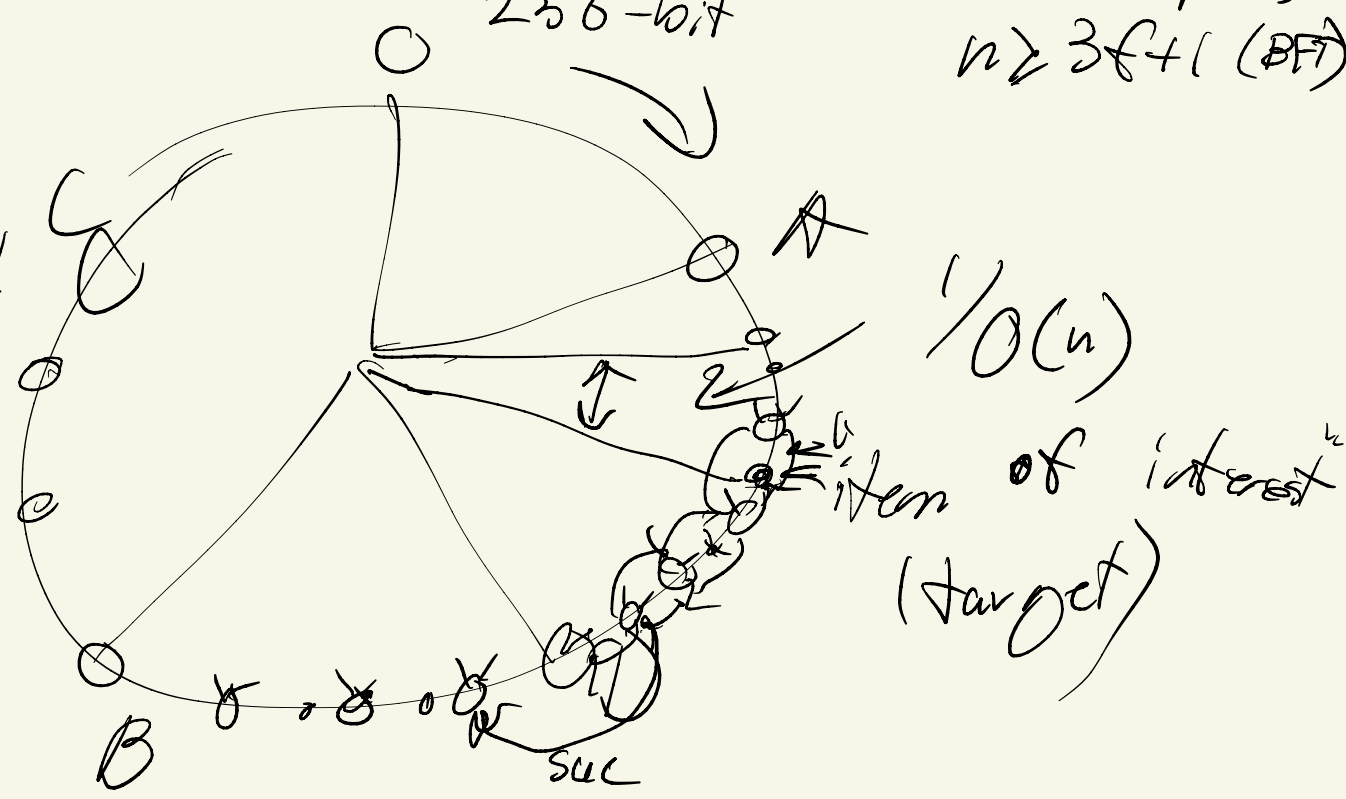
CS-438 Decentralized Systems Engineering

Fall 2021

Week 9

Sybil attacks

- "Sybil": psychological study of patient with multiple personality disorder
- Douceur (MSR): "The Sybil Attack"
  hard to make "open" decentralized systems secure
  - Consensus: threshold security $n \geq 2f+1$ (paxos)
    $n \geq 3f+1$ (BFT)
  - DHTs
    eg. Chord
    DoS
    - deny
    - replay attacks
    - isolate node



"Key mining"
Eclipse attack

Sybil defenses

weak proxies: IP addresses
Email addresses
mobile phone number

- Proof-of-Work, - Storage, - Stake, ...

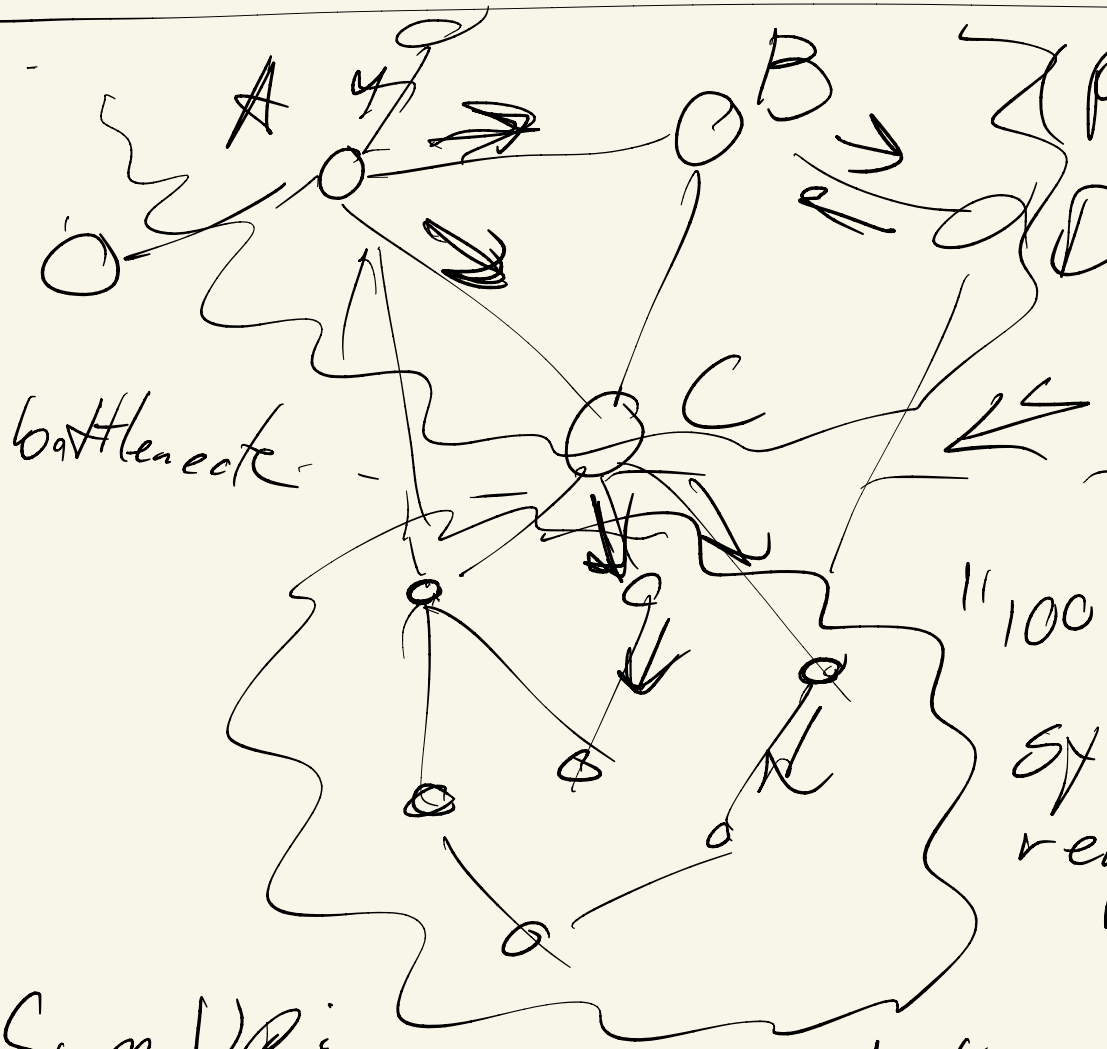
"Proof of investment / consumption"

- Strong identities: PKI, verified logins (usually centralized)

Decentralized: ENS (Ethereum name system), Namecoin
PGP trust network SPKI/SDSI,
Self-sovereign Identity
is "identity" Sybil resistant?

- Proof of personhood
  - Government-issued identity — anonymized / pseudonymized (CanDID)
  - Biometric identity: Aadhaar, Worldcoin
  - Trust networks (Upala, Circles, ...)
  - Pseudonym parties (online or offline) Idena
    Turing tests

Trust-based Sybil defenses



(PGP key signing)

"honest region"

← attack edges

Sum Up:
D asks "is content good?"
- send voting tokens

- Detection
  - clustering

- Resistance
  - Sum Up,
  - Sybil Guard,
  - Sybil Limit,
  - Whanau