# Toward Secure ”One-Person-one-Vote” Online Participation

Prof. Bryan Ford
Decentralized/Distributed Systems (DEDIS)


W3C Credentials – August 7, 2018

# The Sybil Identity Problem

Internet has no protection from malicious users cheaply creating a few (or many) fake accounts

- Online ballot stuffing, fake upvotes/reviews
- Sock puppetry, bot armies pushing fake news
- Whack-a-mole: “banned” trolls just resurface

Fundamental unsolved decentralization problem

- John Douceur, “The Sybil Attack” [IPTPS ‘01]
- Bitcoin PoW is another disastrous failed attempt

# Mapping the Known Solution Space

Major approaches proposed so far:

- “Real names” based on verified identities
- Biometric collection in central database
- Proof-of-Investment: CAPTCHA, PoW, PoS, …
- Graph analysis on trust networks
- Pseudonym parties

# “Real names” and verified identities

Trusted third-party verifies government-issued ID

- Blue checkmarks, banking KYC checks, …

Downsides:

- Privacy-invasive, excludes poor/undocumented
- Cumbersome, expensive verification process
- Fake IDs relatively easy, cheap to acquire
- Vulnerable to 1 compromised/coerced verifier

# Biometric collection & verification

Collect fingerprints, iris, etc., record in database

- Appeals: efficiency, automation, security(?)
- Large-scale trials by India, United Nations

Downsides:

- Even more privacy-invasive, surveillance risks
- False positives & negatives create big problems
- One hacked scanner could still register many fake “people” with unique biometric fingerprints

# Proof-of-Investment

Rate-limit Sybil attacks via artificial barrier-to-entry

- CAPTCHAs: waste time proving you're human
- PoWork: prove you wasted compute energy
- PoStake: prove you have money to invest

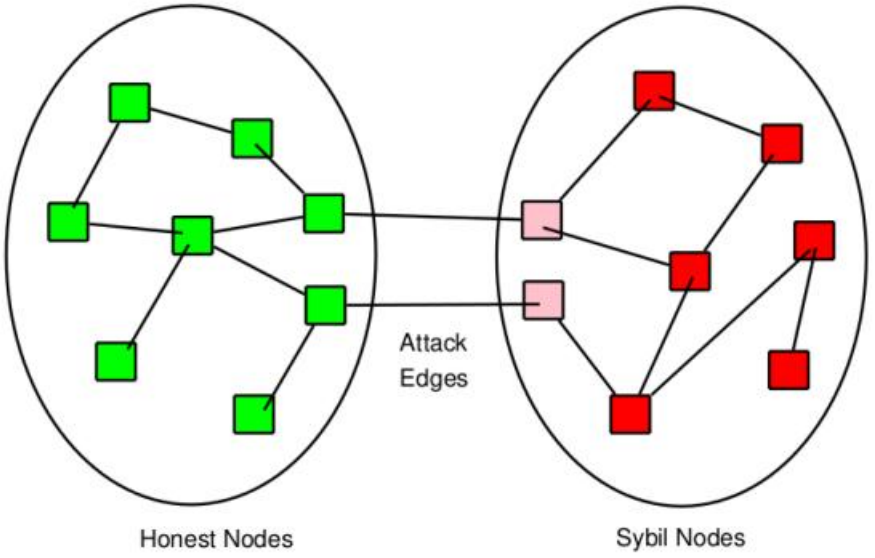
Downsides:

- Undemocratic: not "one-person-one-vote"
- More money, more voice: "rich get richer"

# Graph analysis on trust networks

Classic P2P idea in SybilLimit, SumUp, etc.

Assumes *nodes* are cheap but *edges* are expensive to a Sybil attacker




Downsides:

- Secure & usable “trust networks” don’t exist
  - Facebook/LinkedIn/etc: many friend promiscuously
- Only weak defense against *massive* cheating
  - Easy for many people, or everyone, to *cheat a little*

# Pseudonym Parties

Build *anonymous* one-per-person tokens

- Physical security: real person has one body, can be in only one place at a time
- Synchronized events similar to, but simpler than, in-person voter registration or PGP key signing
- No ID checking, no biometrics, no trust network

Downsides:

- Requires some organization in the physical world
- Those who want one must show up, periodically