



THE GRAINGER COLLEGE OF ENGINEERING
SIEBEL SCHOOL OF COMPUTING AND DATA SCIENCE

CS 521

Technological Foundations of Blockchain and Cryptocurrency

Grigore Rosu

Topic 1 – Short History of Money



Thanks!

To Professors

David Tse (Stanford)

Sriram Viswanath (UT Austin)

Sreeram Kannan (UW – now at EigenLayer)

Non Metal Money

500 BC
For centuries



Image by [Bertramz](#) on Wikimedia. License: CC BY

Salt Bars - Ethiopia

13th century BC
Until 20th
century!



Image in the public domain by [Gary Todd](#)

Cowrie Shells - Nigeria

20,000 years?
11th – 14th c. in England
Abolished in 1834



Image by [Sandstein](#) on Wikimedia. License: CC-BY

Tally Sticks - England

Yap – Micronesia
Until 20th century
2000+ y.o. “ledger”



Image by [Yusuke Kawasaki](#) on Wikimedia. License: CC BY

Rai Stones - Yap

Metal Money

8th – 4th c. BC
Ancient Italy



Bronze Aes Rude - Rome

© Chuy1530 on Wikipedia. All rights reserved. This content is excluded from our Creative Commons license. For more information, see <https://ocw.mit.edu/help/faq-fair-use/>

17th – 18th c.



Cooper Plate - Sweden

© StAnselm on Wikipedia. All rights reserved. This content is excluded from our Creative Commons license. For more information, see <https://ocw.mit.edu/help/faq-fair-use/>



Bronze Spade - China

Image by [Mary Harrsch](#) on flickr. License CC BY-NC-SA

10th – 2nd c. BC
China (Zhou dyn.)
Abolished 221 BC (Qin dyn.)

Minted Money



Image by [Scott Semans World Coins](#) License: CC BY.

Bronze Yuan - China



Image by [Dadero](#) on Wikimedia. License: CC0.

Silver Dekadrachm - Greece



Image is in the [public domain](#).

Gold Aureus - Rome

Paper Money



Jiaozi Promissory Note - China



5 Pound Note - England

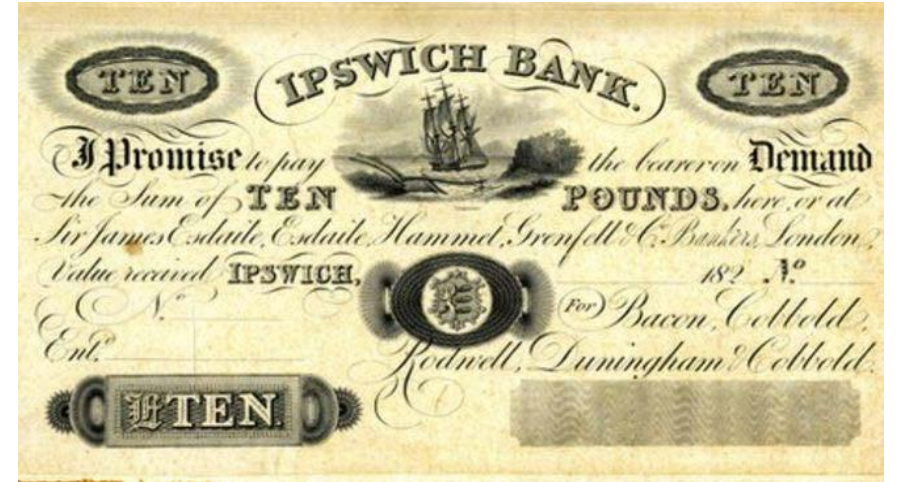


Continental Note – U.S.

Private Bank Notes



Australia



United States



Canada



England

Ledgers

Principal Recordings of Accounts



Proto Cuneiform
Uruk, ca 3000 B.C

1747 ⁽¹⁾ Mr. Bailly Washington D ^r				1747 ⁽²⁾ Per contra . 6 th L. J. D			
Sept 10 th	To two books	2/6	2 6	Sept 20 th	By a two foot Gunter	1/8	1 8
	To one D ^r Lomborg	2/6	2 6	Jan 11 th	By cash paid Robert Washington	1/8	1 8
July 20 th	To Cash D ^r Mr Lewis for 500 Nails		1 8	July 18 th	By Cash Received	2/6	2 6
1753	2 Pieces of paper Letter 2 Pieces of Leather			Sept 19 th	By 3 rd of Nov		
Aug 10 th	1 pound of Thread & 56 small nails			Nov 5 th	By 3 rd of Nov		

Personal Ledger
George Washington
1747

Ledgers

- Principal Recordings of Accounts
- Economic Activity
- Financial Relationships
- Types of Ledgers
 - Transaction vs Balance
 - General vs Supporting or Subsidiary or just Sub
 - Single Entry vs. Double Entry

Good Ledgers

- Immutable
- Consistency
- Timestamped
- Ownership
- Accuracy
- Description of Transaction
- Comprehensive

Payment System

A Method to Amend & Record Changes in Ledgers for Money

Deposits & Negotiable Orders



Ledgers – Early Money



Image by [sandsteir](#) on Wikimedia. License: CC-BY

Tally Sticks - England



Image by [Yusuke Kawasaki](#) on Wikimedia. License: CC BY

Rai Stones - Yap

Fiat Currency

- Social & Economic Consensus
- Represented by Central Bank Liabilities & Commercial Bank Deposits
- Relies upon System of Ledgers Integrated into Fractional Banking System
- Accepted for Taxes
- Notes & Coins are Legal Tender for All Debts Public & Private
- Unique Tax Treatment



Image by [epSos.de](#) on Wikimedia. License CC BY.

Central Banking, Money & Ledgers

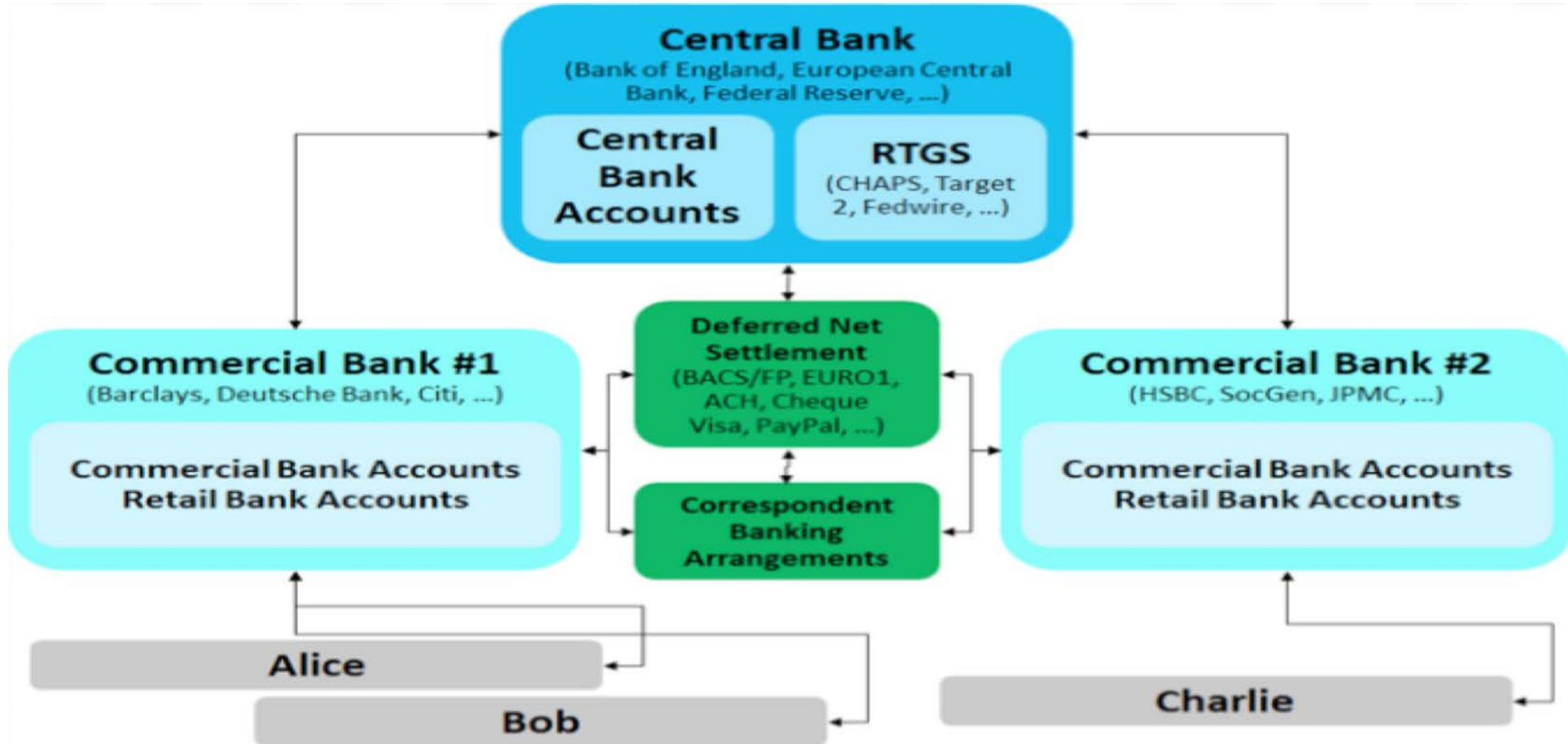
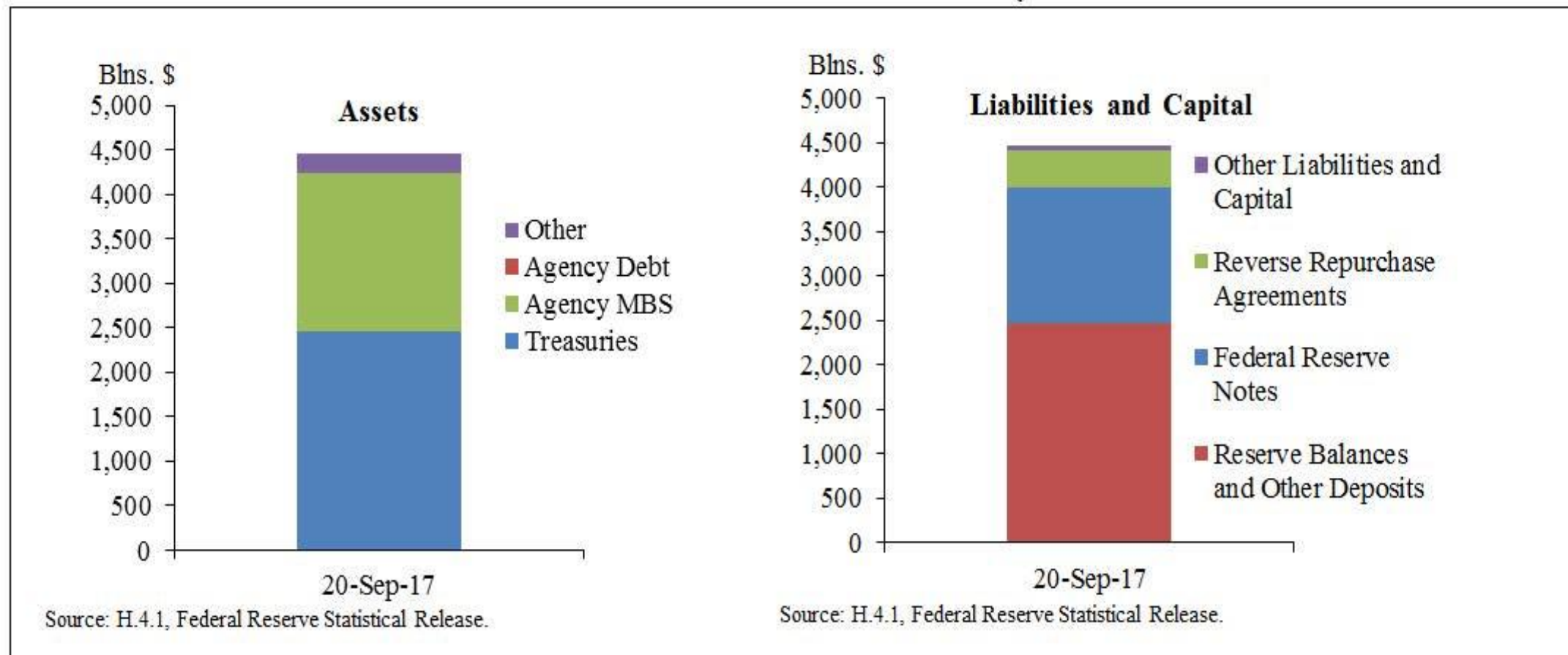


Image by Richard Gendal Brown from "Thoughts on the Future of Finance." Used with permission.

Central Banking, Money & Ledgers

Panel 1: Assets and Liabilities Today



Note: As of 9/5/18, Treasuries \$2.3, MBS \$1.7, Federal Reserve Notes \$1.6, Bank Reserves \$1.9 & Treasury Reserves \$0.3

Credit Cards

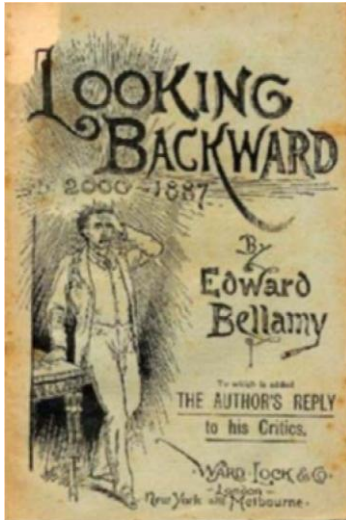


Image is in the public domain.

Term 'Credit Card'
Edward Bellamy's
Science Fiction
'Looking Backward'
1887



Charge Plates &
Credit Coins
Late 1880s – 1960s



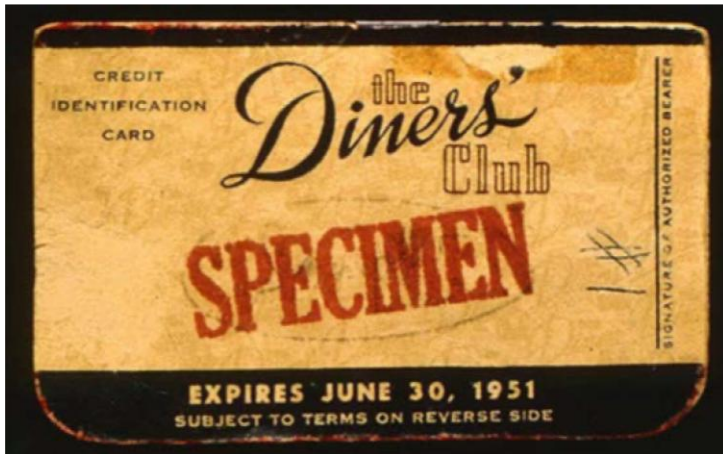
First Bank Card
Charge-It
First National Bank
Brooklyn, 1946



Merchant Credit Cards
Late 1920s – 2000s

© Bloomingdale's, First Bank, Ft. Worth General Tire Company, and Hotel La Salle. All rights reserved. This content is excluded from our Creative Commons license. For more information, see <https://ocw.mit.edu/help/faq-fair-use/>

Credit Cards



First General Merchant Card
Diners' Club
1949



American Express
First Plastic Card
1959

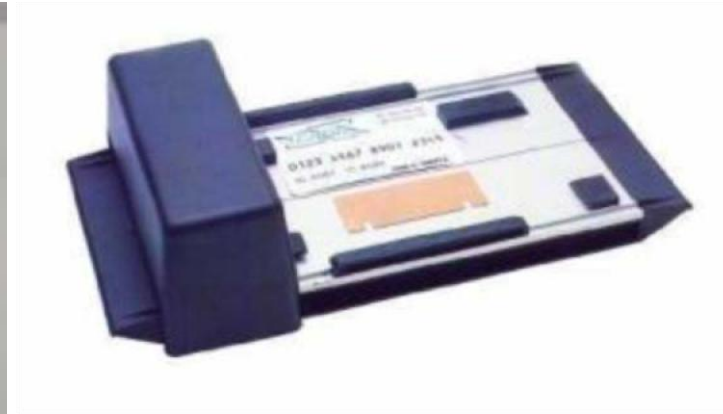


Bank of America
First General Purpose
Credit Card
1966

Credit Card Processing



Slide Card Imprinter
1950s

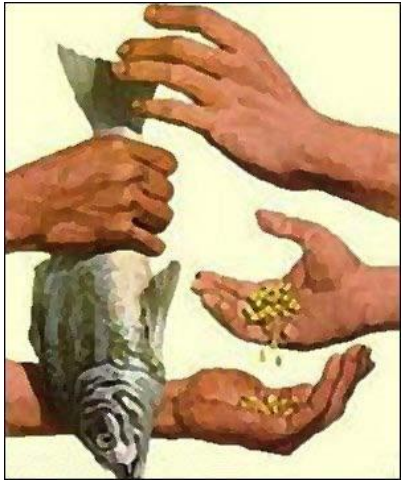


Visa Imprinter
1979



Payment Terminal
2018

Role of Money



© Source Unknown. All rights reserved. This content is excluded from our Creative Commons license. For more information, see <https://ocw.mit.edu/help/faq-fair-use/>

Medium of Exchange



Image by [Rob Pongsajapar](#) on flickr. CC BY.

Store of Value



Image by [ajalfaro](#) on flickr. CC BY-NC-SA

Unit of Account

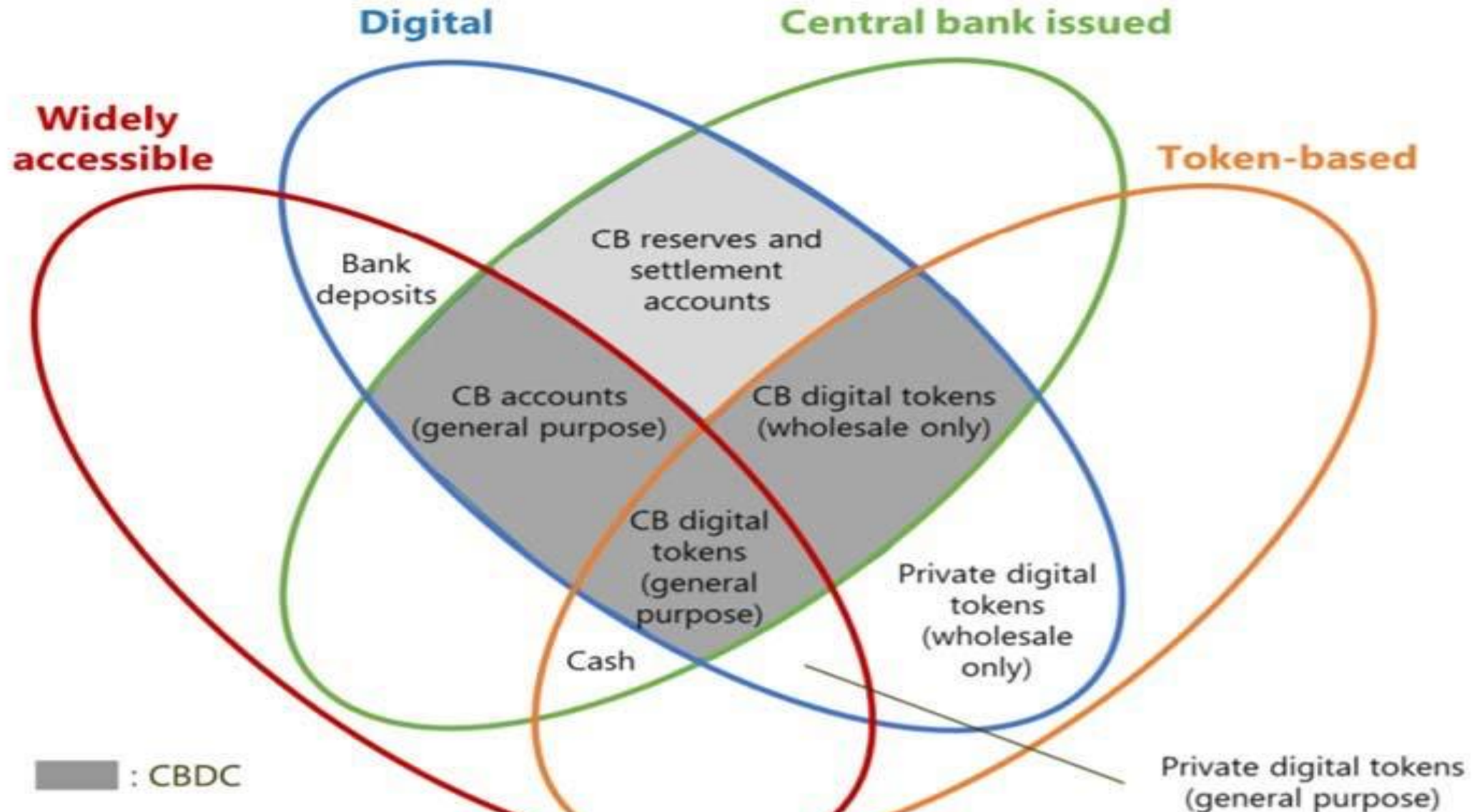
Characteristics of Money

- Durable
- Portable
- Divisible
- Uniform/Fungible
(Crawford v. Royal Bank 1749)
- Acceptable
- Stable - Limited supply - Hard to Counterfeit

Design of Money

- Token vs. Account Based
- Physical vs. Digital
- Private Sector vs. Central Bank
- Widely Accessible vs. Wholesale

The Money Flower



Early Cryptographic Digital Currencies ... All Failed

- DigiCash (David Chaum) – 1989
- Mondex (National Westminster Bank) - 1993
- CyberCash (Lynch, Melton, Crocker & Wilson) – 1994
- E-gold (Gold & Silver Reserve) – 1996
- Hashcash (Adam Back) – 1997
- Bit Gold (Nick Szabo) – 1998
- B-Money (Wei Dai) - 1998
- Lucre (Ben Laurie) – 1999

Why did Early Digital Currencies Fail?

- Merchant adoption
- Centralization
- Double spending
- Consensus

Double Spend attack

- A simple attack:
 - When one person can use the same coin multiple times to buy things
- Easily solved with a centralized system
- Much harder when decentralized

Digital & Mobile Payments



1998



1999



2003



2007



Mobile App

2011



2011



2013



2014

The Riddle Remained

How to move value
peer-to-peer
without any
trusted central intermediary

Bitcoin: A Peer-to-Peer Electronic Cash System

- From: Satoshi Nakamoto <satoshi <at> vistomail.com>
Subject: Bitcoin P2P e-cash paper
Newsgroups: gmane.comp.encryption.general
Date: Friday 31st October 2008 18:10:00 UTC
- “I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.”

A new layer?: Programmable transactions

