CS 168: Blockchain and Cryptocurrencies

Introduction

Prof. Tom Austin
San José State University

History of currency

- 2000 BC – Receipts represented grain stored in Sumerian temple granaries *(representative money)*
- 600-700 BC – Coins developed in Anatolia, Greece, India, and China *(commodity money)*
  - Value of these coins tied to metal content
- 900 AD – Jiaozi banknote developed in China
  - *fiat* money– valuable because government says so
- 1971 – U.S. breaks away from the gold standard

Oct. 31, 2008

Bitcoin Important Dates

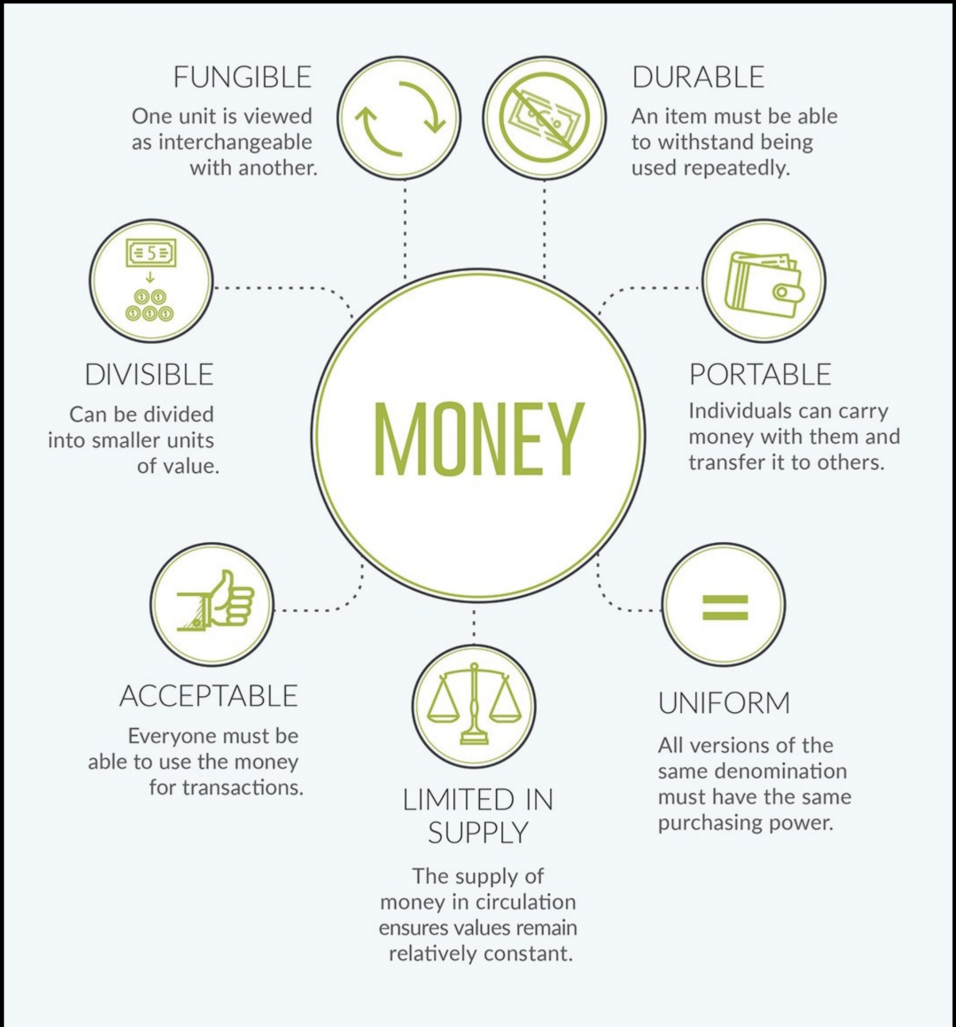
- March 2010 – User tried to auction 10k BTC for $50.
  - No buyers.
- May 22nd, 2010 – 2 pizzas bought for 10k BTC.
- 2011 – matched price of a dollar
- Dec 17, 2017 – $19,783.21
- Dropped to about $6k and stabilized a little.
- Current price: $39,816.90

What is money?

Money is:

- A medium of exchange
- A unit of account
- A store of value

Properties of Money



MONEY

FUNGIBLE

One unit is viewed as interchangeable with another.

DURABLE

An item must be able to withstand being used repeatedly.

DIVISIBLE

Can be divided into smaller units of value.

PORTABLE

Individuals can carry money with them and transfer it to others.

ACCEPTABLE

Everyone must be able to use the money for transactions.

UNIFORM

All versions of the same denomination must have the same purchasing power.

LIMITED IN SUPPLY

The supply of money in circulation ensures values remain relatively constant.

http://money.visualcapitalist.com/infographic-the-properties-of-money/

So what is digital money?

Previous Payment Schemes

- Credit cards
- PayPal
- Other?

So what *don't* these give us?

DigiCash

- Blinded signatures
  - anonymity
- Central clearinghouse
  - double-spending
- Bankrupt in 1998

Why did DigiCash fail?

Bitcoin

- No central authority
- Relies on proof-of-work
- Developed concept of the blockchain

Problems with Bitcoin

- Limited functionality
- Slow
- "Useless" computation
- Mining pools
- ASICs
- Selfish mining attacks

Alternate consensus modes

- *Useful* proof-of-work
- Non-outsourceable PoW puzzles
- Proof-of-stake
  - Coin age
  - Staked tokens
- Proof-of-space

Ethereum

- Smart contracts for building distributed applications (dApps).
- "Gas" to pay for computation.

Other protocols

- Dfinity, Algorand, Thunderella
  - High performance blockchains
- Filecoin
  - Blockchain-based storage system
- Tezos
  - Dynamically updateable blockchain
- Others TBD

So why take this course?

We will learn:

- Different cryptocurrency protocols
- Uses of the blockchain

We will go deep – the focus is to learn the fundamentals, maybe not the flavor of the day

Administrative Details

- Green sheet: http://www.cs.sjsu.edu/~austin/cs168-spring24/greensheet.pdf.
- Homework submitted through Canvas: https://sjsu.instructure.com/
- Academic integrity policy: http://info.sjsu.edu/static/catalog/integrity.html

Schedule

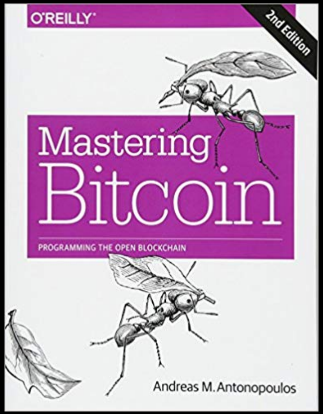
- The class schedule is available through Canvas
- Late homework will not be accepted
- It will change *frequently*
- CHECK THE SCHEDULE BEFORE EVERY CLASS

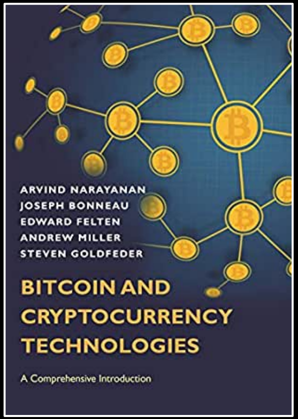
Prerequisites

- **CS 166** or equivalent, *grade C- or better*
- Show me proof
  - –If you don't, I will drop you.

Resources

Andreas M. Antonopoulos
"Mastering Bitcoin", 2nd ed.





- Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder, "Bitcoin and Cryptocurrency Technologies", (free, pre-pub version).

Other references TBD.

Grading

- 30% -- Homework assignments (individual work)
- 20% -- Class project (team work)
- 20% -- Midterm
- 20% -- Final
- 10% -- Participation (labs and drills)

Participation: Labs

- No feedback given (usually)
- I will look at them
- If you have questions, ask me

Homework

- Done *individually*.
- You may *discuss* the assignment with others.
- **Do your own work!**

How to fail yourself and your friend

If two of you turn in similar assignments:

you both get a 0

Project

- Build your own blockchain-based cryptocurrency
- Build an interesting App
- You may work with a partner if you want

Office hours

- MacQuarrie Hall room 216.
- Mondays 10-11am, via Zoom.
- Thursdays noon-1pm, in-person.
- Details (including rescheduling) at http://www.cs.sjsu.edu/~austin/office-hours-updates.txt

"Please forgive the long letter; I didn’t have time to write a short one."
--Blaise Pascal

Two Kinds of Email

- Emails with lots of detailed information and subtle nuances.
- Emails that people read.

Try to send the 2nd kind

Before next class

- Install Node.js from https://nodejs.org/en/
- Read Section 1 of Okamoto and Ohta's "Universal Electronic Cash". https://link.springer.com/content/pdf/10.1007/3-540-46766-1_27.pdf