

CS-438

Decentralized Systems
Engineering


Fall 2022

Week 9

Attacks - Sybil attacks

- Byzantine - "can misbehave in arbitrary ways"
 - Byzantine fault tolerance (BFT) - try to tolerate
 - but assume that total # of nodes is known + their identities
- Sybil attacks - can create many false nodes, users, identities
 - Douceur, "The Sybil Attack"

Implications

- compromise threshold-based security (t -of- n)
"creeping compromise" (slowly increase t, n)
- DHTs: eclipse attacks → censor nodes, K/v pairs 
- compromise consensus - force particular decision, rewrite history, equivocate (multiple histories)

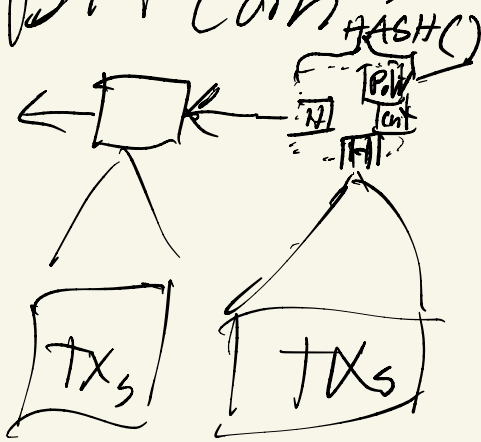
Defences - "human-centric"

- Stronger identities
 - Sign up with phone # (WhatsApp)
 - with credit card
 - Financial services: with ID checking (KYC)
- "Proof of personhood" - prove personhood w/o ID
 - CAPTCHA - online humanness test
 - gap between humans & AIs shrinking
 - still only rate-limiter
- ...

Defences — non-human-centric

- Closed / permissioned
 - organizations, consortia — large investment

- Bitcoin: Proof-of-work — automated solving crypt-puzzles



open / permissionless "anyone" can join
+ Sybil resistant

- not efficient
 - not environmentally friendly
- ...
- Proof-of-stake

Human-centric defenses

"Proof-of-personhood"

Bases for security or "1-to-1"ness

- Traditional identity / proxies (phonet# cc, KIC)
 - deterrent: cost, threat of jail, paper trail
- Biometric identity (India-Aadhaar) collect biometrics deduplication
- Social / trust networks
- Presence test - (CAPTCHA)
 - pseudonym parties - Encounter
 - virtual/online - IDENA.io

Social / trust networks

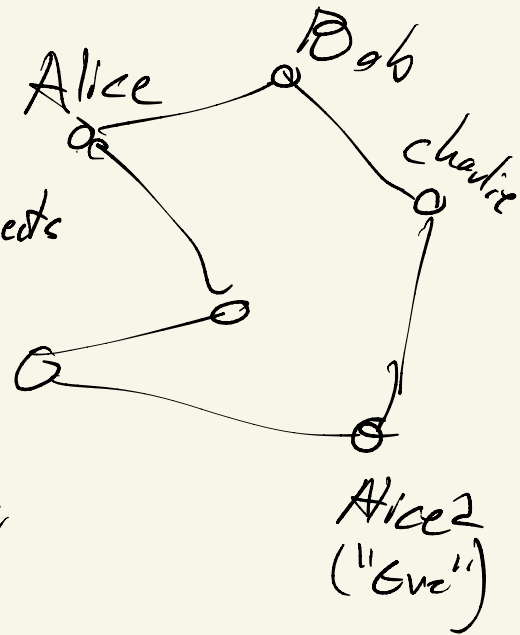
- PGP - "pretty good privacy" - E-mail encryption
trust network approach to identity
"key-signing parties"

- Facebook, OSNs ...

- Recent blockchain community projects
- Kleros, pi network, humanity DAO,

- Sybil-resistant?

- Idea: cost of "honest links"



Link Bottleneck Sybil resistance

- Sybil Guard, Sybil Limit, SumUp, Whanau
- Eve

