2021

The E-Banknote as a 'Banknote' : A Monetary Law Interpreted

Benjamin Geva
Osgoode Hall Law School of York University, bgeva@osgoode.yorku.ca

Seraina Neva Grünewald
Radboud University Nijmegen, s.grunewald@jur.ru.nl

Corinne Zellweger-Gutknecht
University of Basel

Source Publication:

Oxford Journal of Legal Studies 41:4, 1119 – 1148

AUTHORS' Original Version (AOV)—07NOVEMBER2020

Pre-edited

FINAL VERSION IS FORTHCOMING IN *OXFORD JOURNAL OF LEGAL STUDIES* (OJLS)

And is already published Advance Access online:

Digital Object Identifier (DOI)
https://doi.org/10.1093/ojls/gqab019
Version of Record:
https://academic.oup.com/ojls/advance-article/doi/10.1093/ojls/gqab019/6284236

DRAFT- DO NOT CITE OR QUOTE WITHOUT AUTHORS' PERMISSION

THE E-BANKNOTE AS A 'BANKNOTE': A MONETARY LAW INTERPRETED[*]

by

Benjamin GEVA,
Professor of Law,
Osgoode Hall Law School York University, Toronto
bgeva@osgoode.yorku.ca

Seraina Neva GRÜNEWALD
Professor of Law, Chair for European and Comparative Financial Law,
Radboud, University Nijmegen
s.grunewald@jur.ru.nl

Corinne ZELLWEGER-GUTKNECHT
Professor of Law,
University of Basel
corinne.zellweger-gutknecht@unibas.ch

[*] The article draws on a study submitted by the three co-authors to the European Central Bank (ECB) under its Legal Research Programme 2020 (topic 2): Corinne Zellweger-Gutknecht, Benjamin Geva, and Seraina Neva Gruenewald, 'The ECB and € E-Banknotes' (Draft of 31 July, 2020). Any views expressed are only those of the authors and do not necessarily represent the views of the ECB or the Eurosystem. For research assistance in the final stages of the work, the authors are grateful to Simona Ristic of the 2021 Osgoode Hall Law School graduating class.

ABSTRACT: *The article discusses whether an electronic banknote is a 'banknote'. The issue is dealt with as a matter of general statutory interpretation in the context of evolving technologies and institutional arrangements. The article proposes a clear terminology to address concepts underlying digital currencies and access to central bank money and argues that a banknote may be 'written' electronically. The article is critical of both account-based Central Bank Digital Currency (CBDC) and cryptocurrencies and highlights features of non-blockchain token-based alternatives. It sheds light on considerations affecting the selection of a design which is appropriate from both a functional and legal perspective and addresses architectural models for the issuance of e-banknotes.*

KEY WORDS: *banknote; electronic banknote; digital currency; CBDC; cryptocurrency; centrally issued digital currency; central bank; ECB; NCB; ESCB; legal tender; monetary law.*

CONTENTS

1 Introduction

'Money' is broadly defined to consist of anything widely circulating as a medium of exchange so as to be accepted 'in final discharge of debts … without reference to the character or credit of the person who offers it and without the intention of the person who receives it to consume it … .'[1] A national modern monetary system is controlled by the state and yet linked to private deposit banking. Standard monetary objects consist of coins[2] issued by the state and banknotes issued by the central bank, both denominated in the official unit of account. Most payments, at least in volume, are made over the non-cash payment system premised on the use of 'scriptural money.' Its architecture is centralised. Thereunder, a commercial bank[3] maintains deposit accounts for customers, against a fractional reserve, which at least large banks hold in settlement accounts with the central bank.[4] Monetary value held in deposit with

[1] *Moss v Hancock* [1899] 2 QB 111, 116. See also *Reference Re Alberta Statutes* [1938] SCR 100, 116, as well as *Johnson v State* 52 So. 652 (Ala, 1910) and *State v Finnegean* 103 NW 155 (Iowa 1905)

[2] Nowadays, coins represent only a subsidiary form of cash, the issuance of which has traditionally been left to the Treasury or a body closely linked to it (eg the Mint)

[3] Throughout this article, 'commercial bank' or 'bank' is loosely used to mean a regulated entity carrying out a substantial aspect of the 'banking business', which is to be distinguished from the central bank. Primarily, this refers to a deposit-taking bank.

commercial banks and redeemable to banknotes and coins is known as 'commercial bank money' (CoBM). Monetary value held in deposit with the central bank, as well as banknotes issued by the central bank is called central bank money (CeBM), representing a liability of the central bank to the depositor or holder.

For several years now, against the background of private actors commencing to issue private digital currencies, [5] a growing number of central banks [6] have been investigating the possibility and implications of issuing a digital form CeBM for the general public: central bank digital currency (CBDC), also known as retail CBDC (rCBDC).[7]

[4] Large banks also hold deposits for correspondent small banks. On moving away from this tiering structure see eg Evangelos Benos, Gerardo Ferrara, and Pedro Gurrola-Perez, 'The impact of de-tiering in the United Kingdom's large-value payment system' (2017) Bank of England Working Paper No 676 < https://www.bankofengland.co.uk/-/media/boe/files/working-paper/2017/the-impact-of-detiering-in-th-uk-large-value-payment-system.pdf?la=en&hash=5A4F8D6FC3FC9C1003D2265EA351DA9DD67B6143> accessed 7 November 2020

[5] Prominent schemes are Bitcoin, Litecoin, Ether, and Ripples. Many are listed in 'List of Cryptocurrencies' (*Wikipedia*, last edited 2 November 2020) <https://en.wikipedia.org/wiki/List_of_cryptocurrencies> accessed 7 November 2020. See analysis by Saifedean Ammous, 'Can Cryptocurrencies Fulfil the Functions of Money?' (2016) Columbia University, Center on Capitalism and Society Working Paper No 92 <https://poseidon01.ssrn.com/delivery.php?ID=8980310680690200130841000940011151130240080490 6803> accessed 7 November 2020

[6] Most recently, see European Central Bank, 'Report on a Digital Euro' (October 2020) <https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf> accessed 7 November 2020; See also Bank of England, 'Central Bank Digital Currency: Opportunities, Challenges and Design' (Discussion Paper, March 2020) <https://www.bankofengland.co.uk/-/media/boe/files/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design.pdf?la=en&hash=DFAD18646A77C00772AF1C5B18E63E71F68E4593> accessed 7 November 2020; Bank of Canada, 'Contingency Planning for a Central Bank Digital Currency' (February 2020) <https://www.bankofcanada.ca/2020/02/contingency-planning-central-bank-digital-currency/> accessed 7 November 2020

[7] See the most recent overviews at Raphael Auer, Giulio Cornelli, and Jon Frost, 'Taking Stock: Ongoing Retail CBDC Projects' (2020) BIS Quarterly Review, March 2020, 97-98 < https://www.bis.org/publ/qtrpdf/r_qt2003z.htm> accessed 7 November 2020; Christian Barontini and Henry Holden, 'Proceeding with Caution – A Survey on Central Bank Digital Currency' (2019) BIS Monetary and Economic Department, BIS Paper No 101 < https://www.bis.org/publ/bppdf/bispap101.pdf> accessed 7 November 2020; Codruta Boar,

At the moment, the banknote is the only CeBM available to the public. Legislation conferring on central banks the power to issue banknotes, which are accorded the status of legal tender,[8] is common across the world. Such is the case eg in the United Kingdom under s. 1 of the Currency and Bank Notes Act 1954,[9] in the United States under s. 16(1) of the Federal Reserve Act[10] (in conjunction with s. 102 of the Coinage Act[11]), in Canada under s. 25(1) of the Bank of Canada Act[12] (in conjunction with s. 8(1) of the Currency Act)[13] as well as in the European Union under Article 128 TFEU.[14]

Henry Holden, and Amber Wadsworth, 'Impending Arrival – A Sequel to the Survey on Central Bank Digital Currency' (2020) BIS Monetary and Economic Department, BIS Paper No 107 < https://www.bis.org/publ/bppdf/bispap107.pdf> accessed 7 November 2020; George Calle and Daniel Eidan, 'Central Bank Digital Currency: An Innovation in Payments' (2020) (r3 White paper) < https://www.r3.com/wp-content/uploads/2020/04/r3_CBDC_report.pdf> accessed 7 November 2020; Central Bank Digital Currencies Working Group, 'Key Aspects Around Central Bank Digital Currencies: Policy Report' (2019) CEMLA Fintech Forum < https://www.cemla.org/fintech/docs/2019-06-KeyAspectsAroundBankDigitalCurrencies.pdf> accessed 7 November 2020; Johannes Duong, 'Overview of Central Bank Digital Currency – State of Play' (2020) SURF Policy Note, Issue No 158 < https://www.suerf.org/policynotes/12575/overview-of-central-bank-digital-currency-state-of-play> accessed 7 November 2020

[8] Euro Legal Tender Expert Group, 'Report of the Euro Legal Tender Expert Group (ELTEG) on the Definition, Scope and Effects of Legal Tender of Euro Banknotes and Coins' (2009) 4 <https://ec.europa.eu/economy_finance/articles/euro/documents/elteg_en.pdf> accessed 7 November 2020, defined the term by reference to mandatory acceptance in full face value in the discharge of debts.

[9] 1954 (2 and 3 Eliz 2 c 12)

[10] 1913, c 6, 38 Stat 251 (US)

[11] 1965, Pub L No 89-81, 79 Stat 254 (US)

[12] RSC, 1985, c B-2 (CA)

[13] RSC, 1985, c C-52 (CA)

[14] Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C326/47

Invariably, all such legislation was passed when a banknote was printed on paper. This article explores the question of whether, in principle, an electronic or digital banknote ('e-banknote') is a 'banknote' falling within the ambit of such legislation.[15] It addresses the question as a matter of general statutory interpretation, not linked to a specific legal system, in the context of technologies and institutional arrangements. Part 2 examines whether an e-banknote is a 'banknote' from a combined historical, functional, and linguistic perspective. Part 3 examines potential complying designs for an e-banknote, taking into account publicly available information on technology. Part 4 addresses complying architecture and issuance models in the context of existing institutional arrangements. The article concludes that a token-based e-banknote is indeed a 'banknote', so that central banks with banknote issuing power could and should address the optimal design and architecture. Questioning the suitability of cryptocurrencies, the article expresses a preference for a centrally issued design, particularly where it is based on quantum-grade randomness and available offline in emergencies. Regardless, an architecture under which both distribution and transfers of an e-banknote issued by the central bank are run by commercial banks appears to be the most advantageous.

Four contributions of the article are to be specifically noted. First, the article proposes a clear terminology to address concepts underlying digital currencies and access to CeBM. Second, we argue that a banknote may be 'written' electronically. Third, in examining designs, the article breaks away from the current shallow debate that effectively limits digital currencies to cryptocurrencies and makes a case for selecting a design that is appropriate from both a functional and legal perspective. Fourth, we point at the way monetary laws have been interpreted in the past as a general guide. In the final analysis, our interpretation aims at providing firm foundations to the e-banknote as an evolutionary rather than revolutionary concept, so as to align it with existing constitutional and legal frameworks.

2 The E-Banknote: Can a 'Digital Coin' Be a 'Banknote'?

A. What Is a Banknote

[15] This will be in line with the observation in ECB, 'Digital Euro Report' (n 6) 25, albeit with no real analysis, that 'the right to issue "euro banknotes" could be understood to encompass the right to determine the format or medium of "euro banknotes" so as to have them issued in a digital form.'

Not being defined by statute, the banknote is universally recognised as an unconditional promise in writing signed by a banker, engaging to pay on demand a sum certain in money to the bearer, being the holder in possession who presents it for payment. As it is transferrable from one person to another by delivery, free of claims and defences, the banknote is a negotiable instrument.[16] The promise to pay may, however, be implicit by the mere specification of the sum 'payable' on the banknote.[17] At present, banknotes are typically issued by central banks on either paper or polymer and constitute legal tender. Each is counterfeit-resistant and bears a serial number that distinguishes it from any other - even of the same value. The promise to pay is a mere formality,[18] as convertibility to precious metal coins or specie is banned so that the instrument is 'perpetually renewable'.[19]

Over the centuries, the banknote has been transformed. Having evolved from a genuine promise of a commercial banker to pay money to become legal tender, inconvertible, and hence a 'sterile' obligation of a central bank, the banknote continuously adapted to changing economic, technological, and institutional conditions.[20]

B. 'Digital Coins' and 'Digital Currency' – What Are They?

[16] See eg DAL Smout, *Chalmers on Bills of Exchange* (13th edn, Stevens & Sons 1964) 274; AW Rogers, *Falconbridge on Banking and Bills of Exchange* (7th edn, Canada Law Book 1969) 127; Charles Proctor, *Mann on the Legal Aspect of Money* (6th edn, OUP 2005) 25. A leading case is *Banco de Portugal v Waterlow and Sons, Ltd* [1932] AC 452 (HL) 483, 487 (and as to the promise, see also 478, 480). Whether negotiable instruments legislation applies to the banknote is outside the scope of the present discussion.

[17] *Banco de Portugal* (n 16) 487. For the form of the notes involved in that case see eg 460, 480.

[18] For viewing the promissory language as 'merely ornamental', see RG Hawtrey, 'The Portuguese Banknote Case' (1932) 42 Economic Journal 392, 395

[19] *Banco de Portugal* (n 16) 508. See also Article 3(2) of the Decision of the European Central Bank of 13 December 2010 on the issue of euro banknotes (ECB/2010/29) [2011] OJ L35/26, on holders' right to have a euro banknote exchanged at a National Central Bank for other banknotes of the same face value.

[20] For a historical discussion see Benjamin Geva, *The Payment Order of Antiquity and the Middle Ages: A Legal History* (Hart: Oxford and Portland Oregon, 2011) Chs 8, 10,11. See also Helmut Siekmann, 'Deposit Banking and the Use of Monetary Instruments' in David Fox and Wolfgang Ernst (eds), *Money in the Western Legal Tradition* (OUP 2016) 489

As a token representing value, [21] the electronic or digital[22] coin is a distinct entity consisting of data in the form of a unique string of bits. 'This string must have a numeric value, and must have an identity'.[23] Like physical coins and banknotes, digital coins are not paid out of bank accounts, so that their payment does not appear to require intermediation by banks. And yet, exactly as electronic funds transfers, they are paid over the cyber space. Each digital coin may be in the form of a total unspent amount in a wallet[24] or, as will be seen below, to one degree or another, a digital representation of what otherwise would be a distinct physical banknote.

Digital currency is an assortment of digital coins or, more specifically, a system under which digital coins are issued, transferred, and redeemed. A privately issued digital currency may have its own unit of account, fluctuating by reference to the value of an official unit of account, in which case it is self-anchored. Alternatively, it may be a 'claim-check' or stablecoin, either in a unit of account of an official currency or in the value of a specific commodity, whether or not it is backed by a reserve of such currency or commodity.[25]

[21] Practically, 'with properties that suffice to attest to and transfer ownership': Digital Dollar Foundation and Accenture, 'The Digital Dollar Project: Exploring a US CBDC' (2020) 10 <https://static1.squarespace.com/static/5e16627eb901b656f2c174ca/t/5ecfc542da96fb2d2d5b5f15/1590674759958/Digital-Dollar-Project-Whitepaper_vF.pdf> accessed 7 November 2020 (where the quoted language is part of the definition itself).

[22] We do not argue that 'electronic' and 'digital' are identical terms. However, in the present context, they are used interchangeably, with the use of 'digital' being substantially more prominent.

[23] Gideon Samid, *Tethered Money: Managing Digital Currency Transactions* (Elsevier Academic Press 2015) 105.

[24] Such a coin exists only as 'an identifiable address with a balance'. See Corinne Zellweger-Gutknecht, 'Developing the Right Regulatory Regime for Cryptocurrencies and other Value Data' in David Fox and Sarah Green (eds), *Cryptocurrencies in Public and Private Law* (OUP 2019) 57 , 86 n 160

[25] Samid, *Tethered Money* (n 23) 108. For risks created by global privately issued stablecoins, see Anastasia Melachrinos and Christian Pfister, 'Stablecoins: A Brave New World?' (2020) Banque de France Working Paper No 757 <https://publications.banque-france.fr/sites/default/files/medias/documents/wp757.pdf> accessed 7 November 2020

We find alternative definitions to be unsatisfactory. For example, Bitcoin mythological founder Satoshi Nakamoto defined an electronic coin as 'a chain of digital signatures' through which '[e]ach owner transfers the coin to the next'. [26] This defines more the mechanism under which the coin is transferred than the 'coin' itself, and yet envisions the latter as a discrete object. In a similar vein, definitions that focus on 'digital representations of value,'[27] are inadequate. They include account-based products in which the balance is expressed digitally[28] and are thus too broad. Such definitions cover monetary value credited to an account. In the digital age, unless qualified,[29] they also encompass credit posted to commercial bank accounts accessible from a digital device. Equally broad is a definition under which digital currency consists of '[m]onetary value stored electronically that is accepted as a means of payment and whose use is neither based on nor requires funds in a deposit or credit account in a

[26] Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (2008) 2 <https://bitcoin.org/bitcoin.pdf> accessed 7 November 2020

[27] Dong He, Karl Habermeier, Ross Leckow, et al, 'Virtual Currencies and Beyond: Initial Considerations' (2016) IMF Staff Discussion Note SDN/16/03, 8 <https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf> accessed 7 November 2020; Kiff et al, 'A Survey of Research on Retail Central Bank Digital Currency' (2020) IMF Working Paper No 20/104, 5 <https://www.imf.org/en/Publications/WP/Issues/2020/06/26/A-Survey-of-Research-on-Retail-Central-Bank-Digital-Currency-49517> accessed 7 November 2020. See also European Central Bank, 'Virtual Currency Schemes – A Further Analysis (2015) 25<https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf> accessed 7 November 2020. These are definitions for 'virtual currencies' – a term used (in a sense other than game-currency) to denote what we consider 'digital currencies'. See also in the United States: the *Uniform Regulation of Virtual-Currency Business Act*, drafted by the National Conference of Commissioners on Uniform State Laws and approved and recommended for enactment in all the States at its Annual Conference Meeting in its One-Hundred-And-Twenty-Sixth Year, San Diego, California July 14 - July 20, 2017, section 102(23).

[28] Indeed, the IMF Taxonomy Figure in He et al, 'Virtual Currencies' (n 27) 8 specifically covers Pay-pal and e-money balances.

[29] Among the three sources cited in n 11, at least the first two qualify it in a way that specifically excludes CoBM, but not other account-based systems.

financial institution'.[30] A balance-based 'electronic money' product,[31] issued by a commercial bank, falls into this definition. However, its record, accessible from a device without resort to the bank's computer system, can be viewed as premised on a decentralised bank account.[32] As such, it is a type of account-based product and not a digital coin.

A digital currency scheme means a system under which digital coins are issued, transferred, and redeemed. The rules under which such system operates constitute its protocol. We distinguish three schemes of digital currencies. A scheme under which a digital currency is issued, transferred, and redeemed over a distributed ledger is *decentralised*. Conversely, a scheme under which a digital currency is issued, transferred, and redeemed over a centralised ledger is *centralised*. Finally, a digital currency transferable under a decentralised protocol – such as over a distributed ledger and yet issued centrally – is *hybrid*.[33]

A centralised protocol (just like a decentralised protocol) does not depend on the intermediation of bank accounts and is thus entirely different from a centralised architecture in account-balance payment systems. Furthermore, payment in digital currency, made from one digital device to another, does not necessarily require the intermediation of a dedicated electronic network. Depending on its design, connectivity may be over the Internet or a telecommunication carrier. A centralised protocol may further necessitate the intermediation of either an operator of a central switch or a custodian acting as a virtual store or warehouse person for the coins.

[30] Ben Fung, Scott Hendry, and Warren E Weber, 'Canadian Bank Notes and Dominion Notes: Lessons for Digital Currencies' (2017) BOC Staff Working Paper 2017-5 <http://www.bankofcanada.ca/wp-content/uploads/2017/02/swp2017-5.pdf> accessed 7 November 2020

[31] CPSS, *Security of Electronic Money: Report by the Committee on Payment and Settlement Systems and the Group of Computer Experts of the Central Banks of the Group of Ten Countries* (Basle: BIS 1996) 5 <https://www.bis.org/cpmi/publ/d18.pdf> accessed 7 November 2020

[32] Alan L Tyree, 'The Legal Nature of Electronic Money' (1999) 10 JBFLP 273, 276.

[33] For this tripartite classification, see He et al, 'Virtual Currencies (n 27), where a third criterion – on top of issuance and transfer – is added *viz* 'mechanisms to implement and enforce internal rules on the use and circulation of the currency'.

Underlying decentralisation, the distributed ledger is an asset database that can be shared across a network of multiple sites, geographies, or institutions. Blockchain is an underlying technology, requiring the Internet to support and maintain its peer-to-peer network that enables digital implementation of a distributed ledger. Being a computerised ledger on a distributed network, it generates a single version of the record on each computer. In essence it is:[34]

> 'a type of a database that takes a number of records and puts them in a block … Each block is then "chained" to the next block, using a cryptographic signature. This allows block chains to be used like a ledger, which can be shared and corroborated by anyone with the appropriate permissions.'

Accuracy of the ledger is corroborated under a method determined under rules adhered to by participants. Record security and visibility to authorised users is ensured by cryptography.

A 'cryptocurrency' denotes a digital currency in which encryption techniques are used to regulate the generation of units of currency[35] and verify the execution of payment transactions on a decentralised network. [36] Cryptography is thus used in

[34] UK Government Chief Scientific Adviser, 'Distributed Ledger Technology: Beyond Block Chain' (2016) Government Office for Science Report, 17 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf> accessed 7 November 2020

[35] This distinctive feature is unfortunately missing in UK Jurisdiction Taskforce, 'Legal Statement on Cryptoassets and Smart Contracts (2019) The LawTech Delivery Panel, paras 24-34 <https://35z8e83m1ih83drye280o9d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/11/6.6056_JO_Cryptocurrencies_Statement_FINAL_WEB_111119-1.pdf>accessed 7 November 2020, where the focus (particularly in para 28) appears to be on the control of the asset (rather than on its generation) by cryptographic means.

[36] This definition slightly modifies the one from The Wolf of Crypto, 'Basic Cryptocurrency Starter Guide' (*Medium*, 18 September 2017) <https://medium.com/@Wolfofcrypto/basic-cryptocurrency-starter-guide-8f2071ea85de> accessed 7 November 2020. Specifically, we replaced 'transfer of funds' by the 'execution of payment transactions' to point at payment by the transmission of 'coins' rather than 'generic value' in the forms of funds. See also 'Cryptocurrency' (*Wikipedia*, last edited 3 November 2020) <https://en.wikipedia.org/wiki/Cryptocurrency> accessed 7 November 2020, stating '[a] cryptocurrency (or crypto currency) is a digital asset designed to work as a medium of

cryptocurrencies to express and protect the value of the coins (the sequence of the bits), to prevent counterfeiting and fraudulent transactions as well as to perform validation, execution, and recording. These functions are carried out on a distributed ledger, such as a blockchain. Thereon, each block contains a cryptographic hash or algorithm that links it to the previous block, along with a timestamp for the transactions from that block. The network allows online payments to be sent directly from one party to another without going through a bank or any other account-holding centralised counterparty.[37]

It is argued that developers of cryptocurrencies 'simply migrated the cryptographic tools used to safeguard communication and applied them to safeguard digital currency.' Thus, the argument continues, such developers made cryptocurrencies vulnerable to erosive cryptographic intractability. [38] Moreover, 'some of the most widespread cryptographic methods currently used in cybersecurity' are likely to become exposed to successful attacks by quantum computers.[39] This will undoubtedly undermine the integrity of cryptocurrencies. In the ongoing fight against counterfeiters and fraudulent copiers, centralised schemes are better positioned to apply superior defence measures to protect the integrity of the database as well as enhanced security procedures in both coin and identity verification upon redemption and in trade. [40]

exchange that uses strong cryptography to secure financial transactions, *control the creation of additional units*, and verify the transfer of assets' (emphasis added).

[37] Not every decentralised system is that of a cryptocurrency. For a visual demonstration of the point see He et al, 'Virtual Currencies' (n 27) 8, Figure 1. We do not adopt the taxonomy proposed by that figure.

[38] Samid, *Tethered Money* (n 23) 26.

[39] Sara Castellanos, 'Visa, JPMorgan Are Already Preparing for Potential Quantum Cyberattacks' *The Wall Street Journal* (New York, 9 October 2020) <https://www.wsj.com/articles/visa-jpmorgan-are-already-preparing-for-potential-quantum-cyberattacks-11602255213> accessed 7 November 2020

[40] See eg Samid, *Tethered Money* (n 27) 92-94 and cf 125-27, as well as 25, 98-100, albeit focusing on the advantage of paying with digital coins over that of paying in scriptural money, which may expose account data to hackers.

Bit-minted money is proposed as the answer to these drawbacks. Unlike a cryptocurrency, bit-minted money is not hinged on a mathematical riddle that even as it cannot be solved at present, may be solved in the future. Rather, bit-minted money, while utilised in schemes using crypto tools for messaging and storage, is fitted on a completely different foundation, thriving to randomness[41] - also known as quantum or pure randomness, premised on unpredictability.[42]

C. Does a Digital Coin Fall Into the Definition of a 'Banknote'?

The feasibility of paper money is 'associated with the two Sinic inventions of paper and printing'.[43] An ongoing process of improving printing, enhancing security features, and replacing paper by polymer, facilitated by technological advances, has been precipitated by a search for more savings and convenience as well as confidence, safety, and security.[44]

Throughout its evolution, the banknote has remained 'written', even as the meaning of 'written' has expanded to cover printed, stamped, embossed and in theory also engraved.[45] At the same time, we argue, the 'writing' requirement has been functional.

[41] For the superior protection of randomness premised on 'a cipher which use[s] no mathematical complexity but instead call[s] for large amounts of randomness' see eg Carsten Stöcker, 'Randomness: The Fix for Today's Broken Security' (*Medium*, 9 November 2017) <https://medium.com/@cstoecker/randomness-the-fix-for-todays-broken-security-39ea7dc3a89b> accessed 7 November 2020

[42] ibid

[43] AJ Toynbee, *A Study of History* (Abridgement of Volumes VII-X by DC Somervell, OUP 1957) 62

[44] See in general Don Cleveland IBNS LM-136A, 'History of Printed Money' <https://www.theibns.org/joomla/index.php?option=com_content&view=article&id=251&Itemid=127> accessed 7 November 2020; more specifically on existing security features see Jeff Desjardin, '10 Banknotes From Around the World, and Their Security Features" (*Visual Capitalist*, 18 June 2018) <https://www.visualcapitalist.com/10-banknotes-around-world-security-features/> accessed 7 November 2020; as well as Giesecke & Devrient, 'Security Features for Staying One Step Ahead of the Counterfeiters' (*Bankenoteinfo*) <http://banknoteinfo.net/security-features/> accessed 7 November 2020

[45] For example, under Schedule 1 to the Interpretation Act 1978 (UK) ch 30, 'writing' includes 'typing, printing, lithography, photography and other modes of representing or

In the case of the banknote, it is premised on the need to have a record, both as a matter of evidence to secure attribution, permanence, integrity, and authenticity, as well as to facilitate simple transferability. Once technology allows these functions to be performed through a novel medium, as is the case with the digital coin, there is no longer a reason to insist on the written format more than on the existence of a genuine obligation to pay metallic money. The accommodation to a changed environment ought not to be limited to the nature of the obligation and bypass the media.

The definition of a banknote[46] does not include an independent requirement of being a tangible object. [47] Rather, the tangibility feature derives from the 'writing' requirement as envisioned prior to the electronic age. At that time, there was no way of 'writing' on an intangible media; writing in the air was (and is) meaningless. However, with new technologies, it has become possible to write on something intangible. We write an email much the same as we write a postcard or a letter. What paper or any other tangible media gives to writing is permanence – which technologically can now be accorded to an intangible record in the cyberspace. Accordingly, we argue, notwithstanding the fact that it is a uniquely generated item of information and as such, an intangible, the digital coin may nevertheless be seen as 'written', or at least, functionally equivalent to 'written'.

Liability on a banknote requires signature. Generally speaking, a 'signature' may be written, lithographed, facsimiled or stamped on a document (or anything else tangible) with the intent of authenticating liability on a contract. [48] The key is, however, a

reproducing words in a visible form ...'. A creative interpretation may treat words in a permanent record 'visible' on a computer screen as satisfying the writing requirements: Leif Gamertsfelder, 'Electronic Bills of Exchange: Will the Current Law Recognise Them?' (1998) 21:2 UNSWLJ 566

[46] See Subpart 2 (A)

[47] Under UCC 1-201(43), 'writing' is defined to include 'printing, typewriting, or any other intentional reduction to tangible form.' This is in contrast to UCC 1-201 (31), under which 'record' is defined to mean 'information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.' It is recommended to revise UCC Article 4A by expanding 'writing' to include 'medium stored in an electronic or other medium and retrievable in perceivable form.' Such a distinction is for the purposes of the interpretation of the Uniform Commercial Code. Nonetheless, it is not flawless, as for example, it is hard to understand why an inscription is on a record and not in writing.

permanent record for the authentication of liability. Accordingly, the electronic authentication of an electronic record that substitutes writing will satisfy the signature requirement.

Observations to such ends were already made in the common law.[49] In one case, the court did not doubt that 'if a party creates and sends an electronically created document then he will be treated as having signed it to the same extent that he would in law be treated as having signed a hard copy of the same document.'[50] In another case, the court considered an email as written.[51]

Accordingly, a claim-check digital coin, being a claim to a specified 'quantity' denominated in the official unit of account, falls into the definition of a banknote. This is true as long as the signatory issuing bank is unconditionally liable to pay to the bearer on demand a sum certain in the stated fiat money. Moreover, the claim check digital currency must fulfil the *function* of a 'banknote' as discussed below.

D. Does the Digital Coin Fulfil the Function of a 'Banknote'?

As a negotiable instrument, the paper banknote is both a chattel and obligation, or else, it is both a chose in possession and a chose in action.[52] As a 'document in which a right is incorporated in such a way that it cannot be claimed nor transferred to others ...without the document' it can be theorised on the same basis as the Germanic *Wertpapier*, [53] which would have fallen under Article 965 of the *Swiss Code of*

[48] See eg Rogers, *Falconbridge on Banking* (n 16) 440-441, 443, 444

[49] Simon Gleeson, *The Legal Concept of Money* (OUP 2018) 176 para 9.47.

[50] *Pereira Fernandes v Mehta* [2006] 1 All ER (Comm) 885 para 28

[51] *Golden Ocean Group v Salgocar Mining Industries* [2012] EWCA Civ 265

[52] Relating both to 'a chattel, a tangible scrap of paper' and 'a bundle of contracts', a claim to a negotiable instrument thus involves not only 'the right to possess a thing but [also] the right to sue several persons [liable to it]': Zechariah Chaffee Jr, 'Rights in Overdue paper' (1918) 31 Harv L Rev 1104, 1109

Obligations.[54] Stated otherwise, the obligation on a banknote (sterile as it is nowadays) is embodied in the chattel, so as to inure to the benefit of the possessor of the chattel.

Indeed, the transfer of possession is a requirement to the transfer of title to – and hence payment in – money.[55] Accordingly, for the digital coin to function as a written banknote, it must be not only be 'signed' and 'written', but also embodied in an object of property, capable of being moved from the exclusive control of one person to that of another.

As for the first characteristic, that of an object of property, common law recognises proprietary features of an intangible right even where it is not a chose in action, as long as the right is 'definable, identifiable by third parties[,] capable in its nature of assumption by third parties and [has] some degree of permanence or stability.'[56] Accordingly, it was held that cryptocurrencies are to be treated as property.[57]

[53] According to Denis V Cowen and Leonard Gering, *The Law of Negotiable Instruments in South Africa Vol. One: General Principles* (5th edn, Juta 1985) 94, the word 'wertpapier' cannot be well translated to English, so that words such as 'security' or 'commercial paper' do not convey its accurate meaning.

[54] *Swiss Code of Obligations*: English Translation of the Official Text (Swiss-American Chamber of Commerce 2003). On the German *Wertpapier,* see in general L Dabin, *Fondements du droit cambiaire Allemand* (Faculté de droit de Université de Liège 1959). For a comprehensive discussion on the German conceptual framework, and as to whether it sheds additional light on the nature of a negotiable instrument, see Cowen & Gering, *Negotiable Instruments* (n 53) 79-98, where a slightly different translation, albeit to the same effect, of the Swiss provision is reproduced at 82. Their negative conclusion as to whether the *Wertpapier* sheds additional light on the nature of a negotiable instrument at 110 is criticised by JT Pretorius' book review in (1986) 103 SALJ 151, 154-56. On the negotiable instrument as *Wertpapier* see also FR Malan, JT Pretorius, and SF Du Toit, *Malan on Bills of Exchange, Cheques and Promissory Notes in South African Law* (5th edn, LexisNexis 2009) 4, 7.

[55] David Fox, *Property Rights in Money* (OUP 2008) paras 3.32-3.42.

[56] *National Provincial Bank v Ainsworth* [1965] AC 1175 [1247]-[1248], [1965] 2 All ER 472 [494] (HL, per Lord Wilberforce)

[57] First in *B2C2 Limited v Quoine PTE Ltd* [2019] SGHC (I) 03 (Singapore International Commercial Court) para 142; followed in *AA v Persons* [2019] EWHC 3556 (Comm) para 61. In reaching its conclusion, *AA v Persons* also treated the UK Jurisdiction Taskforce, 'Cryptoassets and Smart Contracts' (n 35) as persuasive and yet not being an authoritative statement of the law (para 27). For a full discussion see *AA v Persons* paras 35–85 (and, to a

Civilians may have been more dogmatic.[58] Nevertheless, drawing on Gaius' distinction between *res corporales* and *res incorporales*, Nicholas maintains the existence of 'abstract things, such as a debt or *a right of way*' that cannot be possessed and yet can be owned.[59] He concludes that the 'the law of things includes all those rights which are capable of being evaluated in money terms.'[60]

The fulfilment of the second characteristic, that of transferability from hand to hand, requires, first, an exploration of the mechanics of payment in digital currency and, second, an assessment of the legal treatment of the mechanism. For its part, the mechanics of payment in a digital coin depends on the specific design of the coin and its underlying scheme. A common denominator for all mechanisms is the use of a telecommunication network and the availability of a validating intermediary, designed to prevent double payment. To both such ends, several scenarios are available:

1. Being in control of a digital coin 'affixed' to a single Internet domain, for which it attorns to the payer. A 'bailee'[61] complies with the payer's instructions and executes them by attorning to the payee, thereby causing 'possession' in the

lesser extent, also paras 86–99). For mostly earlier scholarly discussion see David Fox, 'Cryptocurrencies in the Common Law of Property' in Fox & Green, *Cryptocurrencies* (n 24) 139, 152-54 paras 6.38-6.41. See also Christopher Hare, 'Cryptocurrencies and Banking Law: Are There Lessons to Learn?' in Fox & Green, *Cryptocurrencies* (n 24) 229, 237 n 53; Gleeson, *The Legal Concept of Money* (n 49) 166 para 9.10. Another discussion is by G A Walker, 'Financial Technology Law - A New Beginning and a New Future' (2016) 50:1 TIL 137. For another perspective, see Sarah Jane Hughes, 'Property, Agency, and the Blockchain: New Technology and Longstanding Legal Paradigms' (2019) 65 Wayne L Rev 57

[58] See in detail eg Daniel Carr, 'Cryptocurrencies as Property in Civilian and Mixed Legal Systems' in Fox & Green, *Cryptocurrencies* (n 24) 177

[59] Barry Nicholas, *An Introduction to Roman Law*, (Clarendon Press 1962) 106. Indeed, 'incorporeal things' are recognised by the Institutes: *The Institutes* (Book II Title II) translation reproduced in RW Lee, *The Elements of Roman Law* (4th edn, Sweet & Maxwell 1956) 114 and discussion at 110

[60] ibid 98 (emphasis added)

[61] We agree with the UK Jurisdiction Taskforce, 'Cryptoassets and Smart Contracts' (n 35) paras 87-88 that strictly speaking no 'bailment' can exist with respect to a 'digital banknote', except that we address below the option of 'control' as a functional equivalent to 'possession.'

coin to be transferred from the payer to the payee. Alternatively, such a system may be viewed as run by a central switch operator which, at the instruction of the payer, transfers the control of the coin from the payer to that of the payee; [62]

2. A 'coin' in the form of an unspent transaction output (UTXO)[63] in the payer's wallet, reflecting earlier transactions, is transformed into a new UTXO in the payee's wallet. Where the payer does not use up the entire UTXO, payment is carried out by splitting the payer's UTXO into two UTXO's: one in the sum of payment going to the payee's wallet, and the second in the amount of the balance of the UTXO remaining in the payer's wallet.[64]

[62] This method of payment is put forward by WingCash, now Open Payment Network (OPN):<https://wingcash.com/> and <https://openpaymentnetwork.us/, > both accessed 7 November 2020, discussed in Subpart 3(C).

[63] The term is explained in eg 'What's a UTXO? A Guide to Unspent Transaction Output (UTXO)' (*Komodo*, 26 July 2018) <https://komodoplatform.com/whats-utxo> accessed 7 November 2020

[64] This is eg Nakamoto, 'Bitcoin' (n 26). See also eg Stuart Hoegner, 'What is Bitcoin?' in Stuart Hoegner (ed), *The Law of Bitcoin* (iUniverse 2015) 1; Neil Guthrie, 'The End of Cash? Bitcoin, the Regulators and the Courts' (2014) 29 BFLR 355. For its mechanics, see Jonathan Levin, 'Bitcoin: New Plumbing for Financial Services' (*Coindesk*, 29 November 2014), <http://www.coindesk.com/bitcoin-new-plumbing-financial-services/> accessed 7 November 2020. See also Nicholas Wenker, 'Online Currencies, Real-World Chaos: The Struggle to Regulate the Rise of Bitcoin' (2015) 19 Tex Rev L & Pol 145; Jacob Hamburger, 'Bitcoins vs. State Money Transmission Laws: Protecting Consumers or Hindering Innovation?' (2015) 11 J L Econ & Pol'y 229. See also 'Bitcoin' (*Wikipedia*, last edited 2 November 2020), <https://en.wikipedia.org/wiki/Bitcoin> accessed 7 November 2020; 'What Is Bitcoin?' (*Coindesk*, last edited 18 August 2020) <http://www.coindesk.com/information/what-is-bitcoin> accessed 7 November 2020; Benjamin Wallace, 'The Rise and Fall of Bitcoin' (*Wired*, 23 September 2011) < https://www.wired.com/2011/11/mf-bitcoin/> accessed 7 November 2020; 'Blockchains - The Great Chain of Being Sure About Things' (*The Economist*, 31 October 2015) < https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things> accessed 7 November 2020. See also 'How bitcoin works' (*Wikipedia*, last edited 4 February 2018) <https://en.bitcoin.it/wiki/How_bitcoin_works> accessed 7 November 2020

3. The payer sends from his or her device to the payee's device a 'coin' or any split of it. The payee may (but is not required to) validate the coin authenticity with the 'mint'.[65]

Payment under each scheme is premised on the transfer of control of the digital coin. The functional equivalence with the transfer of possession of a paper banknote is obvious. For example, in a case of digital coins accessed by keys, Fox speaks of a presumption in favour of control by the public key holder as the 'intangible analogue of the familiar (…) presumption that possession is evidence of title'.[66]

Undoubtedly, this principle guided the drafters of the UNCITRAL Model Law on Electronic Transferable Records (2017)[67] (MLETR). Thereunder, Article 11 MLETR treats 'exclusive control of [an] electronic transferable record' as a functional equivalent of 'the possession of a transferable document or instrument.' 'Transferable document or instrument' is defined in Article 2 MLETR to mean:

> a document or instrument issued on paper that entitles the holder to claim the performance of the obligation indicated in the document or instrument and to transfer the right to performance of the obligation indicated in the document or instrument through the transfer of that document or instrument.

In turn, Article 2 MLETR defines 'electronic record' to mean 'information generated, communicated, received or stored by electronic means'. [68]

Article 8 MLETR renders information that is 'accessible so as to be usable for subsequent reference' the functional equivalent of 'writing'. Similarly, MLETR's Article 9 provides that where 'a reliable method is used to identify [a] person and to indicate that person's intention in respect of the information contained in [an]

[65] This is BiMint, further discussed in Subpart 3(C)

[66] David Fox, 'Cryptocurrencies in the Common Law of Property' in Fox & Green, *Cryptocurrencies* (n 24) 157 para 6.50

[67] Model Law on Electronic Transferable Records, A 72/17, UNCITRAL, 2017 <https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/mletr_ebook_e.pdf> accessed 7 November 2020

[68] For when an electronic record becomes an 'electronic transferable record' see MLETR (n 67) Article 10(1)

electronic transferable record', a legal signature requirement by that person is satisfied.

Article 11(1) MLETR goes on to provide that the 'exclusive control of [an] electronic transferable record' established by 'a reliable method', which also identifies the person in control, meets a legal requirement for 'the possession of a transferable document or instrument'. Additionally, under Article 11(2) MLETR, 'the transfer of control over [an] electronic transferable record' is the equivalent for the 'transfer of possession of a transferable document or instrument'.[69]

Indeed, the banknote is a signed transferable document or instrument, entitling its holder to claim from the signer the performance of an obligation indicated therein. For its part, in a digitised form, the banknote is an electronic transferable record, authenticated by an identified person, which is under the exclusive control of the one entitled to enforce the obligation it contains. Transferability in the former format is by the physical delivery of the paper banknote, while transferability in the latter format is by the transfer of control over the electronic record of the banknote.

In conclusion, a digital coin falling into the definition of a 'banknote' may fulfil the function of a paper banknote. Its transferability to a bona fide transferee for value free of any claim or defence is a quality to be accorded to it by the law.[70]

E. The Digital Coin as an E-Banknote: Monetary Law and the History of the Banknote

Throughout its history, the written banknote transformed in substance in response to ongoing advancing technological conditions, changing market demand, and evolving

[69] In this context, Article 15 of MLETR (n 67) provides that: 'Where the law requires or permits the endorsement in any form of a transferable document or instrument, that requirement is met with respect to an electronic transferable record if the information required for the endorsement is included in the electronic transferable record and that information is compliant with the requirements set forth in articles 8 and 9.' This, however, is irrelevant for the banknote, which is payable to the bearer and thus transferable by mere delivery.

[70] *Miller v Race* (1758), 1 Burr 452, 97 ER 398 [401]

institutional frameworks. With technology facilitating the change in the media, the move to digital is just another step in the same process.

The role of statutory law in the evolution of the banknote was not to lead, but rather to facilitate, developments for societal benefit. Hence, statutes and constitutional powers in relation to money ought to be interpreted in the spirit of accommodating new developments, harnessing them for the protection of the public, but not hindering them.

In England, for example, the law followed the emergence of banknotes, originally issued in the course of the 17th century by goldsmiths as receipts for moneys deposited with them.[71] Even in the absence of an explicit note issuing power under its establishing statute,[72] the Bank of England began, shortly after its establishment, to issue to depositors, 'probably to a very considerable extent',[73] notes payable to the bearer.[74] These were characterised by Lord Mansfield as 'as much money, as guineas themselves are; or any other current coin, that is used in common payments, as money or cash'.[75] The Bank of England notes were made legal tender by statute as late as under s. 6 of the *Bank of England Act,* 1833.[76]

For its part, the issuance of the banknote in the USA, first by practice then by statute, bypassed a rigid interpretation of a federal constitutional power under Article 1 Section 8 of the US Constitution 'to coin money',[77] which has been taken to give the

[72] The Ways and Means Act 1694 (UK) 5 & 6 Will & Mar, c 20, s XIX

[73] *Bank of England v Anderson* (1837), 3 Bing (NC) 589 [654], 132 ER 538 [562], per Tindal CJ (CP)

[74] JM Holden, *The History of Negotiable Instruments in English Law* (Reproduced by WM W Gaunt & Sons 1993, The Athlone Press 1955) 89-90

[75] *Miller* (n 70)

[76] (UK) 3 & 4 Will IV, c 98

[77] For constitutional aspects of money issuance in the US see eg Thomas Wilson, *The Power 'to Coin' Money: The Exercise of Monetary Powers by the Congress* (ME Sharpe 1992); Ali Khan, 'The Evolution of Money: A Story of Constitutional Nullification' (1999) Univ Cincinnati Law Rev 393. The full text of the US Constitution is at eg

power to issue only full-bodied metallic money.[78] Market (and government) demands were met by the issuance of banknotes, originally by state chartered banks with no statutory basis, later by national banks, and finally by the Federal Reserve – first by its regional Reserve Banks and subsequently by the Board of Governors of the Federal Reserve System.[79] All such banknotes have served as money, even as only the latter are accorded legal tender status. All were held not to be in violation of the US Constitution.

Reflecting on this history, Khan observed that:

> Money is a living creature of the market and its form changes to facilitate commercial transactions in an ever more efficient, convenient, safe manner. As such, most innovations in monetary practices are attributable to the decisions of the market…[80]

Accordingly, as far as the banknote is concerned, 'entrenchment in the legal system was the affirmation of a simple monetary tradition: the market creates, modifies, and recreates the concept of money. The law simply recognises and changes, often *ex post facto*.'[81] An obvious takeaway from this is that 'no legal text, not even the most authoritative, such as the United States Constitution can fully predict how the future will discard some of the most obvious paradigms.'[82]

<https://www.archives.gov/founding-docs/constitution-transcript> accessed 7 November 2020

[78] Khan, 'Evolution of Money' (n 77) 393

[79] For a succinct summary see eg Warren E Weber (formerly of the Federal Reserve Bank of Minneapolis), 'Government and Private E-Money Like Systems: Federal Reserve Notes and National Bank Notes' (2015) BOC Working Paper 2015-18, 3 <https://www.bankofcanada.ca/wp-content/uploads/2015/06/wp2015-18.pdf> accessed 7 November 2020: 'Throughout most of U.S. history, bank notes have been issued either solely by private banks or solely by the government through the Federal Reserve System, the central bank.'

[80] Khan, 'Evolution of Money' (n 77) 396, quoting Cyril James, 'International Cooperation in the Field of Money: A Strand of Economic History in Money and the Law 1' (1945) 1-2

[81] Khan, 'Evolution of Money' (n 77) 414

[82] ibid 397

These observations are confirmed by the shifting nature of the banknote - first in substance, and ultimately, we argue, in form. Principles of law that recognised the paper banknote, even in the absence of a statute, are good to recognise the e-banknote as a matter of statutory interpretation of any statute conferring banknote issuing power.

3 POTENTIAL TECHNICAL DESIGNS OF E-BANKNOTE SCHEMES

A. Introduction

A digital money that is privately issued is often referred to as 'virtual currency'.[83] This contrasts with what is known as a 'central bank digital currency' or 'retail CBDC'[84] ('rCBDC')[85] scheme, where the central bank either issues directly, or possibly fully

[83] See eg Benjamin Geva, 'Disintermediating Electronic Payments: Digital Cash and Virtual Currencies' (2016) 31: 12 JIBLR 661, 664-666, albeit acknowledging that uniform terminology is not universally accepted. For the adherence of the ECB to that term in the proposed meaning, see originally European Central Bank, 'Virtual Currency Schemes' (2012) 13 <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf> accessed 7 November 2020, and as amended in ECB, 'Virtual Currency Schemes' (n 27) 25. Finally, according to Phoebus L Athanassiou, *Digital Innovation in Financial Services – Legal Challenges and Regulatory Policy Issues* (Kluwer Law International BV 2018) 77, 'virtual currencies" are 'digital representations of value, which despite not being issued by a central bank or another public authority, nor "attached" to a fiat currency (subject to notable exceptions) are voluntarily accepted by natural or legal persons, as means of exchange, and which are stored, transferred and traded electronically, without a tangible, real-world representation'. However, we do not share his view that lack of 'attachment' to a fiat currency is a normal feature, as this will exclude claim-checks to fiat currencies or stablecoins. At the same time, his view on the matter is not unique: denomination in its own unit of account appears to be an element in the definition of 'virtual currency' (that is, privately issued digital currency) in He et al, 'Virtual Currencies' (n 27) 7

[84] Athanassiou, *Digital Innovation* (n 83) 185 generically defines CBDCs as: 'centrally issued digital equivalents of *fiat* money (…) that are not intended as parallel units of account, which fulfil some of the functions of money (namely as means of payment and stores of value), and which can facilitate proximity and long-distant payments alike.' However, we find the qualification in the definition to be puzzling, as CBDC is certainly used as a medium of exchange as well.

backs the issuance of, digital currency available to the public at large. Under the first option, the central bank, as the issuer, may nevertheless delegate functions to the private sector. Particularly, it may distribute the e-banknotes to the public through commercial banks and/or other intermediaries, exactly like it presently distributes physical banknotes. Alternatively, under the second option, a central bank may authorise licensed entities, particularly commercial banks, to issue their own banknotes, while fully backing them with a 100% reserve of CeBM. Various options of these architecture and issuance models are discussed in Part 4. This part lays down design options.

B. Token-Based vs. Account-Based Schemes

In light of the common use of 'scriptural money', there is an inclination to address rCBDC as an amendment to, or correction of, scriptural money, by way of making scriptural CeBM available to the public at large, rather than only to (large) commercial banks. In this context, account-based schemes are discussed as a rCBDC option. In the simplest sense, such schemes will allow members of the public to hold accounts with the central bank similar to the accounts held at the central bank by (large) commercial banks.

In Subpart 2 (B), we distinguished between a digital coin and an account-based product. The former is a distinct entity consisting of data in the form of a unique string of bits expressing a specified number of units of value. The latter reflects generic value.[86] Anonymity of the payer is easier to instil in a token-based scheme. Indeed, in comparison with payment by transferring funds, payment in token-based digital currency works like payment in cash: '[t]he value of the transaction is verified regardless of the identity of the payer', even without exposing the payer's hackable account.[87] What matters is the authenticity of the payment objects, rather than the availability of funds to the payer. Hence, we argue that token-based schemes mimic the features of banknotes more closely than account-based schemes.

We also go further and argue that access by the public to CeBM in the form of e-banknotes, being token-based products, is more beneficial than access to scriptural

[85] A 'wholesale' scheme is for the settlement of interbank payment and is outside the scope of the present discussion.

[86] For discussion of account vs token-based approaches see Bank of England, 'CBDC' (n 6) 46-47

[87] Samid, *Tethered Money* (n 23) 50

CeBM, whether or not the latter is viewed as a rCBDC product. Moreover, a token-based system maximises the advantages to be drawn from new technologies.

The so-called account-based rCBDC schemes are said to fall into two broad categories:

1. 'Plain sovereign money'[88] schemes, under which CeBM becomes available to members of the public in accounts on the books of the central bank.[89]

2. 'Electronic money' schemes under which digital devices 'loaded' with CeBM are distributed to the public[90] through commercial banks.[91]

Both proposals would impose 'a large administrative burden' on the central bank that 'could distract it from its other functions in [regulating] and managing monetary policy.' Furthermore, the central bank, 'a state-owned enterprise', would undertake pure market functions, in which it 'would have no commercial incentive to innovate

[88] Beware of inconsistent use of terminology. Andrew Jackson, 'Sovereign Money - Paving the Way For a Sustainable Recovery' (2013) Positive Money <https://positivemoney.org/wp-content/uploads/2013/11/Sovereign-Money-Final-Web.pdf> accessed 7 November 2020 uses the term to denote central bank money distributed directly and gratuitously to business to fund infrastructure projects.

[89] For now, this is of course contrary to specific statutory limits on the eligibility for holding an account with the central bank, such as under Article 17 of Protocol (No 4) in the Statute of the European System of Central Banks and of the European Central Bank [2016] OJ C202/230. See also s 18 (1) (l.1) and (l.3) of the Bank of Canada Act (n 12)

[90] We suppose such a scheme was implemented in Ecuador, though it is not described with great precision by Everett Rosenfeld, 'Ecuador becomes the first country to roll out its own digitalcash' *CNBC* (9 February 2015) < https://www.cnbc.com/2015/02/06/ecuador-becomes-the-first-country-to-roll-out-its-own-digital-durrency.html#:~:text=In%202000%2C%20Ecuador%20moved%20to,system%20again%E2%80%94using%20digital%20currencies> accessed 7 November 2020

[91] For electronic money, see CPSS, *Security of Electronic Money* (n 31), particularly at 5. For e-money redeemed in CoBM, see Tobias Adrian and Tommaso Mancini Griffoli, 'The Rise of Digital Money' (2019) IMF Fintech Note No 19/001, 4 < https://www.imf.org/en/Publications/fintech-notes/Issues/2019/07/12/The-Rise-of-Digital-Money-47097> accessed 7 November 2020

[payment] services'.[92] Accordingly, under a variation of the first proposal, customers' accounts on the books of the central bank would be operated through, and managed by, commercial banks.[93]

The ECB Digital Euro Report is cognisant of the point. As 'an electronic form of central bank money accessible to all citizens and firms', and complementing cash and central bank deposits, the digital euro is defined by the Report to denote 'a liability of the Eurosystem recorded in digital form.'[94] This rejects the availability of the digital euro as a simple deposit with a central bank. At the same time, albeit contradicting itself, side by side with the token-based option, the Report keeps open the option of an account-based product that 'could be implemented by opening accounts directly with the Eurosystem or through supervised intermediaries.' [95]

Central bank scriptural money, particularly in the form of 'sovereign money,' may not be easily accessible outside the country of the currency, especially to non-residents. Regardless, public access to central bank scriptural money side by side with public access to commercial bank money could be confusing. At the same time, exclusive public access to scriptural central bank money has monetary policy implications. In a way, it goes to a radically different model of monetary system and banking. Such a model was first envisaged a long time ago, albeit as a mode of full-reserve banking, under which commercial banks maintain 100% reserve of CeBM and do not create

[92] Ben Dyson and Graham Hodgson, 'Digital Cash: Why Central Banks Should Start Issuing Electronic Money' (2016) Positive Money, 15 http://positivemoney.org/wp-content/uploads/2016/01/Digital_Cash_WebPrintReady_20160113.pdf accessed 7 November 2020

[93] For a precedent from Sri Lanka, albeit for investors' securities accounts operated by intermediaries on the books of the central bank, see Payment & Settlement Systems Act, No 28 of 2005, Chapter II Securities Accounts, ss 6-10 <https://www.cbsl.gov.lk/sites/default/files/cbslweb_documents/laws/acts/en/Payment_settlement_sys_act.pdf> accessed 7 November 2020. This variation differs from the 'electronic money scheme' in envisioning customers' accounts on the books of the central bank, rather than CeBM money booked in a master account with the central bank and loaded on customers' digital devices.

[94] ECB, 'Digital Euro Report' (n 6) 2, 6

[95] ibid 25

CoBM beyond such reserve.[96] An alternative model, under which the public would have access to CoBM backed by fractional reserve, as well as to either CeBM[97] or CoBM backed by full reserve, is bound to only confuse the public.

In any event, an ‘account-based [system] (…) uses a reconciliation-intensive, message-based approach to adjust entries in a ledger’,[98] in which ‘the operator of the system authenticates the sender to ensure authorization to update account balances on a potentially centralised account ledger.’[99] Conversely, since ‘[i]n a token-based system, the token contains all information necessary for the recipient to verify the legitimacy of the transaction (…)[,] the recipient can verify [on his or her own] the object transferred (i.e., the token)’,[100] which brings efficiency gains.

Finally, without an identity tied to it, a figure recorded in a bank's server in the form of a bit string could easily be changed by a hacker who penetrates into the bank's computer.[101] ‘It is this very fact that allows a hacker to sneak into the [bank] computer and alter the figure from $1.00 to $100.00 or to withdraw whatever he wishes.’[102] Conversely, inasmuch as its unique bit string expresses its identity, a digital coin is less exposed to alteration and is less hackable.[103]

[96] Patrizio Lainà, ‘Proposals for Full-Reserve Banking: A Historical Survey from David Ricardo to Martin Wolf’ (2015) 4:2 Economic Thought 1, 12 <http://et.worldeconomicsassociation.org/files/WEA-ET-4-2-Laina.pdf> accessed 7 November 2020

[97] For such a dual system see Dyson & Hodgson, ‘Digital Cash’ (n 92) 25 – 28

[98] Digital Dollar Foundation & Accenture, ‘Digital Dollar Project’ (n 21) 10

[99] ibid 18

[100] ibid 17

[101] See in general Martin Carnogursky, ‘Metadata: A Hacker's Best Friend” (*Sweepatic Blog*, 25 July 2017) <https://blog.sweepatic.com/metadata-hackers-best-friend/> accessed 7 November 2020

[102] Samid, *Tethered Money* (n 23) 25

[103] Even as this risk exists, albeit to a lesser extent, in relation to cryptocurrencies. See eg Mike Orcutt, ‘Once Hailed as Unhackable, Blockchains Are Now Getting Hacked’ (*Technology Review*, 19 February 2019)

For all these reasons, we are critical of account-based schemes and confine the subsequent analysis to token-based schemes.

C. rCBDC-Proposals

(i) Forerunners

A few specific central bank cryptocurrency schemes have been floating around.[104] In the US, proposals have been made for Fedcoin, a central bank-issued, centrally created cryptocurrency, to be available to the public at large.[105] Digital coins would be centrally issued on a blockchain-style decentralised ledger, but nevertheless with the central bank being in full control of quantity, timing, and fixed value in denominations of the national fiat currency unit of account. Effectively, transactions would be validated by an independent notary nominated by the central bank.[106] A similar

<https://www.technologyreview.com/2019/02/19/239592/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/> accessed 7 November 2020

[104] See Morten Bech and Rodney Garratt, 'Central bank cryptocurrencies' (2017) BIS Quarterly Review, 55 <https://www.bis.org/publ/qtrpdf/r_qt1709f.pdf> accessed 7 November 2020. See also Katrik Hegadekatti, 'Towards Regional Monetary Unions Through Blockchain Networks' (2017) MPRA paper No 82838 <https://mpra.ub.uni-muenchen.de/82838/> accessed 7 November 2020; Heike Mai, 'Why Would We Use Crypto Euros? Central Bank-Issued Digital Cash – A User Perspective' (2018) Deutsche Bank Research, EU Monitor - Global Financial Markets < https://www.dbresearch.com/PROD/RPS_EN-PROD/PROD0000000000462095/Why_would_we_use_crypto_euros%3F_Central_bank-issued.pdf?undefined&realload=AUZhed5TZJrd66fm7bUNX5nzqhETkSQKYFU3hggUfq1yGmBeOh9ffx7iGDKwM7VgffZiG4jDkN7Sk1Sjl6sCVg==> accessed 7 November 2020. Finally, cf Digital Dollar Foundation & Accenture, 'Digital Dollar Project' (n 21) 11, speaking of a 'new transactional infrastructure such as distributed ledger technology', but failing to elaborate or be otherwise specific.

[105] See eg Wendy McElroy, 'Fedcoin: The U.S. Will Issue E-Currency That You Will Use' (*Bitcoin,* 12 January 2005) <https://news.bitcoin.com/fedcoin-u-s-issue-e-currency/> accessed 7 November 2020

[106] Victoria Dodev, 'On the (Un)Feasibility of Fedcoin: Implementing a Central Bank Backed Digital Currency in the United States' (2018) SSRN <https://ssrn.com/abstract=3642880> accessed 7 November 2020

proposal was made in the UK for RSCoin.[107] For its part, interest in FedCoin has recently been revived.[108]

Another proposal is for a NationCoin, a ‘Regulated and Sovereign Backed Cryptocurrency’ (‘RSBC’). The scheme envisages cryptocoins, which as with Bitcoin, would be created by, and transacted over, a blockchain. Upon their creation, cryptocoins would be stored and released to the public by a Digital Asset Reserve as RSBC, at the fixed value of the national unit of account. Transactions would be verified by ‘miners’ who would be paid freshly minted cryptocoins.[109]

(ii) Libra[110]

Proponents of cryptocurrencies are attracted to the amenability of a rCBDC regulated by blockchain to an algorithmic monetary policy.[111] A prominent cryptocurrency project is that of the most recent version of Libra, under which a single-currency stablecoin is backed by a reserve consisting of cash or cash equivalent in the given

[107] See George Danezis and Sarah Meiklejohn, ‘Centrally Banked Cryptocurrencies’ (2015) University College London <https://eprint.iacr.org/2015/502.pdf> accessed 7 November 2020. In part, this article is too technical to the uninitiated in computer science and related subjects (including myself). ‘RSCoin is the core of a system of scalable and auditable transactions, not a full product’ which thus could be used as a basis for either a retail or wholesale product (Email message to the author from George Danezis, dated 4 December 2017).

[108] See eg Ann Saphir, ‘Fedcoin? The U.S. Central Bank Is Looking Into It” (*Reuters*, 5 February 2020) <https://www.reuters.com/article/us-usa-fed-brainard/fedcoin-the-u-s-central-bank-is-looking-into-it-idUSKBN1ZZ2XF> accessed 7 November 2020

[109] Kartik Hegadekatti and Yatish S G, ‘Generation, Security and Distribution of NationCoins by a Sovereign Authority’ (2016) SSRN <https://ssrn.com/abstract=2888347> accessed 7 November 2020

[110] See eg Philipp Sandner et al, “The Digital Programmable Euro, Libra and CBDC: Implications for European Banks” (2020) SSRN <https://ssrn.com/abstract=3663142> accessed 7 November 2020

[111] See eg Jack Solowey, ‘Digital Delegation Doctrine: Central Bank Digital Currencies and the Future of the Separation of Powers’ (2019) 12 NY Univ J Law Lib 874

currency and in the full amount of the issue.[112] Being in essence a private global stablecoin initiative, its infrastructure is available for a rCBDC.[113]

To facilitate agreement among all validator nodes on the ledger transactions, the Libra Blockchain adopted the Libra Byzantine Fault Tolerance (LibraBFT) consensus protocol:

> The main guarantee provided in this approach is resilience against to Byzantine failures – preventing individual faults from contaminating the entire system. LibraBFT is designed to mask any deviation from correct behavior in a third of the participants. These cover anything from a benign bit flipping in a node's storage to fully compromising a server by stealing its secret keys.[114]

Thus, even if up to one third of the network-validated nodes are compromised or fail, BFT consensus is designed to function correctly. This class of consensus protocols enable high transactions throughput, low latency, and a more energy-efficient approach to consensus than the 'proof of work' protocol used in some other blockchains. For its part, the Libra Association pledges it will perform due diligence on prospective validators.

Previous blockchain projects view the blockchain as a collection of blocks of transactions. Conversely, the Libra Blockchain will be a single data structure that records the history of transactions. At the same time, in order to securely store transactions, data on the Libra Blockchain will be protected by Merkle trees, a data structure used by other blockchains that enables the detection of any changes to existing data.[115]

[112] For details see 'Libra White Paper v2.0' (*Libra*, April 2020) <https://libra.org/en-US/white-paper/> accessed 7 November 2020, on which the discussion below relies.

[113] Libra White Paper Paper v2.0 (n 112) s 04; ECB, 'Digital Euro Report' (n 6) 12

[114] The LibraBFT Team, 'State Machine Replication in the Libra Blockchain', 2 <https://developers.libra.org/docs/state-machine-replication-paper> accessed 7 November 2020, modified to incorporate updates to the Libra payment system as found in the White Paper v2.0 (n 112)

[115] For 'merkle tree' being a transaction data linked together with hash references in a turned upside-down tree-like fashion, see eg Daniel Drescher, *Blockchain Basics* (Apress 2017) 77-78

In the Libra payment process, transactions will be signed cryptographically so that even if all validators are compromised, no falsified transactions from addresses with secure signature keys can be accepted as committed.

(iii) WingCash[116]

WingCash' s proposal is for a non-blockchain-based rCBDC. In 2015, the United States Federal Reserve established a 331-member Faster Payments Task Force to support a broader effort to improve the speed, safety, and efficiency of payments.[117] On March 29, 2016, McKinsey & Company was selected to support Faster Payments Task Force efforts to assess faster payments solution proposals from various providers across the United States payments industry.[118] Among the 17 faster payments solutions, WingCash tied for first place.[119] Its proposal is described as:

> A software platform that would be owned and operated by the Federal Reserve and the Governing Organization.[120] The Federal Reserve would issue digital currency (digital Fed notes) and is tied to the Internet domain (Fednotes.com).

This faster payment solution proposal 'seek[s] to make it possible for any entity to transfer value electronically using methods that seek to preserve and to emulate physical currency.' Accordingly, its Faster Payments Network (FPN) would allow

[116] WingCash is now Open Payment Network (n 62). The proposal discussed here was put forward by it under its original name and hence we refer to the design under that name.

[117] Federal Reserve System, 'Strategies for Improving the U.S. Payment System' (2015) <https://fedpaymentsimprovement.org/wp-content/uploads/strategies-improving-us-payment-system.pdf> 7 November 2020

[118] Federal Reserve (Press Release), 'Federal Reserve Engages in Effort to Access Faster Payments Solutions' (*Federal Reserve*, 29 March 2016) <https://www.federalreserve.gov/newsevents/pressreleases/other20160329a.htm> 7 November 2020

[119] See Faster Payments Task Force, 'The U.S. Path to Faster Payments – Final Report Part Two: A Call to Action' (2017) 13 < https://fasterpaymentstaskforce.org/wp-content/uploads/faster-payments-task-force-final-report-part-two.pdf> accessed 7 November 2020

[120] Defined in the Glossary as '[t]he executive officers, board of directors and board of advisors responsible for governing the Faster Payments Network [FPN]'.

‘persons and businesses to hold and transfer digital Fed notes for payment, with the direction of payment flow from the Payer directly to the Payee.’

Thus,[121]

> … the FPN specifies a single Internet domain (…) where the Federal Reserve publishes digital bills and coins (Fed notes). Each Fed note is a unique web page with an immutably assigned URL that includes both a currency code (e.g., USD) and a unique identifier similar to a serial number (…). Combined these components form a unique immutable address for each Fed note …

The Fed notes would constitute legal tender so as to be the equivalent of US physical currency. ‘[E]ach Fed note is assigned a single, permanent, monetary unit of value’ as well as ‘a field that stores the URL of the issuer (…) and a field that stores the URL of the current holder ….’[122] Each Fed note would be cryptographically ‘signed’ by the ‘Fed’ using ‘asymmetric (public key) cryptography’ (PKC), with the Fed also acting as the Certificate Authority (CA). Fed notes would be transferred by means of an exchange of cryptographically ‘signed’ messages from the payer to the Fed (with a copy to the payee), followed by a message from the Fed to the payee. With the completion of each payment, the FPN would update the ‘possession’ of attribute of the Fed note from the payer to the payee. In the process, the Fed would thus act not only as the issuer, but also as a controller of the Internet domain associated with each Fed note and as a custodian of the transfer record.

The WingCash proposed solution envisages the use by the Fed of the WingCash platform. It is a platform that allows a safe and secure transfer of value among individuals and businesses. The Network has two distinct parts: one allowing the Treasury to design and issue digital Fed notes and the second to be operated by the Fed (either directly or through a Governing Organization). The latter would consist of a global directory service distributing the digital notes and recording their transfer. Initial distribution would be made by the Fed to banks, which would make the digital

[121] WingCash (Proposer), ‘Faster Payments QIAT’ (2017) Solution Proposal – Faster Payment Task Force, 11, 14 <https://drive.google.com/file/d/0B_CNPQWTRQwuZWhqbDUzNVJsNGc/view> accessed 7 November 2020. Benjamin Geva, co-author of this article, contributed to the legal analysis.

[122] ibid 11

notes available for withdrawals to their customers. Both successful competition and interoperability with existing networks such as ACH and cards is anticipated.

(iv) BitMint

BitMint money, developed by *BitMint*, was identified as 'the only candidate qualifying as a universal digital representation of worldwide currencies.'[123] Its digital currency, unlike all known cryptocurrencies, does not rely on algorithms that could be cracked by quantum computers. Having considered different strategies, *BitMint* chose quantum-grade randomness as the basis for future currencies. Each coin has a unique identity; however, the identity of the bits does not determine the value of the coin. The value of the coin is determined by payload string. The identity string and the payload string are based on pure randomness and are fused together, inseparably. A coin trader can extract a substring, containing an identity string and payload string, and pass it to another, as payment.

Users receive a coin to their device like a text message. They can then split the coin to make payment for any sum up to the sum of the coin. Payment is carried out by directly transmitting the bits that comprise the coin split to the payee's device under any communication method, without real time intervention of any remote server. Thus, BitMint facilitates continuous payment simultaneously made in real time during the purchase – as for example, when a buyer fills his or her car's fuel tank at a gas station.

Having a unique identity, a coin can be made tethered money, so that it is possible to tie to it terms of use, an expiration date, an intended purpose, a time of payment, or a designated redeemer.[124] In addition, the BitMint digital money framework enables uninterrupted payment online and offline (the latter meaning it is not dependent on network availability),[125] that fits centralised or decentralised regimen, and allows peer-to-peer payments – all of which makes it fit to become legal tender.

[123] Helmut Scherzer, 'Chapter 36: On the Quest to the Ultimate Digital Money' in Claudia Linnhoff-Popien, Ralf Schneider, and Michael Zaddach, *Digital Marketplaces Unleashed.* (Springer 2018) 36.6.

[124] Samid, *Tethered Money* (n 23) 108. See at 50, where the author discusses tethering as a way to protect the holder of BitMint coins in case the digital device on which they are held is stolen. We should, however, observe that whether this will protect the dispossessed owner from a bona fide purchaser for value is a question of law.

BitMint is centrally minted. Its rCBDC solution is a digital-fiat currency claim-check to a defined quantity of a specific commodity, including a fiat currency.[126] It can be issued either directly by a central bank[127] or by a private issuer such as a commercial bank,[128] ideally holding 100% reserve.

BitMint digital currency may be operated either as a unified global digital money platform or decentralised, in a system in which each central bank operates its own CBDC mint. Central banks can, however, choose any distribution and/or authentication channel, whether of BitMint's delegated authentication solution or delegated to 'designated dealers', such as commercial banks, delegated Mints and/or distributed ledgers network (eg blockchain, Ethereum). When authenticating on a distributed ledger, only the identity of the coin is exposed; there is no need to expose the value, such as when authenticating cryptocurrencies. When several central banks of various countries launch their own respective rCBDC, or if one large country chooses to authorise several local Mints, there will be full interoperability through BitMint's InterMint.[129]

BitMint's technology enables controlled privacy, from full anonymity to full traceability and anything in between, in compliance with regulatory requirements in

[125] We thus do not use the term 'offline' in its more common sense, namely, delayed authentication, as for example in 'Offline Payments' (*Chargebee*) <https://www.chargebee.com/docs/offline_payments.html> accessed 7 November 2020, where offline payments are defined to mean 'transactions processed asynchronously.'

[126] For detailed information on BitMint see eg 'BitMint' (*website homepage*) <http://www.bitmint.com/> accessed 7 November 2020; 'BitMint' (*Start-Up Nation Central*) <http://finder.startupnationcentral.org/company_page/bitmint/> accessed 7 November 2020 and sites and videos accessible through it; 'BitMInt – Identity Bearing Money' (*Medium – BitMint News*) <https://medium.com/@bitmintnews> accessed 7 November 2020 and articles thereunder

[127] For details, see Gideon Samid, 'Bitcoin.BitMint: Reconciling Bitcoin with Central Banks' <https://eprint.iacr.org/2014/244.pdf> accessed 7 November 2020

[128] DigFin (Banking & Payments), 'Q-Pay Could Mark the Next Sea Change in Finance' (*DigFinGroup*, 8 January 2019) <https://www.digfingroup.com/bitmint-q-pay/> accessed 7 November 2020

[129] David Lee Kuo Chuen (ed), *Handbook of Digital Currency* (Elsevier Academic Press 2015) ch 20

each jurisdiction. The coin itself can carry its chain of custody (optional) that can be bypassed only by court order.[130] Each coin is equipped with smart contracts capabilities. Through its quantum randomness generation process, distribution management model, and technical architecture, BitMint retains the basic characteristics of having quantum security, resisting counterfeiting, and discouraging money laundering. This eliminates, or at least substantially reduces, the possibility of misuse or participation in illegal acts, while also protecting individuals' privacy rights.

BitMint is inoculated against quantum attack because it is vaccinated with quantum randomness as the critical ingredient for construction of a comprehensive financial platform. That platform is designed to move and store money quickly, efficiently, conveniently, and securely. Not being a cryptocurrency, BitMint is not underlined by complex cryptographic algorithms that may crash against quantum computers.

(v) Assessment

The ECB Digital Euro Report stresses that the digital euro is neither a crypto asset nor a stablecoin.[131] However, this statement ought to be taken with a grain of salt. We take its first part to mean that the digital euro will not be a self-anchored cryptocurrency such as Bitcoin, since the Report does not preclude a claim-check cryptocurrency. The second part means that the digital euro will not be a claim to the euro, but rather a euro of its own. However, this is the same as saying that the paper banknote is not a promise to pay money, but *is* money. Accordingly, we do not understand the ECB Digital Euro Report to reject an e-banknote promising to pay in euro. Nor do we take the Report to reject (or provide reasons for the rejection of) a cryptocurrency along the lines of Libra.

Our own assessment is that a public digital currency in the form of a cryptocurrency, even if it is a claim-check/stablecoin, has a few drawbacks from both a legal and a technological perspective. In a cryptocurrency, the coin consists of the total available in the wallet. Stated otherwise, a coin is not handled as a unique and separate entity from the beginning of a payment transaction to its end. Finality of payment is also less clear in a DLT-based system. Furthermore, in a cryptocurrency, the sequence of the

[130] See eg Gideon Samid, 'BitMint: Non-Speculative Digital Currency (The Future of Money)' (*Youtube,* 7 August 2014) <https://www.youtube.com/watch?v=f5UfpW1kS4Y> accessed 7 November 2020

[131] ECB, 'Digital Euro Report' (n 6) 50, annex 2

bits represents the value of the coin. Since it is unique to each coin, it is that sequence which gives the coin its identity. Accordingly, insofar as each coin in WingCash and BitMint has both an identity and a specific value, as separate functions and from the beginning of the transaction to its end, among the three designs we presented, they both stand closer to the paper banknote.

The WingCash coin, being a digital representation of the fiat currency banknote, is closest to the paper banknote. At the same time, the BitMint payment transaction better assimilates payment in cash, as it does not require any intermediation. BitMint also facilitates a continuous payment, coin splitting, and tethering. Furthermore, a unique key feature of BitMint, which is not reported to exist for the others, is the lack of complete dependence not only on the Internet, but also on any communication network. As such, it appears to meet a universal access requirement,[132] implying a degree of independence from a communication network, particularly the Internet. This facilitates access by unbanked people and non-holders of digital devices, as well as access in case of network failure, particularly in a disaster situation. Thereby, BitMint payment is assimilated to the payment in physical banknotes.

Thus, while substantially enhanced through the use of smartphones and Internet, BitMint payments may be made over simple mobile phones over the cellular network. When using more sophisticated devices, proximity BitMint payments, which may be badly needed in emergency situations, can be made even without any communication network. For example, the payer's device may generate a QR code[133] of which the payee's device takes a picture, thereby completing the payment. A payment may also be made via NFC,[134] which most smart phones possess. Finally, trust facilitating

[132] See eg John Miedema et al, 'Designing a CBDC for Universal Access' (2020) BOC Staff Analytical Note 2020-10 <https://www.bankofcanada.ca/2020/06/staff-analytical-note-2020-10/> accessed 7 November 2020

[133] 'QR codes', short for 'quick response' codes, are square-shaped black-and-white symbols that people can scan using a smartphone to learn more about a product. These encrypted squares can hold links, coupons, event details, and other information that users might want to take with them for referring to later: Corey Wainwright, 'How to Make a QR Code in 8 Easy Steps'(HubSpot Blog, last edited 14 July 2020) <https://blog.hubspot.com/blog/tabid/6307/bid/29449/how-to-create-a-qr-code-in-4-quick-steps.aspx > accessed 7 November 2020

[134] NFC (Near field communication) is 'a method of wireless data transfer … that detects and then enables technology in close proximity to communicate without the need for an internet connection': Cameron Faulkner, 'What is NFC? Everything You Need to Know' (*TechRadar*, 9 May 2017) <https://www.techradar.com/news/what-is-nfc> accessed 7 November 2020

payment may be generated by the payee's inspection of a Hard Wallet containing the money. The Hard Wallet is a physical device that can dispense identity-bearing digital currency. It could be either an independent device, serving unbanked or underbanked people as well as people with no mobile phone, or a chip embedded in a smart phone, but working offline. Payment issued from the Hard Wallet can be taken in by a second Hard Wallet, which will further pay to another Hard Wallet, creating a payment ecology of digital money for long periods without the benefit of a communication network.[135] Therewith, '[a]ll that the payee has to do is to attach a simple measuring device to the physical wallet, take instant measurements and compare them to the pre-loaded figures published by the manufacturer. If the two sources agree, the payee is satisfied, and regards the bits that subsequently flow out from this wallet as bona fide money.'[136]

At the moment, blockchain technology seems to lead the way in CBDC research and projects.[137] However, it remains to be seen, regardless of legal interpretation, whether a DLT-based CBDC can provide the required quantum security, speed, and scalability to grow into a replacement of physical cash, being a legal tender and an enabler for fee-free, frictionless, instantaneous, and unconditional money transfer with legal finality of value between any two parties.

[135] For a scientific exposition see Gideon. Samid, 'BitMint Hard Wallet: Digital Payment without Network Communication : No Internet, yet Sustained Payment Regimen between Randomness-Verifiable Hard Wallets ' (IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), Vancouver, BC, Canada 2020) 1-7 <https://ieeexplore.ieee.org/abstract/document/9216456> accessed 7 November 2020

[136] Gideon Samid, 'Security Notes: Digital Transactions without the Internet' (*Digital Transactions*, 1 October 2020) <https://www.digitaltransactions.net/magazine_articles/security-notes-digital-transactions-without-the-internet/> accessed 7 November 2020

[137] See eg Philipp Sandner, 'The Digital, Programmable Euro: Statement by the FinTech Council of the German Federal Ministry of Finance (Unofficial Translation)' (*Medium*, 30 July 2020) <https://medium.com/@philippsandner/the-digital-programmable-euro-5c1c0b39ae2c> accessed 7 November 2020. See also Raphael Auer, Giulio Cornelli, and Jon Frost, 'Rise of the Central Bank Digital Currencies: Drivers, Approaches and Technologies' (2020) BIS Working Paper No 880, 5 <https://www.bis.org/publ/work880.htm> accessed 7 November 2020

4 ARCHITECTURE AND ISSUANCE MODELS

A. Introduction

The previous discussion established that an e-banknote, being a digital coin containing a promise to pay the bearer a sum certain in money, is a 'banknote.' Accordingly, e-banknotes may be issued by a central bank under its statutory powers to issue banknotes. The discussion further presented designs that may serve as e-banknotes and assessed their suitability. However, a simple truism is that the use of banknotes, whether in paper or digital format, requires mechanisms to make them available to, and usable by, the public. Thus, paper banknotes issued by the central bank are purchased by and physically delivered to commercial banks, which effectively sell them to their customers, to whom they are physically delivered at branches and ATMs. In turn, the customers use them in payment by physically delivering them from payers to payees. This part addresses corresponding mechanisms that ought to be established for the issuance, distribution, redemption of, and payment in, e-banknotes.

We read statutory powers to issue banknotes[138] to include the power to redeem them. We also assume the existence of central banks' powers to address mechanisms for the transfer of, and payment in, banknotes, which are particularly relevant in the case of e-banknotes. Such powers to distribute and run a transfer system may be seen as either incidental to the banknote issuance power or part of the powers that exist in relation to the payment system.[139] The ensuing discussion on rCBDC models assumes such powers to exist.

rCBDC models are often divided into direct, hybrid, and indirect.[140] In the direct model, the central bank issues the digital euros and runs its transfer system.[141] At this point, in a hybrid system, the central bank then issues its digital euros to the public,

[138] Eg those cited in n 1, 2, and 4.

[139] As in eg the EU under Article 127(2) TFEU, as further implemented by Article 22 of the ESCB/ECB Statute (n 89)

[140] See eg ECB, 'Digital Europ Report' (n 6) 39-41; Raphael Auer & Rainer Böhme, 'The Technology of Retail Central Bank Digital Currency' (2020) BIS Quarterly Review 88-93 <https://www.bis.org/publ/qtrpdf/r_qt2003j.pdf > accessed 7 November 2020

[141] ECB, 'Digital Euro Report' (n 6) 40, Figure 3; no corresponding model in Auer et al (n 137)

but the distribution and transfer system is run by intermediaries.[142] Under the indirect model, the central bank issues the currency to intermediaries, which issue to the public their own currency, fully backed by the central bank issued currency. Those intermediaries also run the inter-customer transfer system.

We do not fully adopt this classification, together with its terminology. In our view, it is not adequately fine-tuned to take into account all reasonable scenarios. Particularly, it focuses strongly on the transfer of e-banknotes, while addressing their distribution to the public in a rather rudimentary way. It also does not take into account the option of having commercial banks act on behalf of the central bank in issuing e-banknotes. Further, especially concerning hybrid models, a distinction between intermediated and direct distribution to end-users is missing – and thus developed by the authors here.

While as a rule, commercial banks are not authorised to issue legal tender banknotes, we see a role for them and acknowledge that the greater their role in the architecture, the more space becomes available for autonomy, and thus competition, as well as innovation, albeit at the cost of a greater need for interoperability. For simplicity's sake, we also assume that under each option, redemption is exactly the reverse operation of issuance.

B. Issuance (and Redemption) Options

Under the first four scenarios outlined here, a member of the public holding an e-banknote has a direct claim against the central bank.

(i) Full direct option

Both the distribution and transfer system are run by the central bank.

In this scenario, the central bank deals directly with e-banknote holders.[143] Holders purchase e-banknotes directly from the central bank, typically paying out of bank accounts or, in theory, in paper banknotes. The central bank runs a comprehensive network linking all e-banknote holders. As with any of the other systems set out below,

[142] ECB, 'Digital Euro Report' (n 6) 41, Figure 4 and 'intermediated' model in Auer et al (n 137) 20

[143] As it does not involve intermediaries, this model has no corresponding model in ECB. 'Digital Euro Report' (n 6) 39-41

this option does not require the opening or use of accounts in a central bank by members of the public.

(ii) Limited direct option

Distribution is run by commercial banks, while the transfer system is operated by the central bank.

As far as distribution is concerned, this scenario mimics the current system for paper banknotes.[144] Commercial banks buy e-banknotes from the central bank, paying out of their reserve accounts. Commercial bank customers purchase e-banknotes (issued by the central bank) from their own commercial banks and typically pay for them by having their respective accounts with their commercial bank debited. As in Subpart 4(B)(i), a holder of an e-banknote has a direct relationship with the issuing central bank. Moreover, as in Subpart 4(B)(i), the central bank runs a comprehensive network linking all e-banknote holders.

(iii) Hybrid-intermediated option

Both the distribution and transfer system are operated by commercial banks.

This option replicates the scenario discussed in Subpart 4(B)(ii), with the exception that the inter-customer transfer system is also run by commercial banks (rather than the central bank).[145] As in Subpart 4(B)(ii), commercial banks buy e-banknotes from the central bank. Upon the issuance of an e-banknote to the commercial bank, the reserve account of the commercial bank at the central bank is debited. Commercial bank customers purchase e-banknotes (issued by a central bank) from their own commercial banks and typically pay by having their respective accounts with their commercial bank debited.

(iv) Hybrid-direct option

Both the distribution and transfer system are operated by commercial banks.

[144] This model is comparable to the one used in ECB, 'Digital Euro Report' (n 6) 40, Figure 3

[145] This model is comparable to the one used in ibid 41, Figure 4 (the latter however does not distinguish intermediated and direct distribution).

Unlike in the scenario set out in Subpart 4(B)(iii), commercial banks issue the e-banknotes as agents for the central bank. Upon the issuance of an e-banknote to the holder, the reserve account of the ('issuing') commercial bank at the central bank is debited. This scenario differs from the option addressed in Subpart 4(B)(iii) in facilitating the issuance of e-banknotes by one or more commercial banks on behalf of the central bank. The task delegated to a commercial bank is purely ministerial and does not involve policy choices. Instead, the issuing commercial bank acts strictly as instructed by the delegating central bank.

(v) Backed option

Both the distribution and transfer system are operated by commercial banks.

In contrast to the four scenarios above, a holder of an e-banknote does not have a direct claim against the central bank. At the same time, as long as the system runs properly, the holder has the security of full backing by the central bank, as if the e-banknote was issued by the central bank itself. While we assume that an e-banknote issued by a commercial bank is not legal tender, it is redeemable (ie payable) in legal tender, namely banknotes (whether in paper or electronic form) issued by the central bank.

In this scenario, authorised commercial banks issue e-banknotes in their own names so that each commercial bank has a direct relationship under each e-banknote with the respective holder. The latter will not be in privity with the central bank. However, to the extent that the e-banknotes are fully backed by CeBM, the chance is that they circulate as monetary objects in discharge of payment obligations. What is envisaged in the scenario is not a system of private issuance of fiduciary digital currencies.[146] Hence, issues identified in the old system, under which paper banknotes were issued by commercial banks as a form of CoBM,[147] are not anticipated to arise.

[146] With regard to which we recognise the need for government intervention as in Ben Fung, Scott Hendry and Warren E Webber, 'Swedish Riksbank Notes and Enskilda Bank Notes: Lessons for Digital Currencies' (2018) BOC Staff Working Paper 2018-27 <https://www.bankofcanada.ca/wp-content/uploads/2018/06/swp2018-27.pdf> accessed 7 November 2020

[147] The experience with the old system is discussed by Ben Fung, Scott Hendry, Warren E Weber, 'Canadian Bank Notes and Dominion Notes: Lessons for Digital Currencies' (2017) BOC Staff Working Paper 2017-5 <https://www.bankofcanada.ca/wp-content/uploads/2017/02/swp2017-5.pdf> accessed 7 November 2020

In fact, this model mimics the issuance of written banknotes in the UK by a few designated banks in Scotland and Northern Ireland.[148] Such banknotes are not accorded legal tender status, but are accepted in payment as a matter of practice.[149] By law, these banknotes are required to be fully backed by earmarked sterling obligations of the Bank of England.[150] Similarly, in the scenario envisaged under this option, commercial banks may be authorised to issue e-banknotes, fully backed by CeBM.

C. Final Observations

1. In all scenarios, the central bank keeps its position as a facilitator or catalyst, as well as an overseer (or even regulator), of the claim-check e-banknote system.[151] Only in the scenarios set out in Subparts 4(B)(i) and 4(B)(ii), where the central bank is involved to one degree or another in distribution and transfer, will it also be an operator or direct provider.

2. Operationally, the scenarios set out in Subparts 4(B)(iv) and 4(B)(v) may be the same. In each case, a commercial bank earmarks funds from its reserve account with its central bank, against which it issues the e-banknotes. However, in each such scenario, the legal implications of the central bank's liability and legal tender status are quite different.

[148] See Banking Act 2009 (UK) pt 6, particularly s 213. For HM Treasury Consultation Document see HM Treasury, 'Banknote issue arrangements in Scotland and Northern Ireland' (2005) Consultation Document <https://webarchive.nationalarchives.gov.uk/+/http:/www.hm-treasury.gov.uk/media/7/0/banknote_issue_arrangements_210705.pdf> accessed 7 November 2020

[149] See eg Northern Ireland Assembly, 'The Status of Scottish and Northern Irish Banknotes' (2008) Briefing Note 122/08 <http://archive.niassembly.gov.uk/io/research/2008/12208.pdf> accessed 7 November 2020

[150] Scottish and Northern Ireland Banknote Regulations 2009, SI 2009/3056 issued by the Treasury under ss 215-220 of the Banking Act 2009 (UK)

[151] For these central bank functions in the payment system see in general Ben Fung, Miguel Molico, and Gerald Stuber, 'Electronic Money and Payments: Recent Developments and Issue' (2014) BOC Staff Discussion Paper 2014-2, 19 < https://www.bankofcanada.ca/wp-content/uploads/2014/04/dp2014-2.pdf> accessed 7 November 2020

3. While in the scenarios discussed in Subparts 4(B)(iv)and 4(B)(v), commercial banks' funds in their reserve account are earmarked, in the scenarios addressed in Subparts 4(B)(ii) and 4(B)(iii), a commercial bank uses such funds to pay its central bank for the e-banknotes to be purchased. The difference appears to be that in the scenarios dealt with in Subparts 4(B)(iv) and 4(B)(v), funds are debited from the reserve account only upon the redemption of each e-banknote, while in the scenarios discussed in Subparts 4(B)(ii) and 4(B)(iii), funds are debited to the commercial bank's reserve account as soon as the e-banknotes are purchased.

4. Commercial banks' reserve funds at the central bank are not involved in the scenario addressed in Subpart 4(B)(i). In that scenario, a holder 'purchases' the e-banknote directly from the issuing commercial bank.

5. In the final analysis, the scenario addressed in Subpart 4(B)(iii) - that of the hybrid intermediated option, under which both distribution and transfers of an e-banknote issued by the central bank are run by commercial banks - may be the most advantageous. This is so because it implements an optimal balance between a visible holder's claim against the central bank and the maximum operational role for commercial banks.

5 CONCLUSION

In conclusion, as a matter of law, a token-based e-banknote is a 'banknote'. While it is beyond the expertise of the authors to assess the reliability of technologies available for a complying e-banknote, a survey and proper explanation of existing designs and potential architectural models, as undertaken in this article, is essential for the selection of the desired e-banknote scheme.

On the basis of technological information publicly disseminated, subject to verification to be undertaken by technology experts, this article has pointed to the preferability of a centrally issued design based on quantum-grade randomness and available offline. An architecture premised on a hybrid-intermediated option, under which both distribution and transfers of an e-banknote issued by the central bank are run by commercial banks, appears to be the most advantageous. It gives the e-banknote holders a direct claim against the central bank, while capitalising on the expertise, infrastructure, and innovative potential of commercial banks, with a view to distribution and transfer systems.

Two final observations bear mentioning. First, while 'monetary sovereignty' allows each jurisdiction to move on its own in selecting and implementing its preferred e-banknote scheme, the global economy will be enhanced enormously by the adoption of a universal design and model, which will afford a high degree of interoperability and facilitate a smooth operation of foreign exchange markets. Second, we strongly recommend that the selection of the desired design and model, whether locally or universally, should be made in the context of the existing economic order and should not be used to leverage agendas of new economic orders such as, for example, the use of Bitcoin by libertarians. An agenda for a new economic order is unlikely to generate the consensus required on both the national and global level for the selection of an optimal design and model.

Inasmuch as a professional and apolitical process is recommended, our preference is to leave the tasks of selecting and implementing a rCBDC scheme to central banks. To that end, central banks' ability to rely on existing statutory provisions in selecting and implementing the optimal design and model, as demonstrated in this article, is a step in the right direction.