# CRYPTOASSETS

*Legal, Regulatory, and Monetary Perspectives*

*Edited by* CHRIS BRUMMER


OXFORD

# Cryptoassets

# Cryptoassets

## *Legal, Regulatory, and Monetary Perspectives*

*Edited by*

CHRIS BRUMMER

OXFORD
UNIVERSITY PRESS

OXFORD
UNIVERSITY PRESS

Oxford University Press is a department of the University of Oxford. It furthers the University's objective of excellence in research, scholarship, and education by publishing worldwide. Oxford is a registered trademark of Oxford University Press in the UK and certain other countries.

Published in the United States of America by Oxford University Press
198 Madison Avenue, New York, NY 10016, United States of America.



Library of Congress Cataloging-in-Publication Data

Names: Brummer, Chris, 1975– editor
Title: Cryptoassets : legal, regulatory, and monetary perspectives / Chris Brummer.
Description: First edition. | New York : 2019.
Identifiers: LCCN 2019017648 | ISBN 9780190077327 (paperback) | ISBN 9780190077310 (hardback) | ISBN 9780190077334 (pdf) | ISBN 9780190077341(epub)
Subjects: LCSH: Cryptocurrencies—Law and legislation. | Cryptocurrencies.
Classification: LCC K4431 .C79 2019 | DDC 343/.032—dc23
LC record available at https://lccn.loc.gov/2019017648

1 3 5 7 9 8 6 4 2

Paperback printed by Marquis, Canada
Hardback printed by Bridgeport National Bindery, Inc., United States of America

**Note to Readers**

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is based upon sources believed to be accurate and reliable and is intended to be current as of the time it was written. It is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional person should be sought. Also, to confirm that the information has not been affected or changed by recent developments, traditional legal research techniques should be used, including checking primary sources where appropriate.

*(Based on the Declaration of Principles jointly adopted by a Committee of the American Bar Association and a Committee of Publishers and Associations.)*

# Contents

# Contributors

**Itai Agur** is an Economist in the Macro-Financial Division in the Research Department of the International Monetary Fund.

**Anil Ari** is an Economist in the Macro-Financial Division in the Research Department of the International Monetary Fund.

**Douglas Arner** is the Kerry Holdings Professor in Law and cofounder of the Asian Institute of International Financial Law (AIIFL) at the University of Hong Kong.

**Irving Aw** is Counsel (Tax Law) in the Legal Department of the International Monetary Fund.

**Chris Brummer** is a professor at Georgetown University Law Center and the Faculty Director at Georgetown's Institute of International Economic Law.

**Ross P. Buckley** is the KPMG Kaw—King & Wood Mallesons Chair of Disruptive Innovation, a Scientia Professor, and a member of the Centre for Law, Markets and Regulation at UNSW Sydney.

**Nic Carter** is a Partner of Castle Island Ventures and the Cofounder and Chairman of Coin Metrics, Inc.

**Anton N. Didenko** is a Research Fellow and a member of the Centre for Law, Markets and Regulation at UNSW Sydney.

**Benjamin Geva** is a professor at Osgoode Hall Law School of York University in Toronto, Canada.

**Aurelio Gurrea-Martínez** is an Assistant Professor of Law at Singapore Management University.

**John Kiff** is a Senior Financial Sector Expert in the Monetary and Capital Markets Department of the International Monetary Fund.

**Trevor I. Kiviat** is an associate at Davis Polk & Wardwell LLP, where he advises on the novel strategic, operational, and regulatory issues facing digital currency-based businesses.

**Alexander Lipton** is the Chief Technical Officer of Silamoney and a Connection Science Fellow at Massachusetts Institute of Technology.

**Tommaso Mancini-Griffoli** is a Deputy Division Chief in the Monetary and Capital Markets Department of the International Monetary Fund

**Alex Marthews** is the National Chair of Restore the Fourth—a nonprofit that campaigns against unconstitutional mass government surveillance.

**Maria Soledad (Sole) Martinez Peria** is Chief of the Macro-Financial Division in the Research Department of the International Monetary Fund.

**Jai Massari** is a partner in the Financial Institutions Group of Davis Polk & Wardwell, LLP.

**Cyn-Young Park** is the Director for Regional Cooperation and Integration, Economic Research and Regional Cooperation Department of the Asian Development Bank.

**Emilija Pashoska** is a research assistant with the ADA Chair in Financial Law (Inclusive Finance) at the Faculty of Law, Economics and Finance of the University of Luxembourg.

**Adina Popescu** is a Senior Economist in the Strategy, Policy, and Review Department of the International Monetary Fund.

**Nydia Remolina León** is a research associate at Singapore Management University´s Centre for Artificial Intelligence and Data Governance, and a legal advisor for innovation, digital transformation, and policy affairs at Grupo Bancolombia.

**Céline Rochon** is a Senior Economist in the Strategy, Policy, and Review Department of the International Monetary Fund.

**Catherine Tucker** is the Sloan Distinguished Professor of Management at MIT and Research Associate at NBER.

**Christophe Waerzeggers** is Senior Counsel (Tax Law) in the Legal Department of the International Monetary Fund.

**Angela Walch** is a professor at St. Mary's University School of Law and a Research Fellow at the Centre for Blockchain Technologies at University College London.

**Petal Walker** is Special Counsel at WilmerHale.

**Dirk Zetzsche** is a Professor of Law and ADA Chair in Financial Law (Inclusive Finance) at the Faculty of Law, Economics and Finance of the University of Luxembourg, and Director of the Centre for Business and Corporate Law at Heinrich-Heine-University in Düsseldorf.

**Bo Zhao** is an Economist in the Economic Research and Regional Cooperation Department of the Asian Development Bank.

# 1
# Introduction

*Chris Brummer*

Rarely a day goes by where the upsides—or downsides—of various cryptoassets are not discussed and debated by financiers, regulators, or technologists in the world's leading newspapers and social media. And the debates can be intense. For some, cryptoassets come close to a technological panacea. Cryptocurrencies such as bitcoin, or smart contracts on the Ethereum platform, promise to swiftly disintermediate traditional finance, and usher in technological revolutions comparable to the rise of the internet. Meanwhile, for others, cryptoassets are at best fraudulent, and at worst sources of financial instability. Internationally renowned economists, such as *l'enfant terrible* of cryptocurrency skepticism, Nouriel Roubini, do not hesitate to describe proponents as "crypto zealots" and "mentally psychotic," and point to the extreme highs—and lows—experienced in cryptoassets markets in 2018 as proof of the flaws underpinning the currency.

Differences in opinion start with the very name of just what to call these new financial products. This book adopts the most neutral appellation—crypto "asset"—though even it inherently raises its own immediate questions. In conversations about any new technology, especially one that can take shape as an investment, utility, or payment instrument, what you call an instrument can necessarily lead to conclusions about whether (and how) one should regulate it. If it's an asset, commentators immediate opine, shouldn't it be taxed like property? Or if you call it a currency (such as "crypto currency" or "virtual currency"), then conceptually, you think about it just as that—and with all the attendant economic, tax, and regulatory consequences for finance ministries and others. And if you call it something else—say a "derivative" to the extent to which any transaction requires time for the delivery of a cryptoasset due to mining or data processing—another regime or framework will come to mind. In all, if you're not careful, the question one poses about cryptoassets quickly becomes the answer, even when you're just grappling with defining what you're trying to study.

What cryptoassets have in common is that they depend primarily on cryptography and "distributed ledger" technologies to memorialize and track transactions. Cryptography refers to algorithmic techniques used to protect information by encrypting it into formats accessible to individuals only if they possess a special key. Distributed ledgers, meanwhile, are databases that store

Cryptoassets. Chris Brummer.

records through a peer-to-peer network of computers that is not confirmed by any one entity, and is managed by multiple participants.

As will be emphasized frequently in this book, cryptoassets are used in many different ways, and are generally catalogued as comprising either a medium of exchange ("digital money" or "cryptocurrency"), devices for accessing an online service ("utility token"), or investments—or all three at once. As a medium of exchange, cryptoassets can take the form of "digital money," and as such may be accepted by persons and market participants in commerce. By contrast, as utilities, cryptoassets are like tokens in a pinball machine in an arcade—you use them to access something you want to use, whether it be an online game or cloud storage facility. Finally, cryptoassets can also constitute investments, and are even used to raise capital. Most notably, cryptoassets can comprise the consideration that developers give to investors in initial coin offerings (ICOs). In these offerings, investors provide developers with government-backed fiat money, or they might deliver to developers other cryptocurrencies that can be traded in for fiat money. In any event, the actual cryptoassets given to investors in return are investments—and expected to appreciate—and might have investment-like features, providing holders with rights to dividends or more.

The operating system driving the way cryptoassets are transferred, and records stored, is a special kind of distributed ledger system called a *blockchain*, which links transactions together as time goes on and more transactions take place. The amount and kind of information that any particular blockchain can store can vary immensely, and range from tracking ownership of referenced assets among pseudonymous participants, as in the Bitcoin blockchain, to the public identification of payers and payees, along with account balances and other transactional details. Certain kinds of blockchains, such as the Ethereum platform, can additionally utilize "smart contracts," or programmable forms of digital money, where payments are made only when certain conditions are satisfied, such as a date passing or a service having been rendered.

Importantly, blockchains do not record individual transactions one at a time. Instead, series of transactions are stored as data in individual blocks. As a result, rules are necessary to show when and under what circumstances a new block can be added to a preexisting one to create a chain of blocks, or blockchain. The rules relied on to dictate how new information is added to these data structures are collectively referred to as a *consensus mechanism*.[1]

Most of the chapters in this book will explore these concepts in greater depth, from different perspectives, but it is useful to note from the outset that "proof of work" is the name given the consensus mechanism used on most blockchains.[2] In a proof-of-work system, members must provide a valid cryptographic hash for a block, or in layman's terms, guess a series of correct cryptographic games by providing the right numeric values for each.[3] The individual (or computer)

that correctly identifies the numbers involved in the guessing game is then confirmed by other members of the network and receives cryptocurrency as determined by the blockchain's protocol as a payment, or reward, for "mining" the transaction.[4] Coins that have been credited to the account of the miners can then be sold or transferred via subsequent transactions.

In some blockchains, an alternative "proof of stake" approach is used to validate transactions. In these systems, it is the user's stake, or ownership of a certain number of cryptocurrency units, that empowers and directs the formation of new blocks, distinguishing it from the proof-of-work system, where new blocks are created by performing a certain amount of computational work.[5] Miners for the system, sometimes called "forgers," are expected to put up their "stake" as a kind of operational insurance for other participants; if a forger validates a fraudulent transaction, she loses her holdings, as well as her rights to forge blocks in the future.[6]

Finally, some blockchains are permissionless, while others are permissioned. A permissionless blockchain allows anyone to participate in consensus operations. Such are thus in a sense both open-access and public. Permissioned systems, by contrast, allow only actors blessed by designated authorities to participate in building consensus and validating transactions.

## I. Cryptoasset Controversies

Cryptoassets are, if nothing else, controversial. Cryptoasset advocates cite a number of potential benefits associated with cryptoassets that if realized could prove transformative for the payments industry. Blockchains, for example, are often described as immutable—unable to be edited or deleted—thereby allowing in some (though not all) instances greater security than traditional banking systems. Furthermore, because cryptoassets leverage peer-to-peer infrastructures, they enable applications across borders at low costs, and are poised to transform international remittances.

Cryptoassets are also often supported by highly decentralized blockchains and operating processes, enabling open and transparent points of access for stakeholders; all the while, nongovernmental and private cryptoassets operate independently of central banks, and as such are subject, according to proponents, to less political manipulation.

Finally, many proponents contend that cryptoassets have the potential to disintermediate an oligopoly of intermediaries dominating the legacy financial system. Blockchain technology exemplified by Bitcoin provides a novel tool for untrusted parties to come to agreement on a record of transactions, without using a middleman such as a bank.[7] Similarly, smart contracts driven by the

Etherium blockchain could be used such that money—whether it be fiat or a cryptoasset—is only sent from one party to another when certain conditions are satisfied, such as a date passing or a service having been rendered. A host of manual processes can be automated, reducing or eliminating the need for all kinds of intermediaries such as escrow agents and banks, as well as compliance and claims processing.[8]

Yet cryptoassets pose considerable potential risks as well—and have engendered biting criticisms from skeptics. Volatility and market integrity are common concerns: Investments in cryptoassets were valued at $830 billion in early 2018 before collapsing, losing according to some reports over 75% of their market capitalization. Discoveries of fraud jumped as well, as forcing enforcement actions by regulators.

And although markets for cryptoassets are small, especially when compared to the stock and bond markets, the pseudonymity and weak cybersecurity of many blockchains are raising questions about the implications of cryptoassets for financial stability and money laundering.[9] All the while, the increasing institutionalization of cryptoassets—including plans to integrate cryptoasset technologies into capital markets and central banking—are pushing financiers and regulators alike to closely scrutinize cryptoasset applications and underlying value propositions.

As we will see in this book, cryptoassets are not just novel instruments; they also challenge longstanding economic models and regulatory strategies. Traditionally, supervisors tasked with supervising new markets (or underregulated ones) have identified and catalogued relevant intermediaries, regulated them as gatekeepers, and issued rules relevant to these gatekeepers in order to achieve goals related to efficiency, investor protection, capital formation, and market integrity. In the decentralized ecosystems characterizing many cryptoassets, however, where anyone can play certain key roles impacting the design and operation of a cryptoasset, such models are difficult, and perhaps impossible, to translate into effective regulatory practice resembling anything like earlier iterations.

The puzzle becomes all the more difficult given the virtual nature of these assets, and the fact that they are digital instruments, tradeable and transferable online. Cryptoassets are routinely released and traded throughout the world, and can be accessed in terminals strewn across jurisdictions and to far-flung parts of the world. Different countries may, furthermore, have very different conceptions as to just what a cryptoasset is, and how it should be categorized and regulated. Galvanizing a global, coordinated strategy is difficult, if not impossible, with stakeholders and even countries initiating the regulatory process from very different vantage points.

## II. An Overview of This Volume

Against this backdrop of issues, this collection of chapters, written by some of the world's leading experts, attempts to demystify cryptoassets through a series of different investigations, across economics, law, and the social sciences. Given the economic and legal questions raised, a distinctly interdisciplinary approach is deployed, with experts hailing from law firms, technology firms, the academy, and the International Monetary Fund. With its origins tied to Washington's Fintech Week, and the interdisciplinary Crypto Asset seminar cosponsored by the IMF and Georgetown University Law Center, the volume seeks, like the conference, to provide cutting-edge analysis and understanding of cryptoassets—and cryptoasset regulatory policy—for educated generalists.

The book begins with a history of money and payments. in chapter 2, "Cryptocurrencies and the Evolution of Banking, Money and Payments," Benjamin Geva, a professor at Osgoode Hall Law School, discusses cryptocurrencies in the context of a historical perspective on the evolution of money, payment, payment intermediation, and commercial banking. Geva points at the latter as the catalyst for national and global networks for book-based payments. Geva goes on and distinguishes between two types of scriptural money, each being value held on deposit, facilitating both book-based payments and redemption to fiat money/banknotes. The first is held by the public on deposit with commercial banks which is demotivated in and redeemable to fiat money/banknotes. The second is in the form of claims against the central bank being available to commercial banks. The latter may make their own payments with it and both redeem and purchase with it fiat money/banknotes to be sold by them to their customers. He discusses options for making scriptural central bank money directly or indirectly available to the public and distinguishes such options from central bank digital-currency schemes.

A sweeping survey of the evolution of payments systems from antiquity to modern age, is followed in Chapter 2 by an outline of the inauguration of electronic payments and the role of the central bank in issuing fiat money as well as in the architecture of the contemporary payment system. Geva then proceeds to discuss the emergence of digital currencies and explores their impact on money, payments, and the banking industry. He distinguishes between cryptocurrencies and other types of digital currencies, between decentralized and centralized schemes, as well as between digital currencies issued privately and by central banks. He concludes by pointing at the challenge cryptocurrencies present to state-issued currency, and more in general, at both the potential and limits of payment disintermediation by digital means. Geva also points at the unstable value and inefficiency inherent in blockchain technology; he predicts, however, that as technology improves, some confluence of

traditional banking and digital services may be possible whereby banks themselves enter into the digital currency space, just as digital currency providers become more active and important services providers for traditional bank customers.

The next chapter, "Deconstructing 'Decentralization': Exploring the Core Claim of Crypto Systems," by Angela Walch, begins a conceptual exploration of the concept of "decentralization." She describes the current use of the word "decentralized" as often used to denote resilient systems that lack power centers, even though the term is in fact, highly contested, ambiguous, and, depending on the circumstances, incorrect. Indeed, as with some other descriptors of blockchain technology, the adjective "decentralized" proves to be an overstatement, Walch argues, and can lead to problematic consequences where authorities rely on an unsubstantiated conclusion that a given blockchain (or blockchains generally) is (are) "decentralized." She thus counsels that courts, regulators, and even potential adopters or users of cryptoassets (whether directly or through other financial products) should use other factors to inform their decisions about a blockchain. Specifically, in examining decentralization, a forensic examination should be undertaken to begin to assess how decision-making authority is exercised within a blockchain system.

Chapter 4, "Cryptoasset Valuation: Theory and Practice," by Nic Carter, provides a much-needed primer on valuation strategies for cryptoassets. Mr. Carter identifies the core features that underpin the value of most cryptoassets as encompassing: (1) the degree of unique access to network services; (2) real asset backing; (3) cash flows from an underlying network, including "proto-equity" linked from business cash flows; (4) consumability; and (5) governance rights.

In the next chapter, "Toward a Stable Tokenized Medium of Exchange," Alexander Lipton argues that existing banking and payment systems are rapidly becoming obsolete and misaligned with the new challenges of the modern economy. While open access internet protocols have unleashed a wave of creativity and growth in numerous fields, banking is not one of them. The reason stems mostly from the fact that internet protocols for money and identity, while needed, are conspicuously absent at present.

In light thereof, Lipton argues that a regulatorily compliant fiat-backed token, which can be viewed as an electronic analogue of cash, can help to fill this gap. According to the author, all decentralized crypto coins are inherently unstable, which makes them less than useful for commercial applications. Indeed, contrary to often-made claims, it is not possible to build a truly decentralized stable token. He thus makes the bold conclusion that any potentially successful stable token has to be at least partially centralized, with varying degrees of decentralization. He then describes four approaches to building stable tokens including

fully collateralized custodial tokens, partially collateralized custodial tokens, tokens overcollateralized with cryptos, and dynamically stabilized tokens, and conclude that only fully collateralized tokens can be stable, even under extreme circumstances. The author then introduces narrow banks and describe their important role as anchors of a diverse digital banking ecosystem and potential emitters of central-bank-backed digital cash.

The book then turns to regulatory strategies. Chapter 6, *The Law and Finance of Initial Coin Offerings,* by Aurelio Gurrea-Martínez and Nydia Remolina, covers regulatory strategies currently under development for cryptoasset transactions utilized to raise capital for online projects. These transactions, again called ICOs, entail more than $21 billion raised in 2018. Yet how they should be regulated is raising a myriad number of responses across jurisdictions. Because of their investment-like features, regulators are trying to determine when and under what circumstances the cryptoassets are offered investors in return for their capital constitute securities. Similarly, ICOs—even when they do not involve security-like cryptoassets—are raising novel issues for authorities from an accounting, finance, corporate governance, data protection, anti-money-laundering, and insolvency law perspectives. Along with offering a comparative and interdisciplinary analysis of ICOs, this chapter provides a set of recommendations for approaching ICOs in a way that may promote innovation and firms' access to finance without harming legal certainty, investor protection, market integrity, and the stability of the financial system.

Chris Brummer, Jai Massari, and Trevor Kiviat extend the analysis of ICOs by exploring key questions of transparency in chapter 7, "What Should Be Disclosed in an Initial Coin Offering?." In the chapter, the authors note that disclosures in initial coin offerings (ICOs) have ranged widely from informative to incomplete to fraudulent. This uneven quality has spurred investors, quite understandably, to call for the registration of ICOs in order to facilitate better disclosures.

The authors argue, however, that registration under the 1933 Securities Act is, as currently enacted, a weak mechanism for mandating the disclosures needed for informed investments in ICO tokens. Many ICO issuances offer nontraditional, non-financial rights that require and involve different pricing considerations than traditional common equity and debt, and are embedded in technical systems unanticipated by the New Deal. They thus conclude that ICOs necessitate a reconceptualization of long-standing disclosure obligations and safeguards, as well as a revamped approach toward entities tasked with validating disclosures. To highlight their point, they provide a forensic analysis of key provisions in the Securities Act's Form S-1, crowdfunding's Form C, Form 1-A for Regulation A+, and Rule 144A, highlighting their inadequacy

in providing investors with key information relevant to informed investing in cryptoassets.

Petal Walker expands on the question of registration and moves to the institutional backdrop for blockchain technologies in a closely related derivatives sector, in "Blockchains and Risk Management Infrastructure of the Derivatives Industry." To begin chapter 8, Walker examines how (and whether) blockchain technologies would be interoperable enough to function in derivatives markets, and subject to derivatives markets regulations. She then extrapolates ways in which a blockchain-based derivatives market could possibly reduce risk, as well as some of the risk concerns about blockchain raised by market participants, including language gap risks. Finally, she examines how the application of today's risk-based registration regime on tomorrow's market may actually increase risk.

Importantly, Dr. Walker suggests that there may have to be fundamental regulatory changes in order to successfully integrate blockchain technologies into derivatives markets in ways that help achieve both market efficiency and transparency. For instance, she proposes that Congress explore a new registrant category in order to capture contract writers. However, Walker recognizes that there are still significant challenges even here, none perhaps most important than human capital—and an absence of technical expertise at the CFTC (U.S. Commodity Futures Trading Commission), the primary agency tasked with oversight of derivatives markets. Furthermore, blockchains would by their nature introduce unprecedented enforcement challenges. It is, as she notes, highly unlikely that regulators would allow the ultimate owner of a significant segment of market activity to be a computer network in which no individuals can explain errors, answer questions, and ultimately be held accountable. But deciding whom to regulate, especially in a decentralized ecosystem, could prove as difficult as operationalizing enforcement itself.

In chapter 9, "Difficulties in Achieving Neutrality and Other Challenges in Taxing Cryptoassets," Christophe Waerzeggers and Irving Aw seek to provide an overview of the main challenges and key considerations for policymakers designing a tax law framework for cryptoassets. This chapter highlights difficulties tax systems face in achieving neutrality when determining the tax treatment of cryptoassets using existing income tax and VAT principles and concepts. Similar to arguments presented by Brummer et al. and Walker, Waerzeggers and Aw emphasize limitations of existing principles when faced with new technologies and business models.

The chapter begins by explaining the challenges of classification based on the wide variation in the underlying economic functions of tokens. These at times hybrid variations in economic functions have caused many jurisdictions striving toward neutrality to adopt a case-by-case approach toward taxing gains arising from the disposal of cryptoassets. Next, the authors examine key

features of securities tokens—cryptoassets that serve as securities. Securities transactions, they observe, are typically exempt from VAT. Among its most interesting insights are the logic of a functional application of VAT principles to cryptoassets, and an which could support an argument for the exemption of a supply of a hybrid token that is both a debt and utility token from VAT, as opposed to the supply of a hybrid token that is an equity and utility token where the administrative difficulties in quantifying the implicit fees in margin-based supplies are not applicable. The chapter then concludes with an examination of the challenges in adopting a realization or disposition basis to the taxation of gains on cryptoassets and in valuing cryptoassets, as well as the challenges of taxing gains derived by miners and validators from ensuring the integrity of the blockchain. Expanding on concepts introduced in Nic Carter's overview of valuation, it considers specific valuation challenges that arise for tax purposes in employment remuneration, hard forks, token airdrops, token pre-financing, and token burning.

In chapter 10, "Blockchain and Identity Persistence," Alex Marthews and Catherine Tucker explore "smart contracts"—programmable forms of digital money, and their implications for privacy. They observe that the unique value proposition of "smart contracts" based on blockchain technology is the creation of a permanent public record of agreed-upon transactions that cannot be changed retroactively. This is, to be sure, attractive in terms of reducing the potential for fraud: persons entering into a smart contract pre-commit both their current self and their future selves, no matter what changes occur to them or to their circumstances. However, Marthews and Tucker argue, even in an age of increasing adoption of distributed ledger technologies, self-reinvention remains important. For individuals, it is important to preserve the ability to assume new identities both formally and informally, and from a surveillance perspective, it is important to prevent governments from reliably associating a particular cryptoasset transaction with a particular person.

Marthews and Tucker instead encourage an expanded and refined understanding of what it means for a blockchain use case to "protect privacy," and in particular, how such use cases can encourage a notion of personal identity that is inflexible and matches poorly with individuals' notions regarding their identities. They review several proposed use cases that present this problem in an especially acute form and highlight good practices to preserve space for self-reinvention.

In chapter 11, the book moves to issues of non-U.S. cryptoasset supervision with "Policy and Regulatory Challenges of Distributed Ledger Technology and Digital Assets in Asia." Authored by Douglas Arner, Ross Buckley, Dirk Zetzsche, Bo Zhao, Anton Didenko, Cyn-Young Park, and Emilija Pashoska, the chapter explores the spectrum of DLT, its major uses (focusing cryptocurrencies and

ICOs), and policy and regulatory responses, particularly in Asia. The authors take the time to demystify key aspects of blockchain systems, while also carefully disentangling concepts that are often (incorrectly) used interchangeably, such as distributed ledgers and blockchains. They also conduct a comprehensive analysis of regulatory statements and disparate policy approaches in Asian countries toward cryptocurrency, blockchain, and ICOs. The chapter provides data on total capital raised through ICOs, in Asia, and analyzes the distribution of ICOs by country and region. The chapter argues that from a policy perspective, the most appropriate regulatory approach to DLT is one based upon function, with different instruments and systems regulated as appropriate given their function, based on a crowdfunding typology around donation, reward / use, currency / payment, and investment. Financial regulation would only focus on those in the latter two categories and leaving the former two to consumer protection, general contract and industry standardization – but noting that these areas need further development in order to support the appropriate development of the market.

In the final chapter, "Casting Light on Central Bank Digital Currency," IMF experts tackle one of the most contested issues in macroeconomics: the desirability of creating central bank digital currencies (CBDCs). CBDCs are effectively a new kind of digital currency, one issued by a central bank and which could be used as legal tender. In the chapter, the authors explain the basic design and functional characteristics of two potential forms of CBDCs: account-based and token-based. They then develop a conceptual framework to differentiate and analyze CBDCs as compared to other forms of money, including commercial bank deposits, "narrow finance" solutions such as pre-funded mobile payments, and cryptocurrencies. This framework is then applied to explore the design considerations critical in the development of an effective CBDC from the perspective of an end user.

After analyzing the utility usefulness of CBDCs from the viewpoint of end users, the authors turn to an assessment of whether CBDCs can advance the public policy goals of the central bank, including the social dimensions of money—improving financial inclusion and efficiency—and considerations for financial integrity, financial stability, and effectiveness of monetary policy transmission. The chapter concludes with an overview of central banks' publicly announced efforts or pilot programs related to CBDCs and the status and common features of these initiatives.

# 2

# Cryptocurrencies and the Evolution of Banking, Money, and Payments

*Benjamin Geva**

## I. Introduction

In the modern economy, payments are typically made by means of transfers through bank accounts, and otherwise the delivery of cash in the form of banknotes and coins. As conduits of funds transfers, banks operate as intermediaries between payers and payees. They also distribute to their customers banknotes issued by the central bank. The recent emergence of cryptocurrencies, facilitating payments outside the banking system, as well as in items not created throughout banking operations, has put to test these fundamentals and particularly challenged the architectural premises of the present banking system.

This chapter discusses cryptocurrencies in the context of a historical overview of the evolution of money, banking, and the payment system.[1] Section II addresses money, payment, and payment intermediation. Drawing on my previous work,[2] Section III sets out the evolution of commercial banking to facilitate national and global networks for book-based payments. Section IV takes us to the cyber-age. It addresses both electronic banking as a form of payment intermediation and the availability to the public of central bank balances as a challenge to payment intermediation. Cryptocurrencies, as a type of digital currencies, are discussed in Section V, which goes on to examine the challenge they present to state-issued currency, payment intermediation, and the roles of banks in the payment systems. The Conclusion points at an irony: even as a challenge to banking, cryptocurrencies emerged as an outgrowth of an enhancement to banking. For their parts, centralized digital currencies may be linked to banking and the legacy monetary system. While changes of unknown scope and magnitude may be inevitable, banks, "banking," and payment intermediation are unlikely to disappear, at least in the foreseeable future.

* Professor, Osgoode Hall Law School York University; Counsel, Torys LLP, Toronto, Canada; bgeva@osgoode.yorku.ca. For research assistance in the final preparation of the manuscript I am grateful to Alexander Davis of the 2019 Osgoode graduate class.

Cryptoassets. Chris Brummer.

## II. Money, Payment and Payment Intermediation

Money was defined to consist of anything that widely circulates 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 . . . ."[3] Over the centuries, coins and banknotes issued by the authority of the state have become the standard monetary objects in all countries, so as to collectively be called "cash" or "currency."[4]

The earliest coins were struck in Lydia (a city-state in Asia Minor) around 700 B.C.E.[5] During antiquity and the Middle Ages, having evolved from a commodity traded for its use value into currency transferred in payment of debts,[6] the coin became the standard circulating object denoting a prescribed monetary value.[7] It was fundamentally a piece of metal fashioned into a prescribed shape, weight, and degree of fineness, stamped by the issuer under the authority of the sovereign with certain designs, marks, and devices.[8] During the seventeenth century C.E., the banknote appeared as an obligation to pay coins or specie. Originally, the obligor thereon was a goldsmith, the predecessor of the deposit bank in England.[9] Ultimately, in the course of the eighteenth century, following the establishment of the Bank of England in 1694,[10] the promise to pay on banknotes circulating as money became that of the central bank.[11]

At its inception, and in theory[12] until the nineteenth century C.E., the value of a coin, at least in its ideal form, was primarily determined by reference to the weight of the precious metal it contained. At the same time, by definition, inasmuch as they are mere obligations to pay, banknotes are "fiat money," namely, of positive nominal value, notwithstanding the (relatively) worthless intrinsic value of the material of which they are made.[13]

Until the modern era, a monetary unit of account was anchored in the value of a specified weight of a prescribed metal. This gave the monetary unit of account its external value in terms of that metal, and facilitated the establishment of an international system under which the value of each national unit of account could be ascertained by reference to all other national units of account.[14] Furthermore, until the modern era, the issuer's obligation to pay, measured by reference to a unit of account, was to actually pay that amount in specie, at least in coins. In England, this was originally true for banknotes issued by private bankers,[15] and subsequently, to banknotes issued by the Bank of England.[16] For a coin, the issuer's obligation was in the form of a guarantee as to its actual metallic content, or at least the redemption thereof.

To this day, current coins and banknotes are typically issued under state authority; at least for banknotes, the issuer is usually the central bank. However, other than the issue of coins and banknotes under state authority, by modern times, the framework just described above has been eroded. First, in the course

of the nineteenth century, the coin reflecting a fraction of the unit of account became a token, that is, a piece of metal of a value lower than which it denotes. The division of the basic unit of account into fixed token denominations at equal abstract subunits[17] is called by economists the "standard formula".[18] Thereunder, the prescribed sum of such token denominations is convertible at a fixed exchange rate to each other denomination and to the basic unit, regardless of their own metallic composition.[19]

Next, in the first half of the twentieth century C.E., convertibility of banknotes ceased to exist; that is, the obligation to pay in specie embodied in a banknote became unenforceable.[20] Thus, at present, banknotes and coins express abstract obligations; they are tokens convertible to other tokens. Finally, during the second half of the twentieth century, even the measurement of the unit of account by reference to a specified quantity of a given precious metal was abolished.[21] The external value of the standard national unit of value is now determined only by reference to the value in which that national unit of value is traded in international financial markets by reference to each other national unit of accounts.

Payment in cash is by physical delivery from one person (payer) to another (payee). This is a face-to-face process that does not requires intermediaries. More specifically, "payment" is "a bilateral act which requires the [payee] to accept the [payer]'s act of tender,"[22] and is completed on the passage of possession in the money[23] when the payee takes delivery, thereby manifesting the acceptance of the tender.[24]

From the beginning, payment in cash had flaws, and under some circumstances was impractical. Particularly, this is due to costs and risks associated with the storage, carriage, and transportation of cash. Other concerns have been scarcity of cash and the inevitable cumbersome process of handling and paying in cash large sums of money. In a nutshell, an effective solution has been in the form of payment made to the payee, under the payer's instructions, by an intermediary who typically owed money to the payer.[25] Such payment would discharge both the payer's debt to the payee and the intermediary's debt to the payer. An optimal such an intermediary was a deposit-taker, that is, banker, being a debtor to all depositors. When payee preferred payment into payee's account with another banker (rather than in cash) the two bankers, that of the payer and that of the payee, settled periodically by paying the balance due for customers' payments going in both directions. Bankers kept funds with each other and ultimately with a central counterparty. Over the centuries, both national and global non-cash payment systems so evolved.

At the heart of such a system stands the commercial bank. The essence of commercial banking has been the taking of deposits (or other repayable funds)

from the public and lending.[26] Linked to these functions is the provision of inter-account payment services.[27]

Historically, commercial banking (banking) emerged as a form of financial intermediation between savers (depositors) and borrowers. The banker (or bank)[28] took from the public deposits either in specie or in commodity money; what was deposited was both owed by the banker to the depositors and at least in part available to be lent by the banker to borrowers. Loans were mostly credited into borrowers' deposit accounts with the lending bankers in part to be used by borrowers to make payments. In this environment, payment intermediation in the form of non-cash payment services evolved as an outgrowth of deposit-taking or, more in general, of maintaining deposit accounts for customers, whether the original depositors, or the borrowers who deposited the proceeds of the loan.[29] This business model has been workable as long as not all depositors required payment in specie from the banker at the same time. In normal circumstances, it sufficed for a banker to keep at hand enough specie or cash to satisfy reasonable demand. Monitoring depositors' payment activity in accounts facilitated credit decision-making and led to specialization in advancing information-intensive non-traded loans, which became a principal niche for a profitable commercial banking business as well as effective financial intermediation for the economy as a whole.

Already way back in antiquity[30] the evolution of mechanisms for payments initiated by the issue of payment orders had been part and parcel of the emergence of "banking" as a form of financial intermediation between depositors to, and borrowers from, the depositary.[31] Furthermore, over centuries the architecture of the banking system evolved to satisfy the need to carry out non-cash payment transactions between customers of separate banks by the creation of interbank networks. For its part, lending out of deposits generated a fractional reserve system that necessitated the establishment of liquidity facilities to ensure the smooth flow of payments. Finally, for their part, banknotes, of which at present mainly consist of cash, originated as circulating receipts for deposited funds.

## III. Deposit Banking, Payment Services, and Paper Money: Historical Perspective on Payments Intermediation

The modern payment system has been described as consisting of "a complex set of arrangements involving such diverse institutions as currency, the banking system, clearing houses, the central bank, and government deposit insurance."[32] The latter element is helpful but not universally present, and yet all

are components of what can broadly be described as a commercial (deposit) banking system.

Notwithstanding the substantial enhancement in complexity and importance of banking in the modern economy, its fundamentals are not at all novel.[33] What follows is an abbreviated account of the evolution of payment intermediation and that of paper money as an outgrowth of deposit banking.

## A. Antiquity

*Ancient Mesopotamia* has been identified as the cradle of banking operations.[34] It earned this title due to the emergence of institutions providing all core banking activities, namely, deposit taking, lending[35] and payment services even prior to the emergence of "monetized" coins. However, this was a secondary activity for such institutions; moreover, credit was made available by depositaries out of their own capital[36] and without dipping into deposits.[37] As well, each customer's deposit may have been physically segregated.[38] Payment and withdrawal orders were inscribed on tablets, and yet could be oral. Each payment order directed the drawee to pay either to a payee known to the drawee or to a payee to be properly identified.[39] Payment was made in specie; there appears to be neither evidence for the execution of non-cash payments from one account to another nor any trace of inter-institutional clearing and settlement.

There is a historical debate on the possible origins of money in the Ancient East, particularly in Mesopotamia; specifically, there is a disagreement on whether distinct items of value were actually used exclusively as means of payments, and thus approximated coins.[40] However, it seems to be universally agreed that nascent "banking operations" in Mesopotamia preceded the emergence of money, in the sense of standardized metallic pieces, in fixed denominations, whose value is certified by the ruler's stamp.[41] Rather, various commodities served as both units of account and means of payment. Based on their comparative or relative value, such commodities served as a basis for a price system, as well as actual means or money of payment. Principal commodities were grain and precious metal, usually barley and silver.[42] Having both (1) actual use value or intrinsic utility, and (2) economic value facilitating their use to provide a standardized means for the measurement of the value of other commodities as well for paying for all such other commodities, such items constituted "primitive money."[43]

The emergence of the bank as a distinct type of institution took place in *Ancient Greece*.[44] More specifically, the process took place in the Mediterranean territory on which Ancient Greek civilization expanded,[45] almost throughout the entire classical period of that civilization.[46]

Thus, in the course of the sixth century B.C.E., shortly after the appearance of coined money as a medium of exchange in commercial transactions,[47] money-changing surfaced as a profession. Shortly thereafter, the money changer came to accept deposits of coined money, mix them,[48] and lend out of them, so as to gradually become a banker. A banker effectively kept a running account for each customer, posting to it each deposit and withdrawal.[49] A withdrawal from a customer's account could be made for the entire or part of a balance due on deposited money, either by the depositor himself, or by a designated payee (or on his behalf) in pursuance of the depositor's instruction.

For each payment to a designated payee, having received the payment order and being in possession of cover, the payer's banker sent a note to the payee. Having made an appropriate entry on his books in the payee's favor, the banker became accountable to the payee, regardless of whether the payee kept an account with that banker. A payee who did not have an account at the payer's bank could demand payment in cash, or where the advice note issued by the banker was made out to the payee "or order," the payee could appoint an agent, usually another banker, to come to the payer's banker and claim on the payee's behalf payment in cash over the counter. Alternatively, the payee's banker may have been prepared to credit the payee's account in advance, on the basis of the advice note issued to the payee by the payer's banker and presented to the payee's banker by the payee, and in anticipation of subsequent payment by the payer's banker. Payment by payer's banker to the payee's banker could be effectuated either in coins, or as part of either bilateral or multilateral setoff. No interbank clearing system, whether bilateral or multilateral, existed in Ancient Greece.[50]

Compared to Ancient Greece, the institutional scene in *Ancient Rome*[51] was more complex;[52] and yet, this complexity did not lead to an overall advancement in banking practices. Nonetheless, in three major respects Roman banking practice went beyond that of the Greek. *First*, the receiver-banker could be treated as the first money transmitter, to whom funds are delivered with the view of making a specific payment. However, money transmission by a receiver-banker may have developed under narrow circumstances, in the context of private auctions,[53] and in any event did not extend to cover payment between geographically distant parties. *Second*, as in Ancient Greece, there was in Ancient Rome neither an intra-city nor intercity multilateral interbank clearing and settlement system.[54] However, nascent interbank correspondent arrangements, under which one bank held funds in an account with the other, developed, particularly in the same city,[55] but also in different cities so as to facilitate payments between geographically distant parties.[56] A non-cash payment could have been carried out between accounts of two depositors, either in the same bank, or in two banks situated in the same small town or within a specific market, whether permanent or periodic.

*Third*, deposit bankers operated under strict bookkeeping requirements, and were obligated to record their monetary operations in account books called *rationes*. An account book (*ratio* in singular) was also known as a *ratio accepti et expensi* ("an account of deposits and payments") and *ratio implicita proper accepta et data* ("a complex account including both deposits and payments"). A deposit banker was required to make such books available for production in a trial involving a client, even where the deposit banker was not a party to the litigation.[57] For his part, the deposit banker was obligated to maintain books, to account for the various entries, and to state a balance owed between himself and the customer.[58]

Payment services were operated in conjunction with deposit banking in *Greco-Roman Egypt*.[59] Public granaries in Greco-Roman Egypt, connected into a network of grain depositaries, operated a countrywide system of payment in agricultural products, such as oil and wine. Particularly however, they ran grain warehouse banking, facilitating payments out of and into deposits of grain, for both public authorities and individuals.[60] The system maintained grain accounts and recorded transfers. For each yearly harvest of each type of grain the various deposits were physically amalgamated so that credit to an account reflected a claim to a share in the mixture rather than to a physically segregated or separate deposit; it seems though, that no lending was made out of the mixture, so that full reserve was held to back all credits to the deposit accounts.[61]

Book-based transfers could occur between accounts in the same granary, same region, or different regions. For an inter-granary transfer, an adjustment was made not only to transferor's and transferee's accounts, but also over a system of inter-granary accounts.[62] A comprehensive account management system thus existed in each granary, in each region, as well as in Alexandria, from which the entire system was overseen. Effectively, this was the forerunner for a nationwide credit-push giro mechanism,[63] under which payment orders were executed by means of crediting and debiting accounts.[64] The system was however doomed to wither away together with the disappearance of specie and kind as universal mediums of exchange.[65]

So far as the monetary economy of Greco-Roman Egypt[66] was concerned, the banking system formed a network and assumed a key role in carrying out treasury operations for the central government and other public authorities. Each regional royal bank operated in conjunction with a network of village banks, which effectively functioned as branch offices for royal banks or more precisely, as points of collections and disbursements of funds[67] throughout the various districts of the country. However, the Royal Treasury, or the *basilicon*, in Alexandria,[68] did not serve as a central bank;[69] it neither maintained accounts for all deposits throughout the country, nor received surplus balances for such accounts, other than for the king. Nor did the *basilicon* oversee the

operation of the entire network; it did not even maintain accounts for the various royal banks into which adjustments for inter-district transfers could be made. Rather, each royal bank kept a separate set of records for its own account holders. Effectively, together with its village bank network, a royal bank operated as a stand-alone independent bank. It follows that there was no infrastructure facilitating a countrywide system for inter-district non-cash payments from an account in one royal bank to an account in another.

Throughout the Ptolemaic era,[70] both royal and private banks maintained deposit accounts for individuals.[71] Available documentation supports the existence of funds transfers from one account to another[72] in private banks[73] as well as for tax payments from accounts maintained in royal banks.[74] Documentation further supports the existence of bilateral correspondent relations between private banks, namely instances where one bank holds an account with another.[75] At the same time, there is no indication of any multilateral bank clearing arrangement; and certainly, any claim to the existence in Greco-Roman Egypt of a "centralized state giro system"[76] is not well founded.

Royal banks in Ptolemaic Egypt pioneered a nascent check system.[77] The drawer would issue a non-transferable check to the payee and send a "control note" to the drawee bank, which would match it with the check upon its presentation. Checks were non-transferable. The payee would present the check to the payer's bank, either in person or through an agent, and be paid usually in cash Alternatively, payee could have his account credited with the payer's bank. In the further alternative, where the payer's bank kept an account with the payee's bank, payee would instruct the payer's banker to draw on the payee's banker a check payable to the payee. The payee would then present that check to the payee's bank, which would then debit the account of the payer's bank and credit that of the payee. Being drawn by one bank on another, the check issued by the payer's bank was the forerunner of a bank draft or money order.[78] Check use had been eclipsed in Egypt in the course of the Roman period.[79]

## B. Middle Ages

In *West Europe*, during the early centuries of the Middle Ages,[80] the economy collapsed and trade was reduced to a trickle. The monetary economy survived only in a rudimentary form[81] and banks disappeared from the West after the fourth century C.E.[82] Banking services reappeared in Europe in the later part of the Middle Ages to satisfy the growing demands of trade. "Genoa happens to preserve the earliest notarial minute books that have survived (from 1154 on) . . . [which] are the first source that contains a fairly large number of documents showing bankers at work."[83] Deposit banking, in the form of taking

deposits and lending out of them in the depositary's own name, was reborn in Italy and "exported" elsewhere[84] in the course of the twelfth and thirteenth centuries, as part of a commercial revolution that took place as of the eleventh century or so.[85]

As originally in Ancient Greece, it was the money changer who commenced to take deposits, mix them, and lend out of them. By 1350, in becoming bankers,[86] money changers developed a system of local payments by book transfers, with the view of eliminating "[t]he great inconvenience of making all payments in specie, especially the waste of time involved in counting coin."[87] The system that developed was strictly local; no facility for inter-city book transfers is known to have existed throughout the Middle Ages.

Thus, between the late thirteenth and early fourteenth century the money changers of Venice, the *campsores*, became bankers.[88] They accepted deposits, lent out of them, and provided book transfer payment services from and to current accounts kept with them.[89] To eliminate fraud, a book transfer required the attendance of both payer and payee at the bank.[90] Ultimately, in some cases, the payer's attendance could be dispensed with and the payer's banker was prepared to act on the payer's instruction presented by the payee. The Medieval non-transferable check was thus born, as a payment order issued by the payer to the payee instructing the payer's banker to pay to the payee, as well as authorizing the payee to collect from the banker. It was however not widely used.[91]

Bankers held accounts with each other, which possibly allowed for intra-city interbank transfers[92] which may have been settled only on irregular intervals. Each bank kept with it only a fractional reserve, namely, a limited amount of coined money, ready to satisfy an anticipated demand for cash withdrawal; it lent or invested most of the money received on deposit. Availability of payment by book transfers, recognized by early fourteenth century legislation in Venice, allowed banks to reduce cash holdings and increase their investments and credit extensions.

However, throughout the Continent, during the fifteenth century, private deposit banks declined. Repeated bank failures undermined the confidence of merchants and further triggered hostility by public authorities.[93] Together with a chronic shortage of good coins, the increased risk in keeping money with a banker led to a devaluation of "bank money" compared to that of "coined money."[94] Ultimately, in a process that "did not gain momentum until the last quarter of the sixteenth century," public banks gradually replaced private banks in commercial centers.[95] Heralding this development, Venice gave rise to a "distinctive style" of banking, referred to as giro banking, under which the primary purpose of banks was the making of payments on behalf of customers rather than making loans.[96] For its part, the Bank of Amsterdam, "established in 1609

under the guarantee of the city,"[97] was a leader among the post-medieval public banks.[98]

During the late Middle Ages, and to accommodate intercity commerce, exchange banking evolved in Continental Europe side by side with deposit banking.[99] It was practiced by large merchants who lent to exporters located in one market, who in turn sent goods for sale in another market. Repayment was made out of the proceeds of the sale, in the destination market, by the seller's correspondent to the lender's correspondent in that market.[100] This practice gave rise to the bill of payment, being the predecessor of the bill of exchange.[101] For their part, exchange bankers formed an intercity network that gave rise to the emergence of an elaborate multilateral clearing and settlement arrangement, implemented by them periodically in medieval fairs.[102]

## C. Post-Medieval Era

Against this background the modern banking system, accommodating the present payment system, was born in post-medieval *England*. Its roots are in the institutional transformation of the goldsmiths' system and the establishment of the Bank of England that followed.[103]

The process involved (1) the transformation of the business of individual goldsmiths into that of deposit bankers who accepted deposits, and lent out of them, including by discounting bills of exchange. As bankers they also facilitated depositors' check payments out of and into the deposits; (2) the existence of a tight network of all such goldsmiths ready to extend credit to each other, so as to allow for reciprocal correspondent banking services. Such services have facilitated interbank debt clearing and settlement, originally on a bilateral and later on a multilateral basis, leading to the establishment of a clearinghouse. This allowed risk reduction, enhanced efficiency, and the generation of common services that brought upon further development;[104] (3) the establishment of the Bank of England, originally as a lender to the government and then, having adopted goldsmiths' practices, gradually evolving in the subsequent two centuries into a modern central bank. As such it maintains settlement accounts for deposit bankers (being the successors of goldsmiths) so as to facilitate interbank final settlement as well as to become a lender of last resort;[105] and (4) the issuance of banknotes, first as circulating obligations of goldsmiths evidencing either deposits or loans, then as paper money issued by the goldsmiths, and ultimately, as paper money, "legal tender," exclusively issued by the Bank of England.[106]

Both correspondent banking and customer payment activity required intensive monitoring by the goldsmith-bankers. In turn, this facilitated credit

decision-making and led to specialization in advancing information-intensive non-traded loans. Such lending became a principal niche for a profitable commercial banking business as well as effective financial intermediation for the economy as a whole. In providing such loans, as well as in issuing banknotes and discounting bills of exchange, the goldsmith-bankers came to provide a reliable source of liquidity to the economy.

For its part, in departing from the model of the earlier Continental public bank, the Bank of England complemented private commercial banks without competing with or endeavoring to substitute for them. Rather, being their bank maintaining for them accounts,[107] it became able to furnish them with a source of liquidity so as to be a lender of last resort. As well, it provided them with the efficiency of multilateral settlement in reserve accounts held with it. In both ways, it gradually became as a "central bank" an integral part of the private bank network.[108]

The banknote was issued first by the goldsmith-banker,[109] originally possibly as a "warehouse receipt" for deposited coins, and subsequently against a fractional reserve of coins or metal.[110] The power to issue banknotes was taken over by the Bank of England,[111] with convertibility ultimately ceasing to exist altogether in the course of the twentieth century.[112] Using funds on deposit at the central bank, commercial banks buy banknotes from the central bank and sell them for use to the public, against funds held by their customers on deposit with them. As they are exchanged out of and back into deposits "according to customer payment habits," as a form of cash, banknotes (together with coins), are not the principal form of money, a role now preserved to money deposited in banks[113]

The integration of banks into a banking network, consisting of commercial banks multilaterally clearing in a clearinghouse[114] and settling on the books of the central bank, which is an integral part of this network, has led to a fundamental albeit subtle change in the mode of the creation of money through "banking." Thus, deposits made to commercial banks are typically not anymore in the form of specie or commodity money. Rather, they are primarily created by lending into customers' deposit accounts. For its part, an addition to a bank's liquid assets is typically made not in the form of specie or commodity money, but rather in the form of an increase in the sum credited to that bank's own account; at least for a large bank such increase is in the credit to its account with the central bank.[115] Other than by receiving an interbank payment, liquidity designed to meet deposit obligations is obtained at least by a large commercial bank, in the form of credit posted to its account with the central bank, through borrowing in an interbank market, selling government securities, or as a last resort, borrowing from the central bank.

At the same time, non-cash payment activity continues to be primarily carried out over deposit accounts held in commercial banks. Monitoring depositors' payment activity in accounts continues to facilitate credit decision-making and lead to specialization in advancing information-intensive non-traded loans, so as to continue to be a principal niche for a profitable commercial banking business as well as effective financial intermediation for the economy as a whole.[116] This must be true also in an era where credit information may be available from other sources such as credit bureaus.

The architecture, instruments, and institutions of the English system spread globally. At present, commercial banks take deposits from the public, lend into customers' deposit accounts, and provide payment services in conjunction with deposit accounts. In each country, at least all major commercial banks clear multilaterally and settle over deposit accounts they hold with the central bank.[117] They also maintain correspondent relationships[118] with local small banks as well as with cross-border or overseas large banks, so as to create a global network over which in principle non-cash payments can be made by any account holder to another in any currency. Moreover, as a rule, paper money in the form of banknotes is issued in each country by its central bank.

Banknotes, together with coins for small change, constitute cash (or currency). Payment in cash is typically made face to face, without any intermediation. Non-cash payments, whether face to face or between distant parties, require intermediation. Where payer and payee hold their respective accounts with the same bank a non-cash payment is carried out by that bank debiting the payer's account and crediting that of the payee. Where payer and payee hold their respective accounts at two banks that are correspondents, a non-cash payment involves debiting the payer's account by the payer's bank, crediting the payee's account by the payee's bank, and either debiting the account of the payer's bank by the payee's bank or crediting the account of the payee's bank by the payer's bank. In a domestic payment system, at least all major banks hold their accounts with the central bank so that the interbank component of payment between two such banks is carried out as part of the multilateral interbank settlement on the books of the central bank. Otherwise, a non-cash payment requires a chain of settlements on correspondent accounts, with or without settlement on the books of the central bank, or alternatively, one settlement between correspondent banks followed by another settlement on the books of a central bank. To take a simple example for the latter, the interbank component of a non-cash payment in Australian currency from a customer of Bank A in Canada to a customer of Bank B in Australia, assuming that the two are non-correspondent major banks, is carried out by Bank A using its correspondent,

another Australian major bank, which in turn settles with Bank B on the books of the central bank of Australia.

Three principal features characterize payment services facilitated by the modern banking system. *First*, value held on deposit with participating banks, often referred to as "bank money" or more specifically, "commercial-bank money" (or even "ledger money"), is denominated in and is redeemable to fiat money (or banknotes), that is, an official currency or "legal tender." *Second*, such value is in the form of a claim in an account maintained with a bank. Typically, this is an asset account; however, payment may be made by means of a credit card, in which case payment is carried from the payer's credit account rather than asset account having a positive balance in bank money. Also in such a case, payment results in an increase in the sum of bank money available to the payee in the payee's asset account—while the payer becomes obligated to reimburse the payer's bank, typically (if not exclusively) in bank money (originating from the payer's asset account). *Third*, claims against the central bank, often referred to as claims to "central-bank money," are available both to holders of fiat money/banknotes and the banks.[119] The latter multilaterally settle their reciprocal claims on the books of the central bank. Obligations on bank deposits payable on demand are referred to as "scriptural money," being a category covering both commercial and central bank money.[120] In principle, the sum of commercial bank money is a derivative of the sum of central bank money; the former is manipulated by the central bank's power to set interest rates through the sale of government securities to banks and/or lending to banks, primarily with the view of achieving price stability.[121] Gold reserves, which may be assets of a central bank, do not play any explicit role in the creation of the money supply.[122]

The non-cash payment system is then premised on the use of "scriptural money." Its architecture is *centralized*. Thereunder, a bank maintains deposit accounts for customers (who thus keep with it commercial bank money). For its part, a large bank may also maintain deposit accounts (in commercial bank money) for correspondent banks. Finally, the central bank maintains settlement (deposit) accounts at least for large banks (which thus hold with it central bank money).[123] As a whole, the system can be visualized as a pyramid at whose head or apex stands the central bank with which at least large banks hold accounts, and possibly with small banks holding accounts with large banks. Individual and corporate customers are at the bottom or base of the pyramid holding their accounts in banks (whether large or small).[124]

## IV. The Coming of the Cyber-Age: Electronic Payments, E-money, and Access to Central Bank Balances

### A. The Advent of Electronic Banking and E-money

Historically, payment instructions accessing bank money were either oral or, more typically, in writing. Use of telecommunication, first the telegraph and then the transatlantic cable, goes back to mid-nineteenth century.[125] However, the watershed of electronic banking, where payments are processed as well as transmitted electronically, is a development of the second part of the twentieth century. Once it became possible to transmit instructions electronically, from a computer or computer terminal, the electronic funds transfer was born. Telecommunication in the electronic age was originally on cable or wire;[126] subsequently the wireless option became available,[127] and ultimately, instructions could be transmitted over the internet.[128]

Security in electronic funds transfer has been implemented by the physical protection of network components[129] and more recently by the introduction of tamper-resistant access devices and cryptographic data protection. Broadly speaking, "cryptography" (literally: secret writing) denotes "a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it."[130] Strictly speaking, the term points at a specific method to that end, under which "complexity . . . is injected into data so that only those who possess a key . . . can remove the complexity . . . and understand the intended message, while those without the key will not be able to retrieve the hidden message in a timely manner." The "process of applying cryptography to a message so that only its intended readers can understand it" is called "encryption"; the reverse, namely the "process of using a . . . key to recover the intended message from its encrypted form," is called "decryption." Where the sender and receiver of a cryptographic message "share the same key data or mutually deducible key data," encryption is "symmetric." Otherwise, where they do not share the same key data, encryption is said to be "asymmetric." Either way secrecy is achieved by means of the application of mathematical theories. Cryptographic complexity addresses factors relating to the decryption of the message and its result.[131] Security is enhanced by the use of random data[132] to generate keys, since "patterns could be recognized [and] could aid in a brute-force attack."[133] Looking ahead, we note that security will be enhanced by the use of "quantum data," namely, data "marked" by merely being observed so as to alert the ultimate (designated) recipient to the fact that the communication had been intercepted.[134]

Developments exploiting such technological achievements have not been limited to communication. It became also possible to "load" monetary value

(that is, value denominated in an official or, in fact, any unit of account) on a tamper-resistant stored-value device such as a card or personal computer. In such a case, the value became known as "*electronic money*" or "*e-money.*" The majority of e-money schemes have involved "balance-based" products. In such products, devices store and manipulate a numeric ledger, with transactions performed as debits or credits to a balance. Accordingly, this type of e-money is a monetary balance or value recorded electronically on and is available from a *stored-value product* (SVP), such as a chips card, or a hard drive in a personal computer, or a server.[135] Such a record, accessible from the device without resort to the bank's computer system, can be viewed as a decentralized bank account.[136] E-money is said to "differ . . . from so-called *access products*, which are products that allow consumers to use electronic means of communication to access otherwise conventional payment services" in and out of bank accounts.[137]

A minority of e-money products may still operate on devices that store electronic "notes" (sometimes called coins or tokens) that are uniquely identified by a serial number and are associated with a fixed, unchangeable denomination. In such a "note-based" model, transactions are performed by transferring notes from one device to another, and the balance of funds stored on a device is thus the sum of the denominations of all notes on the device. However, as in the "balance-based" products, transferability is typically restricted, and consumer cardholders may usually make payments only to merchants who may clear these payments or deposit the accumulated balances exclusively through their acquiring banks.[138] Such a product provides the link between traditional value-transfer systems to innovative circulating digital coins discussed in Section V of this chapter.

Under a variant of a "balance-based" e-money product, monetary value is not loaded on the device; rather, it is available from a master account, belonging to the issuer or someone acting on the issuer's behalf.[139] As in the case of e-money, monetary value is not available from the payer-debtor's own bank account.[140] However, such prepaid value is in a bank account, even if not that of the payer. Its use entails communication to the issuer and requires the cardholder to access a bank account (even if not his or hers). From this perspective, a prepaid product device is more a variant of an access device rather than of an SVP.

According to Crawford, e-money is truly "money" when it may circulate from one person to another, that is, from one SVP to another, without being "cleared" or intermediated by the issuer.[141] This seems to me to be true for both "balance-based" and "note-based" e-money products. However, upon reflection, also e-money, in all its manifestations, is ultimately a variant of "bank money";[142] thus, whether e-money is purchased in cash or by means of a debit to the purchaser's bank account, the issuer has its own bank account credited

with the amount sold to the purchaser. Where the e-money is purchased from a bank the account credited is the reserve account of the selling bank. Payment in e-money is forwarded to the payee's bank, which credits the payee's account with the amount of payment and forwards the e-money itself for redemption against the value previously credited to the seller's account. In the final analysis, even where prepaid value or e-money is not issued by a bank, a scheme must facilitate the purchase and redemption through banks.

"Electronic banking" enhanced payment services in several other ways. *First*, it introduced electronic processing also to paper-based instruments such as checks.[143] Second, it facilitated new as well as variations of existing products.[144] Third, new players, such as money transmitters[145] or payment institutions,[146] and e-money institutions[147] entered the scene as end-payment institutions in a payment transaction, facilitating domestic and international payments in small amounts to parties who do not have bank accounts. *Fourth*, the power balance in the partnership between financial institutions and telecommunication carriers has shifted, allowing the latter a greater voice and share in the payment market.[148] *Fifth*, in facilitating instant communication, electronic banking allowed the use of risk reduction methods as well as instant authorization leading to an immediate final credit to the payee's account way ahead of the interbank settlement; such may be the case in domestic large value wholesale payment systems,[149] and retail fast payments networks.[150] This is also the case in a typical credit card payment, even when it is carried internationally.[151]

Electronic banking facilitated branchless banking to the detriment of banks with a large branch network.[152] As well, the possible impact of electronic banking on monetary policy has been fiercely debated.[153] At the same time, none of the various facets of electronic banking has affected the architecture of the payment system even as it expanded its scope and globalized it. No wonder, the law governing wireless instructions is the same as the one governing wire orders.[154] For their part, money transmitters, and payment institutions as well as e-money institutions have been using banks as intermediaries in the transfers in which they participate at either end of the transaction.[155] They thus increased rather than decreased payment intermediation. Furthermore, not treating such institutions as deposit-takers hinges on a "benevolent" strict view of "deposit-taking" so as to exclude the delivery of money for a specific purpose.[156] True, a payment instruction issued from a digital device such as a mobile phone rather than from a computer terminal or computer is often said to result in a mobile payment. When the payment scheme is operated over mobile devices it is even described as involving "mobile money." However, in substance, payment orders initiated from a digital or mobile device is a specie of an electronic funds transfer.[157] For its part "mobile money" is a form of "e-money." It is therefore confusing to treat such developments as reflecting a "digitization of state-issue

currenc[y]" even in connection with an online (e-commerce) transaction.[158] Ultimately efficiency is bound either to turn payment institutions into banks or for banks to take over payment institutions, either directly or as subsidiaries, so as to eliminate this unnecessary layer of intermediation. The issue for banks is the adoption of a different level of service rather than the elimination of banks as an essential component in linking between payers and payees.

The broader question however is whether "electronic banking" has not been superseded by "fintech," "snatching" money and payments from the banking system. "Fintech" (stading for 'Financial Technology') refers to the use of technology by IT firms[159] to deliver financial solutions directly to purchasers of financial products such as payment services.[160] Technology designed to deliver financial solutions is however available also to banks whether directly or indirectly by purchase from IT firms. Alternatively, IT firms may become banks and compete with existing banks on equal footing. It is not that "banking" survives while banks die;[161] rather, as an economic model banking has adopted new technologies to be used by old and new types of institutions. Whether and to what extent this remains true in light of subsequent developments is discussed further later on in this chapter.

## B. Availability of Central Bank Account Balances and Their Equivalents to the Public

In reviewing the present architecture of the payment system prior to the fintech era Goodfriend opined that "although valuing deposits at par and holding fractional reserves is efficient for individual banks, it had the potential for generating destabilizing systemwide bank runs." In his view this risk is however "remedied efficiently by central bank monetary policy,"[162] as well as by other payment system policies.[163]

Conversely, reviving and building on old ideas,[164] a recent set of proposals will make central bank money deposits available to the public either directly or indirectly Unfortunately it has become common to treat such a proposal as relating to central bank digital currency (CBDC).[165] This is however confusing; contrary to true digital currency schemes, discussed in Section V, such proposals, discussed immediately below, remain premised on both generic value in bank accounts and banks as payment intermediaries.

A typical rationale, for making central bank scriptural money available to the public is premised on new technological developments:

> Central banking evolved at a time when service provision in local branches was integral to providing banking services. In that world it made sense for the central bank to "wholesale" its core exchange settlement and liquidity

> support services to banks which would then "retail" them to individuals and businesses via their branches, passbooks and cheque accounts. It was impracticable for central banks' services to be provided to individuals.

At the same time, the rationale goes on, "[m]odern technology enables us to extend some core central banking services to individuals and businesses."[166] As a matter of history, the argument is doubtful, as post-medieval public banks, discussed in Section III(B) of this chapter, "retailed" their services to the public. At the same time, it is true that with the increase in the size and geographical scope of the bank customer base, a centralized system is workable only in an enhanced technology environment. Hence, banking-centralization proposals merit consideration.

One proposal premised on this rationale is the provision of payment services to the public exclusively by a designate government agency that will take deposits from the public but will have restricted investment powers so as to be able to invest only in safe assets such as super-collateralized real estate mortgages. Under that proposal, payment transactions will be carried out over deposit accounts with respect to which the liability of the depositary (the government agency) is effectively secured by investment in high-quality assets. On this basis, such deposits will benefit from unlimited guarantee of the central bank. Under that proposal, commercial banks will be able to lend to customers and sell them investment products but be precluded from providing payment services.[167]

However, one may reasonably suppose that in upsetting the delicate balance between the roles of the public and private sectors in the monetary and payment systems, this proposal will be perceived as going too far (or in fact, nowhere). Certainly, in monopolizing payment services in the hands of a government agency, the proposal will stifle competition and give no incentive to innovate. Furthermore, the proposal is not persuasive in mandating a central bank guarantee on the top of the requirement to invest deposited funds in safe assets. I therefore doubt that in a capitalist economy that proposal will persuade policymakers. At the same time, unclothing it from these objectionable elements, the proposal is reminiscent of an earlier idea, that of "narrow banking"; thereunder payment transactions are carried out over bank deposits of which the proceeds are invested in safe assets.[168] "Narrow banking" does not require the superimposition of a central bank guarantee and in fact does not alter the traditional roles of commercial banks as deposit-takers, providers of payment services, and lenders.

Under another proposal the central bank will open accounts and offer payment services directly to the public. This proposal is however said to impose "a large administrative burden" on the central bank that "could distract it from its other functions in [regulating] and managing monetary policy." It is further acknowledged that under the proposal the central bank, "a state-owned

enterprise," would undertake pure market functions, in which it "would have no commercial incentive to innovate [payment] services."[169] To meet these objections, under a variant, it is proposed that public access to scriptural central bank money or its equivalent will be indirect.[170]

There are however two alternative approaches to such a variant. One is premised on "full reserve banking"[171] while the other is of "plain sovereign money."[172] Briefly stated, under the former, the entire quantity of commercial bank money, namely, the total amount of demand deposits with banks, is to be backed by a 100% reserve of central bank money held by commercial banks on deposit with the central bank.[173]

Under the latter, that of "plain sovereign money,"[174] the distinction between the two types of scriptural money is abolished; what exists is only one category of scriptural money: central bank money.[175] It will be available to members of the public in accounts on the books of the central bank; unless operated by the central bank itself, as discussed previously, such accounts will be operated through and managed by commercial banks,[176] possibly in "transaction accounts"[177] that will be distinguished from "investment accounts" of which funds may be invested in designated collections of assets of a broadly similar risk profile. Each investment fund will be a distinct legal and corporate entity. Lending will be carried out of investment funds (possibly as well as from long-term borrowing from the public) and should not create additional money or purchasing power.[178] Investment account holders will bear the risk of nonpayment on the due date, and not being available to them prior to that, sovereign money owed to them will not serve as commercial bank money. Rather, prior to maturity on the investment account, sovereign money deposited in them will be lent by the bank and thus will exclusively be used by borrowers from the bank.[179] Banking will thus fully reclaim its function as an intermediation between savers and borrowers.

Under both approaches commercial banks will cease to create money by lending into customers' deposits. Money creation will be under the exclusive power of the central bank[180] with commercial banks either being limited to issue its "replication" or "shadow" to the public, but not expand its quantity (under the full reserve banking alternative), or being restrained from issuing it at all (under the plain sovereign money alternative).[181] They will however be able to lend and provide payment services.

An analysis of the pros and cons of each alternative, vis-à-vis each other as well as by reference to the current fractional reserve regime, is beyond the scope of this chapter as well as of the competence of this author. At the same time, in relation to the topic at hand, under both alternatives banks will continue to accept deposits, make loans (albeit not out of demand deposits), and provide payment services. For sure, they may face competition from "payment institutions" that do not provide "investment accounts" services as well as lenders providing

"investment accounts" but not "payment accounts." However, it is reasonable to expect that such competitors will be regulated, respectively on the payment, and saving and lending sides, so it will be for banks to leverage the combined services they give to their advantage. For example, as now, monitoring the payment activity of a customer will help a bank in making its lending decision regarding that customer. Hence, a reform under any of these lines will not change the role of commercial banks in the payment system.

What may however change is the legal underpinning of the bank's liability for money deposited in the payments or transactions account. At the moment, a bank is liable to a depositor on a simple debt since money deposited belongs to the bank, which can use it as it wishes.[182] Conversely, under a "full reserve banking" scheme, the bank's obligation may be conceptualized by analogy to that of a securities intermediary under Article 8 of the *Uniform Commercial Code* in the United States[183] as well as under the Uniform Securities Transactions Act in Canada.[184] According to this legislation, under the "indirect holding" regime, a securities intermediary is liable to an investor on a "securities entitlement" against which the securities intermediary must maintain a 100% "financial asset."[185] At the same time, under a "plain sovereign money" regime the customers will have an entitlement from their banks under an "irregular deposit," which envisages a claim premised on an unidentified portion of a mixture of fungible assets (e.g., money) to which ownership passed to the depositary from the various depositors.[186]

In the final analysis, technological feasibility does not necessarily lead to economic justification. For example, as pointed out at the beginning of this section, albeit ahead of fintech, Goodfriend was on record highlighting the public's substantial efficiency gains of the fractional reserve at the cost of accepted risks, which are anyway mitigated by monetary policy, central bank lending, and deposit insurance.[187] To say the least, under the present system, banks are able to share with customers Sprofit realized from lending out of demand deposits; the chance is that, in a regime under which scriptural central bank money is available to the public in any form, payment services will be more costly. Whether and to what extent gains in safety outweigh efficiency losses may be in the eyes of the beholder. This section should be taken as outlining banks' continued role and relative advantage in a central bank scriptural money environment rather than necessarily to unequivocally support of such a regime.

## V. Cryptocurrencies: Heralding a New Form of Money and Payment Disintermediation?

Innovations discussed previously were accessing accounts and transacting digitally, expressing value on the screen of a digital device, storing value in an SVP

so as to give rise to e-money, and making central bank money or its equivalent available to the public. All have not changed the nature of an interbank transfer as a transfer of scriptural money in the form of a balance of monetary value. Nor have they changed the role of the bank as a payment intermediary.

This does not appear to be the case with the emergence of digital currencies. Very much like an electronic payment instruction, a digital coin consists of encrypted data expressed in strings of bits. However, as "an entity that amounts to a string of bits," a coin's string has a numerical value as well as a unique identity.[188] Like physical coins and banknotes, digital coins are not paid out of bank accounts, so their payment does not appear to require intermediation. And yet exactly as with electronic funds transfers, they are paid over cyberspace.

The ensuing discussion excludes currencies not linked to the real economy[189] and is limited to coins that could be liquefied and redeemed, so as to be available for use in real trading, as well as for purchase of goods and services. Payment by such digital coins has the potential of bypassing both the bank account and the centralized multilateral interbank settlement.

A digital currency may be issued either privately or by a central bank.[190] When it is issued privately it may have its own unit of account.[191] Either way, a scheme in which coins are issued and redeemed under a centralized protocol is said to be centralized.[192] A digital currency that is issued, transferred, and redeemed over a *distributed ledger* is decentralized. Finally, a digital currency transferable over a distributed ledger and yet issued by a centralized operator is hybrid.[193]

The distributed ledger underlying decentralization is an asset database that can be shared across a network of multiple sites, geographies, or institutions.[194] 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 computerized ledger on a distributed network, it generates a single version of the record on each computer and in essence is:[195]

> 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 authorized 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 and verify the execution of payment transactions[196] on a decentralized network. Cryptography is thus used in cryptocurrencies to express and protect the value of the coins (the