CS-234
Technologies for Democratic society

Fall 2022

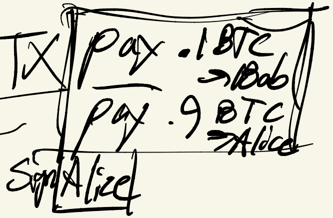
Week 6

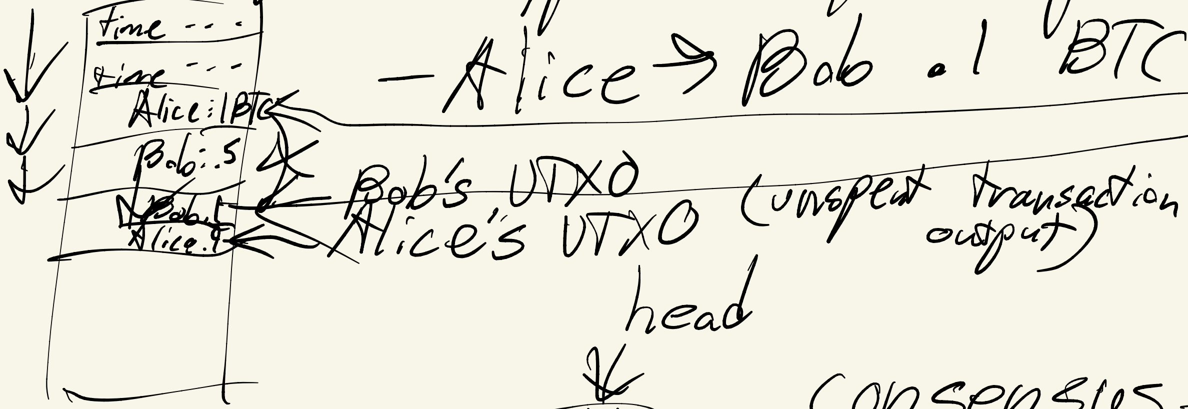
Blockchain, smart contracts, dec. governance

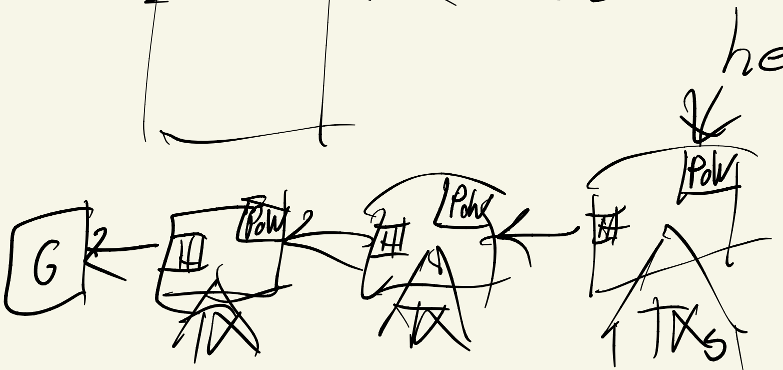
- Bitcoin (2008) – Satoshi Nakamoto
  - Blockchain or distributed ledger

public log/record

  - cryptocurrency: log of asset transfers
  - Alice → Bob .1 BTC: TX





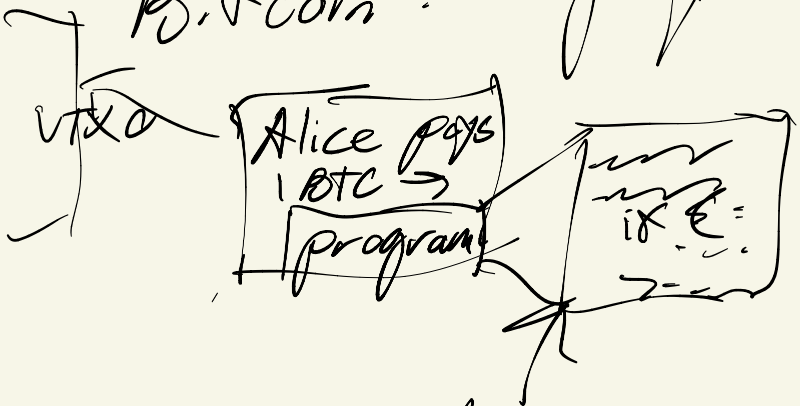


Consensus –
Nakamoto consensus
Proof-of-work

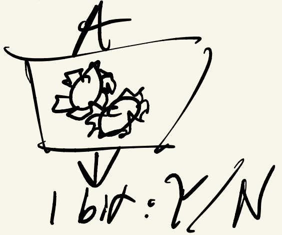
Smart contracts

- script/program stored in a ledger executed jointly by all miners/validators

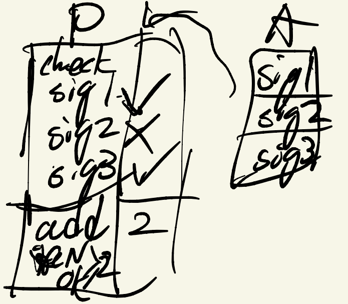
Bitcoin: "pay to script"



predicate:



Example: threshold auth



Bob "spend progrgram's 1BTC"
authorization: " . . A . . . "

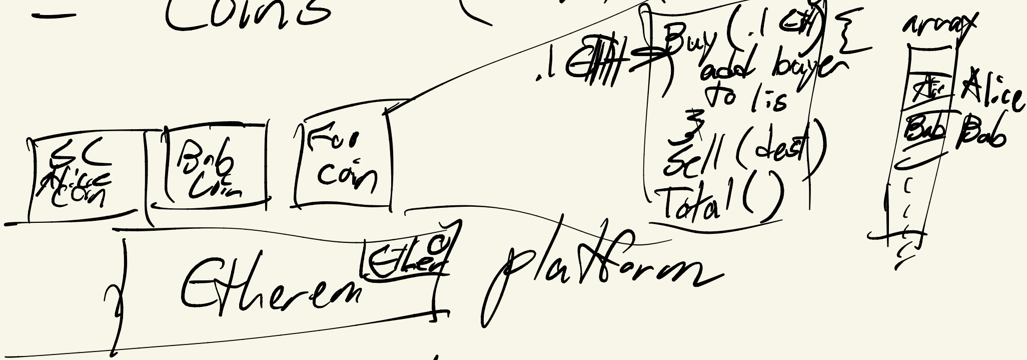
beginnings of "decentralized governance"

Ethereum: Turing-complete language

- Loops, backward branches
- "Gas": instruction quota
  - invoke smart contract (A): max 10,000 gas
- Generalizes expressiveness
  - still deterministic
  - can depend on past Blockchain state
    - no "external" state

Smart contracts - further developments

- "Coins" ("initial coin offerings" - ICOs)

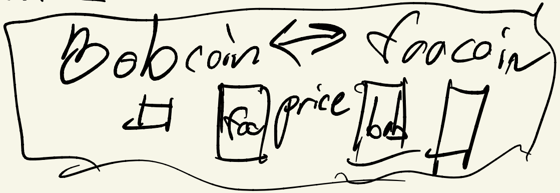


crowdfunding

- first wave of "decentralized finance" (DeFi)

- Decentralized insurance
  AXA "fizzy" - flight delay insurance
  - "Oracle" - earlier: centralized "trust me"
    increasingly: decentralized - Chainlink

- Automated market makers (AMMs)



Decentralized Autonomous Organizations DAO

- Buy into: pay Ether, get coin/stake
- decision-mating / voting

```
propose_vote()
cast_vote(stake, Yes/No)
```

"The DAO" - decentralized VC ~2016

Hack → ETH

→ ETC "Ethereum Classic"