OF THE COMPTROLLER OF THE CURRENCY 3 (Sept. 21, 2020), <https://www.occ.gov/topics/charters-and-licensing/interpretations-and-actions/2020/int1172.pdf> (explaining that banks may engage in cryptocurrency businesses,

Exchange Commission (“SEC”),<sup>160</sup> the Commodity Futures Trading Commission (“CFTC”),<sup>161</sup> and the Financial Crimes Enforcement Network (“FinCEN”)<sup>162</sup> working together and also with their foreign governmental counterparts.<sup>163</sup> Furthermore, except to the extent it is preempted by federal law, such international coordination could involve individual U.S. states, some of which

---

so long as they comply with the applicable laws); *cf. infra* notes 152–153 and accompanying text (explaining why requiring stablecoin issuers to hold such reserves could help to protect against disintermediation). OCC regulations also could apply to any stablecoins “backed by a single fiat currency and redeemable . . . on a 1:1 basis.” SEC FinHub Staff, *SEC FinHub Staff Statement on OCC Interpretation*, U.S. SEC. & EXCH. COMM’N (Sept. 21, 2020), <https://www.sec.gov/news/public-statement/sec-finhub-statement-occ-interpretation>.

<sup>160</sup> Federal securities laws would apply to any stablecoin that the SEC deems a “security.” Strategic Hub for Innovation & Fin. Tech., *Framework for “Investment Contract” Analysis of Digital Assets*, SEC. & EXCH. COMM’N 1, <https://www.sec.gov/files/dlt-framework.pdf> (last visited Aug. 11, 2022). The chairman of the SEC has stated that the agency may have authority over stablecoins because they are backed by securities, “qualify[ing] [them] as investments.” Michaels et al., *supra* note 58 (discussing Tether’s attempt to create a stablecoin backed by corporate bonds and certificates of deposit).

<sup>161</sup> The CFTC may have jurisdiction to oversee stablecoins backed by fiat currency, for anti-fraud and anti-manipulation purposes. *See Summary Overview of Stablecoins and the Law Regarding Stablecoins*, COMMODITY FUTURES TRADING COMM’N 13 (2019), [https://www.cftc.gov/media/2731/TAC100319\\_Stablecoins/download](https://www.cftc.gov/media/2731/TAC100319_Stablecoins/download).

<sup>162</sup> The issuer of a stablecoin would likely be considered to be engaging in a money-service business and required to register with FinCEN. *See* ANDREW P. SCOTT, CONG. RSCH. SERV., R46486, TELEGRAPHS, STEAMSHIPS, AND VIRTUAL CURRENCY: AN ANALYSIS OF MONEY TRANSMITTER REGULATION 1 (2020), <https://fas.org/sgp/crs/misc/R46486.pdf> (“[Money service business] refers to a range of nonbank financial institutions that provide, among other things, money transmission services, prepaid and other payment instruments, currency exchanges, and check cashing.”).

<sup>163</sup> Stablecoins are cryptocurrencies, meaning they have a token-based digital form that is secured by cryptography, such as blockchain. *See, e.g.*, Harish Natarajan, Solvej Krause & Helen Gradstein, *Distributed Ledger Technology (DLT) and Blockchain* 3 (World Bank Grp., Working Paper No. 122140, 2017), <http://documents1.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf> (discussing cryptocurrency and cryptography); Jake Frankenfield, *Cryptocurrency Explained with Pros and Cons for Investment*, INVESTOPEDIA, <https://www.investopedia.com/terms/c/cryptocurrency.asp> (last updated May 28, 2022) (offering a definition of “cryptocurrency”). Global stablecoins may pose additional costs. For example, the validity of a token-based payment is determined by verifying the payor’s ownership of the token. *See, e.g.*, Rui Zhang, Rui Xue & Ling Liu, *Security and Privacy on Blockchain*, 52 ACM COMPUTING SURVS., July 2019, at 1, 7 (“A transaction is legitimate if one can prove that the sender has the ownership of the actual [tokens] that are being spent.”). That verification itself may be subject to multiple laws and supervisory requirements. *Cf. Michaels et al., supra* note 58 (observing that “[c]rypto is a global market, [and] the U.S., Europe[,] and China have taken different approaches to oversight”).

are beginning to regulate digital currencies.<sup>164</sup> Further, nongovernmental digital currencies could impair central banks' ability to control monetary policy and possibly undermine confidence in the value or operational continuity of currencies, which could threaten international monetary and financial stability.

To address the complexity of cross-border and multi-national regulatory schemes, policymakers have generally devised two strategies which attempt to minimize regulatory costs and assure legal enforceability. The traditional strategy is to enact a multilateral convention or treaty (the terms being synonymous), which represents an agreement or compact among nations under which each such nation is bound to adhere to the convention's requirements without requiring further action by its legislative body.<sup>165</sup> A more recent, and arguably more innovative, strategy is to formulate a model law for governments to enact uniformly as domestic law in their jurisdictions.<sup>166</sup> Model laws are thus sometimes called uniform laws.

Treaties are more formal than model laws. Treaties are binding upon contracting states and may only be modified or denounced by a treaty amendment.<sup>167</sup> This binding feature provides parties significant certainty that treaty-bound nations will follow through on their commitments and not renege as political winds shift.<sup>168</sup> But some nations may see that greater certainty as a

---

<sup>164</sup> See, e.g., Press Release, N.Y. State: Dep't of Fin. Servs., DFS Continues to Foster Responsible Growth in New York's Fintech Industry with New Virtual Currency Product Approvals (Sept. 10, 2018), [https://www.dfs.ny.gov/reports\\_and\\_publications/press\\_releases/pr1809101](https://www.dfs.ny.gov/reports_and_publications/press_releases/pr1809101). Treasury Secretary Yellen observes, however, that current state regulation of stablecoins "is inconsistent and fragmented, with some stablecoins effectively falling outside the regulatory perimeter." Declan Harty & Rey Mashayekhi, *Top D.C. Financial Regulators Release Stablecoin Report and Urge Congress to Pass Legislation*, FORTUNE (Nov. 1, 2021, 5:04 PM) (quoting Secretary Yellen), <https://fortune.com/2021/11/01/top-d-c-financial-regulators-release-stablecoin-report-and-urge-congress-to-pass-legislation/>. Furthermore, state regulation does not always "[require] issuers to protect reserves or maintain liquidity." See Timothy G. Massad, *Regulating Stablecoins Isn't Just About Avoiding Systemic Risk*, BROOKINGS (Oct. 5, 2021), <https://www.brookings.edu/research/regulating-stablecoins-isnt-just-about-avoiding-systemic-risk/>.

<sup>165</sup> See *Convention*, BLACK'S LAW DICTIONARY (11th ed. 2019) (defining "convention" as "[a]n agreement or compact, esp. one among countries; a multilateral treaty"); see also *Frequently Asked Questions – UNCITRAL Texts*, UNITED NATIONS COMM'N ON INT'L TRADE L., [http://www.uncitral.org/uncitral/en/uncitral\\_texts\\_faq.html](http://www.uncitral.org/uncitral/en/uncitral_texts_faq.html) (last visited Sept. 18, 2022) [hereinafter *UNCITRAL*] (defining a convention as "an instrument that is binding under international law on States and other entities with treaty-making capacity that choose to become a party to that instrument").

<sup>166</sup> See *UNCITRAL*, *supra* note 165 (defining "model law").

<sup>167</sup> See, e.g., Georgie Gaja, Peter Hay & Ronald Rotunda, *Instruments for Legal Integration in the European Community*, in *INTEGRATION THROUGH LAW: EUROPE AND THE AMERICAN FEDERAL EXPERIENCE, 1 METHODS, TOOLS AND INSTITUTIONS: BOOK 2 POLITICAL ORGANS, INTEGRATION TECHNIQUES AND JUDICIAL PROCESS* 113, 153 (Mauro Cappelletti, Monica Secombe & Joseph Weiler eds., 1986) (discussing the preference of European countries for conventions as opposed to model laws).

<sup>168</sup> See *id.* at 153–54.

disadvantage, especially if they are experimenting with new proposals.<sup>169</sup> Moreover, the expectation that a treaty needs widespread consensus can discourage its adoption.<sup>170</sup> Experimentation requires flexibility. The more relaxed nature of a model-law strategy can provide that flexibility.<sup>171</sup> Model laws may be amended or denounced unilaterally by a nation without violating international law.<sup>172</sup> Furthermore, the less formal process of developing and enacting a model law can promote open communication.<sup>173</sup>

Additionally, conventions also can “take months or even years” to enter into force because they do “not become legally binding until a specified number of states complete their national ratification processes and formally agree to be bound by the conditions and obligations of the treaty.”<sup>174</sup> That delay makes a convention particularly unsuitable for global stablecoins, where the market is rapidly developing and forcing regulators “to move faster to contain the risks.”<sup>175</sup> In contrast, a model-law strategy can minimize delay because it becomes effective for each nation as

---

<sup>169</sup> *Id.* at 154; cf. Steven L. Schwarcz, *Soft Law as Governing Law*, 104 MINN. L. REV. 2471, 2480 (2020) (“By promoting open communication, the less formal process of developing and enacting a model law can sometimes be more productive than a treaty approach.”).

<sup>170</sup> Cf. Brad Setser, *The Political Economy of the SDRM 5* (Initiative for Pol’y Dialogue, Working Paper, 2008) [https://policydialogue.org/files/publications/papers/The\\_Political\\_Economy\\_of\\_the\\_SDRM.pdf](https://policydialogue.org/files/publications/papers/The_Political_Economy_of_the_SDRM.pdf) (discussing the “profound difficulties [of] building international consensus behind any sweeping change in global financial regulation”).

<sup>171</sup> See, e.g., John A. E. Pottow, *Procedural Incrementalism: A Model for International Bankruptcy*, 45 VA. J. INT’L L. 936, 984–86 (2005) (discussing possible explanations for the recent success of model laws); cf. Schwarcz, *supra* note 169, at 2479 (“The formality of a treaty can also discourage its adoption. Because of the lengthy negotiation process and their binding nature, treaties are not well suited to address an imminent or controversial global crisis.”).

<sup>172</sup> Gaja et al., *supra* note 167, at 153–54; cf. Charles W. Mooney, Jr., *Extraterritorial Impact of Choice-of-Law Rules for Non-United States Debtors Under Revised U.C.C. Article 9 and a New Proposal for International Harmonization*, in CROSS-BORDER SECURITY AND INSOLVENCY 202 (Michael Bridge & Robert Stevens eds., 2001) (arguing that the all-or-nothing nature of a convention is superior to a model law because a model law may be materially distorted by an enacting jurisdiction).

<sup>173</sup> See Pottow, *supra* note 171, at 984–86 (discussing the informal process of enacting a model law and its benefits).

<sup>174</sup> Pam Slater, *Environmental Law in Third World Countries: Can It Be Enforced by Other Countries?*, 5 ILSA J. INT’L & COMPAR. L. 519, 521 (1999) (“The treaty making process is inadequate as an effective remedy for the world’s accelerating environmental problems because treaties take a very long time to implement.”); cf. Geneviève Saumier, *The Hague Principles and the Choice of Non-State “Rules of Law” to Govern an International Commercial Contract*, 40 BROOK. J. INT’L L. 1, 7 (2014) (referencing “the sometimes stifling methods of treaty-drafting”). Also, the “national ratification processes” of some nations can make it difficult to approve a treaty. See Slater, *supra*, at 521. Under Article II, Section 2, of the U.S. Constitution, for example, a treaty negotiated by the U.S. President does not become effective unless a resolution of ratification is approved by two-thirds of the U.S. Senate. U.S. CONST. art. II, § 2.

<sup>175</sup> *Why Regulators Should Treat Stablecoins Like Banks*, ECONOMIST (Aug. 7, 2021), <https://www.economist.com/leaders/2021/08/07/why-regulators-should-treat-stablecoins-like-banks>.

soon as that nation enacts the uniform text.<sup>176</sup> While an in-depth discussion of each strategy is beyond the scope of this Article, for the foregoing reasons, a model-law strategy should be more successful than a more formal treaty strategy to engage in the urgent and novel experiment of regulating digital currencies.<sup>177</sup>

#### IV. CONCLUSION

The United States, other governments, multinational organizations, and the private sector are urgently exploring the possibility of employing digital currencies, especially for facilitating retail consumer payments domestically and across national borders.<sup>178</sup> A significant portion of the currency transfers among businesses and financial institutions already occur digitally, without the need for cash. The next generation of cashless currency transfers will be retail, involving consumers.<sup>179</sup> Retail digital currencies not only have the potential to improve the speed and efficiency of payments, both domestically and worldwide, but also to broaden financial inclusion to consumers who lack bank accounts because they are poor or remotely located.

This Article examines and critiques the evolving types of digital currencies that are likely to become widely used. These include central bank issued currencies that represent governmental fiat money in digital form. These also include cryptocurrencies such as privately issued “stablecoins,” which are backed by reference assets having intrinsic value, and more generic cryptocurrencies that have no supporting assets.

Although law is critical to the development of these digital currencies, governments are just beginning to envision regulatory design. This Article shows that retail digital currencies present innovative legal issues as well as the types of legal issues normally associated with money and payment systems—including risk of loss, counterfeiting, privacy, money laundering, and consumer protection—although in novel contexts. For example, privately issued stablecoins, if widely used, could impair central banks’ ability to control monetary policy and possibly undermine confidence in the value or operational continuity of currencies, which could threaten international monetary and financial stability. Digital currencies used for making international payments also would require coordinated and effective cross-border regulation and supervision. This Article describes these digital currencies and analyzes how they could be regulated and supervised.

---

<sup>176</sup> See Pottow, *supra* note 171, at 984–86 (discussing the enactment of a model law). Cf. Gaja et al., *supra* note 167, at 154 (explaining why a model-law strategy can sometimes be more productive than a more formal treaty strategy).

<sup>178</sup> Cf. PRESIDENT’S WORKING GRP., *supra* note 62, at 3 (observing in November 2021 that the “rapid growth of stablecoins increases the urgency of this work”).

<sup>179</sup> This Article does not argue that digital currencies should replace cash, merely that they should “coexist[] with cash and other types of money in a flexible and innovative payment system.” Press Release, Bank for Int’l Settlements, Central Banks and BIS Publish First Central Bank Digital Currency (CBDC) Report Laying out Key Requirements (Oct. 9, 2020) [hereinafter BIS Press Release], <https://www.bis.org/press/p201009.htm>. At least in the near future, cash will still be needed for micro-retail payment transactions, especially for unbanked consumers.