MIT Digital Currency Initiative and the University of Brasilia presents

Cryptocurrency Design and Engineering

Lecture 1: Nature of Money and Payments
Taught by: Neha Narula
Date: 09/09/2025
MAS.S62

Introduction

- Introductions
  – Who are we?
  – What is the Digital Currency Initiative?


digital
currency
initiative

Introduction

- Introductions
  - Who are we?
  - What is the Digital Currency Initiative?
- Course information
  - github.com/mit-dci/cde-2025
  - cryptocurrency-f25-staff@mit.edu
  - Tuesdays 1-4 PM E15-359
  - Grading
    - Lectures (20%)
    - Labs (40%)
    - Final project (40%)

Date	Topic	Main Concept	Guiding Questions	Topics Covered	Readings
2025-09-09	1	Nature of money	What is money? Why might we want a new kind of money?	Money as a thing: stones, shells, salt, gold; set of functions: medium of exchange, store of value, unit of account; liability (IOU): fiat money and intermediaries. Banking, eCash, Chaumian eCash. Why they failed.	Optional: What is Money?, On the Origin of Money, Aristotle - Politics, Book I, Part IX, Senate testimony: Investigating the Real Impacts of Debanking in America
2025-09-09	2	Trust Minimization — Network Design	How can a decentralized network implement money and payments without a central authority?	Requirements for decentralized money: scarcity, transferability, verifiability. Bitcoin architecture overview (ledger + consensus + incentives).	Untraceable Electronic Cash (1988), Bitcoin: A Peer-to-Peer Electronic Cash System (2008)
2025-09-16	3	Cryptographic Commitments and Proofs	How can data be securely committed to without revealing it, and why is this critical for digital money?	Cryptographic hash functions. Properties: preimage resistance, collision resistance. Commitments and their use in contracts, blockchains. Merkle trees and proofs.	Hash Functions by Christof Paar

Housekeeping

- Signup sheet
- Register!
- Join class Discord (link on github)
  – https://discord.gg/NvTWtNXybU
- OCW filming the course

Cryptocurrency Design and Engineering

We’re going to answer questions like…

- What is a cryptocurrency?
- What primitives enable cryptocurrencies?
- What are the key design choices and tradeoffs?
- How do we handle scaling, privacy, and security?

What we are not going to do

- How to launch a token
- Investment advice
- Finance, AI

Lecture 1

- What is money and why does money have value?
- Digital payments

Stones, beads, shells, etc.

Image 1

Image 2

Precious metals

Image 3

Analog

Digital

Credit/debit

Image 4

Fiat money

Image 5

Image 6

Commercial bank money

Image 7

Electronic money

Image 8

Image 9

Image 11

Image 10

Image 12

What is money?

- Previous definitions:
  – A set of functions

Classic functions of money

- Unit of account
- Medium of exchange
- Store of value
- (Standard of deferred payment)

William Stanley Jevons
Money and the Mechanism of Exchange
1875

Image 13

Unsatisfying definition

- Why does money have to satisfy all three of these functions?
- Why do all three functions have to be satisfied by the same thing?
- Are all functions equally important?

Why does money have value?

- Commodity theory of money

Commodity theory of money

- Imagine a world with barter…
- *Double coincidence of wants* problem
  – You have sheep, I have chickens
  – I want sheep, but you want wheat
  – We can’t trade ☹️
- What if some prevalent good (with intrinsic value) became the medium of exchange…

What is money?

- Previous definitions:
  – A set of functions

What is money?

- Previous definitions:
  - A set of functions
  - An object with certain properties

Money-as-an-object properties

- Scarce
- Easily verifiable
- Portable
- Durable
- Fungible
- Divisible
- Acceptable

Commodity theory does not align with the historical record

- Cute story, but no anthropological evidence money actually evolved from barter
- Hasn’t stopped the story from still being used in economics text books

David Graeber

Debt: The First 5000 years

2011

What is money?

- Previous definitions:
  - A set of functions
  - An object with certain properties

What is money?

- Previous definitions:
  - A set of functions
  - An object with certain properties
  - A construction of the state

State theory of money

- Almost all widely-used money is a creation of the state
- Money has value because of the state's ability to impose taxes (or because the state can name it legal tender)

Why does money have value?

- Commodity theory of money

Why does money have value?

- Commodity theory of money
- State theory of money (Chartalism)

Thoughts on the state theory

- There is some truth to this
- But it doesn’t seem like the whole truth
- Does money require an authority imposing taxes or legal tender?

What is money?

- Previous definitions:
  - A set of functions
  - An object with certain properties
  - A construction of the state

What is money?

- Previous definitions:
  - A set of functions
  - An object with certain properties
  - A construction of the state
  - A liability

Money is a liability (IOU)

- Money represents a promise to pay on behalf of an issuer
  - The state
  - A commercial bank
  - NehaCoin 😎
- Easy to issue money, challenge is to get it accepted!

Why does money have value?

- Commodity theory of money
- State theory of money (Chartalism)

Why does money have value?

- Commodity theory of money
- State theory of money (Chartalism)
- Credit theory of money

Credit theory of money

- Relies on trust in the issuer to repay its IOUs
- Fiat money: issuer is the state, the promise to pay is circular!
- State is privileged in that it can create laws around money

How do we define money today?

- Most of the money today is an IOU on commercial banks (M1) rooted in trust in central banks
  – Commercial banks hold reserves at the central bank (M0)
  – Central banks hold assets (other currencies, gold), set interest rates, and perform market operations
  – Who can issue money is heavily regulated
- Heterodox theories:

Our understanding of money is constantly changing

- The first central bank (Sveriges Riksbank) was founded in 1668
- Up until 1971 the dollar was on the gold standard

Richard Nixon

Image 15

Is Bitcoin money?

- ✗ Unit of account
- ✗ Medium of exchange
- ✓ Store of value
- ✗ (Standard of deferred payment)

Is Bitcoin money?

- Previous definitions:
- ✗ –A set of functions
- ✓ –An object with certain properties
- ✗ –A construction of the state
- ? –A liability of an issuer

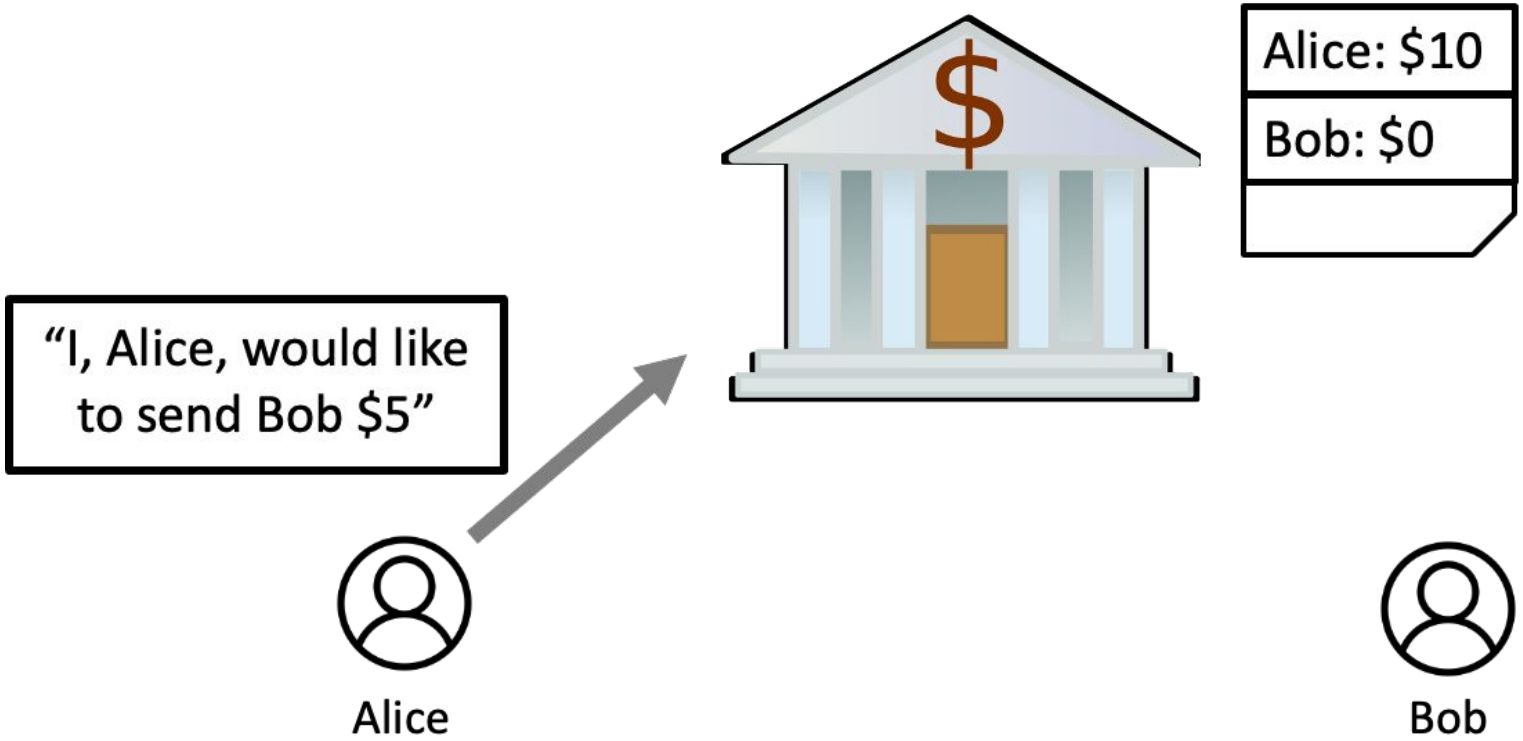
Lecture 1

- What is money and why does money have value?
- Digital payments

Money vs. payments

- Traditionally seen as money is the object, payments are the rails
- You'll see in this course the rails really matter!
  – Digital money isn't really an "object"
  – System properties constrain properties of money

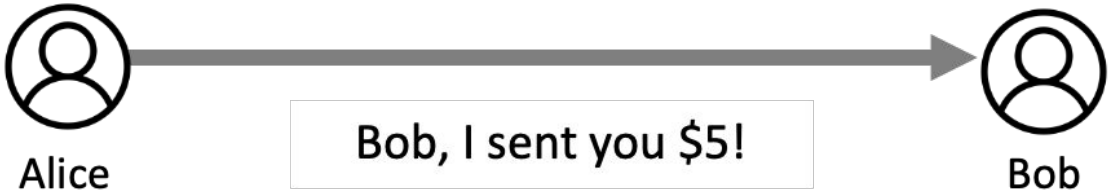
Traditional digital payments



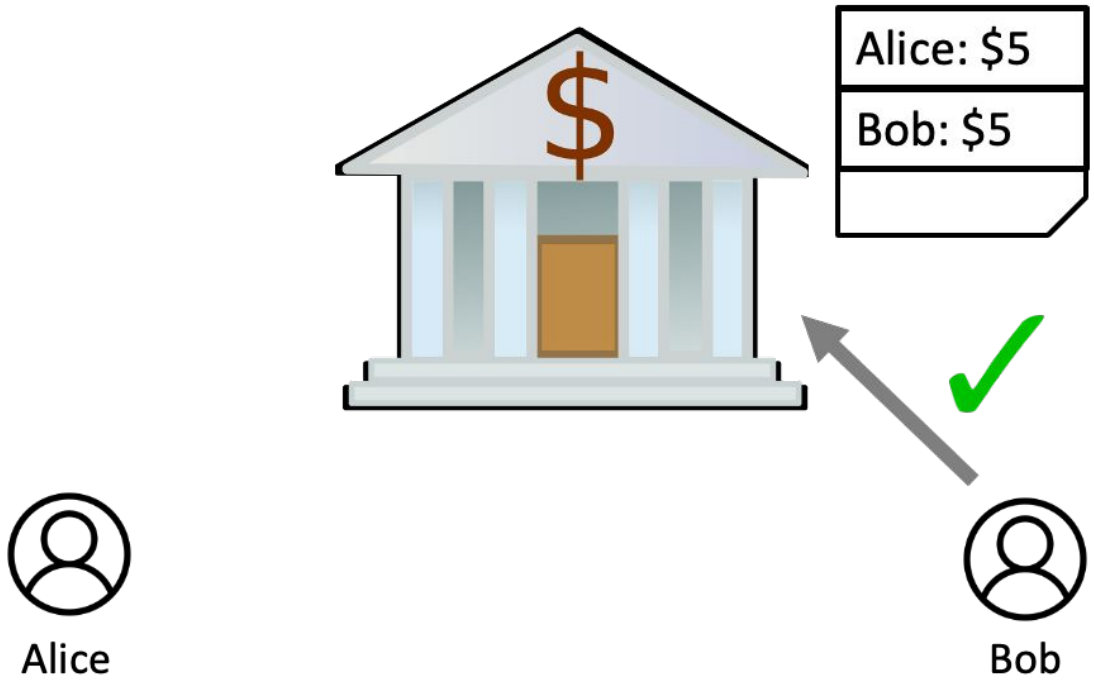
Traditional digital payments

Alice: $5

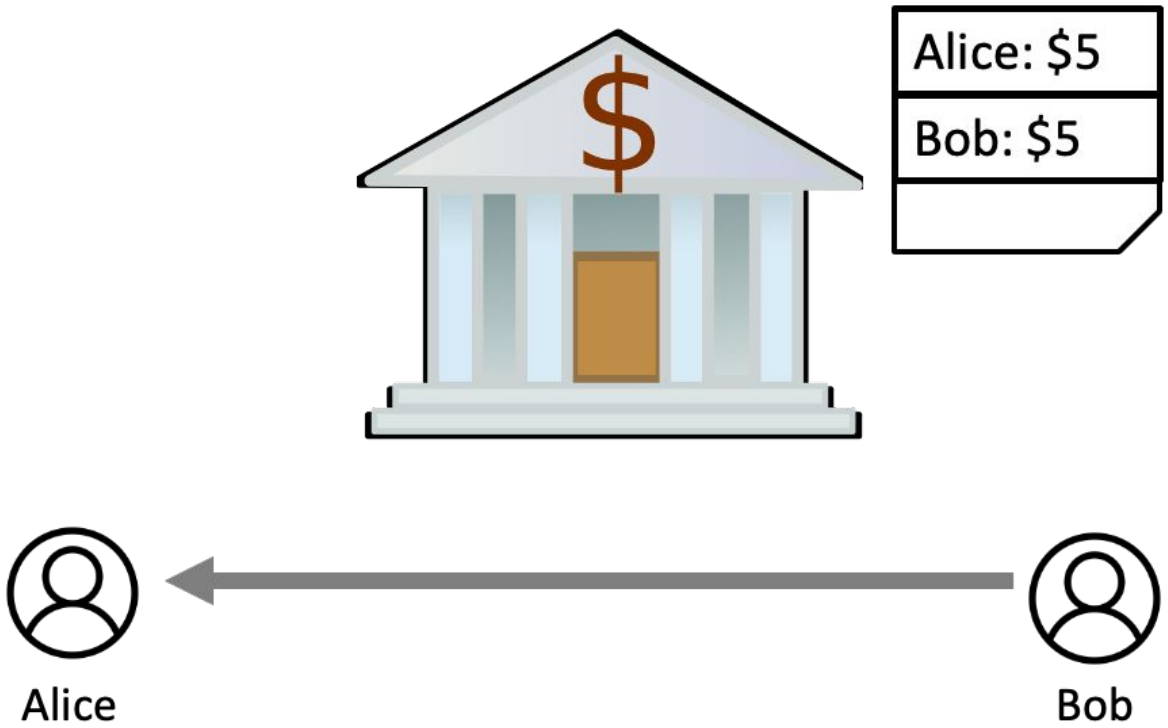
Bob: $5



Traditional digital payments



Traditional digital payments



Pros/cons of banks

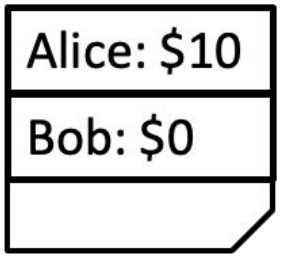
Pros

- Digital payments

Cons

- Not peer-to-peer (bank must be in the middle of every transaction)
  – Bank can fail
  – Bank can delay or censor transactions
- Privacy

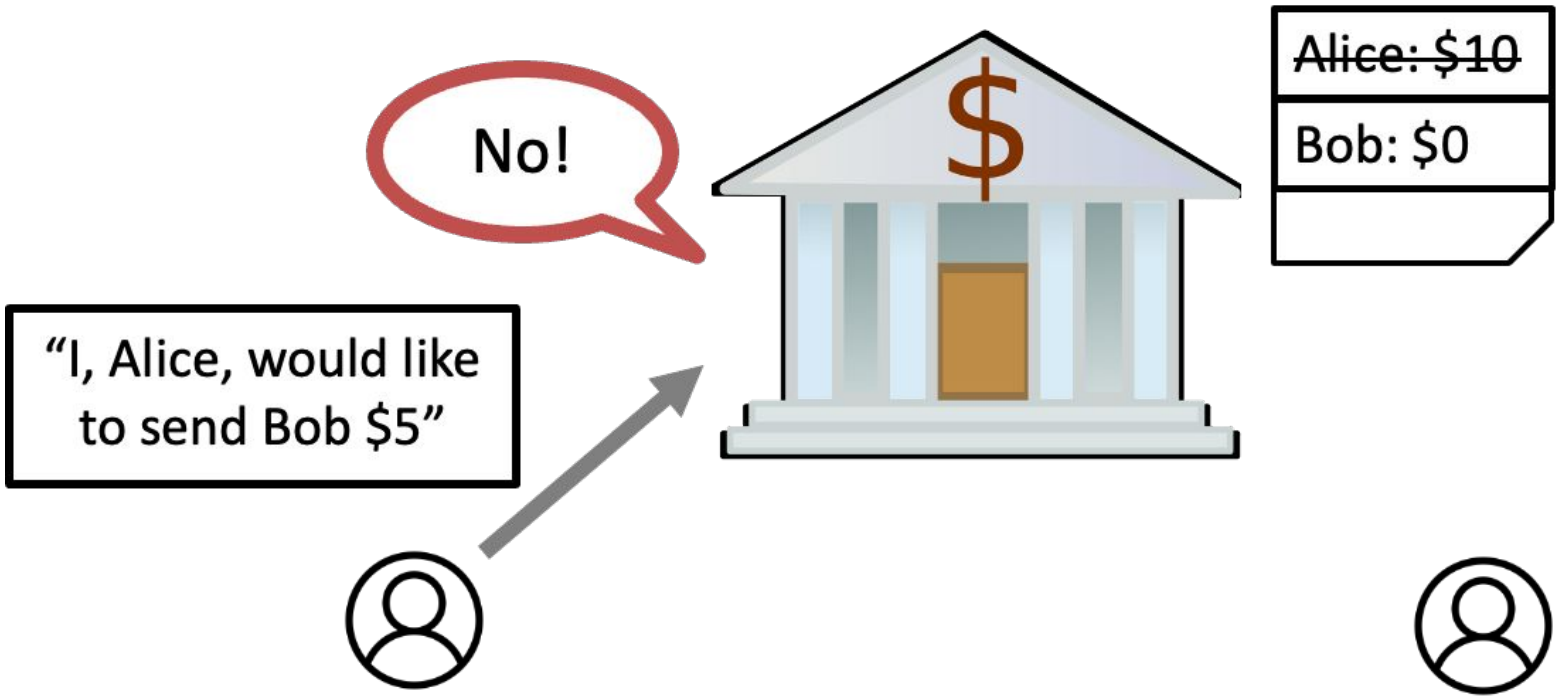
The bank can fail



Alice

Bob

The bank can delay or censor



How might we get peer-to-peer digital payments?

Image Copyrights

Image 1: https://commons.wikimedia.org/wiki/File:Rai_stone_%E7%9F%B3%E8%B2%A8.jpg Yusuke Kawasaki, CC BY 2.0 <https://creativecommons.org/licenses/by/2.0>, via Wikimedia Commons
Image 2: https://commons.wikimedia.org/wiki/File:PNG_Shell_Money_QM-r.jpg Queensland Museum, CC BY-SA 3.0 <https://creativecommons.org/licenses/by-sa/3.0>, via Wikimedia Commons
Image 3: https://www.worldhistory.org/image/5307/greek-coins/ Uploaded by **Mark Cartwright**, published on 14 July 2016. The copyright holder has published this content under the following license: **Creative Commons Attribution-NonCommercial-ShareAlike**.
Image 4: https://commons.wikimedia.org/wiki/File:Ledger.png RaphaelQS, CC0, via Wikimedia Commons
Image 5: https://commons.wikimedia.org/wiki/File:United-states-dollar-usd.jpg Onurasillsoy, CC BY-SA 4.0 <https://creativecommons.org/licenses/by-sa/4.0>, via Wikimedia Commons
Image 6: https://www.flickr.com/photos/dinomite/3397290181 March 30, 2009 at 2:12:55 AM EDT Original License CC BY-SA 2.0 Drew Stephens
Image 7: https://commons.wikimedia.org/wiki/File:CanadianChequeSample.png Airodyssey at the English-language Wikipedia, CC BY-SA 3.0 <http://creativecommons.org/licenses/by-sa/3.0/>, via Wikimedia Commons
Image 8: https://commons.wikimedia.org/wiki/File:Credit-cards_(cropped).jpg Lotus Head from Johannesburg, Gauteng, South Africa, CC BY-SA 2.5 <https://creativecommons.org/licenses/by-sa/2.5>, via Wikimedia Commons
Image 9: https://commons.wikimedia.org/wiki/File:Cashapp.png Meshary Asal, CC BY-SA 4.0 <https://creativecommons.org/licenses/by-sa/4.0>, via Wikimedia Commons
Victor Zheng
Image 10: https://www.flickr.com/photos/157762144@N07/45151811555 November 26, 2018 at 3:17:45 PM EST Old LicensePublic Domain Work New LicenseCC0 (Public Domain Dedication)
Image 11: https://commons.wikimedia.org/wiki/File:Antu_paypal.svg Fabián Alexis, CC BY-SA 3.0 <https://creativecommons.org/licenses/by-sa/3.0>, via Wikimedia Commons
Image 12: https://commons.wikimedia.org/wiki/File:Font_Awesome_5_brands_cc-apple-pay.svg Font Awesome Free 5.4.1 by @fontawesome - https://fontawesome.com, CC BY 4.0 <https://creativecommons.org/licenses/by/4.0>, via Wikimedia Commons

Image Copyrights, continued

Image 13: https://commons.wikimedia.org/wiki/File:William_Stanley_Jevons_portrait_extract.jpg Unknown (via University of Manchester Libraries), CC BY-SA 4.0 <https://creativecommons.org/licenses/by-sa/4.0>, via Wikimedia Commons
Image 14: https://commons.wikimedia.org/wiki/File:David_Graeber_2015-03-07_(16741093492)_(cropped).jpg
Guido van Nispen from amsterdam, the netherlands, CC BY 2.0 <https://creativecommons.org/licenses/by/2.0>, via Wikimedia Commons
Image 15: https://commons.wikimedia.org/wiki/File:Richard_Nixon_presidential_portrait_(retouched).jpg
Toyota Corolla E140 via Department of Defense. Department of the Army. Office of the Deputy Chief of Staff for Operations. U.S. Army Audiovisual Center. (ca. 1974 - 05/15/1984), CC BY-SA 4.0 <https://creativecommons.org/licenses/by-sa/4.0>, via Wikimedia Commons