Bitcoin:
Programming the Future of Money

Topics in Computer Science - ITCS 4010/5010, Spring 2025

Dr. Christian Kümmerle

Lecture 4

Digital & Cryptographic Money

Key functions of money

- Store of Value
- Medium of Exchange
- Unit of Account

First identified by William Stanley Jevons in 1875
(“Money and the Mechanism of Exchange”)

RECAP: PROPERTIES OF MONEY

- **Divisibility:** Ability to be subdivided into various sizes
- **Portability:** Ease of moving across long distances
- **Durability:** Ease of preservation across time
- **Fungibility:** Different units/ items do not differ significantly from each other
- **Verifiability:** Ability of users to easily/cheaply verify integrity of money
- **Scarcity:** Cannot be abundant or easy to produce (“unforgeable costliness”)
- **Non-Monetary Utility:** Usage beyond money

ESTABLISHED HISTORY OF MONEY

- Is there a historical track record that something is working as a money?

CENSORSHIP RESISTANCE OF MONEY

- How difficult is it for an (adversary) external party to prevent the owner of the money from using it?

The Quest for Digital Cash

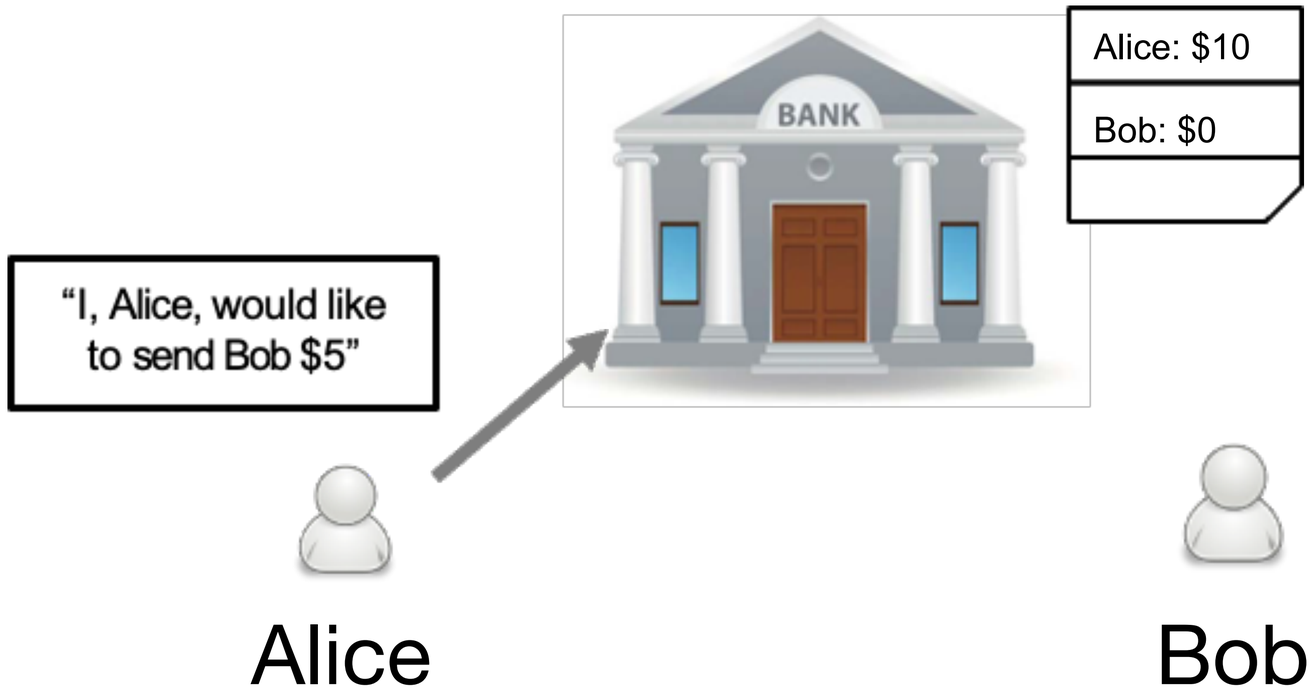
AREN'T PAYMENT ALREADY DIGITAL?

Money as Medium of Exchange over long distances

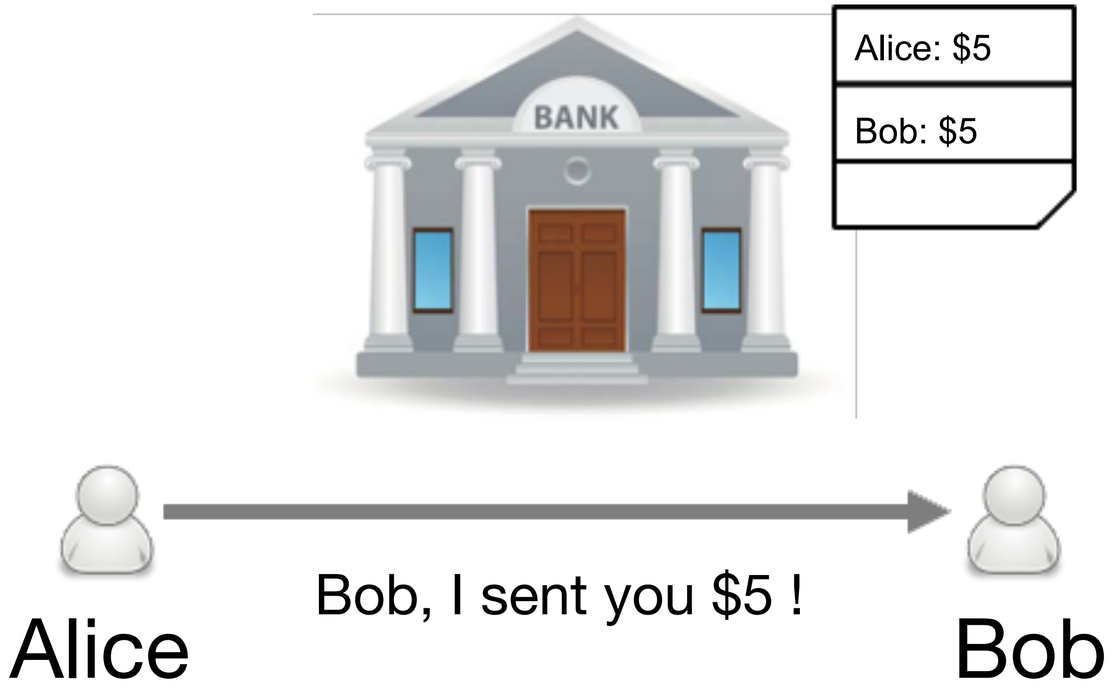
- Since 1837: Telegraphic communication between banks and banks and individuals for money transfers
- Later: Usage of phone, fax, internet…
- From 1973: SWIFT (Society for Worldwide Interbank Financial Telecommunication), standard for international bank wire transfers
- (Credit Cards)
- PayPal
- WeChat Pay, AliPay
- Venmo, CashApp, Zelle

Counter at a branch of Western Union

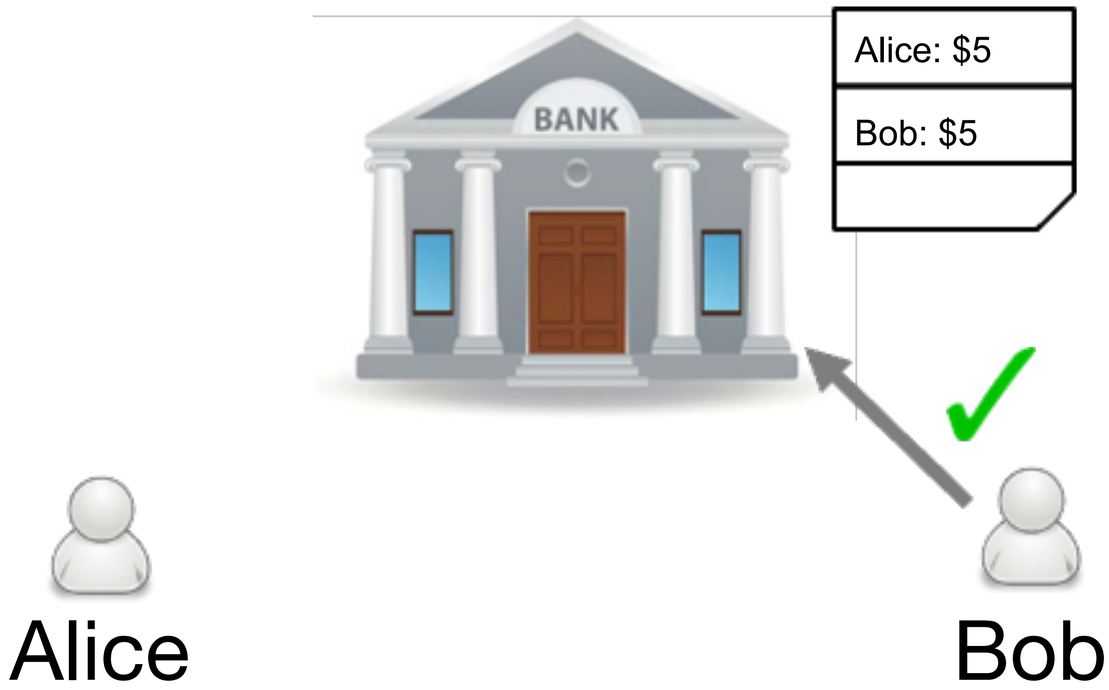
TRADITIONAL PAYMENTS



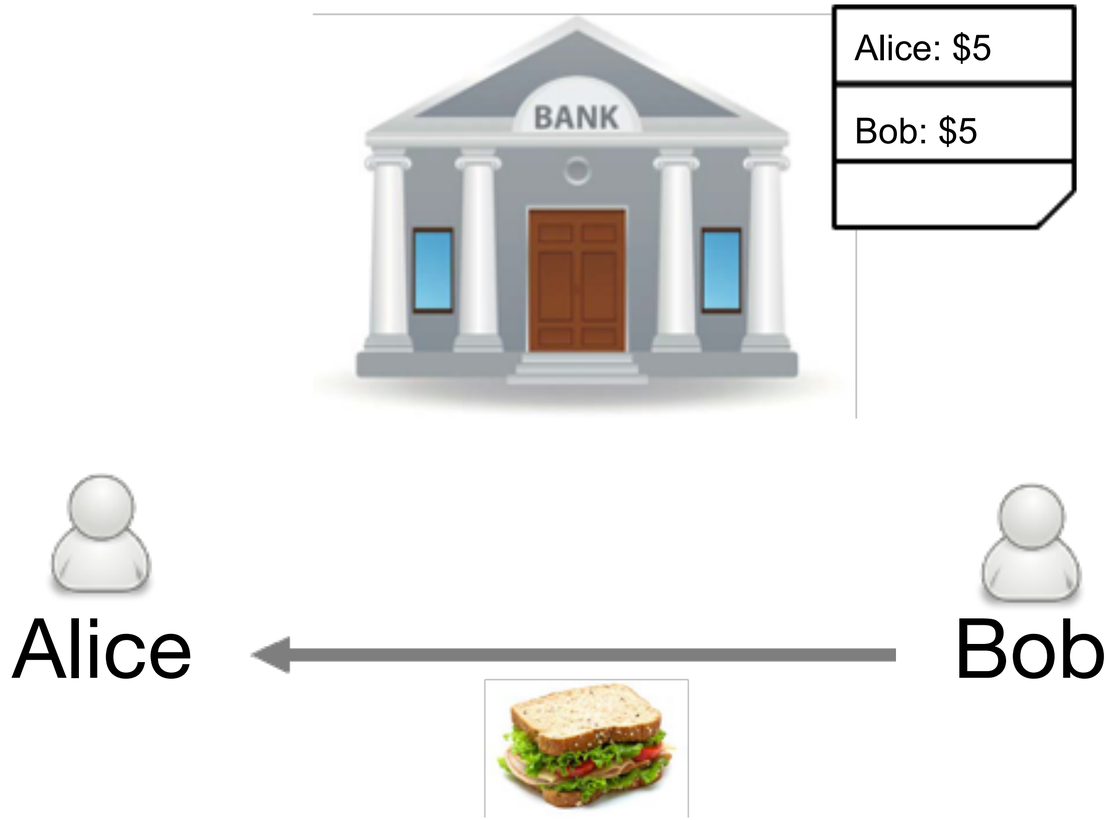
TRADITIONAL PAYMENTS



TRADITIONAL PAYMENTS



TRADITIONAL PAYMENTS



PROS AND CONS OF TRADITIONAL PAYMENTS

Pros

- Digital payments

Cons

- Not peer-to-peer (bank must be reachable during every transaction)
- Bank can fail
- Bank can delay or censor transactions
- Privacy

THE BANK CAN FAIL

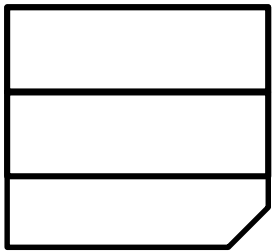
Alice: $10

Bob: $0

Alice

Bob

E-cash

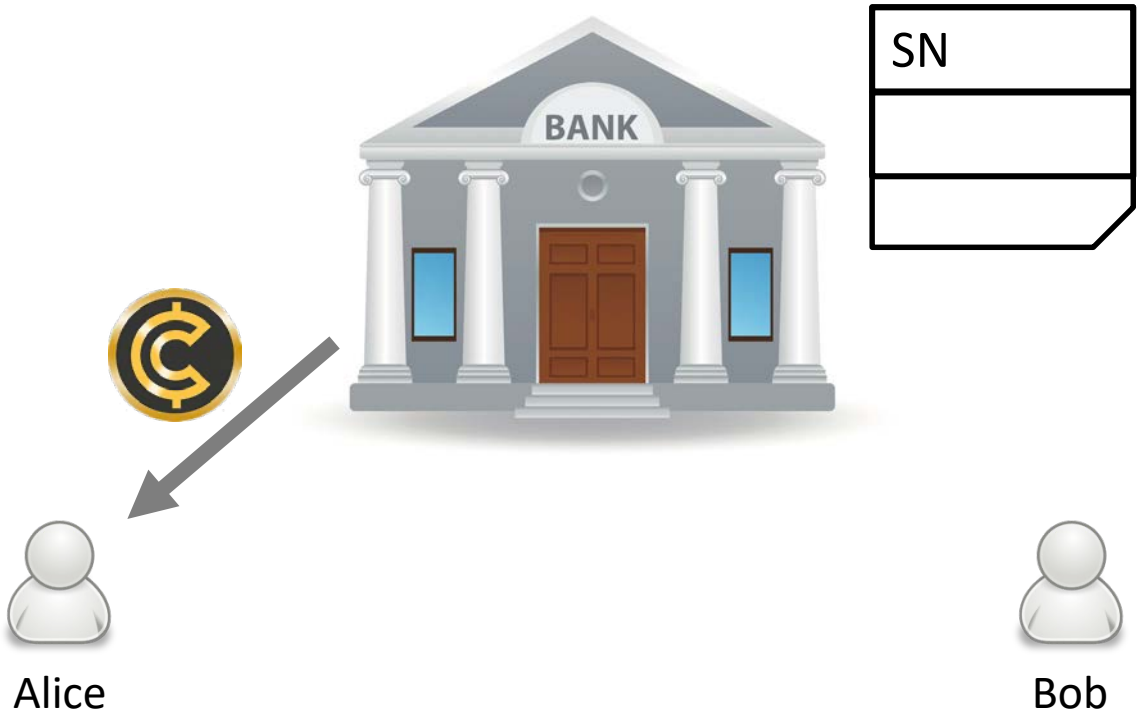


"I, Alice, would like a coin"

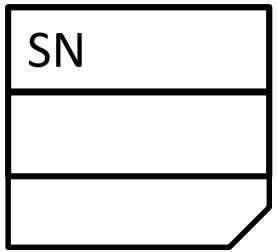
Alice

Bob

E-cash



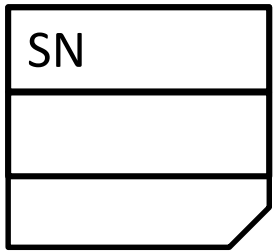
E-cash



Alice

Bob

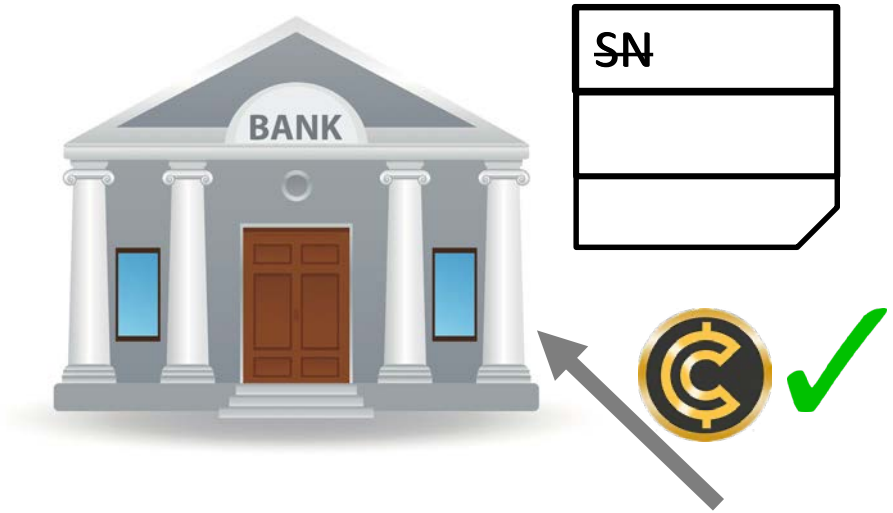
E-cash



Alice

Bob

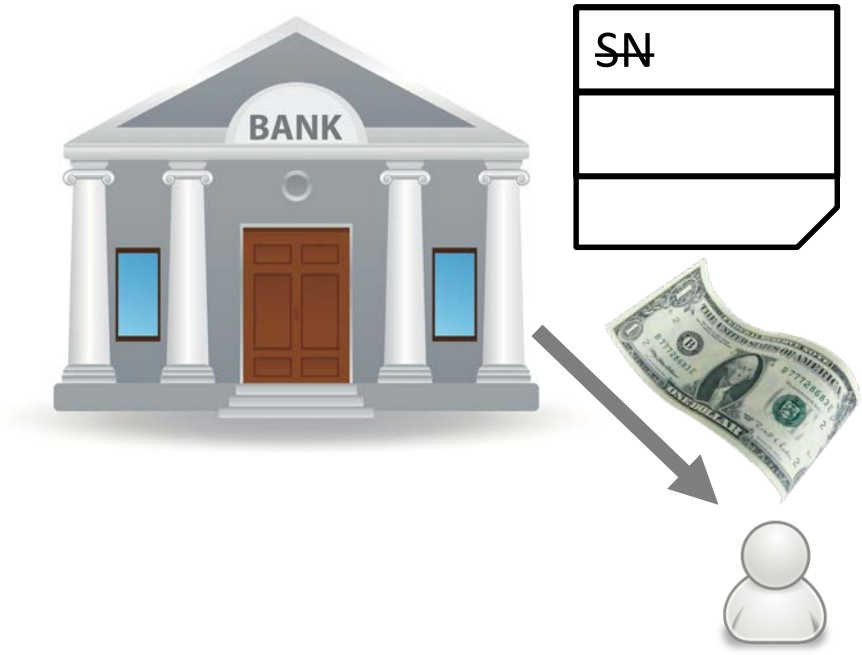
E-cash



Alice

Bob

E-cash



Properties of digital signatures

- Can be only be produced by signer, but verified by everyone
- Are tied to a particular document (the signed document)

Mimics the properties of a physical signature

PROS AND CONS OF “SIMPLE” E-CASH

Pros

- Digital payments
- Peer-to-peer

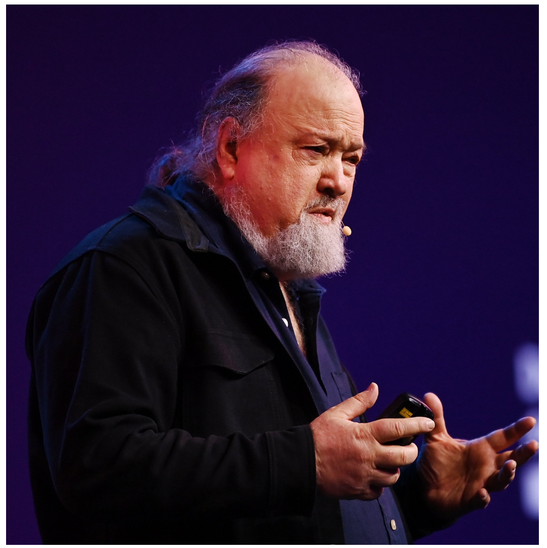
Cons

- Bank needs to be online to verify
- Bank can fail
- Bank can delay or censor transactions
- Privacy

Blind (digital) signatures

- Digital signature, with additional feature:
  Signing party **does not need to know/see**
  the content of signed document

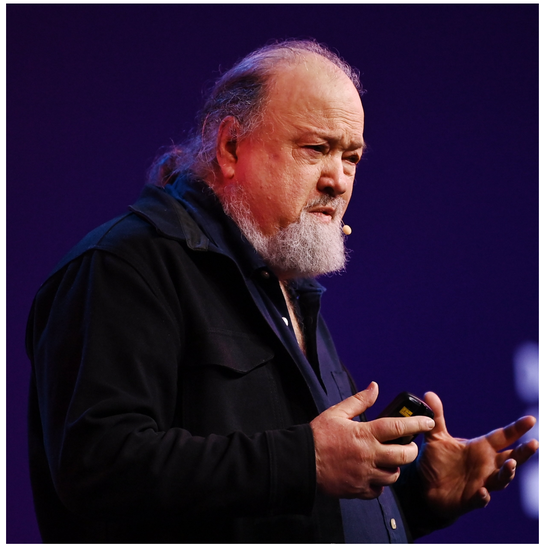
- Key tool to design first attempt for digital cash
- Can be implemented using **public-private key cryptography**



David Chaum (1955-)

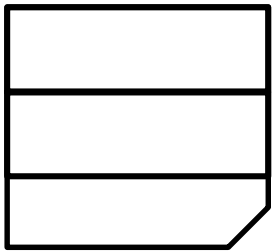
CHAUMIAN ECASH

- Proposed in 1983 by David Chaum
- Addresses fundamental problem:
  How to avoid a “double spend” in private transactions?



David Chaum (1955-)

Chaumian e-cash

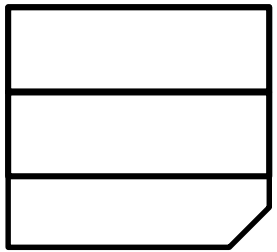


"I, Alice, would like a coin b(SN)"

Alice

Bob

Chaumian e-cash



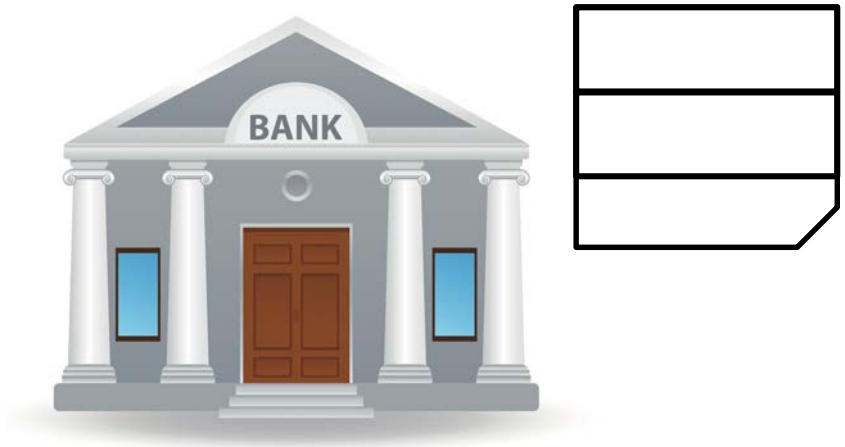
Sig(b(SN))

Alice

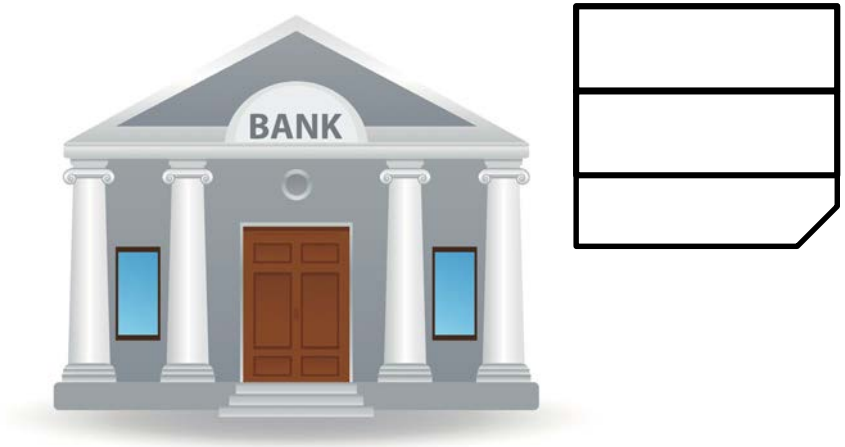
Bob

Sig(SN), SN

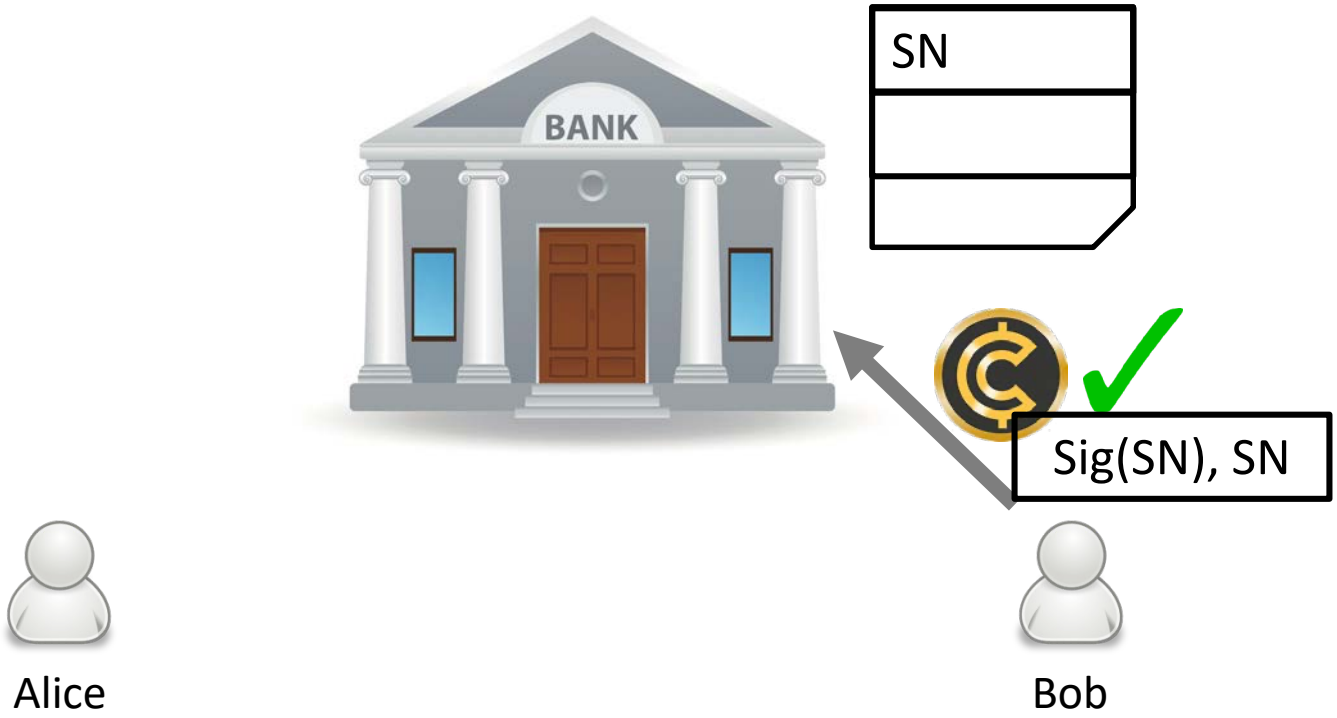
Chaumian e-cash



Chaumian e-cash



Chaumian e-cash



Double spend detection

PROS AND CONS OF CHAUMIAN E-CASH

Pros

- Digital payments
- Peer-to-peer
- Privacy
- Offline double-spend detection

Cons

- Bank can censor withdrawals and deposits

DIGICASH

- Company founded in 1989 by Chaum to commercialize idea
- Banks win 1990’s showed some interest
- Issued “CyberBucks” as a test
- Promise: Not issue more than 1 million units

- Failed adoption by merchants and banks, bankruptcy in 1998

Proponents: Georg Friedrich Knapp, John Maynard Keynes

- Government/state gives value to money by accepting it for payments of taxes ("legal tender")

DENATIONALIZATION OF MONEY

Reading Quiz 2:
F. A. Hayek's "The Denationalization of Money" (1976/1978)

Some key claims:

- Competition of independently issued, private moneys overcomes ills of government-issued currencies
- Market will favor more stable monies over less stable moneys

Friedrich A. Hayek
(1899-1992)
Austrian-British economist and political philosopher

FAILED ATTEMPT: E-GOLD

- Digital currency account system backed by physical gold stored in vaults
- Founded by oncologist Douglas Jackson in 1996
- $2 billion worth of transactions (2005), 5 million user accounts (2009)
- Anyone could open an account
- Irreversible transactions
- Transaction database stored on company servers

Final result:

- Despite attempts to register with government agencies and comply with law, shut down in 2005 due to legal issues
- Criticisms: Facilitates identity theft, phishing, money laundering

Reference: Wired, “Bullion and Bandits: The Improbable Rise and Fall of E-Gold”

HASHCASH

- Proposed by Adam Back in 1997 in cypherpunk mailing list:
  “A partial hash collision based postage scheme”
- Designed to prevent email spam
- Idea: Make a sender of an email do
  easily verifiable, but moderately costly computations
- Uses **cryptographic hash functions**
- Requires output of hash to have fixed number of leading zeros
- First “Proof-Of-Work” system with target level of difficulty

Adam Back (1970-)
British cryptographer

Limitations:

- Hashcash cannot be reused/spent by recipient
- Solution of problem gets easier the more computational resources are used
  -> possible inflation / availability of more and more hashcash over time
- Implemented in open source SpamAssassin, but never widely adapted

BIT GOLD

- Proposed by Nick Szabo in 1998
- Builds on Back's hashcash

- Innovations:
  - Introduces timestamping by chaining of hashing operations
  - Ownership of hashes associated to public keys
  - Transactions through digital signatures via private keys
  - Ownership registry distributed among "club member" servers

Nick Szabo (1964-)
American computer scientist
and legal scholar

Limitations:

- Consensus issues between different servers / versions of registry
- Inflation: Hash of certain difficulty relatively "harder" to produce in 1998 than in 2008
  -> To be addressed by free market, but introduces fungibility issues