

CompSci 461 Secure Distributed Systems

✓ Who Am I? Andrew Stone → Telecom Devices: Tightly coupled Distributed Systems.
→ Bitcoin → BCH → Nemo

✓ What is this course about?

✓ How does it work? (Flipped)

compsci461.org

- Analyzing a System
- What is money?
- Bitcoin Whitepaper

Secure Distributed Systems

collection of independent components that collectively provide a service

↳ Software or a device providing a service

- Unauthorized Access costs more than the value of contents
- takes longer than the resources retain their value.

• Blockchain: what is a blockchain?

How do you analyze a system:

- 1: How is it made?
- 2: What is its API User Interface?
- 3: What does it do?
What are its ramifications on society

• What is Money?

- Scarcity,
 - ? • represent tangible value: marginal utility?
 - acceptability. Unit of account
 - fungibility
 - portability ←
 - durability
-

Money as bits Doesn't ~~work~~ because copy

Ledger → database

↳ security → DB Admin!

→ DB with row security!

↳ to be trustless NO DB Admin

→ removal of rows...

→ prevention of mods even if authorized.

• Why?

• Transparency

→ Lots of people keep copies. ←

→ Useful if it was expensive to modify the DB? ←

