



CS 521

Technological Foundations of Blockchain and Cryptocurrency

Grigore Rosu

Topic 1 – Short History of Money

I ILLINOIS

Thanks!

To Professors

David Tse (Stanford)

Sriram Viswanath (UT Austin)

Sreeram Kannan (UW – now at EigenLayer)

Non Metal Money

I



Salt Bars - Ethiopia

500 BCE - For centuries



Cowrie Shells - Nigeria

13th century BCE - Until 20th century!



Tally Sticks - England

20,000 years? 11th-14th c. Abolished 1834



Rai Stones - Yap, Micronesia

Until 20th century - 2000+ y.o. "ledger"

Metal Money

I



Bronze Aes Rude - Rome
8th-4th c. BCE - Ancient Italy



Copper Plate - Sweden
17th-18th century



Bronze Spade - China
10th-2nd c. BCE - Zhou dyn. Abolished 221 BCE

Minted Money

I



Bronze Yuan - China
Tang Dynasty (618-907 CE)



Silver Dekadrachm - Greece
5th century BCE



Gold Aureus - Rome
1st century BCE - 4th century CE

Paper Money

I



Jiaozi Promissory Note - China

11th century CE - Song Dynasty



5 Pound Note - England

1793 - Bank of England



Continental Note - U.S.

1779 - \$55 Dollars

Private Bank Notes

I



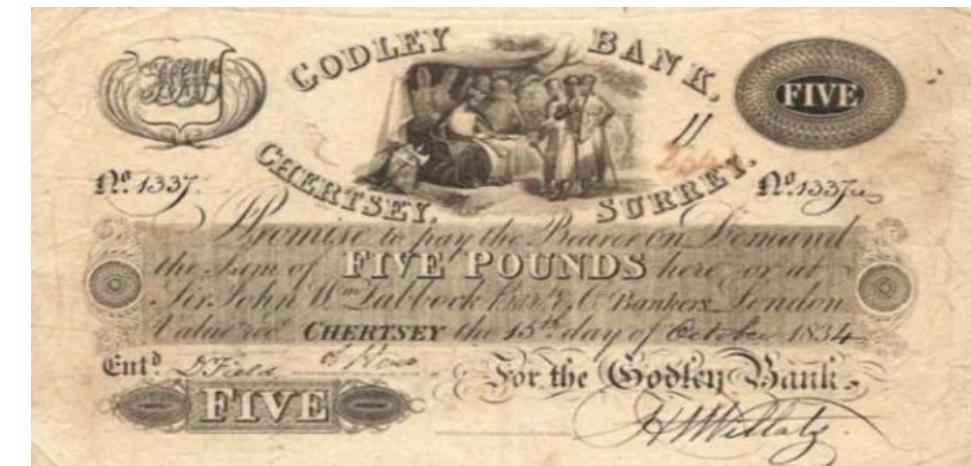
Australia - Commercial Banking Co. of Sydney



Canada - Bank of Prince Edward Island



United States - Ipswich Bank



England - Godley Bank



LEDGERS

Principal Recordings of Accounts

Early Ledgers



Proto Cuneiform

Uruk, ca 3000 BCE

1747	1 st Mr. Baily Washington Dr				
Sept 10	To two Books	2/6	2	6	
	To m ^d Dr. Scomberg	2/6	2	6	
July 20	To Cash P. M. Lewis for 500, 9 Nails	1	0		
1763	2 Pounds of yester Letter 2 Pounds ble Letter 1 pound of thread & 5 lb. small nails				
1747	2 nd Mrs Contra C	2	1	0	
Sept 25	By a two foot Gunter	1/3	0	1	8
Jan 11	By bank paid Robert Washington	1/3	0	2	8
July 10	By Cash Paid				
Sept 9	Contra	2/6	2	6	
Nov 3	By 3 P. M. Lewis				

Personal Ledger - George Washington

1747

Ledgers

I

- 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

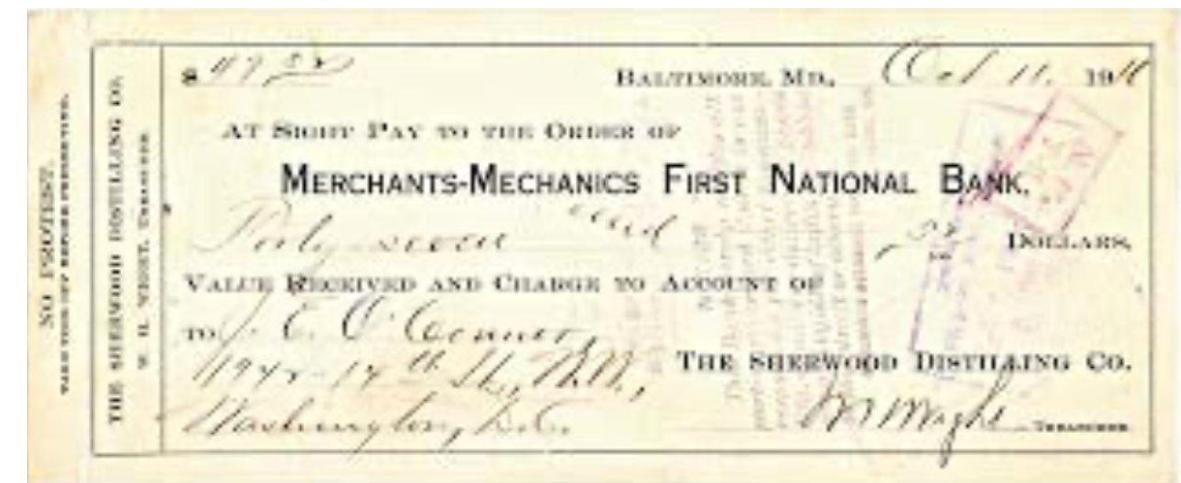
A Method to Amend & Record Changes in Ledgers for Money

Deposits & Negotiable Orders

I



Check - Tombstone, Arizona Territory
Ford, Hudson & Co. Bankers, 1882



Bank Draft - Baltimore, Maryland
Merchants-Mechanics First National Bank, 1911

Fiat Currency

I

- 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



Central Banking, Money & Ledgers

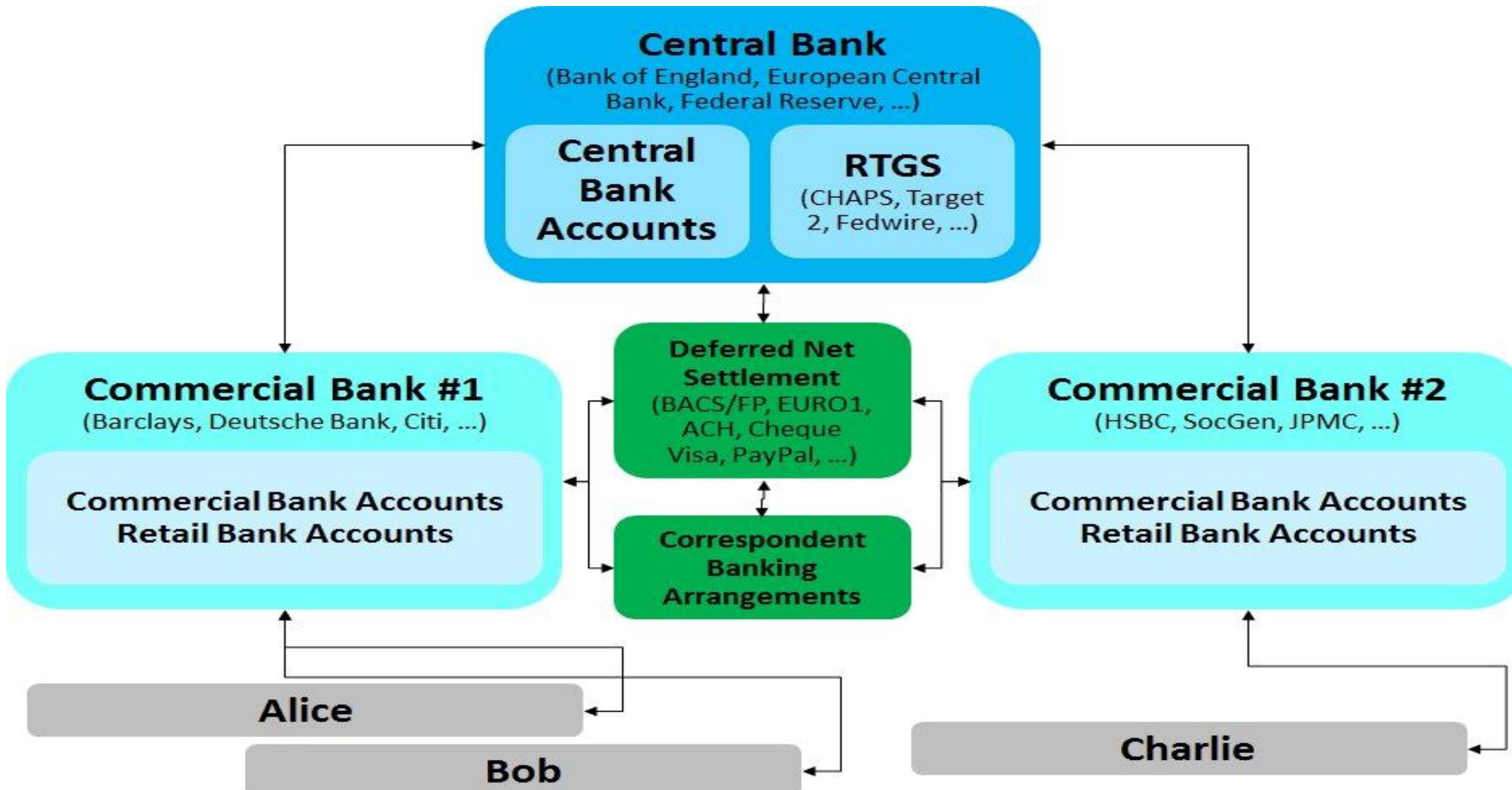
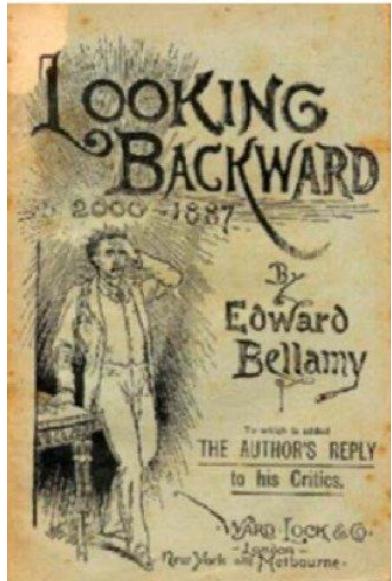


Image by Richard Gendal Brown from "[Thoughts on the Future of Finance](#)." Used with permission.

Credit Cards

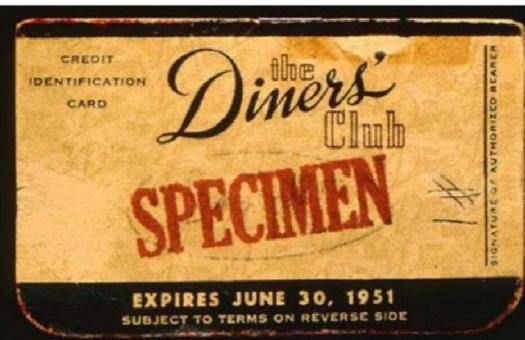
I



Term 'Credit Card'
'Looking Backward'
(1887)



Charge Plates & Credit Coins
Late 1880s – 1960s



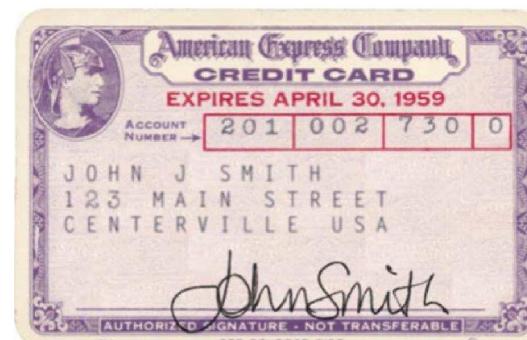
First General Merchant Card
Diners' Club, 1949



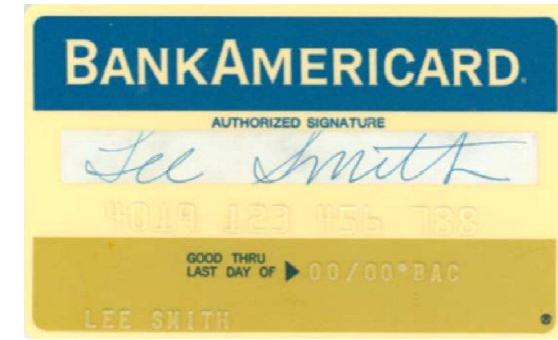
First Bank Card
Charge-It, Brooklyn, 1946



Merchant Credit Cards
Late 1920s – 2000s



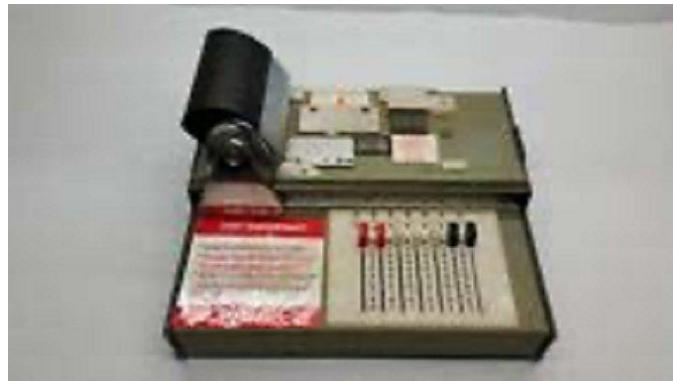
First Plastic Card
American Express, 1959



First General Purpose Credit Card
BankAmericard, 1966

Credit Card Processing

I



Slide Card Imprinter
1950s



Visa Imprinter
1979



Payment Terminal
2018

Characteristics of Money

I

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

Design of Money

I

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

Early Cryptographic Digital Currencies ... All Failed

I

- 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?

I

- Merchant adoption
- Centralization
- Double spending
- Consensus

Double Spend attack

I

- 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

I



1998



1999



2003



2007



Mobile App

2011



Google Wallet

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

I

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

I



- 2009

SSL / TLS - 1996

HTTP- 1990

TCP/IP - 1974

Ethernet - 1974

???

