

Cryptocurrency Engineering and Design

MAS.S62

2/7/2018 Lecture 1

Introduction

- Who we are
 - Neha Narula
 - Tadge Dryja
 - James Lovejoy (TA)
- Digital Currency Initiative
- Course
 - Lectures (20%)
 - Labs (40%)
 - Final project (40%)

Housekeeping

- Signup sheet
- Register!
- <https://github.com/mit-dci/mas.s62>
- fiorenza@mit.edu to join blockchain lunches, W 11:45 AM at Sloan
- Office hours Tuesdays 4-6 PM
- freenode #mass62

Cryptocurrency Engineering and Design

- What is a cryptocurrency?
- How is it different than a regular currency?
- What does it mean to build one?

What we are not going to do

- How to ICO
- Trading advice
- Permissioned blockchains

Origins of Money



SECURITY DEPOSIT RECEIPT

Owner/Lessor: _____

Renter/Lessee: _____

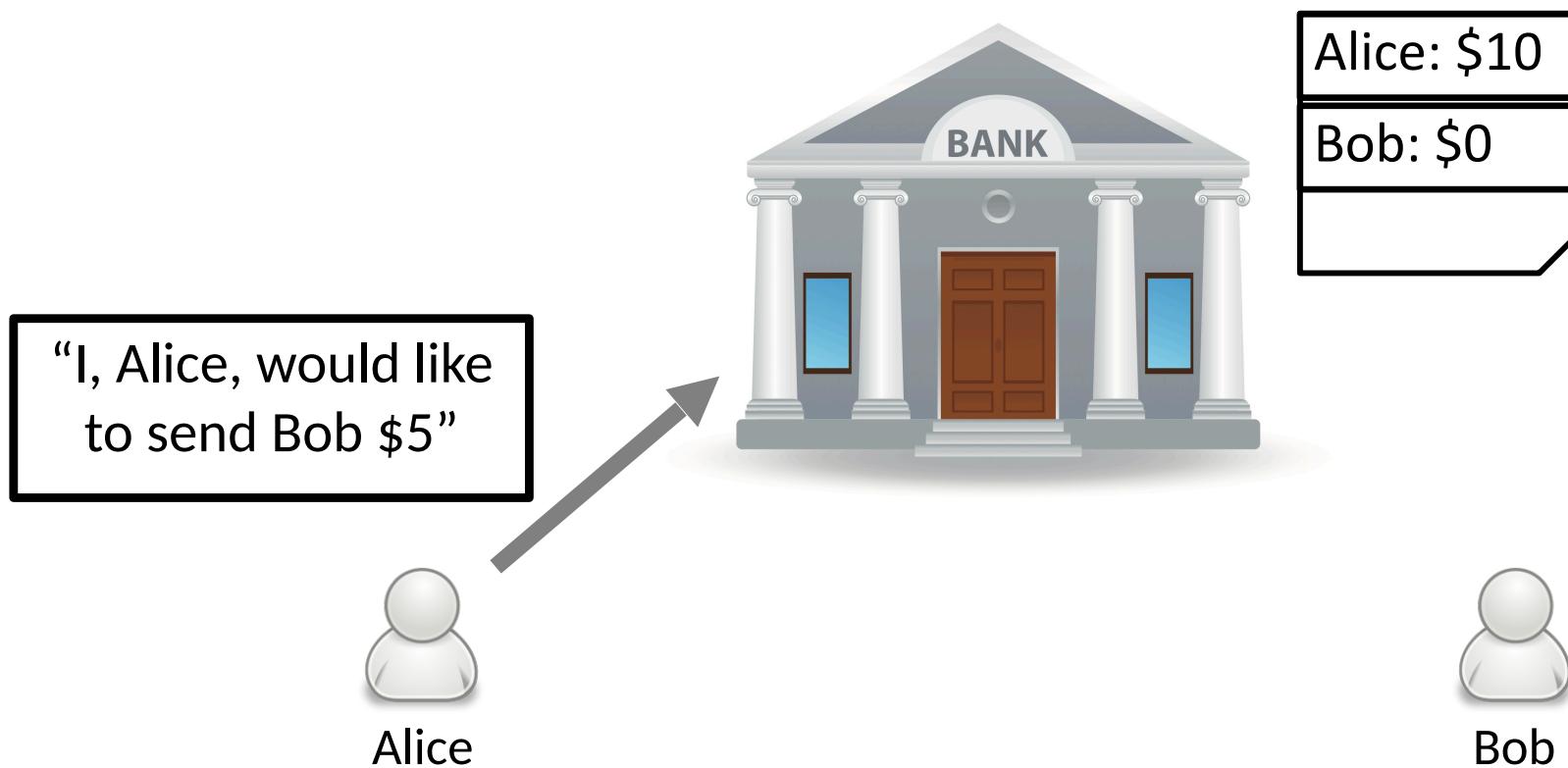
Property Address: _____

Security Deposit Amount: _____

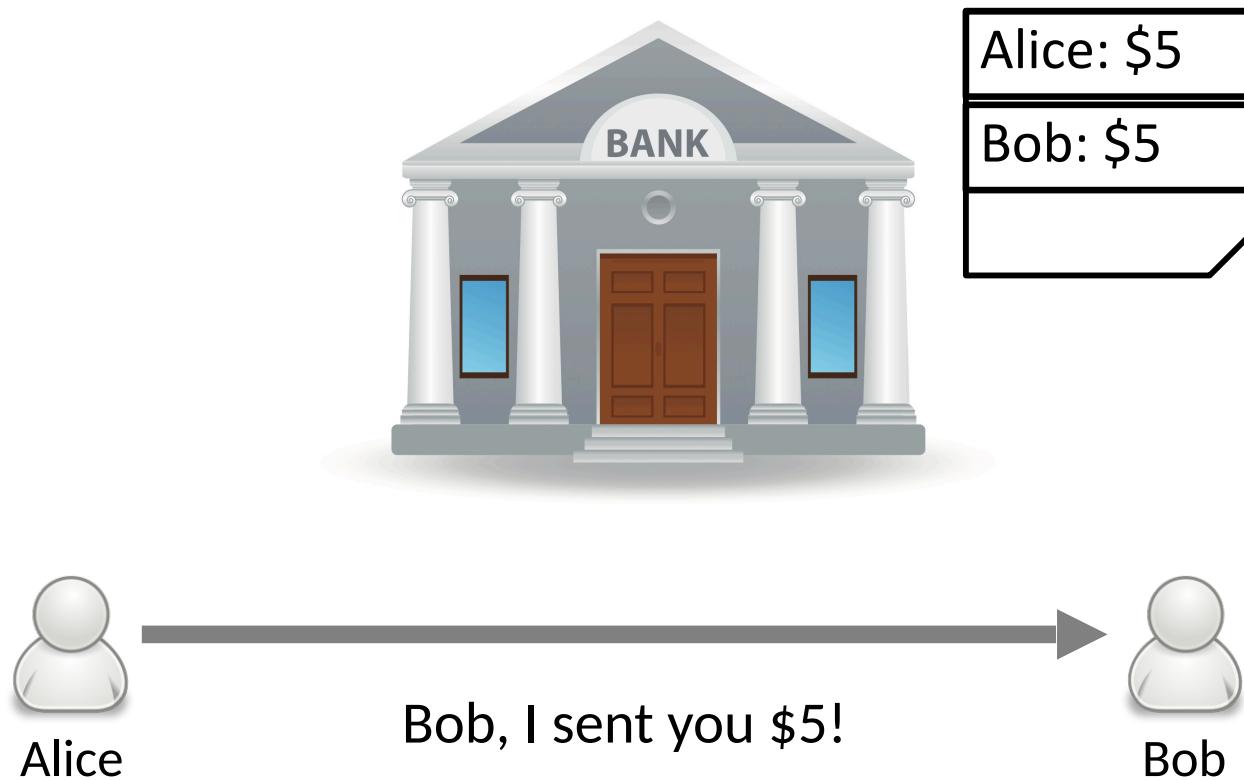
Received From: _____

Name/Address of financial institution where funds will be held:

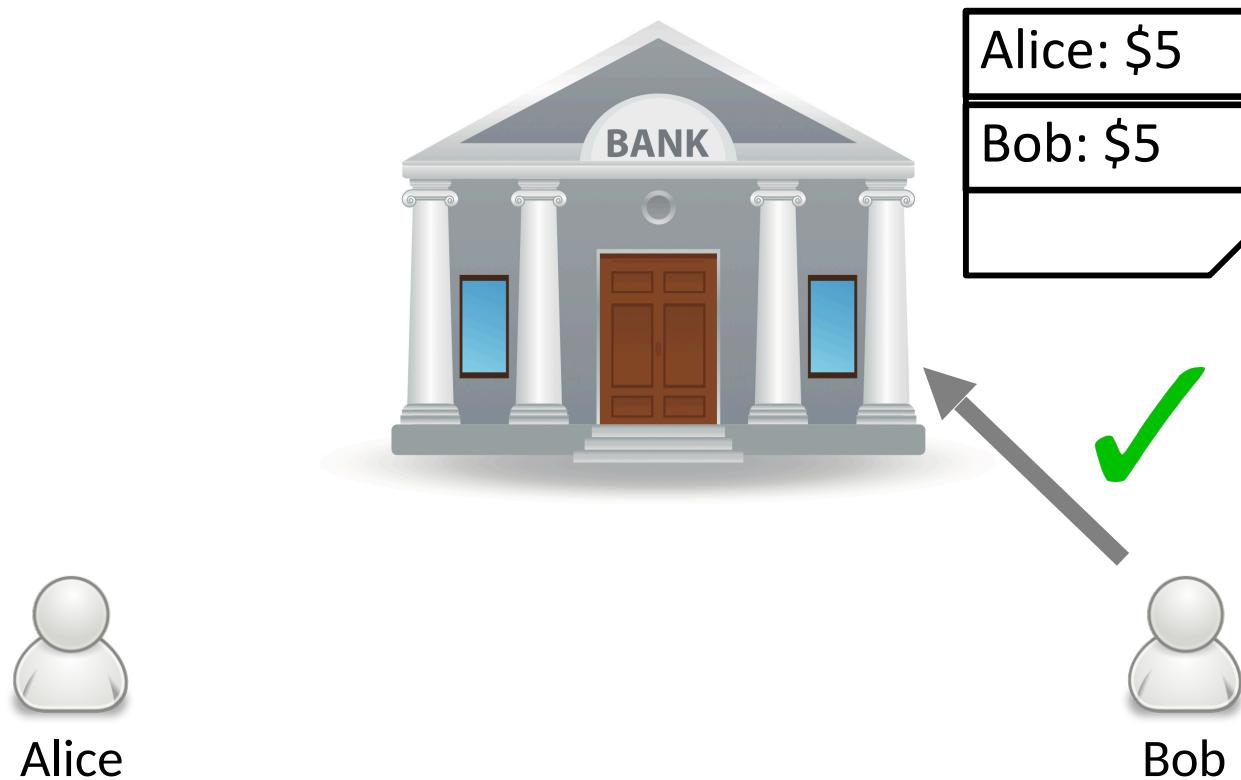
Traditional payments



Traditional payments



Traditional payments



Traditional payments



Alice: \$5
Bob: \$5



Alice



Bob



Pros/cons of banks

Pros

- Digital payments

Cons

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

The bank can fail



Alice: \$10
Bob: \$0

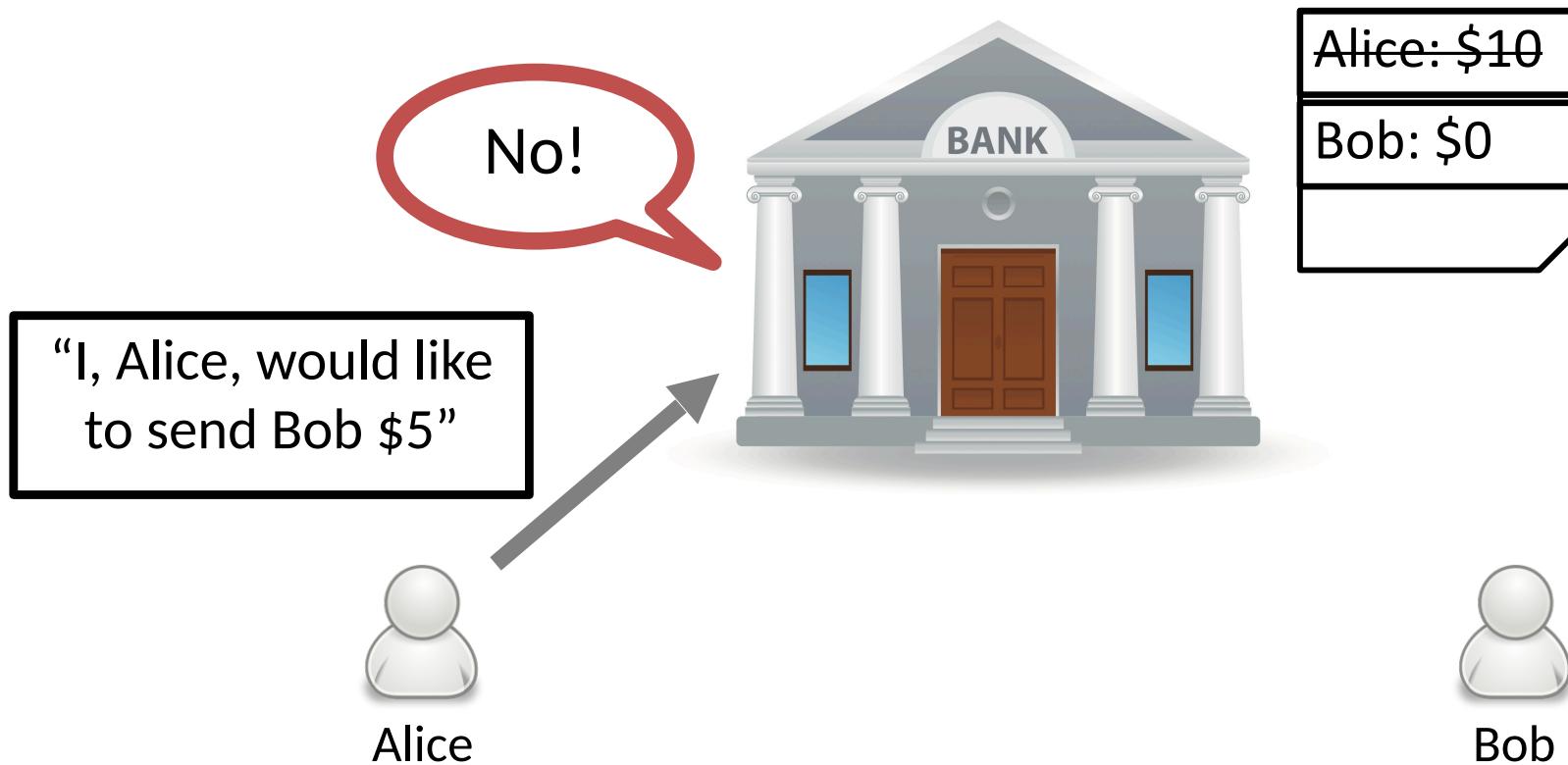


Alice

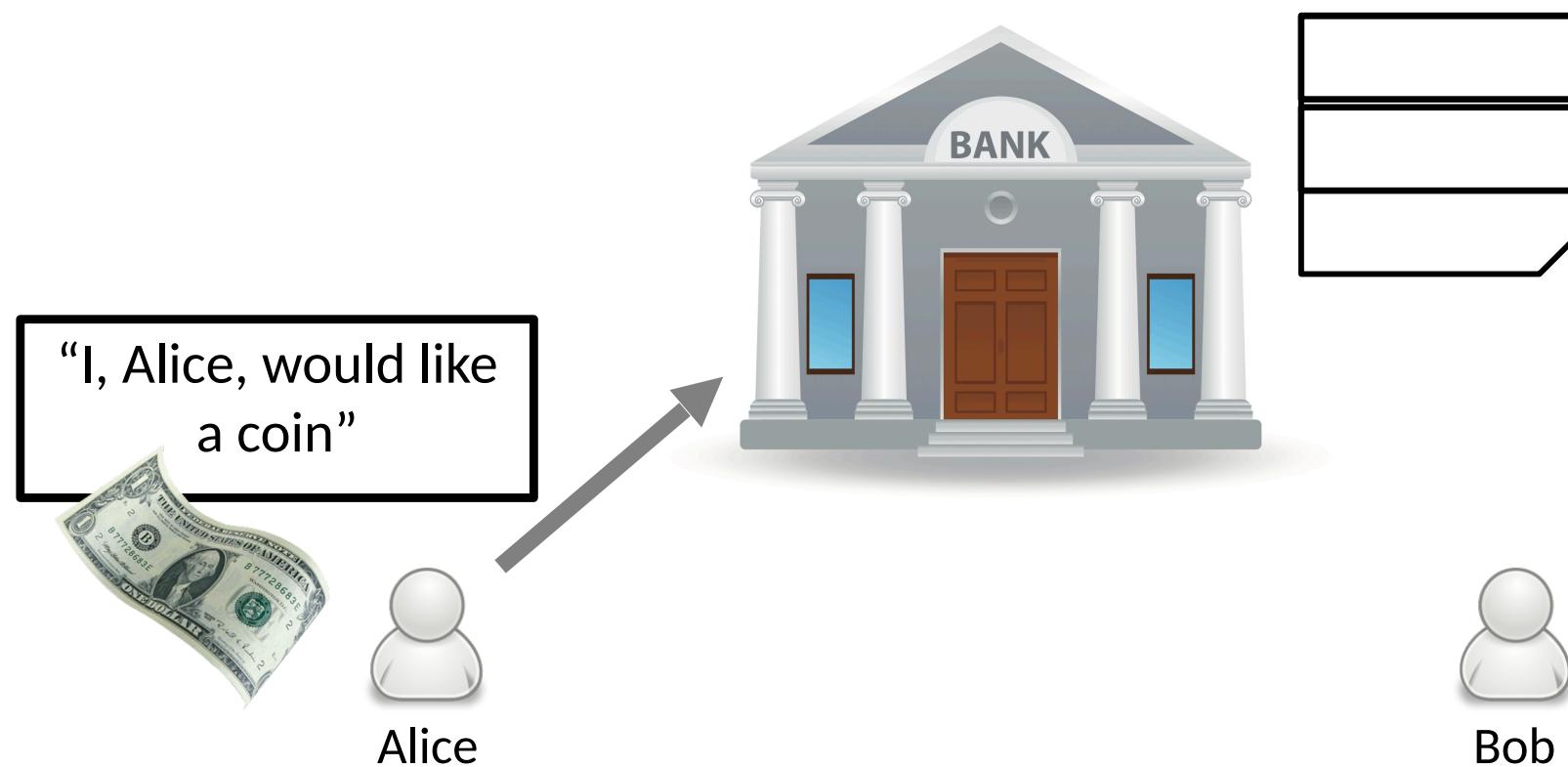


Bob

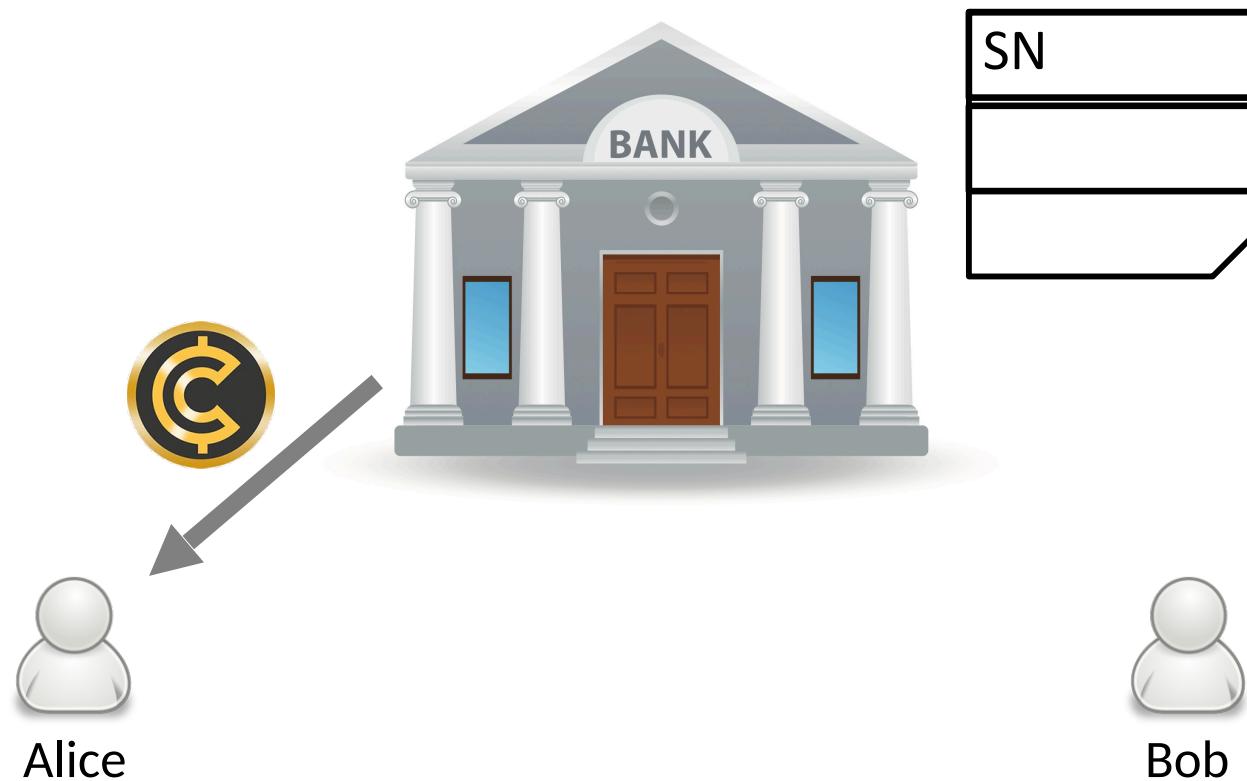
The bank can delay or censor



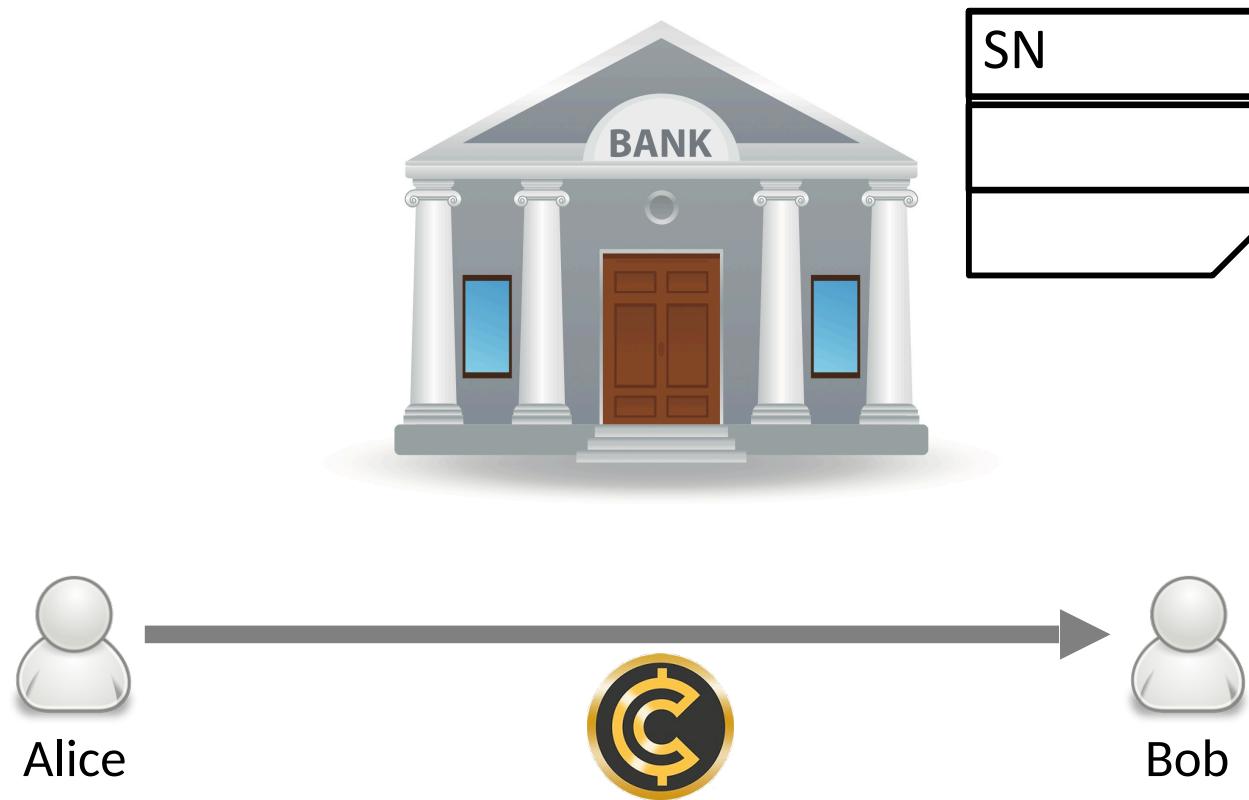
E-cash



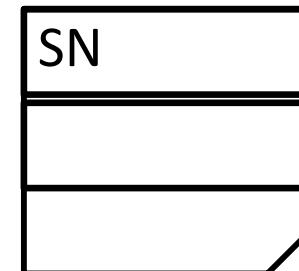
E-cash



E-cash



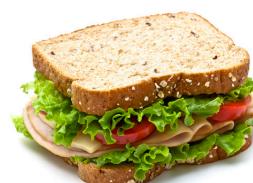
E-cash



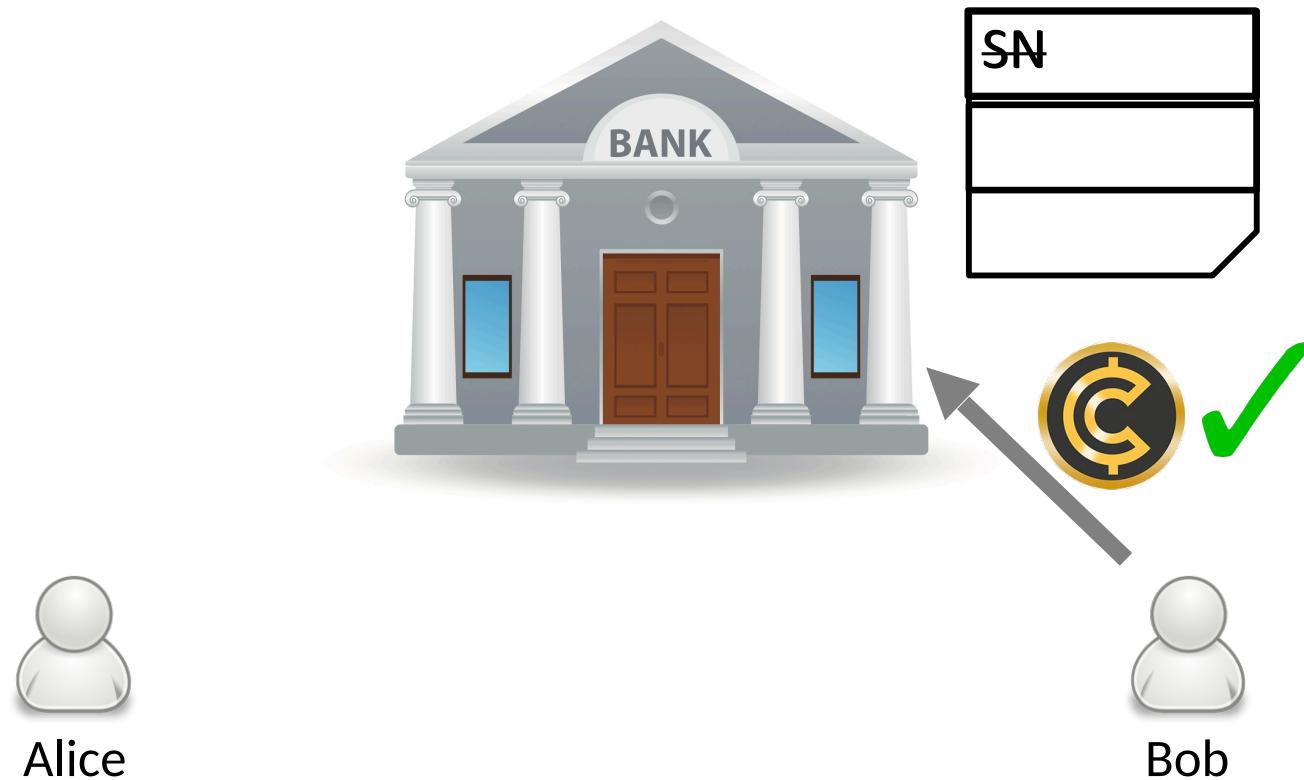
Alice



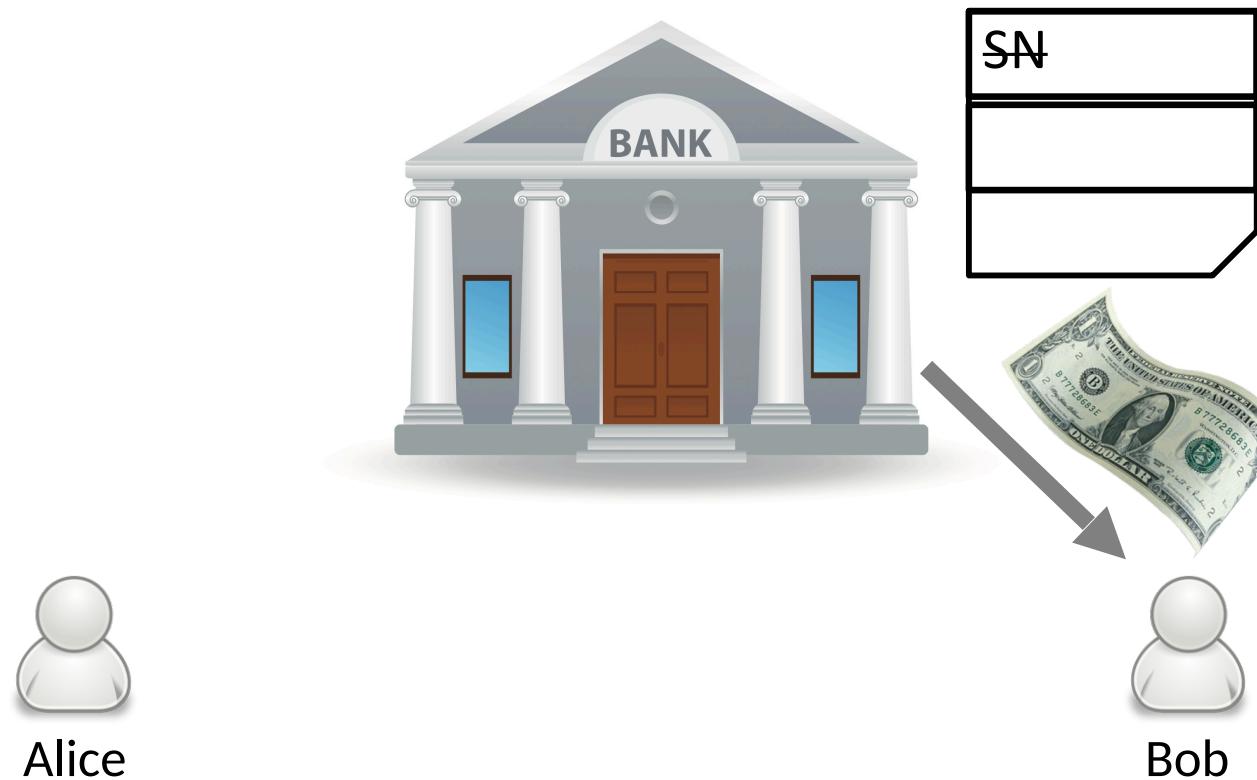
Bob



E-cash



E-cash



Pros/cons of simple e-cash

Pros

- Digital payments
- Peer-to-peer

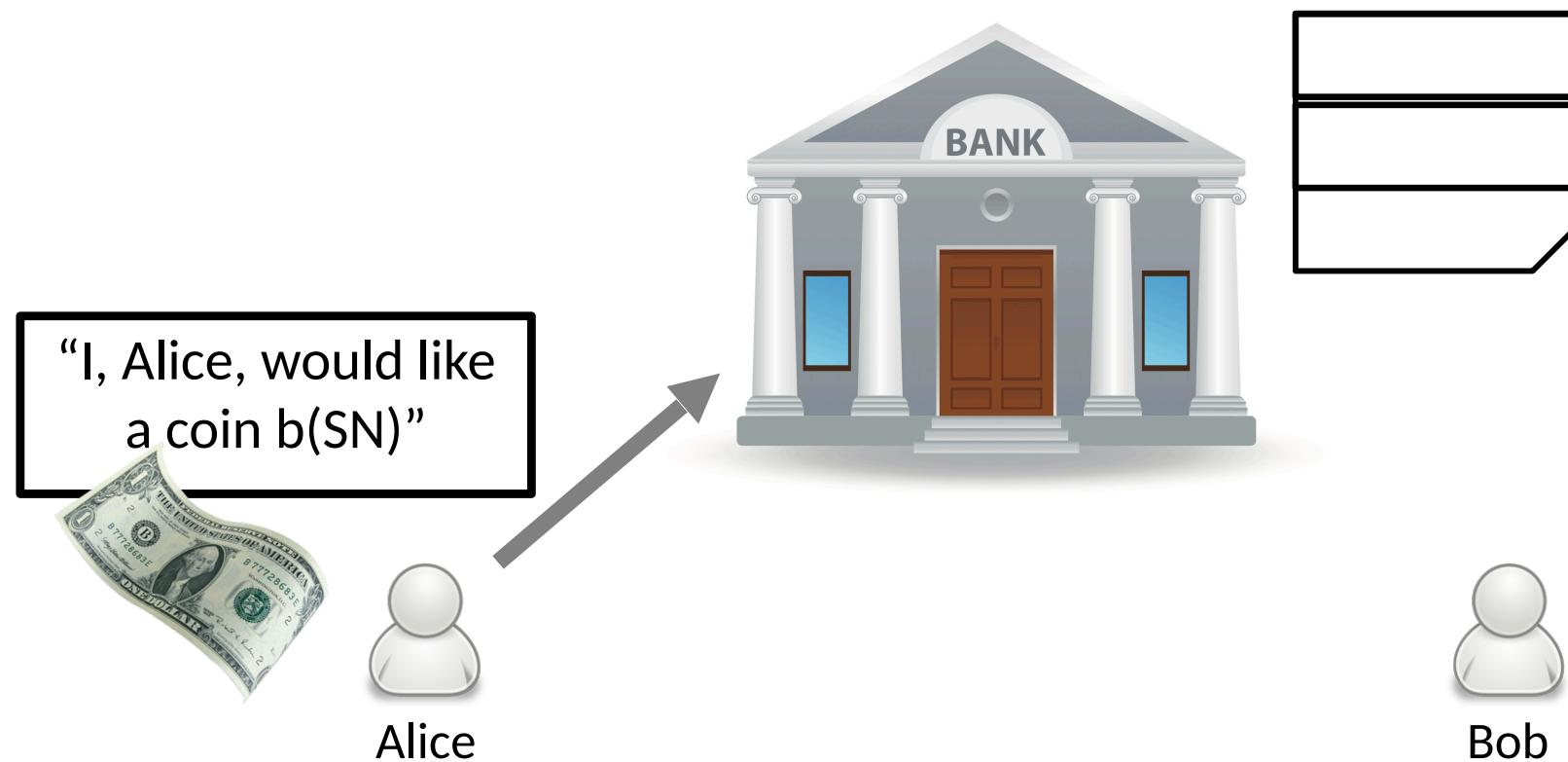
Cons

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

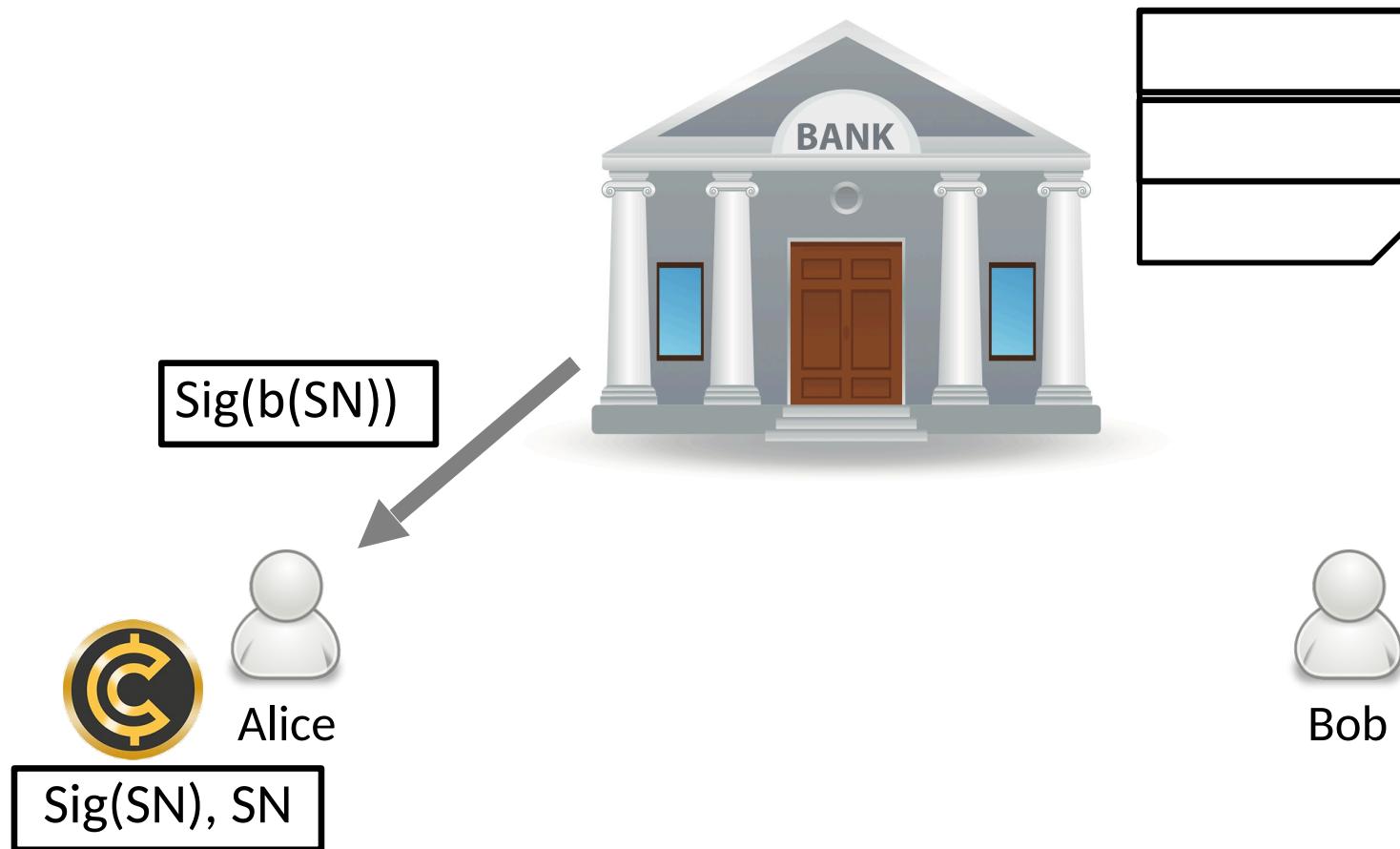
Chaumian e-cash

- Alice can choose SN
- Alice “blinds” her message to the bank so bank can’t see SN
- When Bob redeems, bank doesn’t know payment came from Alice

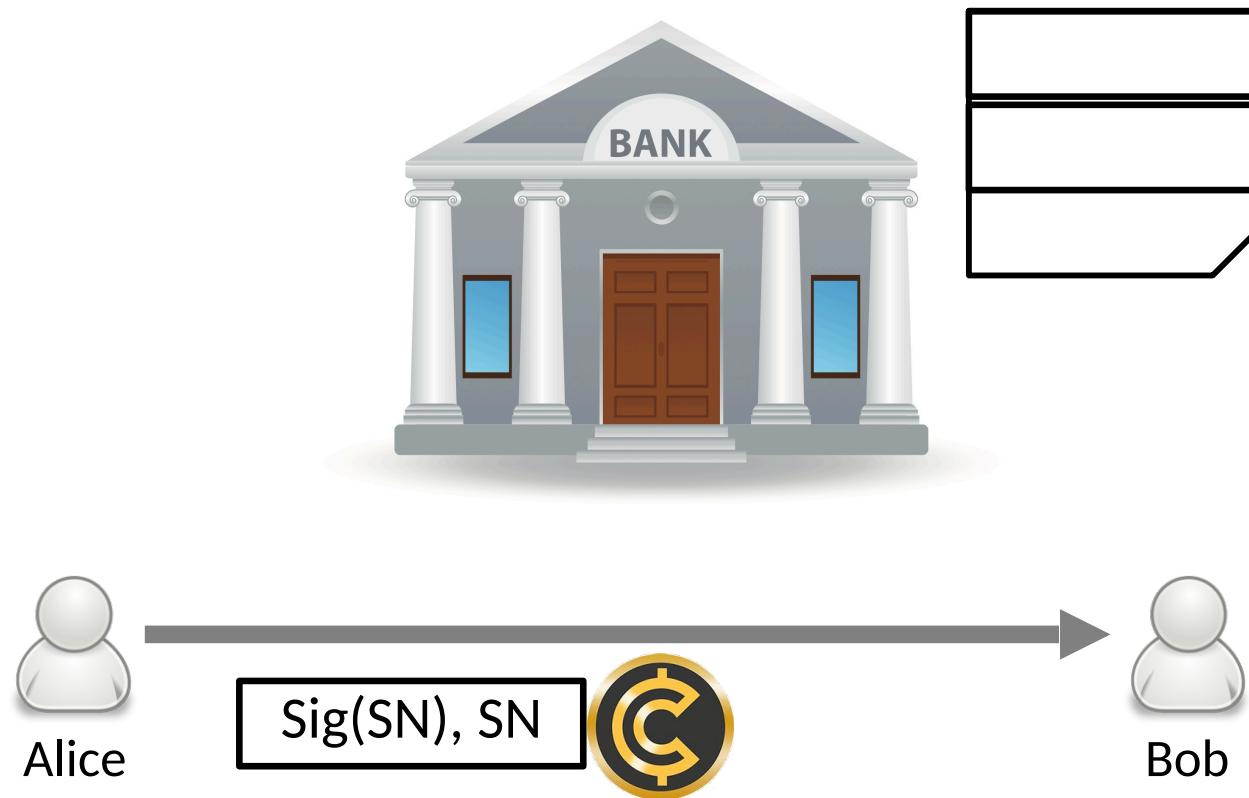
Chaumian e-cash



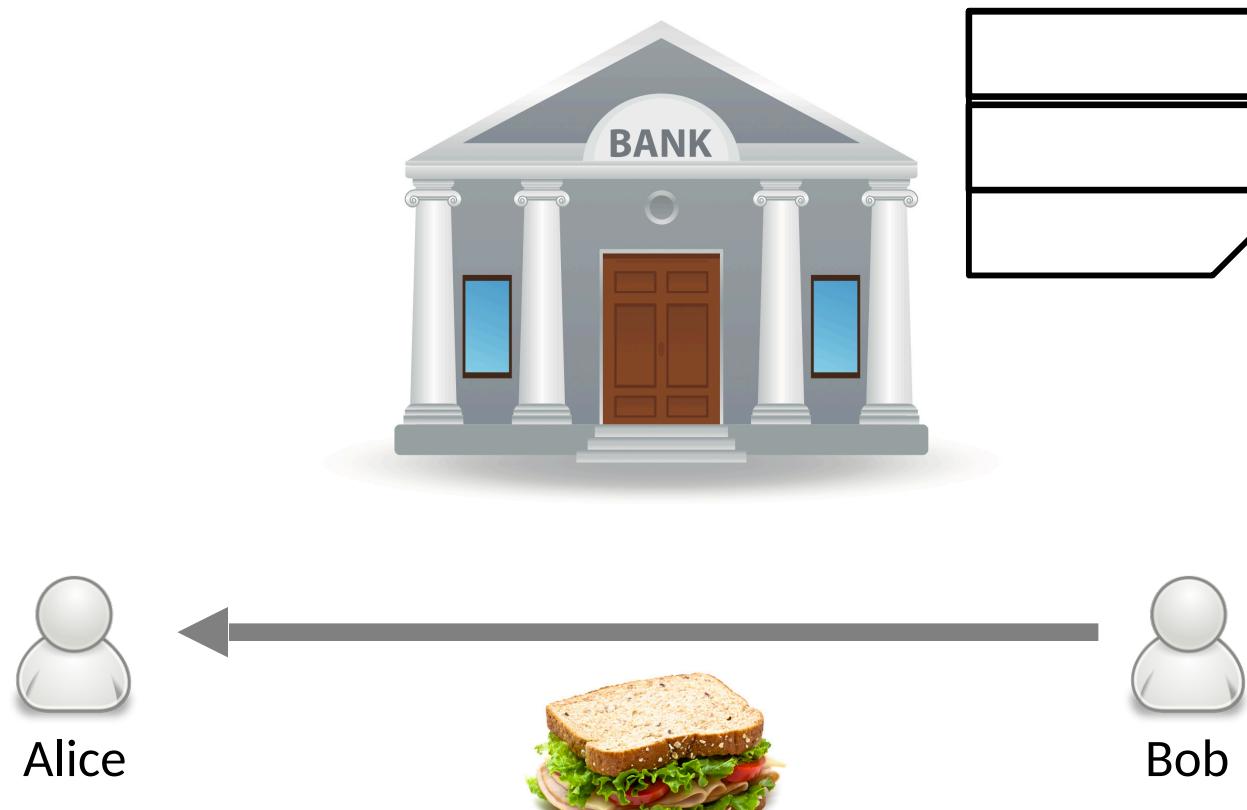
Chaumian e-cash



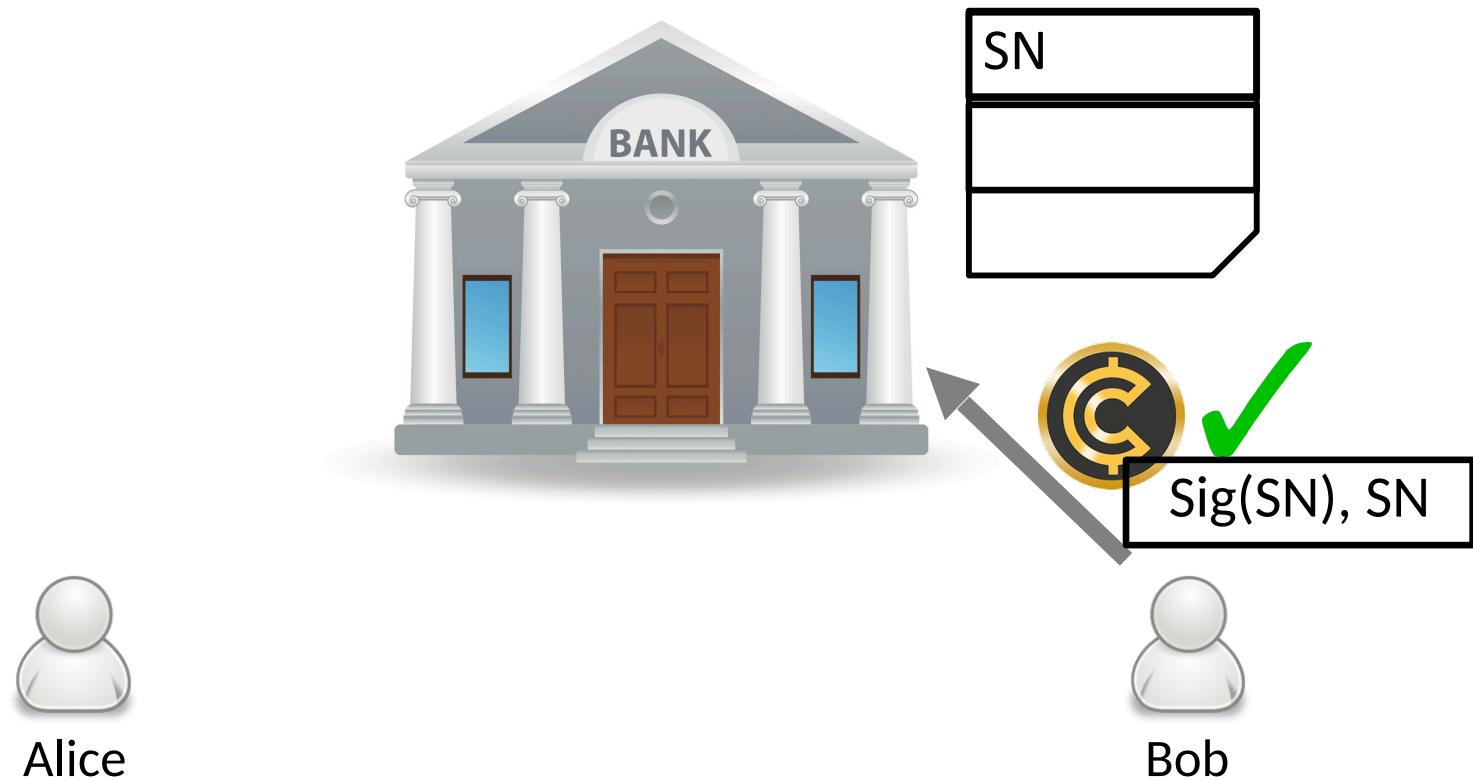
Chaumian e-cash



Chaumian e-cash



Chaumian e-cash



Double spend detection



Pros/cons of Chaumian e-cash

Pros

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

Cons

- Bank can censor withdrawals and deposits

How to build decentralized digital token transfer?

