# CS-234
# Technologies for Democratic society

Fall 2024

Week 6

# Decentralized techalogies - society / democracy

1. UseNet - 1980s, 90s
2. P2P - BitTorrent, IPFS, DHTs.. 2000s
3. Blockchain - 2008 (Bitcoin), 2010s
4. ? ~~Decentralized AI?~~

## Blockchain (Cryptocurrencies, smart contracts, DeFi)

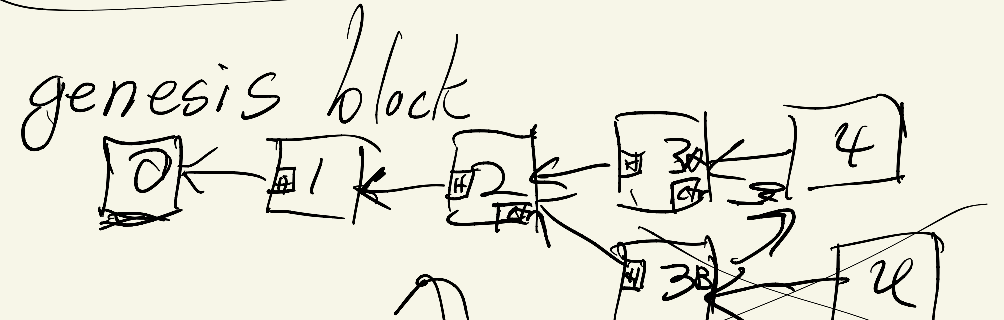
Bitcoin 2008 – Satoshi Nakamoto

decentralized e-currency (e-cash)

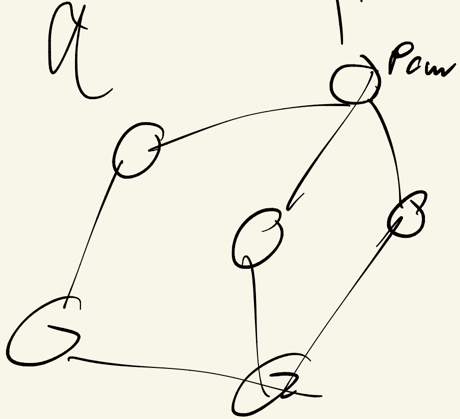
several problems in 1:

- consensus/agreement
- identity/admission control/Sybil attack
- large-scale distributed ledger
- cryptocurrency (Application)

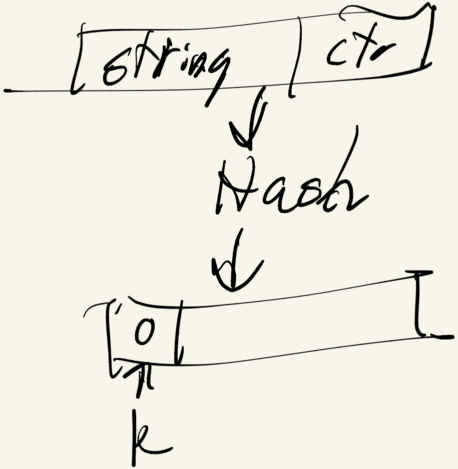
# Bitcoin - ledger structure



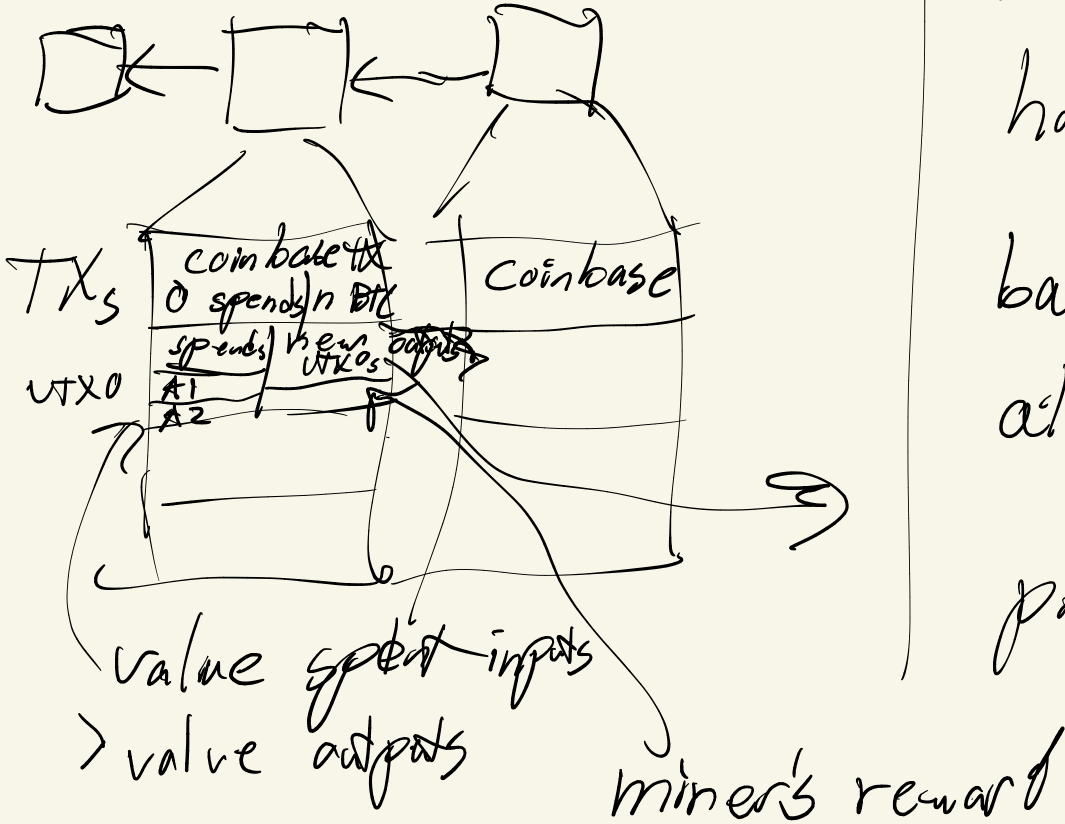
PoW - Proof of Work (crypto-puzzle email spam control)



longest chain
most work
wins



# Bitcoin – cryptocurrency



## Scripting

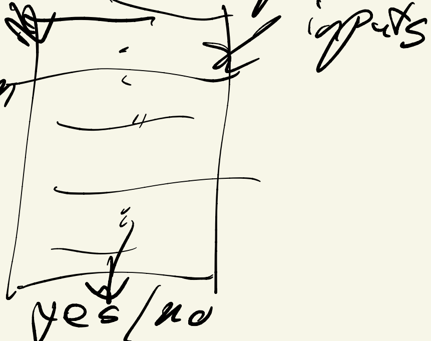
how to "authorize" spending UTXO

base case: pub key

alternate:

pay to script

program

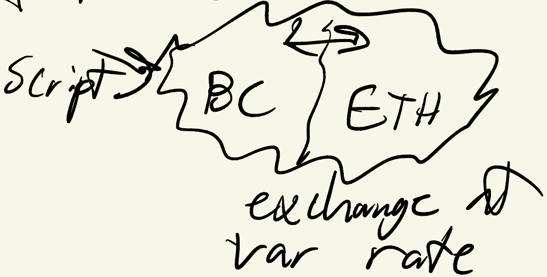


# Bitcoin scripting - limitations

- Limitations:
  - Determinism - Bitcoin & Eth
  - No external input - Bitcoin & Eth
    depend on Oracles (decentralized oracles)
  - No loops - not Turing complete - Bitcoin
    Ethereum: "gas", exchangeable w/ Ether
    script execution consumes gas, has gas limit
  Enables Turing complete smart contracts

# Smart Contract – opportunities

- Custom "coins", currencies → "initial coin offerings" ICOs
- Non-fungible tokens (NFT)
- Automated market makers (AMMs)



- Auctions
- Organizations – Decentralized autonomous organizations (DAOs)