

Steven L. Schwarcz

## Chapter 4: Central Bank Digital Currencies and Law

This chapter examines the legal issues surrounding a ‘retail’ central bank digital currency (CBDC) – one that is used by consumers on a day-to-day basis as an alternative to cash.<sup>1</sup> Most discussions about CBDC focus on its purported benefits and initial design questions. Little is written about how existing laws and regulations will extend to CBDCs or what new regulations will have to be implemented.<sup>2</sup> This chapter engages in that analysis.

The analysis assumes that future retail CBDCs will be account-based, meaning the currency will be represented by book entries in accounts that are held and managed by banks. The central bank will prescribe interest rates on these accounts, and rules and regulations for their governance and use. Much of the existing infrastructure of both central and commercial banks<sup>3</sup> – as well as the widespread application of that infrastructure to so-called ‘wholesale’ electronic funds transfers between businesses and financial institutions<sup>4</sup> – is already account-based,<sup>5</sup> and much of the recent literature on CBDC assumes the account-based system.<sup>6</sup>

- 
- 1 Steven L. Schwarcz is the Stanley A. Star Distinguished Professor of Law & Business at Duke University School of Law and Senior Fellow at the Centre for International Governance Innovation (CIGI). The author would thank Benjamin Geva and Lev Menand for excellent comments and Eric Horsley and Carson Calloway for invaluable research assistance.
  - 2 Patrycja Beniak, ‘Central Bank Digital Currency and Monetary Policy: A Literature Review’, in *MPRA Papers*, No. 96663, 26 October 2019, p. 2, <https://mpra.ub.uni-muenchen.de/96663>.
  - 3 For convenience, this chapter refers to commercial banks broadly, as including all non-governmental banks.
  - 4 See Article 4A of the Uniform Commercial Code (UCC), Prefatory Note.
  - 5 Financial institutions in the United States, for example, hold accounts at the Federal Reserve and use Fedwire to transfer money between these accounts. See Fedwire Funds Service website: *Product Sheet*, <https://www.frb.services.org/assets/financial-services/wires/funds.pdf>.
  - 6 See, e.g., Morgan Ricks, John Crawford and Lev Menand, ‘FedAccounts: Digital Dollars’, in *George Washington Law Review*, forthcoming (15 April 2020), <https://ssrn.com/abstract=3192162> (focusing on a Federal Reserve Bank account-based system).

A retail account-based CBDC would likely use technologies largely already in place at banks and merely extend their access to a wider user base. That is because any account-based digital currency, whether wholesale or retail,<sup>7</sup> would operate through electronic funds transfers.<sup>8</sup> To that extent, digital currency transfers are synonymous with electronic funds transfers.

This calls into question why retail CBDC should be regulated any differently than wholesale electronic funds transfers. As this chapter will show, it should not generally be regulated differently – with relatively few exceptions, such as consumer protection.

Two primary sources of regulation currently govern wholesale electronic funds transfers. Those funds transfers are governed in the European Union by the European Directive on payment services in EU internal markets (the ‘EU Directive’), and in the United States by Article 4A of the Uniform Commercial Code (UCC). As this chapter will show, Article 4A is the more relevant regulatory

---

The digital currency being developed by the People’s Bank of China appears to be an account-based system, though details remain confidential. Cf. Anton N. Didenko et al., ‘After Libra, Digital Yuan and COVID-19: Central Bank Digital Currencies and the New World of Money and Payment Systems’, in *UNSW Law Research Series*, No. 65/2020 (30 SEPTEMBER 2020), <https://ssrn.com/abstract=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 Cryptocurrency Alternative Sovereign Digital Currency and Why Is It Not Like Bitcoin?’, in *South China Morning Post*, 13 May 2020, <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). But cf. Benjamin Geva, ‘Virtual Currencies and the State’, in *Just Money*, 22 April 2020, <https://wp.me/paGDrD-10W> (arguing that efficiency gains from disintermediation favor token-based CBDCs, though with concomitant risks). See also the chapter by Robleh Ali in this volume.

7 All funds transfers can be classified as either wholesale or retail. Bank for International Settlements (BIS), *Annual Economic Report 2020*, 30 June 2020, p. 68, <https://www.bis.org/publ/arpdf/ar2020e.htm>.

8 Cf. Charles M. Kahn and William Roberds, ‘The Design of Wholesale Payments Networks: The Importance of Incentives’, in *Federal Reserve Bank of Atlanta Economic Review*, Vol. 84, No. 3 (1999), p. 30–39, [https://www.frbatlanta.org/research/publications/economic-review/1999/q3/vol84no3\\_design-of-wholesale-payments-network.aspx](https://www.frbatlanta.org/research/publications/economic-review/1999/q3/vol84no3_design-of-wholesale-payments-network.aspx); Committee on Payment and Settlement Systems, ‘The Role of Central Bank Money in Payment Systems’, in *CPMI Papers*, No. 55 (12 August 2003), <https://www.bis.org/cpmi/publ/d55.htm> (observing that wholesale funds transfers between banks are already settled digitally).

precedent because it covers in much greater depth the rights, obligations, and liabilities of banks and other intermediaries involved with the transfers.<sup>9</sup> Article 4A's regulatory framework for wholesale wire transfers also has been widely influential both within the United States and internationally.<sup>10</sup>

In the United States, Article 4A has been enacted in all 50 states<sup>11</sup> and governs both of the principal electronic payment systems – the Federal Reserve wire transfer network (Fedwire), and the New York Clearing House Interbank Payments System (CHIPS).<sup>12</sup> Internationally, Article 4A and the United Nations Commission on International Trade Law's (UNCITRAL) Model Law on International Credit Transfers use the same framework for classifying entities and transactions in wire transfers (for example, both focus on credit transfers and speak in terms of originators/beneficiaries and payment orders to banks).<sup>13</sup> Also, both Article 4A and UNCITRAL's Model Law influenced the EU Directive.<sup>14</sup>

- 
- 9 The European Directive covers both credit and debit transfers, whereas Article 4A covers only credit transfers. See Benjamin Geva, 'Payment Transactions under the E.U. Second Payment Services Directive—An Outsider's View', in *Texas International Law Journal*, Vol. 54, No. 2 (2019), p. 215, [https://digitalcommons.osgoode.yorku.ca/scholarly\\_works/2718](https://digitalcommons.osgoode.yorku.ca/scholarly_works/2718). However, the distinction between credit and debit transfers is not an organizational principle in the Directive. Also, notwithstanding the Directive's slightly broader coverage, it lacks depth compared to Article 4A.
- 10 Mark Sneddon, 'The Effect of Uniform Commercial Code Article 4A on the Law of International Credit Transfers', in *Loyola of Los Angeles Law Review*, Vol. 29, No. 3 (April 1996), p. 1111–1112, <https://digitalcommons.lmu.edu/llr/vol29/iss3/11>; Barkley Clark and Barbara Clark, *The Law of Bank Deposits, Collections and Credit Cards*, 3rd ed., Boston, Warren, Gorham & Lamont, 1990, para. 17.02, (2)(d).
- 11 Uniform Law Commission, *UCC Article 4A, Funds Transfers*, <https://www.uniformlaws.org/committees/community-home?CommunityKey=2985cf6d-9c22-4abe-abf1-1f36f8a27201>.
- 12 Code of Federal Regulations (CFR), title 12, para. 210.25; Clearing House Interbank Payments System (CHIPS), *Public Disclosure of Legal, Governance, Risk Management, and Operating Framework*, June 2020, p. 12, [https://www.theclearinghouse.org/-/media/new/tch/documents/payment-systems/chips\\_public\\_disclosure\\_june\\_2020.pdf](https://www.theclearinghouse.org/-/media/new/tch/documents/payment-systems/chips_public_disclosure_june_2020.pdf).
- 13 See generally Carl Felsenfeld, 'The Compatibility of the UNICTRAL Model Law on International Credit Transfers with Article 4A of the UCC', in *Fordham Law Review*, Vol. 60, No. 6 (1992), p. 53–75, <https://ir.lawnet.fordham.edu/flr/vol60/iss6/4>.
- 14 Cf. Mark Sneddon, 'The Effect of Uniform Commercial Code Article 4A on the Law of International Credit Transfers', cit., p. 1109 (remarking on the influence of UCC Article 4A on the European Commission's proposed Directive on cross-border credit transfers).

Additionally, both Fedwire and CHIPS have choice-of-law provisions which specify that Article 4A will apply to all funds transfers processed in whole or in part by their systems.<sup>15</sup>

Article 4A's framework also includes a consistent vocabulary for describing funds transfers and a precise allocation of rights, obligations, and liabilities among participating financial institutions and their customers, who initiate and receive wire-transfer payments.<sup>16</sup> Transferring funds from one customer's electronic bank account to that of another customer should be the same, in principle, whether the transfer is retail or wholesale.<sup>17</sup> A retail customer would initiate a funds transfer by sending a payment order to his bank; that bank would then (provided its customer's account has sufficient funds) send a payment order through, for example, Fedwire to the beneficiary's bank; and the beneficiary's bank would (again, subject to receiving funds) credit the beneficiary's account.<sup>18</sup>

Thus, while Article 4A is designed for wholesale wire transfers, it should – at least with certain consumer-protection provisions, discussed below – provide a suitable regulatory framework for retail CBDC transactions. To understand why, consider the key legal issues of a retail CBDC: (1) risk of loss; (2) counterfeiting protection; (3) privacy and data keeping; (4) anti-money laundering; and (5) consumer protection.

- 1) *Risk of loss*. Risk of loss includes at least three risks: mistakenly transferring funds to the wrong person; fraud risk, including fraudulently transferring funds to a wrong person; and credit risk, including the risk of the 'receiving bank' paying out before being paid. Article 4A covers these risks as follows.<sup>19</sup>

---

15 CFR, title 12, para. 210.25 (b)(2); CHIPS, *Public Disclosure of Legal, Governance, Risk Management, and Operating Framework*, cit., p. 12.

16 See generally UCC para. 4A. Available in the Legal Information Institute (LII) website: <https://www.law.cornell.edu/ucc/4A>.

17 Cf. Morgan Ricks, John Crawford and Lev Menand, 'FedAccounts: Digital Dollars,' cit., p. 15 (arguing that retail CBDC transactions could use the same wire transfer system currently used by the central bank).

18 Cf. Federal Reserve Banks: *FedNow Service Product Sheet*, <https://www.frbservices.org/assets/financial-services/fednow/fednow-product-sheet.pdf> (describing the payment flow for a credit transfer using the proposed FedNow interbank real-time settlement service, targeted to be available in 2023 or 2024, to enable financial institutions to deliver faster payment services to their customers).

19 The EU Directive provides banks with less discretion in the choice to accept a payment order. This could reduce the bank's incentive to do as much due diligence as it otherwise would.

- (a) *Mistaken transfer*. Under UCC para. 4A–207, a payment order with a nonexistent or unidentifiable person or account does not create a right in a person to receive the payment. Where the name and account number are known to the beneficiary’s bank, however, that bank may pay the person referred to by the account number.<sup>20</sup>

One possible small adjustment appropriate to adapt Article 4A to regulate retail CBDC transactions is in para. 4A–207. Under subsection (a) of that section, if the name or bank account number of a payment order received by the beneficiary’s bank refers to a nonexistent or unidentifiable person or account, no person has the right as a beneficiary to receive the payment – except as provided in subsection (b). Subsection (b) provides that if the name and bank account number associated with a particular payment order refer – unbeknownst to the beneficiary’s bank – to different individuals (i.e., the name to one person and the bank account number to another), the beneficiary’s bank may pay the person referred to by the account number.<sup>21</sup> This level of flexibility may make sense for wholesale wire transfers, because in larger transactions, especially business transactions, the parties may devote more care to provide the correct information – so errors should be relatively rare. Retail wire transfers may be more error prone.<sup>22</sup> For that reason, at least from the customers’ standpoint, the stricter rule of subsection (a), that both the name and bank account number match, make sense. Still, that rule should be balanced by banking realities. At least currently, a ‘very large percentage of payment orders issued to the beneficiary’s bank’ are ‘processed by automated means using machines capable of’ identifying ‘the number of a bank account,’ and ‘without human reading of the payment order itself.’<sup>23</sup>

- (b) *Fraud*. UCC paras. 4A–202 to 4A–204 address authorization and acceptance of payment orders issued in the name of a customer. UCC para. 4A–202(a) points to the law of agency to resolve a dispute where the person identified as sender refuses to pay on the grounds that it did not authorize the payment order. For example, if the payment order is

---

20 Cf. *infra* notes 21–22 and accompanying text (providing a more detailed explanation).

21 UCC para. 4A-207(b).

22 A retail customer, for example, may be more likely to make a mistake when wiring 20 US dollars to a babysitter than a wholesale customer would be when wiring 25,000 US dollars to pay for a shipment of inventory.

23 Official Comment to UCC para. 4A-207, point 2. Available in the D.C. Law Library website: <https://code.dccouncil.us/dc/council/code/sections/28:4A-207.html>.

sent by an officer of a corporation, the question would be whether that officer is an agent of the corporation with the power to authorize payment orders on the corporation's behalf. More commonly, a bank and its customer agree to security procedures that, if followed, result in an authorized payment order.<sup>24</sup>

(c) *Credit risk*. Under UCC para. 4A-405(d), a 'funds-transfer system rule may provide that payments made to beneficiaries of funds transfers made through the system are provisional until receipt of payment by the beneficiary's bank of the payment order it accepted.' UCC para. 405(d) continues by providing conditions that, if met, would entitle the beneficiary's bank to a refund.

2) *Counterfeiting protection*. Counterfeiting is defined as 'the replication or manufacture of a financial instrument [...] with the intent to defraud an individual, entity, or government.'<sup>25</sup> Traditionally, the counterfeiting risk for money has been concerned with illicit production of physical representations of the money, such as the unauthorized reproduction of US dollar bills. The protections involve increasing the complexity and markings of bills.<sup>26</sup> These concerns have no obvious parallel for an account-based CBDC.

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>27</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>28</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

---

24 UCC para. 4A-202(b).

25 Ralph E. McKinney et al., 'The Evolution of Financial Instruments and the Legal Protection Against Counterfeiting: A Look at Coin, Paper, and Virtual Currencies', in *Journal of Law, Technology & Policy*, No. 2 (2015), p. 299, <http://illinoisjltp.com/journal/wp-content/uploads/2015/12/McKinney.pdf>.

26 *Ibid.*, p. 302-303.

27 See Committee on Payments and Market Infrastructures, 'Central Bank Digital Currencies', in *CPMI Papers*, No. 174 (12 March 2018), p. 4, <https://www.bis.org/cpmi/publ/d174.htm> (observing that the form of verification needed differs between token-based and account-based money).

28 Cf. *ibid.*, p. 4, note 5 (observing the double spending problem for digital tokens). This chapter's reference to double spending includes, of course, any multiple spending of the same money in an account.

then quickly withdraws the money.<sup>29</sup> To the extent an account-based CBDC makes use of existing banking technology and systems (which is likely),<sup>30</sup> these counterfeiting risks should be comparable to counterfeiting risks in current wholesale electronic banking.<sup>31</sup>

Article 4A covers these counterfeiting risks. It does not compel a bank to process transactions under conditions that might result in double spending,<sup>32</sup> such as when there are insufficient funds in an account.<sup>33</sup> Furthermore, existing account agreements authorize debits contingent on there being available balances.<sup>34</sup> The current banking system is thus already well guarded against the risk of double spending. A retail CBDC modelled off the current electronic banking system should inherit the same (low) risk of double spending.

Likewise, Article 4A does not compel a bank to process transactions involving an unverified account. A bank has no obligation to accept a payment order.<sup>35</sup> Because acceptance obliges it to pay the receiving bank,<sup>36</sup> a sending bank has

---

29 See, e.g., Lily Hay Newman, ‘How Hackers Pulled Off a \$20 Million Mexican Bank Heist’, in *Wired*, 15 March 2019, <https://www.wired.com/story/mexico-bank-hack> (discussing a transfer initiated by hackers from a phantom account to a real account within the bank).

30 Morgan Ricks, John Crawford and Lev Menand, ‘FedAccounts: Digital Dollars’, cit., p. 3.

31 The security threat caused by a possible centralization of accounts in the central bank would still need to be considered.

32 Neither UCC Article 4A nor the Electronic Fund Transfer Act (EFTA) compels a bank to process a transaction when there are insufficient funds in an account. Under UCC para. 4A-212, absent an explicit agreement, a bank has no duty to accept a received payment order. The EFTA, as codified in part in the United States Code (USC), title 15, para. 1693h (<https://www.law.cornell.edu/uscode/text/15/1693h>), makes insufficient funds in a customer’s account an explicit exception to a bank’s liability for damages caused by a failure to make an electronic funds transfer.

33 Under UCC para. 4A-212, absent an explicit agreement, a bank has no duty to accept a received payment order. The EFTA, as codified in part in USC, title 15, para. 1693h, makes insufficient funds in a customer’s account an explicit exception to a bank’s liability for damages caused by a failure to make an electronic funds transfer.

34 E.g., Wells Fargo Bank, *Deposit Account Agreement (Effective July 24, 2019)*, p. 44, <https://www.wellsfargo.com/fetch-pdf?formNumber=CCB2018C&subProductCode=ANY>. Given both the legal framework (see UCC Article 4A, Prefatory Note) and the account agreements banks have crafted, double spending is a small risk in an account-based system where a third party—the bank—oversees a transaction.

35 Morgan Ricks, John Crawford and Lev Menand, ‘FedAccounts: Digital Dollars’, cit., p. 3.

36 UCC para. 4A-402(c).

an incentive to ensure that funds are available for reimbursement before it accepts a payment order.

- 3) *Privacy and data keeping*. Central bank digital currencies may help to centralize data about the money supply. To the extent CBDC impacts privacy – for example, by making funds transfers easier to trace – how should privacy and access to capital be balanced? Governments generally protect their citizens' privacy better than private entities, such as a non-government sponsor of a digital currency.<sup>37</sup>

It also may be interesting to consider if a kind of central-commercial bank 'federalism' is more effective when it comes to security measures to protect privacy. If the account-based CBDC is a totally centralized system, then any security vulnerability is systemic, everyone will be affected. However, if the account-based CBDC makes use of infrastructure and security measures at commercial banks, then a vulnerability at one bank would not necessarily be present at other commercial banks (because of the variability of security measures in place).

- 4) *Anti-money-laundering laws*. AML laws generally follow the recommendations of the Financial Action Task Force (FATF), an inter-governmental body.<sup>38</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

---

37 Cf. Federal Trade Commission, *FTC Imposes \$5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, 24 July 2019, <https://www.ftc.gov/node/1536925> (reporting that Facebook agreed to pay a penalty of 5 billion US dollars to settle charges that it 'violated a 2012 FTC order by deceiving users about their ability to control the privacy of their personal information'); Natasha Lomas, 'Libra, Facebook's Global Digital Currency Plan, Is Fuzzy on Privacy, Watchdogs Warn', in *TechCrunch*, 5 August 2019, <https://techcrunch.com/?p=1864705> (noting the lack of detailed information on Libra's privacy protections and describing the concerns of a set of international privacy watchdogs); Spencer Bokart-Lindell, 'Can We Trust Facebook to Run a Bank?', in *The New York Times*, 24 October 2019, <https://nyti.ms/32JdwNz> (discussing privacy concerns over Libra).

38 The FATF was established by the 1989 G-7 Summit in Paris, with the mission of addressing the threat posed to the banking system and to financial institutions by money laundering. Its mission expanded in 2001 to counter the use of the financial system for terrorism financing. There currently are 39 members of the FATF, covering many of the largest financial hubs. FATF website: *History of the FATF*, <https://www.fatf-gafi.org/about/historyofthefatf>.

financial system.<sup>39</sup> To this end, it makes recommendations for an AML legal framework in member countries.<sup>40</sup>

If the introduction of a CBDC leaves the commercial banking sector as the retail depository institutions, no change should be needed, in principle, to AML laws because the CBDC would not impact the FATF recommendations. Changes to AML laws might be needed, though, 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 meet the recommendation's requirements.

In practice, however, a retail CBDC might require certain changes to AML laws. For example, FATF Recommendation 10 creates an obligation for financial institutions to conduct customer due diligence (also known as Know-Your-Customer (KYC) laws). If this recommendation requires every retail transaction to be scrutinized, it would impose high transaction costs due to the sheer volume of those transactions.<sup>41</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>42</sup>

- 5) *Consumer protection.* Although UCC Article 4A covers many domestic and international electronic funds transfers, it was designed for use by relatively sophisticated parties, such as businesses and financial institutions.<sup>43</sup> In the United States, the Electronic Fund Transfer Act (EFTA) governs a range of existing retail electronic funds transfers, including ATM deposits and

---

39 FATF website: *What Do We Do*, <https://www.fatf-gafi.org/about/whatwedo>.

40 FATF, *The FATF Recommendations. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*, June 2019, <http://www.fatf-gafi.org/publications/fatfrecommendations>.

41 FATF Recommendation 17 (*ibid.*, p. 16) allows financial institutions to outsource their customer due diligence requirements to third parties; however, liability remains with the delegating party. For a retail CBDC this could mean central banks are outsourcing customer due diligence to commercial banks. It may be preferable, contra Recommendation 17, to have commercial banks responsible to the central bank for failed due diligence.

42 Cf. CFR, title 31, para. 1010.311 (setting US 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').

43 See *supra* note 4 and accompanying text.

withdrawals and most mobile payment apps (such as PayPal, Venmo, and Zelle).<sup>44</sup>

In contrast to Article 4A, the EFTA pays little attention to what electronic funds transfers consist of or how they are carried out; rather, the primary purpose of the EFTA is one of consumer protection: to give consumers certain rights when engaging in electronic funds transfers.<sup>45</sup> For example, the EFTA limits consumer liability for unauthorized transactions,<sup>46</sup> ensures that banks adequately inform consumers of their rights,<sup>47</sup> protects consumers from being charged excessive fees,<sup>48</sup> and gives consumers a means of redressing erroneous transactions.<sup>49</sup>

To illustrate these different regulatory approaches, assume a customer of Bank A accidentally discloses information that enables a third party to make an unauthorized transaction. Under Article 4A, the customer will be liable for the unauthorized transaction so long as Bank A, in good faith, follows a commercially reasonable, and mutually agreed upon, security procedure.<sup>50</sup> Under the EFTA, the customer's liability for the unauthorized transaction is subject to a dollar limitation.<sup>51</sup> Another important difference between Article 4A and the EFTA is the extent to which customers and their banks can vary the terms of their agreements. Article 4A affords much more flexibility to contractually vary the rights and obligations of a party to an electronic funds transfer. So long as Article 4A does not expressly provide otherwise, the terms of a funds transfer can be varied.<sup>52</sup> The EFTA does not permit consumer rights to be waived.<sup>53</sup>

---

44 CFR, title 12, para. 205.3. In part because of the Supremacy Clause of the US Constitution, the EFTA, which is federal law, supersedes inconsistent provisions of Article 4A, which is state law. Cf. UCC para. 4A-108 and Official Comment, point 1 (stating and explaining the EFTA's supremacy).

45 USC, title 15, para. 1693.

46 USC, title 15, para. 1693g.

47 USC, title 15, para. 1693c.

48 USC, title 15, para. 1693o-2.

49 USC, title 15, para. 1693 f.

50 Francis J. Facciolo, 'Unauthorized Payment Transactions and Who Should Bear the Losses', in *Chicago-Kent Law Review*, Vol. 83, No. 2 (April 2008), p. 614, <https://scholarship.kentlaw.iit.edu/cklawreview/vol83/iss2/6>.

51 USC, title 15, para. 1693g(a) (limiting that liability to 50 US dollars if Bank A is properly notified of the unauthorized transaction, and otherwise 500 US dollars).

52 UCC para. 4A-501.

53 USC, title 15, para. 1693l.

These differences between Article 4A and the EFTA reflect their different purposes. Article 4A was written with wholesale funds transactions in mind and contemplates sophisticated users. CBDC regulation thus should draw from Article 4A to the extent such regulation governs how electronic funds transfers should occur – through a series of payment orders between clearly defined parties – and how generally to allocate rights and obligations between those parties. In contrast, the EFTA was written to protect everyday retail customers, and this policy goal is reflected in provisions that limit consumer liabilities and protect their rights. CBDC regulation thus also should draw from the EFTA to the extent regulators regard retail users of CBDC to need overriding consumer protection.

This chapter has so far examined what law should apply to a retail CBDC. A related issue is which regulators should apply that law. Although that issue is largely beyond this chapter's scope, a few observations are in order. When international wholesale funds transfers are made, regulators may supervise the relevant aspects of the transfers at their national level. Consider, for example, a cross-border funds transfer sent through the CHIPS clearing system<sup>54</sup> from a CHIPS participant bank in the United States to a CHIPS participant bank in Germany.<sup>55</sup> Regulators in the United States would supervise the sending bank, and the Federal Reserve regulates the US activities of CHIPS.<sup>56</sup> Regulators in Germany, and Europe more broadly, presumably would supervise the receiving bank.<sup>57</sup> As a result, there is no current need for an international regulator to supervise cross-border wholesale electronic funds transfers, nor would there appear to be a need for such a regulator to supervise cross-border retail electronic funds transfers. This would not rule out, of course, the potential value of

---

54 See *supra* notes 11–14 and accompanying text.

55 Cf. CHIPS, *CHIPS Participants*, last updated 14 August 2020, [https://www.theclearinghouse.org/-/media/new/tch/documents/payment-systems/chips\\_participants\\_revised\\_08-14-2020.pdf](https://www.theclearinghouse.org/-/media/new/tch/documents/payment-systems/chips_participants_revised_08-14-2020.pdf) (listing banks from multiple continents as participants in the CHIPS clearing system).

56 Federal Reserve Board, *Designated Financial Market Utilities*, last updated 29 January 2015, [https://www.federalreserve.gov/paymentsystems/designated\\_fmu\\_about.htm](https://www.federalreserve.gov/paymentsystems/designated_fmu_about.htm); Congressional Research Service, 'Who Regulates Who? An Overview of the U.S. Financial Regulatory Framework', in *CRS Reports*, 10 March 2020, <https://fas.org/sgp/crs/misc/R44918.pdf>.

57 Federal Financial Supervisory Authority, *Banks & Financial Services Providers*, updated 22 March 2016, <https://www.bafin.de/dok/7857910>.

establishing an inter-governmental body, like the FATE, to try to produce best-practice recommendations for international electronic funds transfers.<sup>58</sup>

## Conclusions

As this chapter has shown, a significant portion of the currency transfers among businesses and financial institutions already occur digitally. The primary legal focus of enabling consumers to use central bank digital currency transfers on a day-to-day basis, as an alternative to cash, thus involves consumer protection.

This chapter assumes the feasibility of technology required to manage such a real time, low-cost, 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.<sup>59</sup> Though still in the planning stages, the Federal Reserve is working on its own interbank real-time funds transfer service.<sup>60</sup> And China is already testing a retail CBDC in four cities.<sup>61</sup>

## References

- Bank for International Settlements (BIS), *Annual Economic Report 2020*, 30 June 2020, <https://www.bis.org/publ/arpdf/ar2020e.htm>
- Patrycja Beniak, 'Central Bank Digital Currency and Monetary Policy: A Literature Review', in *MPRA Papers*, No. 96663, 26 October 2019, p. 2, <https://mpra.ub.uni-muenchen.de/96663>
- Spencer Bokak-Lindell, 'Can We Trust Facebook to Run a Bank?', in *The New York Times*, 24 October 2019, <https://nyti.ms/32JdwNz>
- Jonathan Cheng, 'China Rolls Out Pilot Test of Digital Currency', in *The Wall Street Journal*, 20 April 2020, <https://www.wsj.com/articles/china-rolls-out-pilot-test-of-digital-currency-11587385339>

---

58 Cf. *supra* notes 37–39 and accompanying text (discussing FATF recommendations for combating money laundering, terrorist financing, and other related threats to the integrity of the international financial system).

59 CHIPS website: *Real Time Payments*, <https://www.theclearinghouse.org/payment-systems/rtp>.

60 See *supra* note 17 and accompanying text.

61 Jonathan Cheng, 'China Rolls Out Pilot Test of Digital Currency', in *The Wall Street Journal*, 20 April 2020, <https://www.wsj.com/articles/china-rolls-out-pilot-test-of-digital-currency-11587385339>. See also the chapter by Jan Knoerich in this volume.

- Barkley Clark and Barbara Clark, *The Law of Bank Deposits, Collections and Credit Cards*, 3rd ed., Boston, Warren, Gorham & Lamont, 1990
- Clearing House Interbank Payments System (CHIPS), *Public Disclosure of Legal, Governance, Risk Management, and Operating Framework*, June 2020, [https://www.theclearinghouse.org/-/media/new/tch/documents/payment-systems/chips\\_public\\_disclosure\\_june\\_2020.pdf](https://www.theclearinghouse.org/-/media/new/tch/documents/payment-systems/chips_public_disclosure_june_2020.pdf)
- Committee on Payments and Market Infrastructures, 'Central Bank Digital Currencies', in *CPMI Papers*, No. 174 (12 March 2018), <https://www.bis.org/cpmi/publ/d174.htm>
- Committee on Payment and Settlement Systems, 'The Role of Central Bank Money in Payment Systems', in *CPMI Papers*, No. 55 (12 August 2003), <https://www.bis.org/cpmi/publ/d55.htm>
- Congressional Research Service, 'Who Regulates Who? An Overview of the U.S. Financial Regulatory Framework', in *CRS Reports*, 10 March 2020, <https://fas.org/sgp/crs/misc/R44918.pdf>
- Anton N. Didenko et al., 'After Libra, Digital Yuan and COVID-19: Central Bank Digital Currencies and the New World of Money and Payment Systems', in *UNSW Law Research Series*, No. 65/2020 (30 September 2020), <https://ssrn.com/abstract=3622311>
- Francis J. Facciolo, 'Unauthorized Payment Transactions and Who Should Bear the Losses', in *Chicago-Kent Law Review*, Vol. 83, No. 2 (April 2008), p. 605–631, <https://scholarship.kentlaw.iit.edu/cklawreview/vol83/iss2/6>
- Federal Trade Commission, *FTC Imposes \$5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, 24 July 2019, <https://www.ftc.gov/node/1536925>
- Carl Felsenfeld, 'The Compatibility of the UNICTRAL Model Law on International Credit Transfers with Article 4A of the UCC', in *Fordham Law Review*, Vol. 60, No. 6 (1992), p. 53–75, <https://ir.lawnet.fordham.edu/flr/vol60/iss6/4>
- Financial Action Task Force (FATF), *The FATF Recommendations. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*, June 2019, <http://www.fatf-gafi.org/publications/fatfrecommendations>
- Benjamin Geva, 'Payment Transactions under the E.U. Second Payment Services Directive—An Outsider's View', in *Texas International Law Journal*, Vol. 54, No. 2 (2019), p. 211–243, [https://digitalcommons.osgoode.yorku.ca/scholarly\\_works/2718](https://digitalcommons.osgoode.yorku.ca/scholarly_works/2718)
- Benjamin Geva, 'Virtual Currencies and the State', in *Just Money*, 22 April 2020, <https://wp.me/paGDrD-10W>

- Charles M. Kahn and William Roberds, 'The Design of Wholesale Payments Networks: The Importance of Incentives', in *Federal Reserve Bank of Atlanta Economic Review*, Vol. 84, No. 3 (1999), p. 30–39, [https://www.frbatlanta.org/research/publications/economic-review/1999/q3/vol84no3\\_design-of-wholesale-payments-network.aspx](https://www.frbatlanta.org/research/publications/economic-review/1999/q3/vol84no3_design-of-wholesale-payments-network.aspx)
- Natasha Lomas, 'Libra, Facebook's Global Digital Currency Plan, Is Fuzzy on Privacy, Watchdogs Warn', in *TechCrunch*, 5 August 2019, <https://techcrunch.com/?p=1864705>
- Ralph E. McKinney et al., 'The Evolution of Financial Instruments and the Legal Protection Against Counterfeiting: A Look at Coin, Paper, and Virtual Currencies', in *Journal of Law, Technology & Policy*, No. 2 (2015), p. 273–313, <http://illinoisjltp.com/journal/wp-content/uploads/2015/12/McKinney.pdf>
- Lily Hay Newman, 'How Hackers Pulled Off a \$20 Million Mexican Bank Heist', in *Wired*, 15 March 2019, <https://www.wired.com/story/mexico-bank-hack>
- Morgan Ricks, John Crawford and Lev Menand, 'FedAccounts: Digital Dollars', in *George Washington Law Review*, forthcoming (15 April 2020), <https://ssrn.com/abstract=3192162>
- Mark Sneddon, 'The Effect of Uniform Commercial Code Article 4A on the Law of International Credit Transfers', in *Loyola of Los Angeles Law Review*, Vol. 29, No. 3 (April 1996), p. 1107–1135, <https://digitalcommons.lmu.edu/llr/vol29/iss3/11>
- Karen Yeung, 'What Is China's Cryptocurrency Alternative Sovereign Digital Currency and Why Is It Not Like Bitcoin?', in *South China Morning Post*, 13 May 2020, <https://www.scmp.com/economy/china-economy/article/3083952/what-chinas-cryptocurrency-sovereign-digital-currency-and-why>