



# 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



## **Salt Bars - Ethiopia**

500 BCE - For centuries



## **Tally Sticks - England**

20,000 years? 11<sup>th</sup>-14<sup>th</sup> c. Abolished 1834



## **Cowrie Shells - Nigeria**

13<sup>th</sup> century BCE - Until 20<sup>th</sup> century!



## **Rai Stones - Yap, Micronesia**

Until 20<sup>th</sup> century - 2000+ y.o. “ledger”

# Metal Money



**Bronze Aes Rude - Rome**

8<sup>th</sup>-4<sup>th</sup> c. BCE - Ancient Italy



**Copper Plate - Sweden**

17<sup>th</sup>-18<sup>th</sup> century



**Bronze Spade - China**

10<sup>th</sup>-2<sup>nd</sup> c. BCE - Zhou dyn. Abolished 221 BCE



# Minted Money



**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



**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



Australia - Commercial Banking Co. of Sydney



United States - Ipswich Bank



Canada - Bank of Prince Edward Island



England - Godley Bank

# LEDGERS

Principal Recordings of Accounts



# Early Ledgers



**Proto Cuneiform**  
Uruk, ca 3000 BCE

1747 <sup>(1)</sup> M <sup>r</sup> Bailly Washington D <sup>r</sup>				1747 <sup>(2)</sup> Per Contra C <sup>t</sup> L S D			
Sept 10 <sup>th</sup>	To two books	2/6	2 6	Sept 20 <sup>th</sup>	By a two foot Gunter	1/3	1 8
	To m <sup>d</sup> D <sup>r</sup> Leomberg	2/6	2 6	Jan 11 <sup>th</sup>	By bank paid Robert Washington	1/3	1 8
July 20 <sup>th</sup>	To bank P. M <sup>r</sup> Lewis for 500 <sup>l</sup> 10 s		1 8	July 10 <sup>th</sup>	By bank paid	2/6	2 6
1763	2 Pices of paper Letter 2 Pices of 10 <sup>l</sup> Letter						
Aug 10 <sup>th</sup>	1 penny of Thread & 56 small nails						

**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



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



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

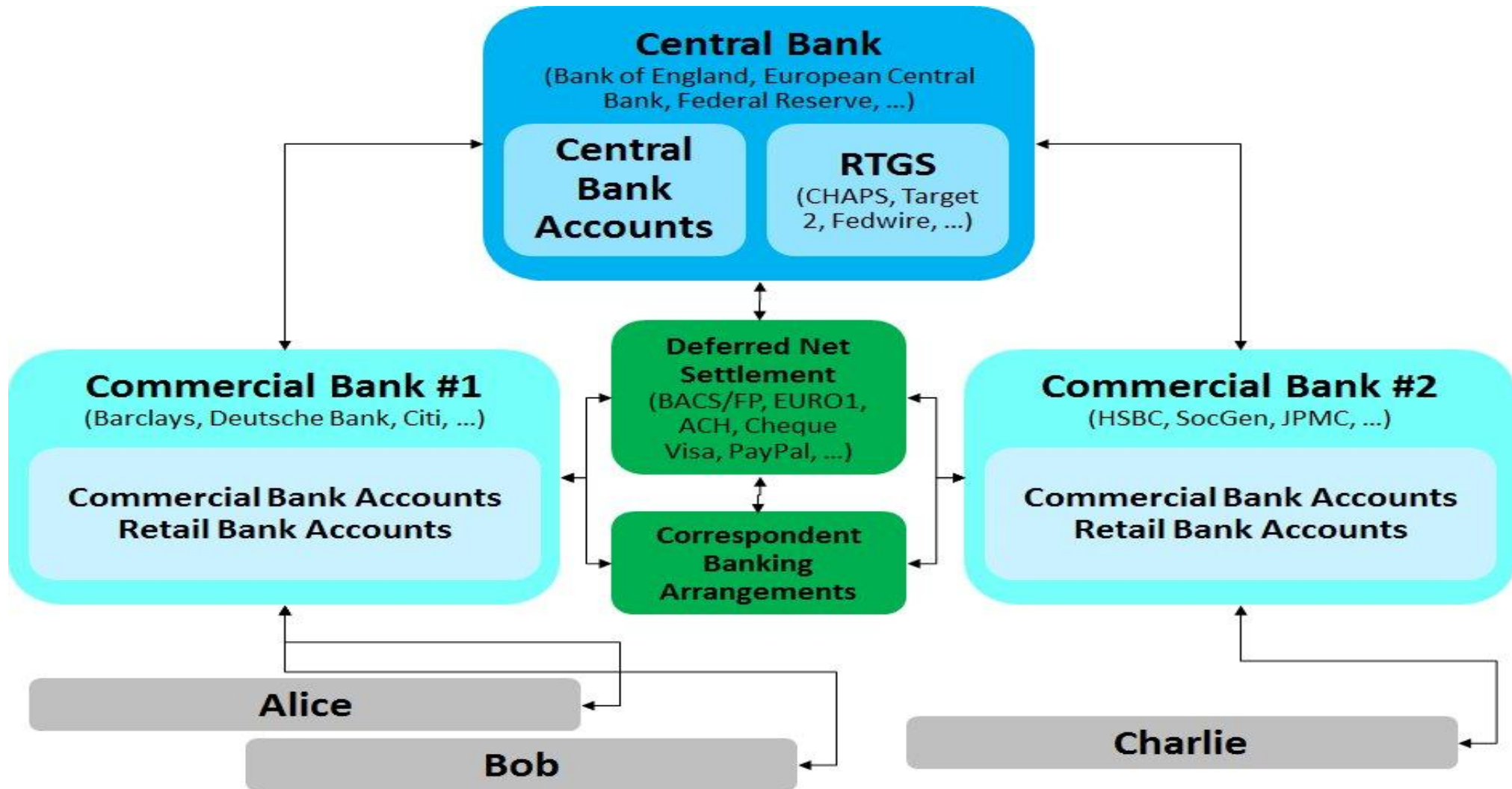
# Fiat Currency

- 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

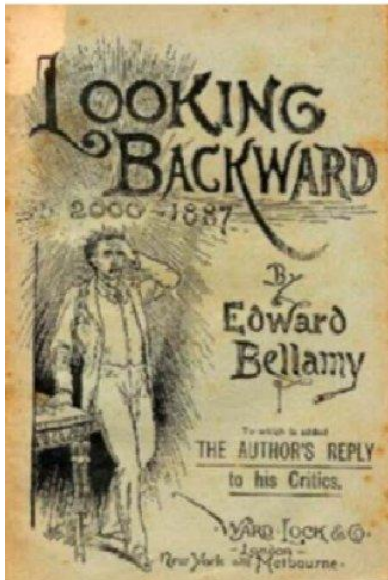




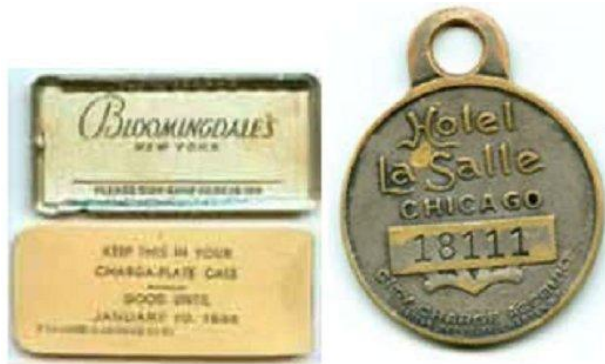
# Central Banking, Money & Ledgers



# Credit Cards



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



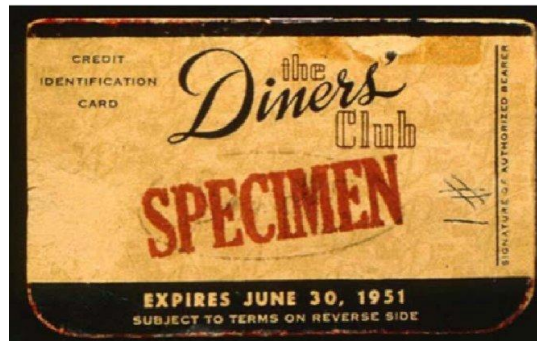
**Charge Plates & Credit Coins**  
Late 1880s – 1960s



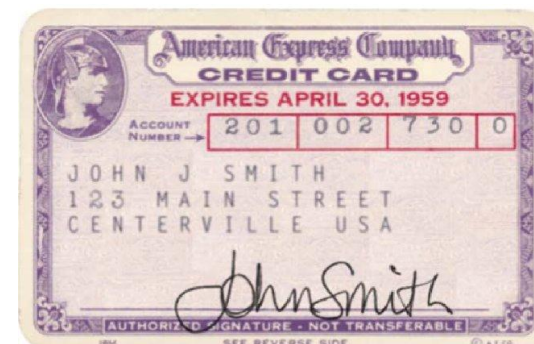
**First Bank Card**  
Charge-It, Brooklyn, 1946



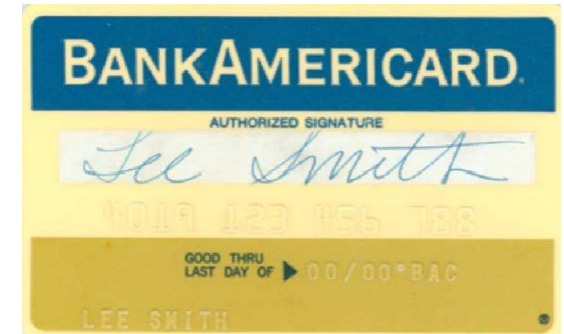
**Merchant Credit Cards**  
Late 1920s – 2000s



**First General Merchant Card**  
Diners' Club, 1949

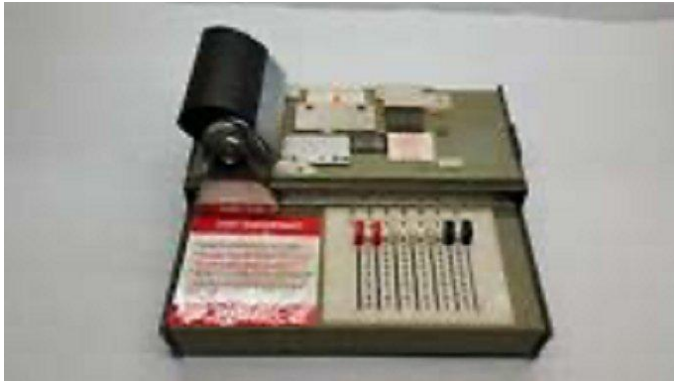


**First Plastic Card**  
American Express, 1959



**First General Purpose Credit Card**  
BankAmericard, 1966

# Credit Card Processing



**Slide Card Imprinter**  
1950s



**Visa Imprinter**  
1979



**Payment Terminal**  
2018



# Characteristics of Money



- Durable
- Portable
- Divisible
- Uniform/Fungible
  - (Crawfurd 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

# 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



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



SSL / TLS - 1996

HTTP- 1990

TCP/IP - 1974

Ethernet - 1974

???

