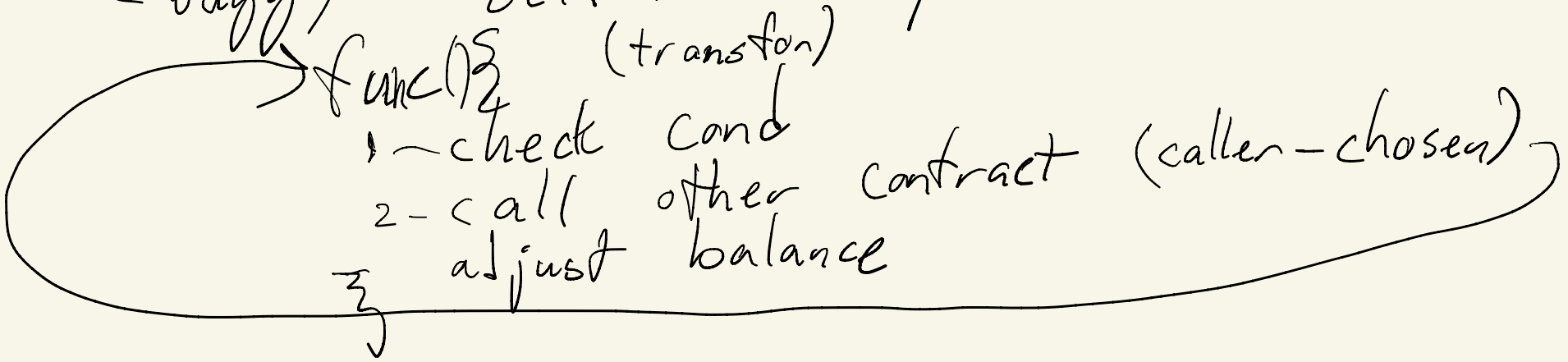
CS-234
Technologies for societal self-organization

Week 13

Decentralized Autonomous Organizations (DAOs)

- an organization serving some purpose existing only in a decentralized system (eg smart contract)
- "The DAO" incident: a particular DAO contract (2016)
  - A community investment organization (crowdfunding)
    - anyone could join, "buy in" as investor
      send in ETH, get stake / voting rights
    - propose projects, vote on them (governance)
  - attracted high percentage of all ETH (~200M)
  - "split" feature: fork your part of equity into "sub-DAO"
    - buggy - self-reentrancy



The DAO

- Attack exploited bug to drain ~50%.
  Main DAO → attacker sub-DAO
- Controversy between "purists" and "pragmatist"
  - difference between letter and intent of contract
  - "too big to fail" — pragmatists won
    most miners made "hack" to revert attack
    some miners dissented, forked "Eth Classic" (ETC)

Decentralized Finance (DeFi)

- Decentralized Oracles (Chainlink)
  - Aggregate information from multiple sources, intermediaries
    - threshold security
  - Incentives (fees, payments)
- Decentralized Exchanges (Uniswap)
  - Ethereum hosts many types of tokens (ERC-20)
  - Automated Market Maker (AMM) - "constant product"
  - Example: trade ETH ↔ USDT (Tether stablecoin linked w/ USD)

Uniswap

- token A, token B — reseres r_A, r_B
- seed AMM contract w/ $r_A, r_B \rightarrow r_A r_B = k$
  - price is always $\frac{r_A}{r_B}$
  - "infinite reserves"
- if $\frac{r_A}{r_B}$ differs from "true" price, then arbitrage opportunity exists