



# Towards Real Democratic DAOs

Prof. Bryan Ford  
Decentralized and Distributed Systems (DEDIS)  
Swiss Federal Institute of Technology (EPFL)  
[dedis.epfl.ch](http://dedis.epfl.ch) – [dedis@epfl.ch](mailto:dedis@epfl.ch)

DAO Symposium – November 28, 2024

# We're facing hard global problems



Climate  
change



Exploding  
inequality

# Global problems need global tools

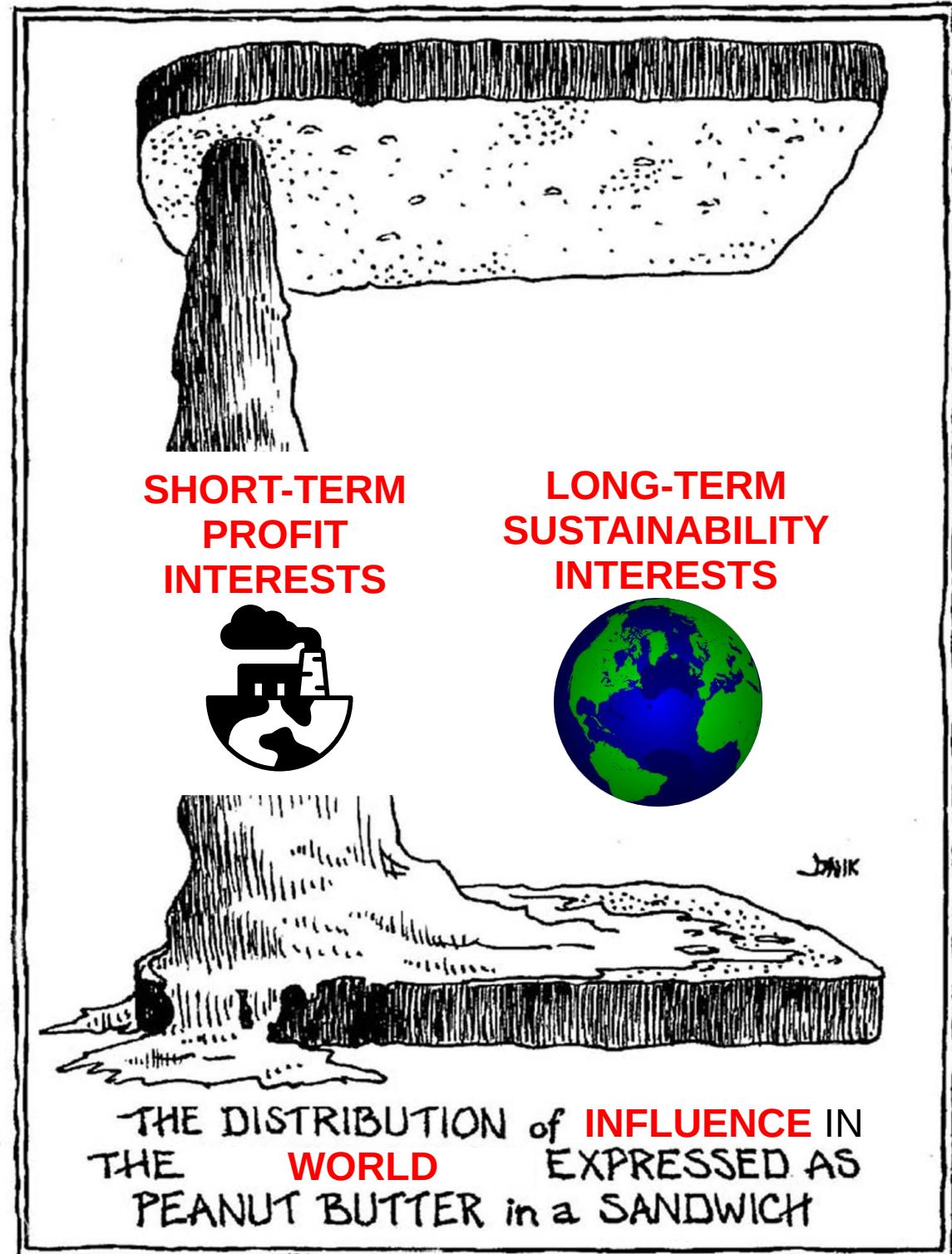


Like DAOs ... *right?*

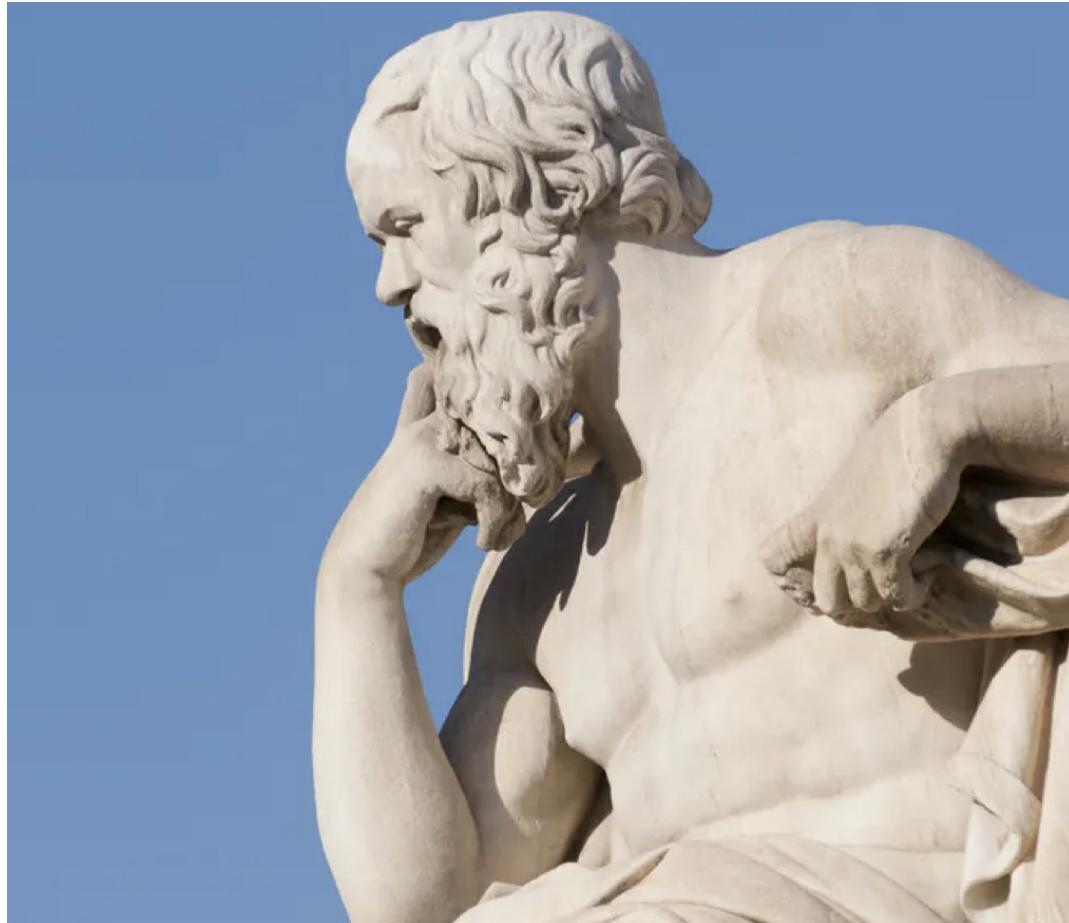
A fundamental  
meta-problem

“Money is power”

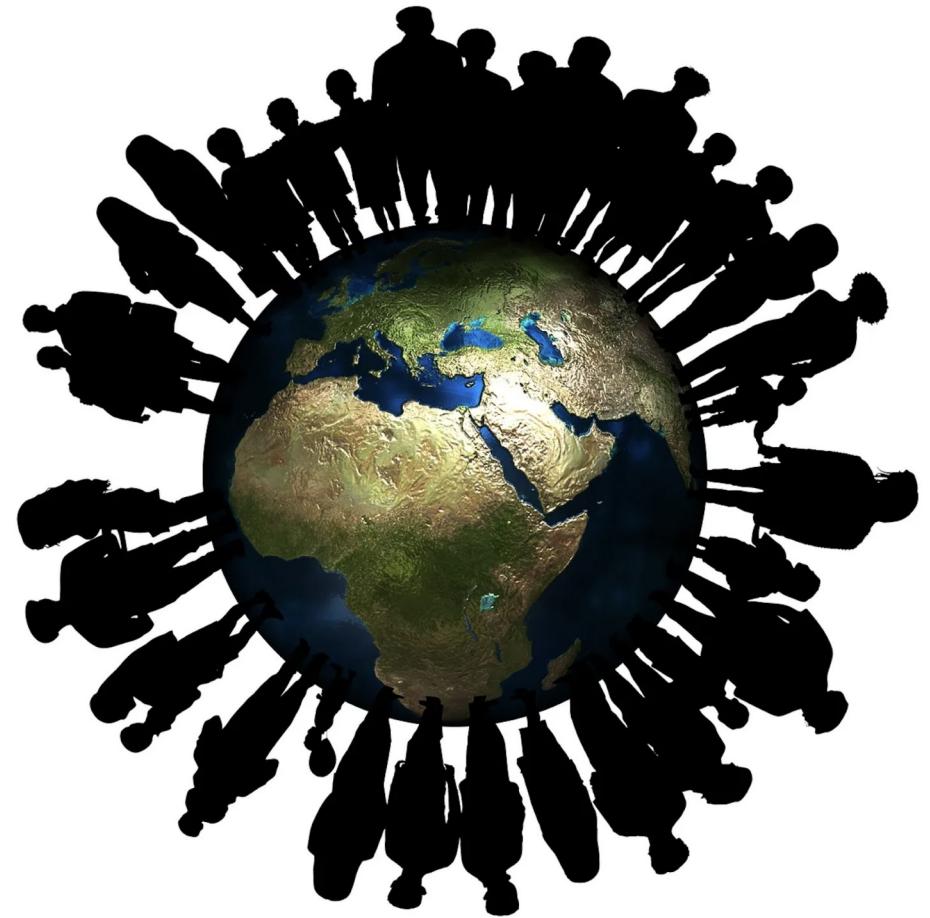
Real solutions  
can't win votes  
dominated by  
entrenched power



# Could global systems like DAOs...



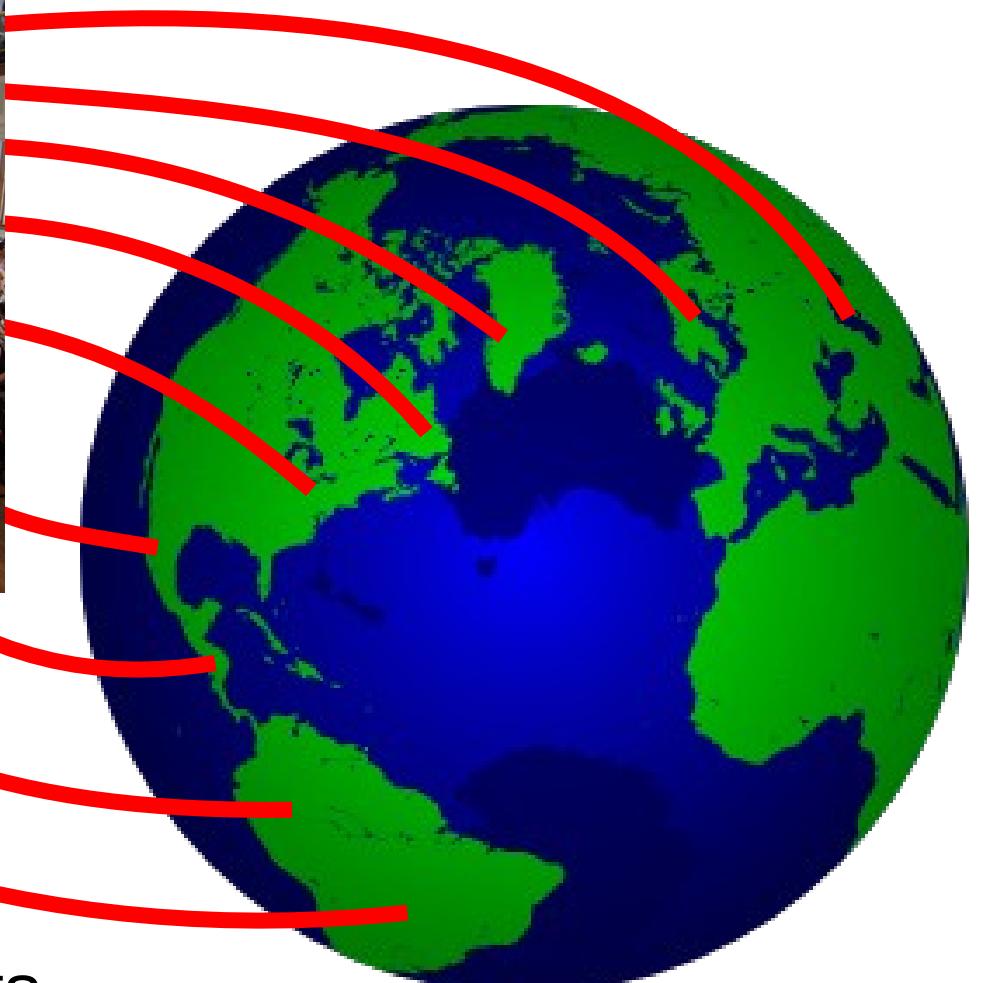
Help us find  
wise solutions?



In everyone's  
collective interest?

# The world's most urgent need

A coherent, secure, inclusive “global town hall”



→ Decisions,  
action plans that  
transparently & securely  
represent everyone's interests

# Talk Roadmap

- **A need: sane collective decision & action**
- A vision: representative global deliberation
- A foundation: proof of personhood
- A challenge: voter coercion, astroturfing
- A program: decentralized systems for all

# Talk Roadmap

- A need: sane collective decision & action
- **A vision: representative global deliberation**
- A foundation: proof of personhood
- A challenge: voter coercion, astroturfing
- A program: decentralized systems for all

# Global town hall: requirements

We need a true *global deliberation platform*  
that gives everyone a voice! ...right?

Like...  
UseNet?  
(R.I.P.)

“The first  
DAO”?



# What UseNet was (thought to be)

## **Netizens: On the History and Impact of Usenet**

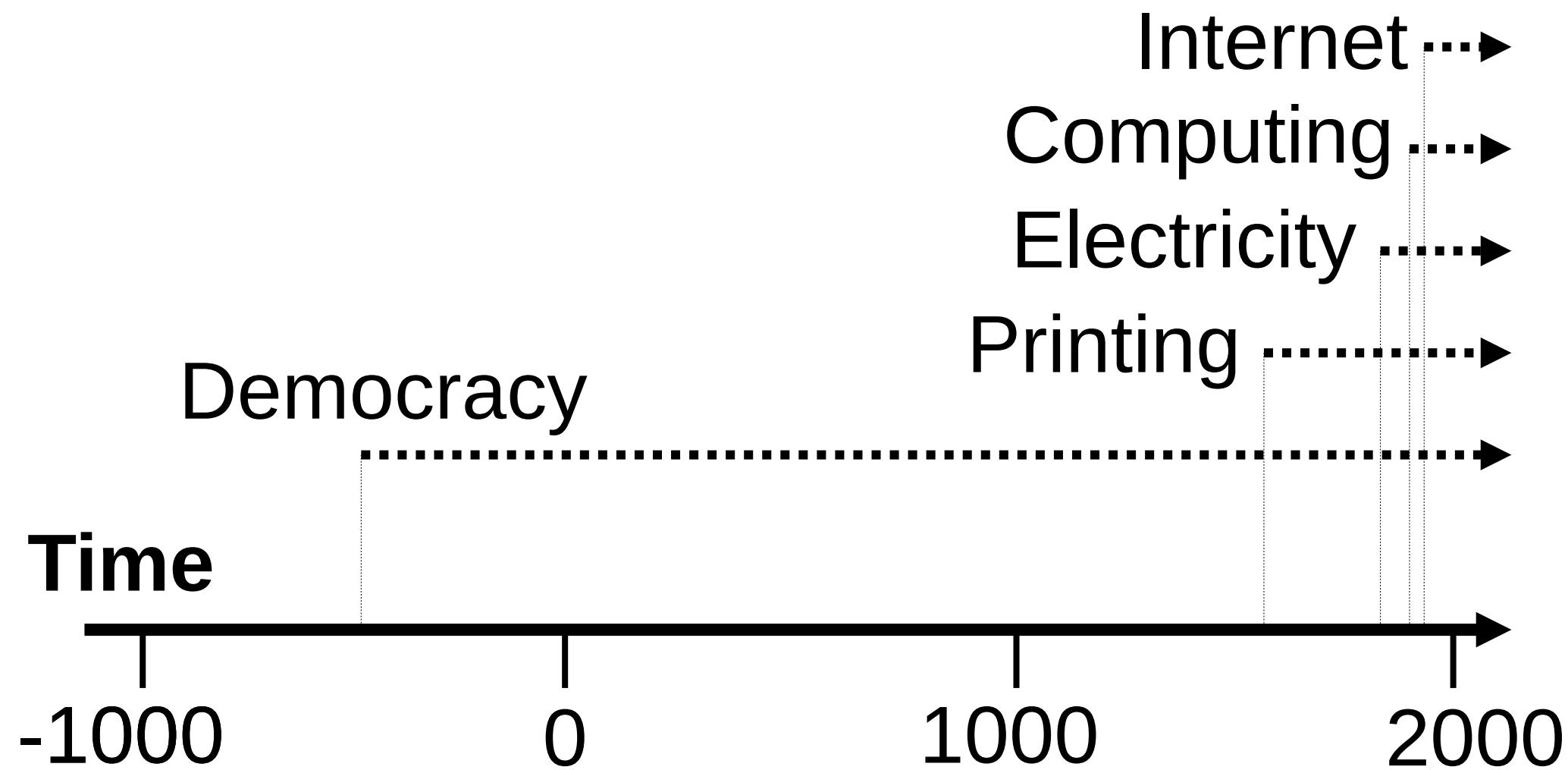
A great historical perspective on how “netizens”  
*thought* UseNet would democratize the world!

Distributed! Decentralized! Democratizing!  
Scalable! (huge, deep newsgroup hierarchy)  
Delay/disruption tolerant! Everyone has a voice!

But... (oops)

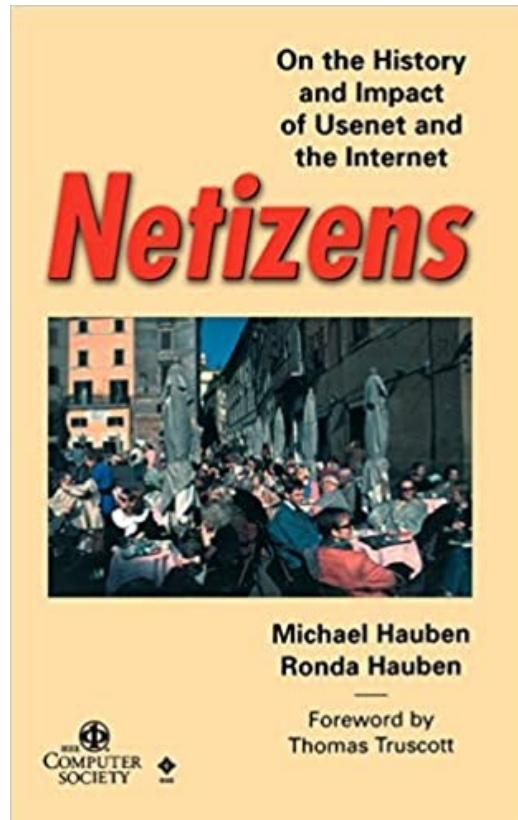
no useful spam control, no effective governance,  
no way to identify (real) people for deliberation, ...

# A few transformative technologies

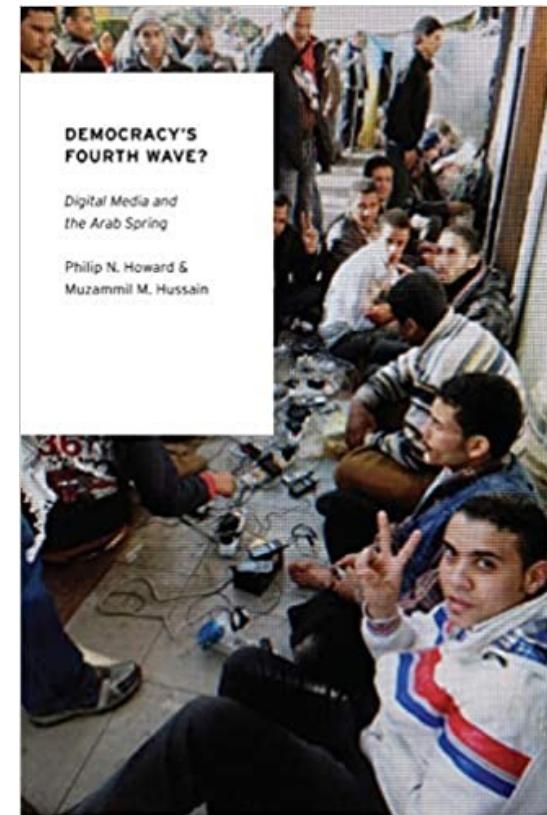


# Is our technology “Democratizing”?

1997



2013



Chapter 18  
“The Computer as a  
Democratizer”

“Democracy’s Fourth Wave?  
Digital Media and the  
Arab Spring”

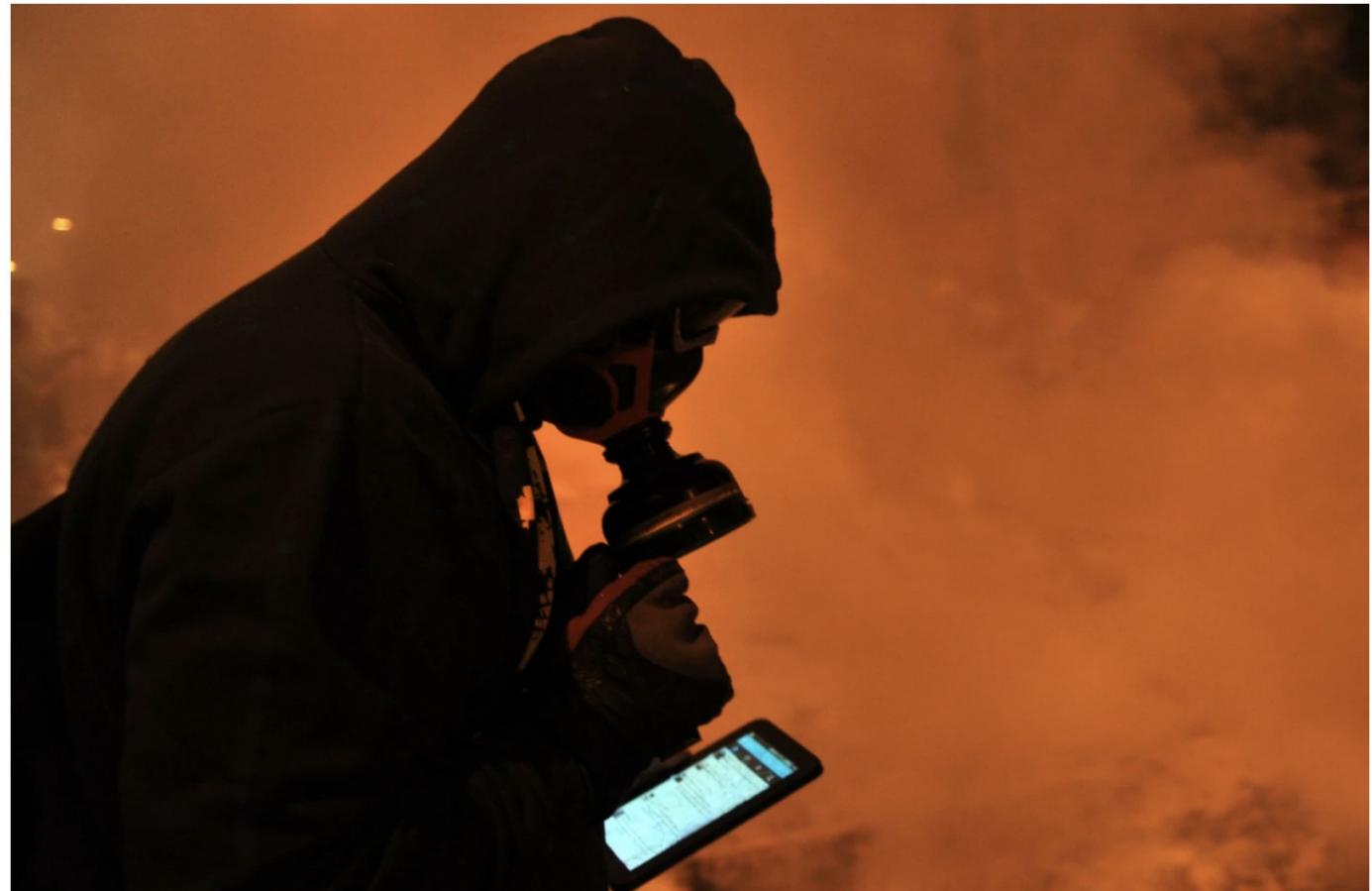
# Is our technology “Democratizing”?

## How Social Media Helps Dictators

It's been hailed as "liberation technology." But it has a darker side.

By [Erica Chenoweth](#)

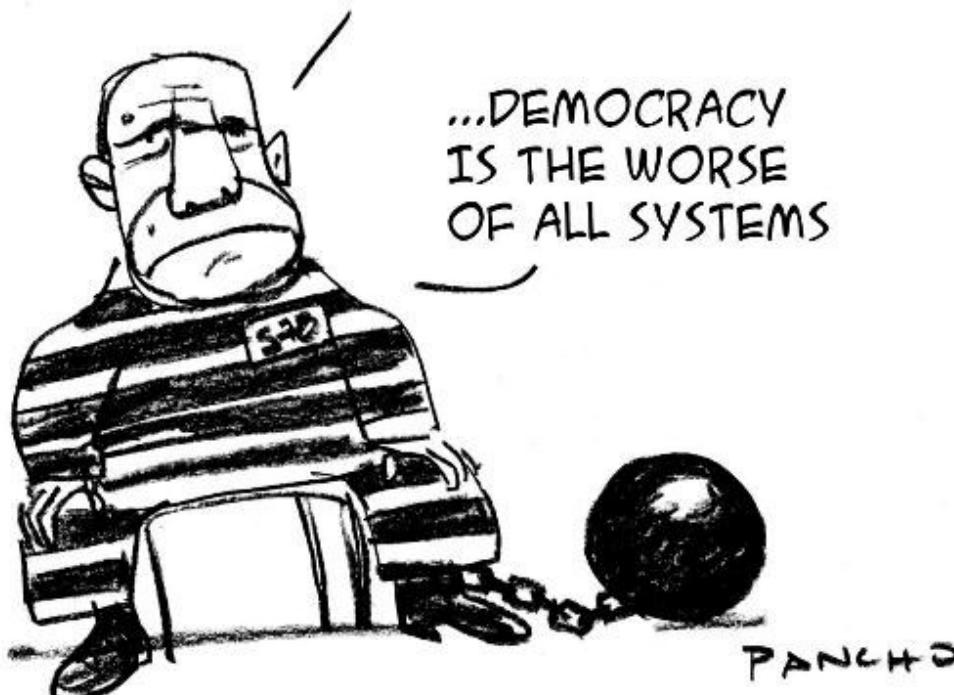
2016



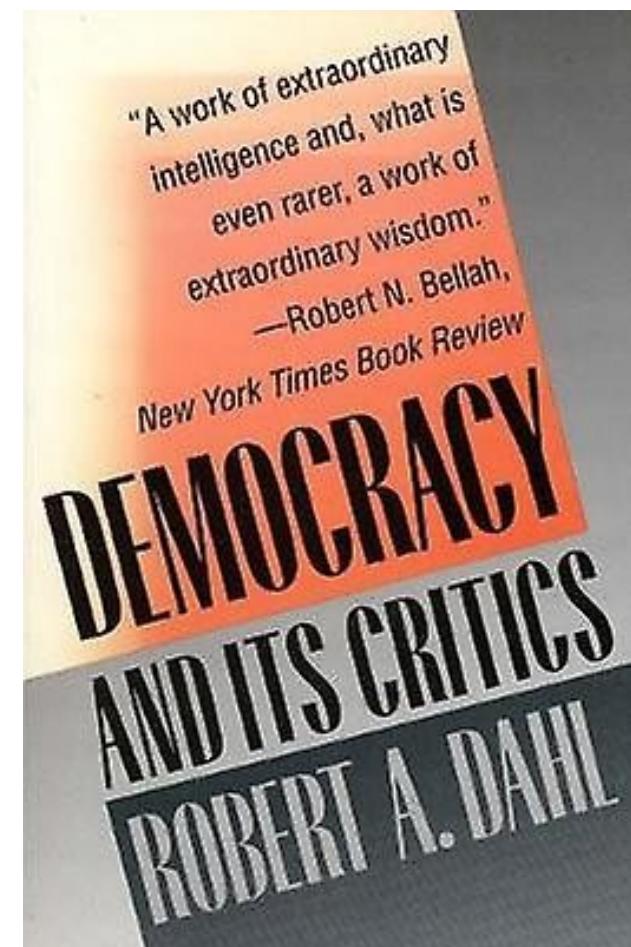
# Why democracy...and what *is* it?

Council of Europe,  
“Democracy”

ALL FORMER  
DICTATORS  
WILL TELL YOU...



Robert Dahl,  
“Democracy & its critics”



# Why democracy...and what *is* it?

Council of Europe,  
“Democracy”

Robert Dahl,  
“Democracy & its critics”

## **Key criteria:**

- Individual autonomy
  - Equality

## **Key criteria:**

- Effective participation
  - Voting equality
- Enlightened understanding
  - Control of the agenda
- Inclusiveness

# Is our technology “Democratizing”?

- Giving “everyone” a voice & a platform



- Equality?
- Enlightened understanding?
- Effective participation?



# Democratic DAOs: requirements

The *real* requirements for “democratic” systems

- Open to participation by all (of course)
- Accessible *anywhere*, even if poorly-connected
- Coherent global-scale discussion, *deliberation*
- Genuinely self-governed, *not* by “guardians”
- One person one vote, *not* one dollar one vote
- Ensure that participants represent *themselves*

UseNet mostly got the first 2...the others are hard!

# Talk Roadmap

- A need: sane collective decision & action
- A vision: representative global deliberation
- **A foundation: proof of personhood**
- A challenge: voter coercion, astroturfing
- A program: decentralized systems for all

# Who gets how much influence?

## Wealth-centric

- One dollar, one vote



[Kera]

## Person-centric

- One person, one vote



[Verity Weekly]

# “Democratizing” requirements

Key requirements based on democratic theory:

- Open to participation by all (of course)
- Accessible *anywhere*, even if poorly-connected
- Coherent global-scale discussion, *deliberation*
- Genuinely self-governed, *not* by “guardians”
- One person one vote, *not* one dollar one vote
- Ensure that participants represent *themselves*

# Who gets how much influence?

## Wealth-centric

- Stock corporations
- Loyalty programs
- Online gaming
- CAPTCHA solving
- Proof-of-work
- Proof-of-stake
- Proof-of-X for most X

## Person-centric

- Democratic states
- Elected parliaments
- Membership clubs
- Committees
- Town hall meetings
- Direct democracy
- Liquid democracy

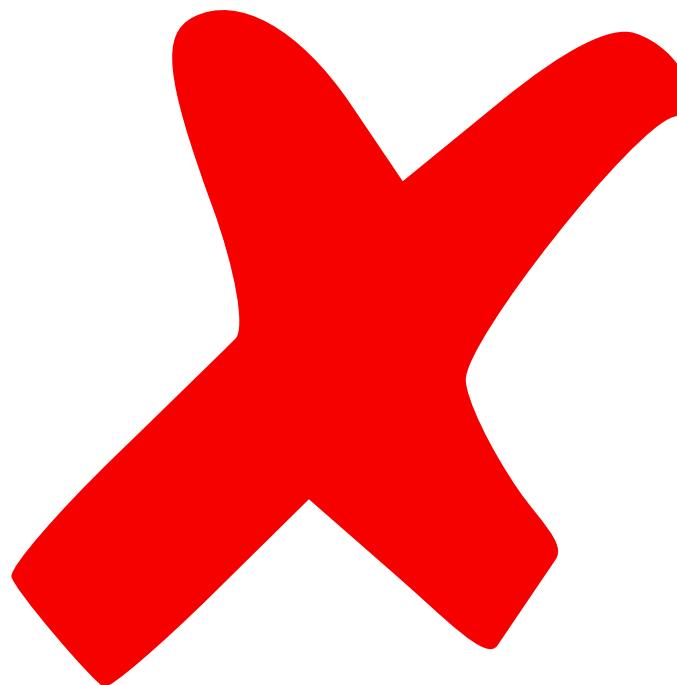
# Contrasting Influence Foundations

**Wealth-centric**



**Largely Solved**

**Person-centric**



**Largely Unsolved**

# Which could help “save the world”?

## Wealth-centric

Been there,  
done that...

it's the status quo!

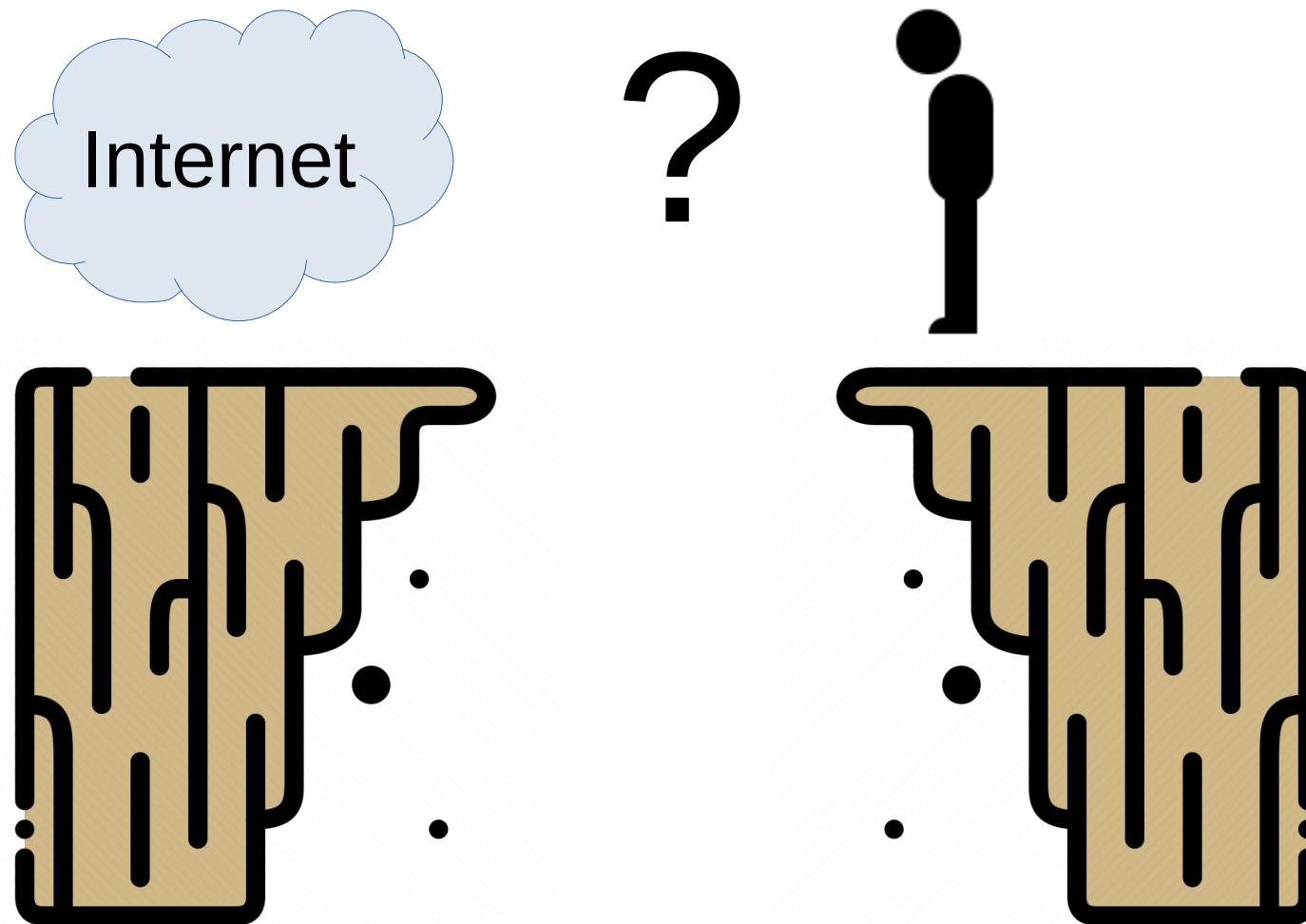
## Person-centric

No guarantee  
of success, but...

No other plausible  
option to get  
**global buy-in**

# A Fundamental Problem

Today's Internet doesn't know what a “person” is

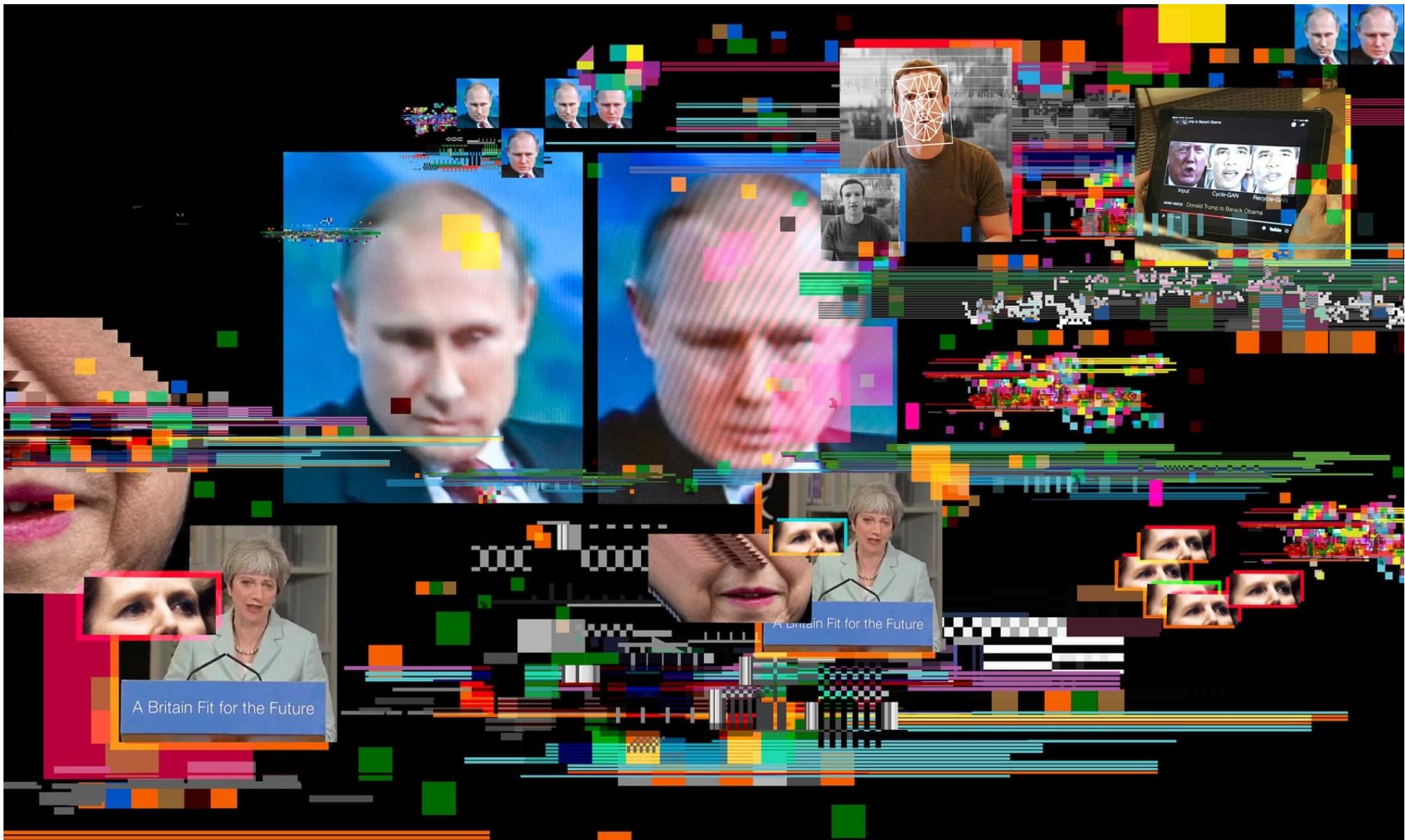


# People aren't digital, only profiles are



[Pixabay, The Moscow Times]

# Fakery is exploding, especially w/ AI



[Ian Sample, The Guardian]

# PoP: brief problem statement

- How to “identify” **real (human) persons...**
  - For online coordination, deliberation, DAOs
  - Ensuring accountability, “one person one vote”
- ...without actually “identifying” them?
  - Protect participant privacy, anonymity, freedom
  - Avoid requiring real ID cards or trackable proxies
- Achieve “**proof of personhood**”  
*without “proof of identity”?*

Preprint: <https://bford.info/pub/soc/personhood/>

# Identity and Personhood in Digital Democracy: Evaluating Inclusion, Equality, Security, and Privacy in Pseudonym Parties and Other Proofs of Personhood

Bryan Ford  
Swiss Federal Institute of Technology in Lausanne (EPFL)

November 4, 2020

# Key desirable (required?) goals

Can we achieve Proof of Personhood that is:

- **Inclusive:** open to all *real people*, not to bots
- **Equitable:** all *people* get equal power, benefits
- **Secure:** correct operation, verifiable by *people*
- **Privacy:** protects rights & freedoms of *people*

“We must act to ensure that technology is designed and developed to serve humankind, and not the other way around”

- Tim Cook, Oct 24, 2018

# Personhood Online: Approaches

- **Documented Identity:** e.g., government-issued
  - Privacy-invasive, IDs not hard to fake or buy
- **Biometric Identity:** India, UNHCR, Worldcoin
  - Huge privacy issues, false positives+negatives
- **Trust Networks:** PGP “Web of Trust” model
  - Unusable in practice, doesn’t address Sybil attacks
- **Physical Presence:** in-person participation
  - Requires no ID, trust, connections: just a *body*
  - Proposed in [Pseudonym Parties](#) [SocialNets ‘08]

# A few Proof of Personhood efforts

- Pseudonym Parties [[Ford, 2008](#)]
- Proof-of-Personhood [[Borge et al, 2017](#)]
- Encointer [[Brenzikofer, 2018](#)]
- BrightID [[Sanders, 2018](#)]
- Duniter [[2018](#)]
- Idena [[2019](#)]
- HumanityDAO [[Rich, 2019](#)]
- Pseudonym Pairs [[Nygren, 2019](#)]
- DFINITY Virtual People Parties [[Williams, 2021](#)]
- Worldcoin [[Worldcoin, 2023](#)]

# PoP based on physical presence

- Ford/Strauss, “**An Offline Foundation for Online Accountable Pseudonyms**” [2008]
  - In-person *pseudonym parties* to create PoP tokens

## An Offline Foundation for Online Accountable Pseudonyms

Bryan Ford

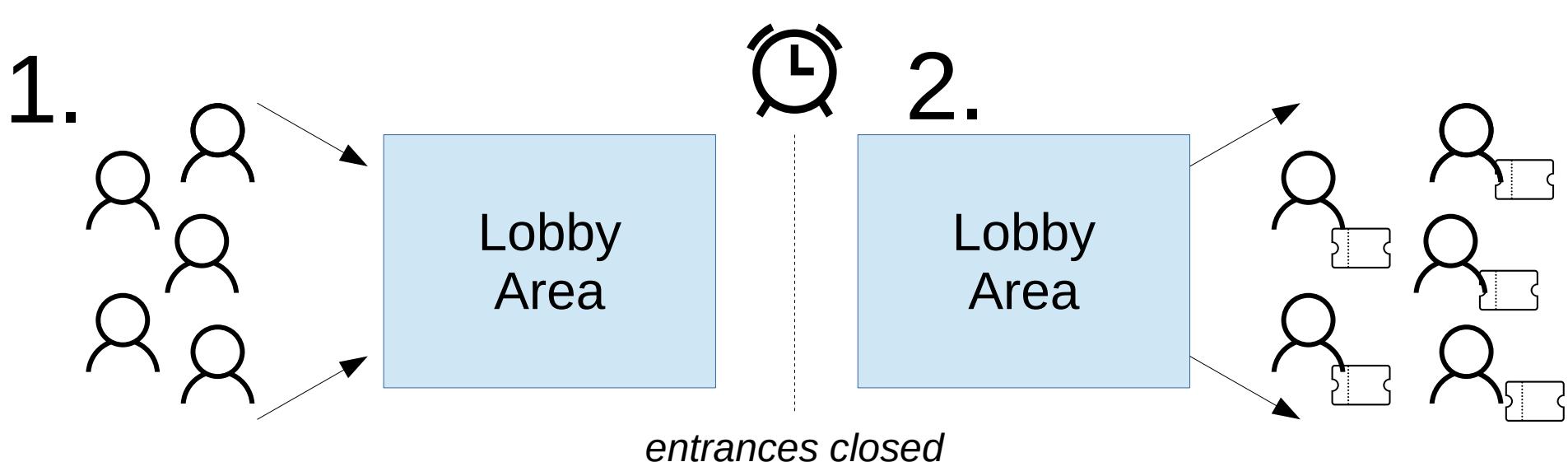
Massachusetts Institute of Technology

Jacob Strauss

# PoP based on physical presence

Principle: real people have only one body each

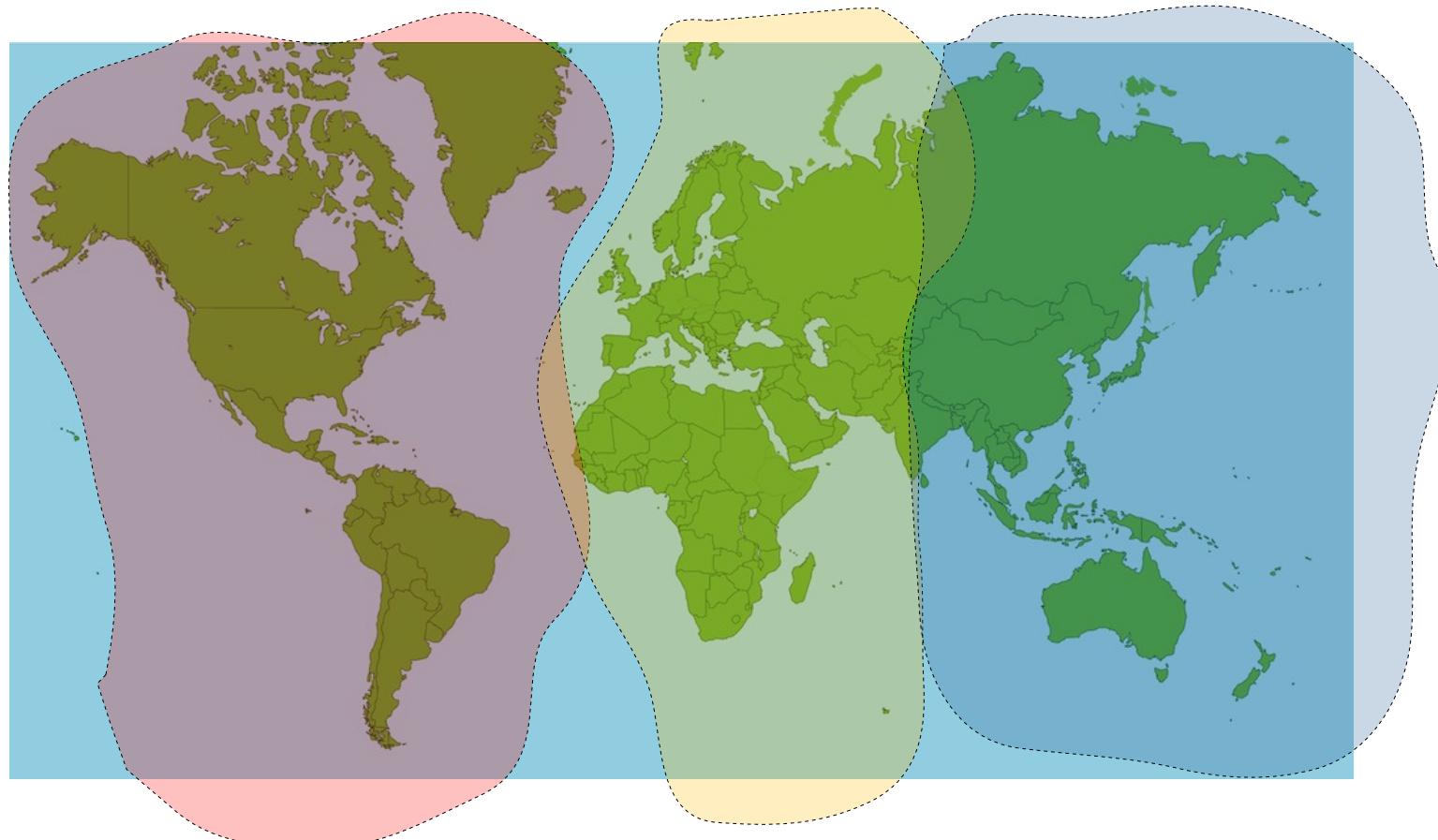
- Attendees gather in “lobby” area by a deadline
- At deadline: doors close, *no one else gets in*
- Each attendee gets one token when *leaving*



# Scalable via *simultaneous* events

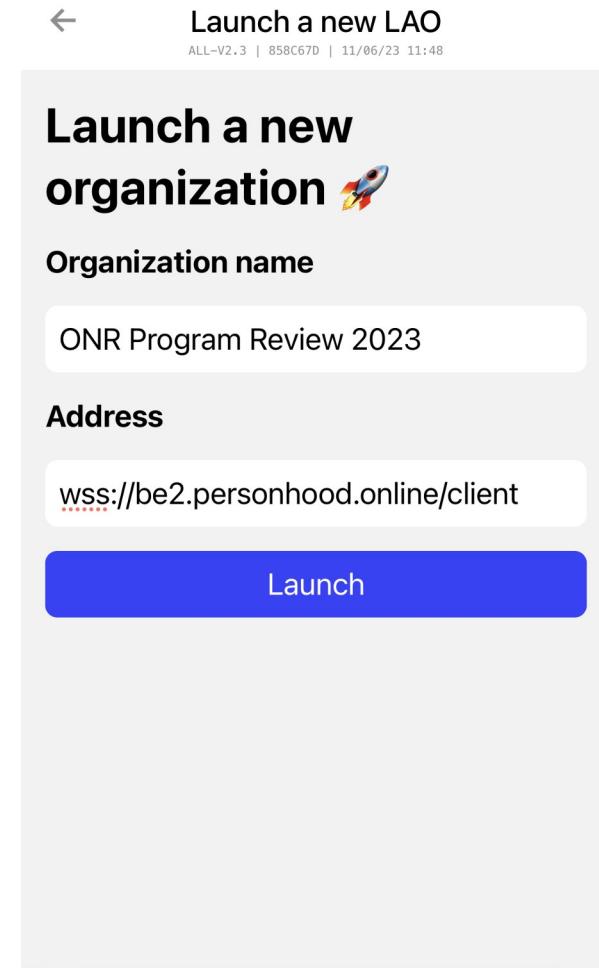
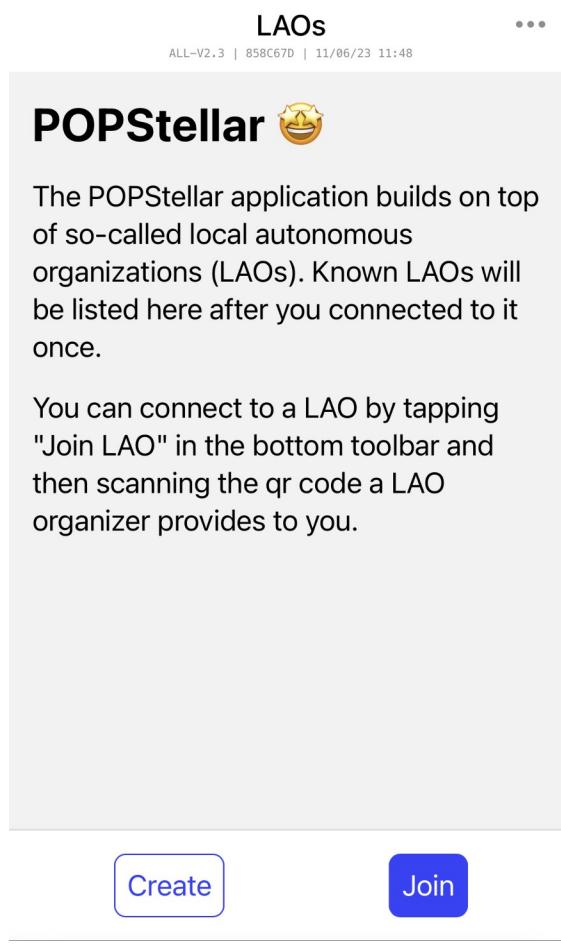
Potentially at many grassroots-organized events

- Even globally, in a few “timezone federations”



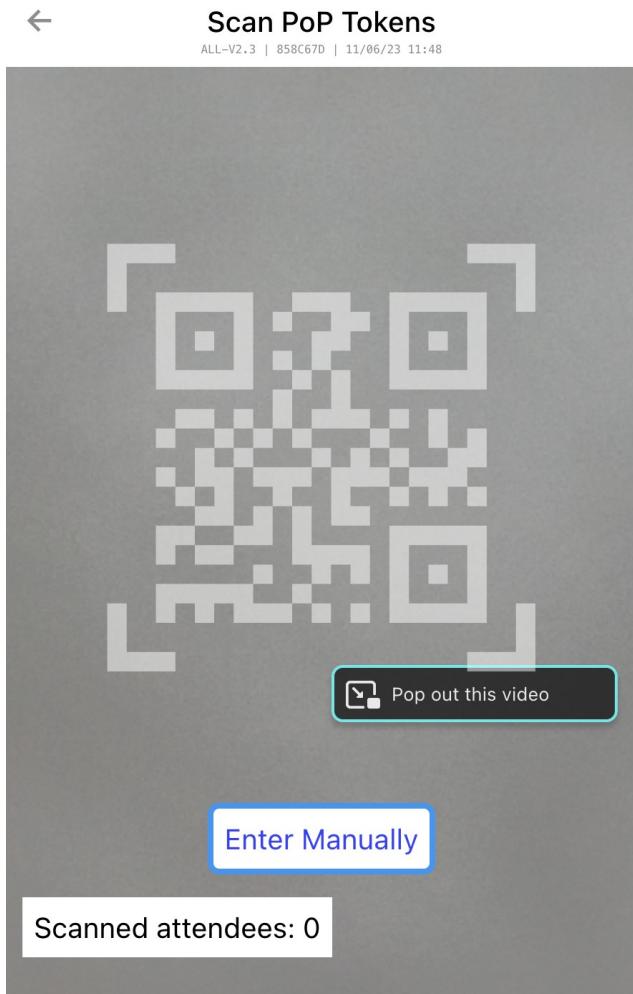
# Local Autonomous Organizations

Any person or group may create an ad-hoc LAO



# Organizer scans attendees' tokens

Organizer:



Participant:

The screenshot shows the 'Roll-Call' screen. At the top, there is a back arrow and the title 'Roll-Call'. Below that, a timestamp 'ALL-V2.3 | 858C67D | 11/06/23 11:48' is displayed. The main content area has a header 'Program Review 2023' and a subtitle 'Harvard Science & Engineering Complex'. It also displays the text 'Ending 18 hours from now'. Below this, there is a section titled 'Description' with a dropdown arrow. The description text reads: 'The Roll Call is currently open and you as an attendee should let the organizer scan your PoP token encoded in the QR Code below.' At the bottom is a large QR code with a central blue circle containing the text 'Scan to add attendee'.

# Encointer: in-person PoP system

- Uses periodic synchronized **encounters** to verify personhood in-person, mint coins, ...



# Anti-tracking PoP tokens

Roll-calls are already privacy-preserving

- Yield PoP tokens with no identifying information

But PoP tokens could still be tracked, correlated

- Pseudonymity is not the same as anonymity!

Goal: blinded untraceable *usage* of PoP tokens

- Pseudonym-friendly but accountable!

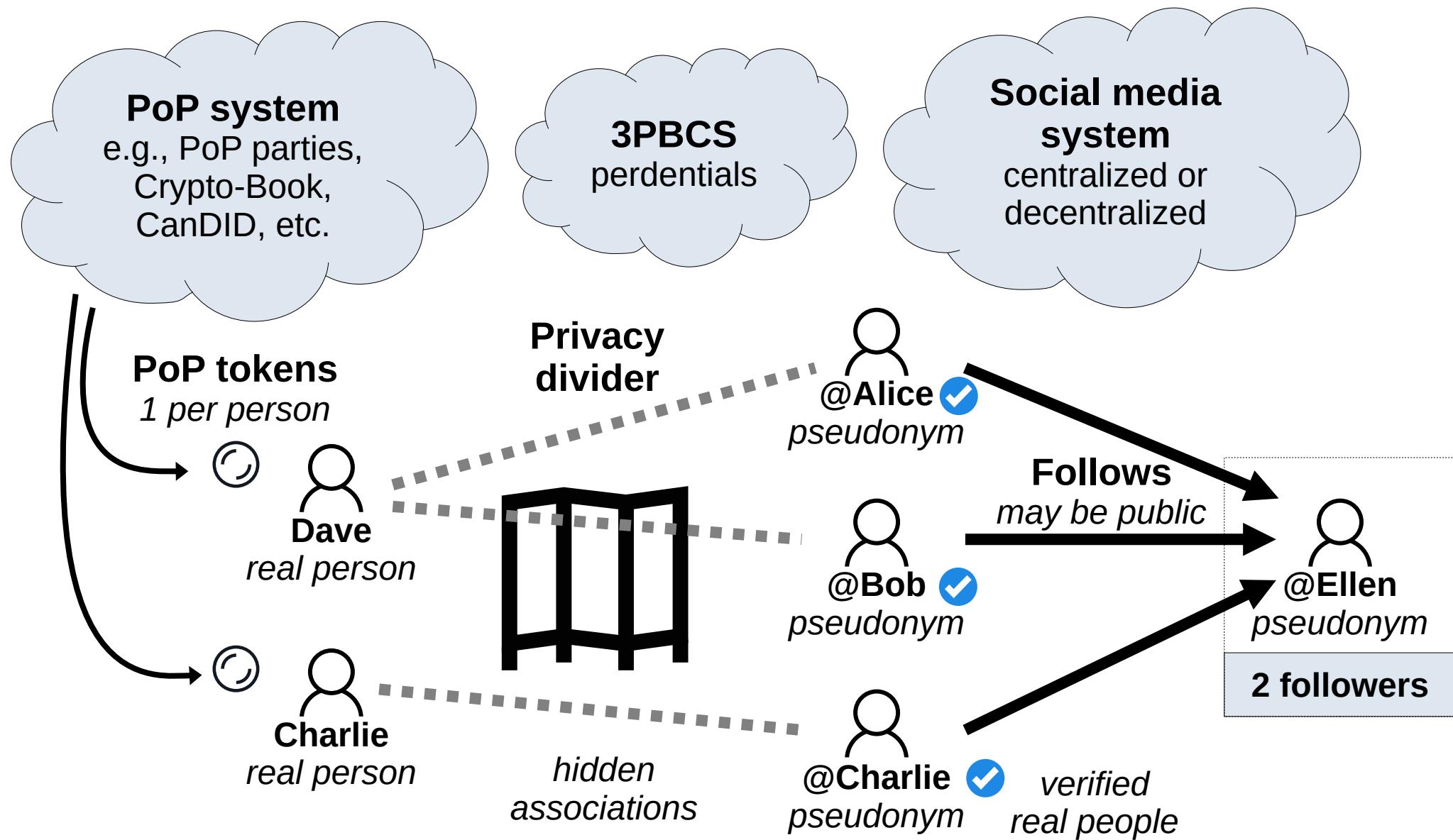
# 3PBCS: a privacy-preserving personhood-based credential system

3PBCS creates **perdentials**: credentials usable to

- Reveal & prove **properties** about the bearer
  - e.g., age > 18, have Ph.D. from U, usual SSI stuff
- Create **pseudonyms** with “real person” status 
  - *Sybils allowed!* professional, personal, hobby...  
- Allow **counts/quotas** with 1-per-person weight
  - Followers, likes, etc. count only *unique real people*

Builds on *any* PoP scheme + Coconut credentials

# Perdentials: an illustrative scenario



# Talk Roadmap

- A need: sane collective decision & action
- A vision: representative global deliberation
- A foundation: proof of personhood
- **A challenge: voter coercion, astroturfing**
- A program: decentralized systems for all

# Collusion and Coercion in PoP

Case study of the **Idena** PoP network, 2019-2022

## **Compressed to 0: The Silent Strings of Proof of Personhood<sup>1</sup>**

*Puja Obhaver<sup>2</sup>, Mikhail Nikulin<sup>3</sup>, Paula Berman<sup>4</sup>*

[https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4749892](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4749892)

# Idena: essential idea

- Account holders (hopefully real humans) participate **online** in **synchronized events**
- Must solve several **reverse Turing tests** (“FLIP” puzzles) in 2 minutes
- Run validation nodes, earn “crypto-UBI”, ...



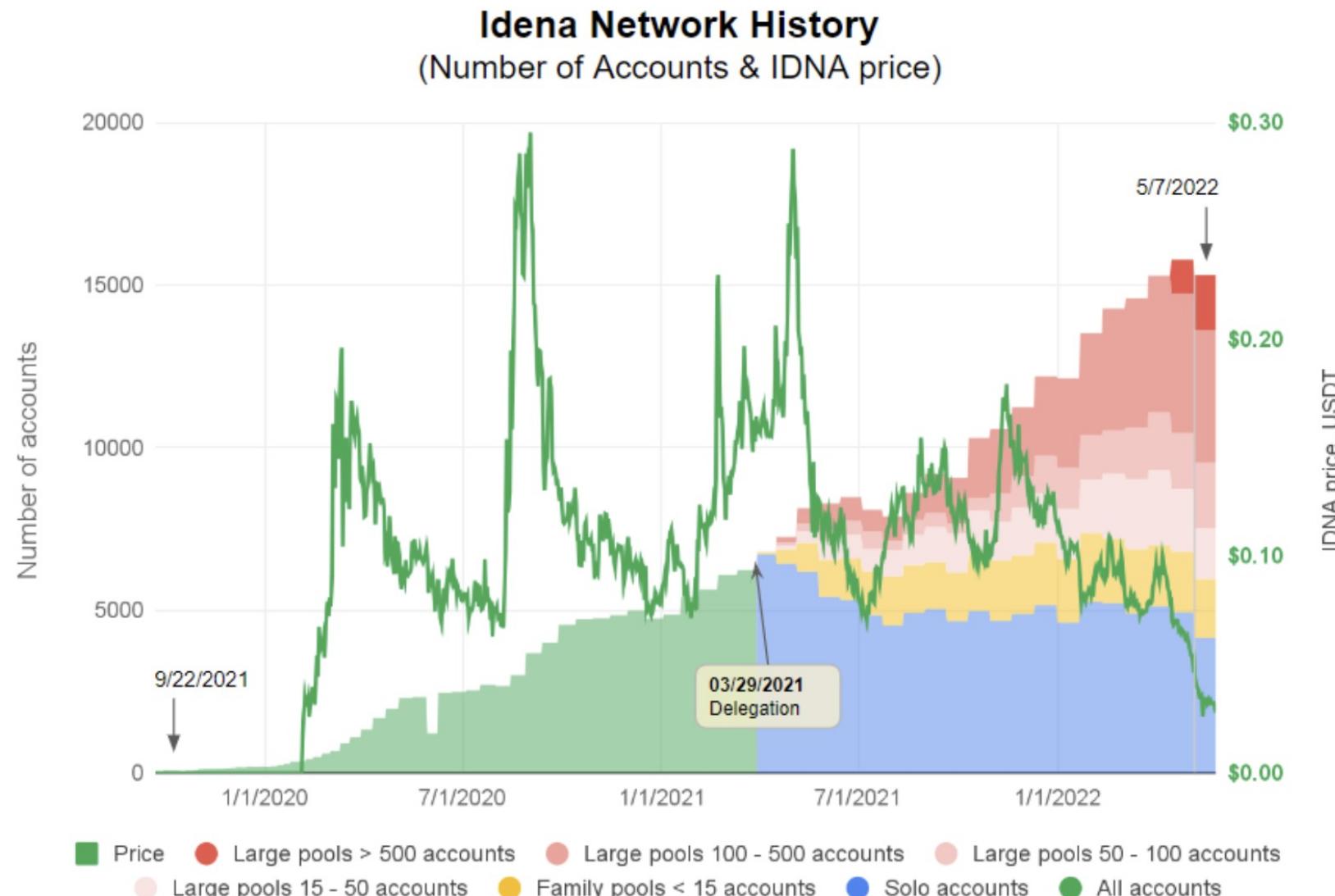
# Idena: the Puppet Pool Takeover

Key lessons from “[Compressed to 0](#)” report:

- FLIP challenges technically **appeared to work** to filter and/or deter automated abuse
- But network increasingly dominated by **pools** paying **real people** to serve as **puppets**
- Pool operators exploit economies of scale, information asymmetry



# Idena: the Puppet Pool Takeover



*Figure 8 : Idena Network History<sup>42</sup>*

# Idena: the Puppet Pool Takeover

Egyptian Pharaoh 10.01.2022



# “Democratizing” requirements

Key requirements based on democratic theory:

- Open to participation by all (of course)
- Accessible *anywhere*, even if poorly-connected
- Coherent global-scale discussion, *deliberation*
- Genuinely self-governed, *not* by “guardians”
- One person one vote, *not* one dollar one vote
- Ensure that participants represent *themselves*

# PoP for deliberation, governance

Can PoP enable online robust self-governance?

- Adds missing “one-person-one-vote” foundation

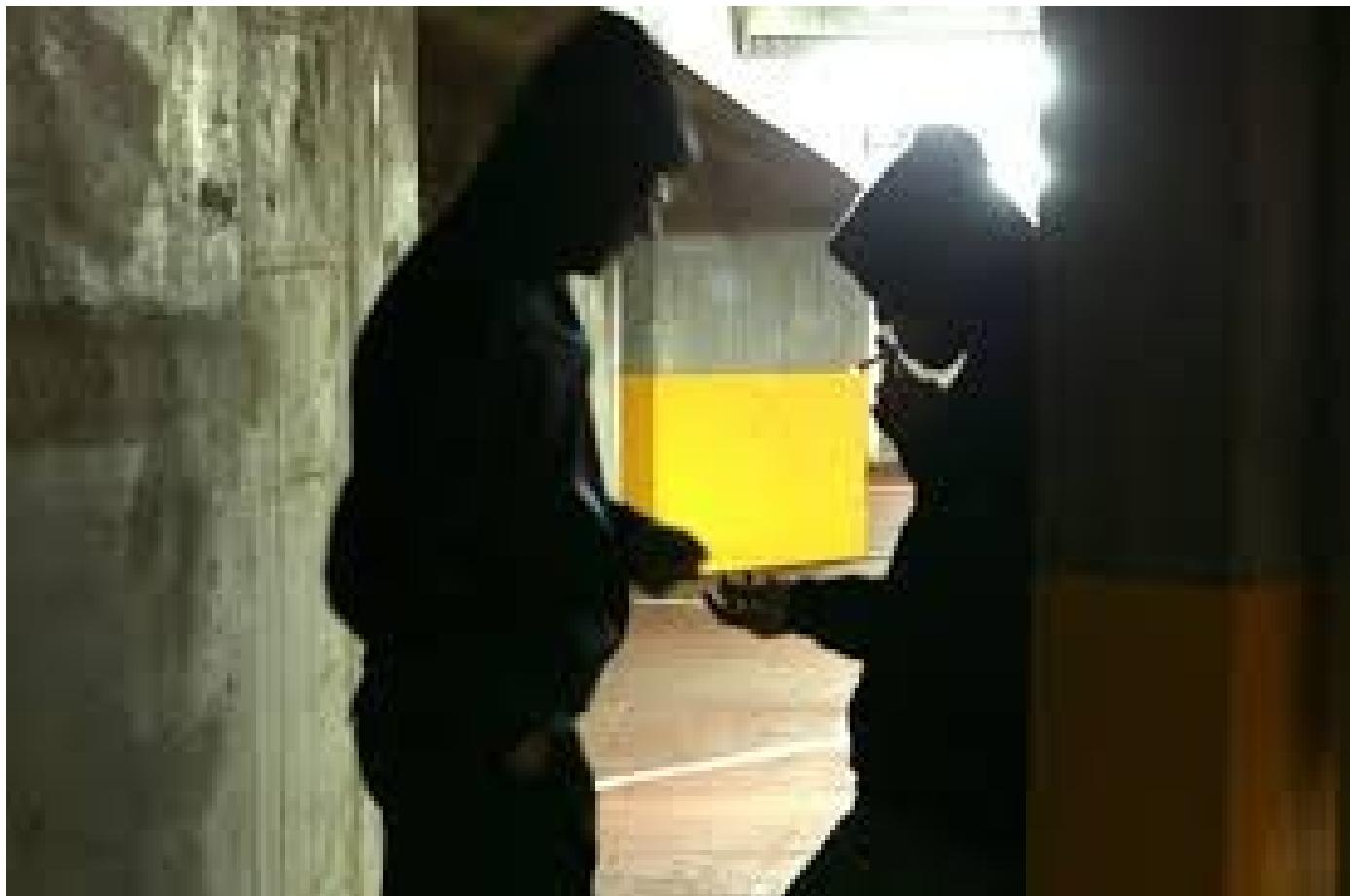
But...

**Whose interests  
do participants  
represent?**



# The Coercion, Vote-Buying Problem

How can we know people vote their **true intent** if we can't secure the environment they vote in?



# The Coercion, Vote-Buying Problem

Both **Postal** and **Internet** voting are vulnerable!

*Election Fraud in North*

*Carolina Leads to New Charges  
for Republican Operative*

**The New York Times**

July 30, 2019



# The Coercion, Vote-Buying Problem

DAOs might make the problem worse!

## Hacking, Distributed



### On-Chain Vote Buying and the Rise of Dark DAOs

*on-chain voting voting e-voting trusted hardware identity selling ethereum*

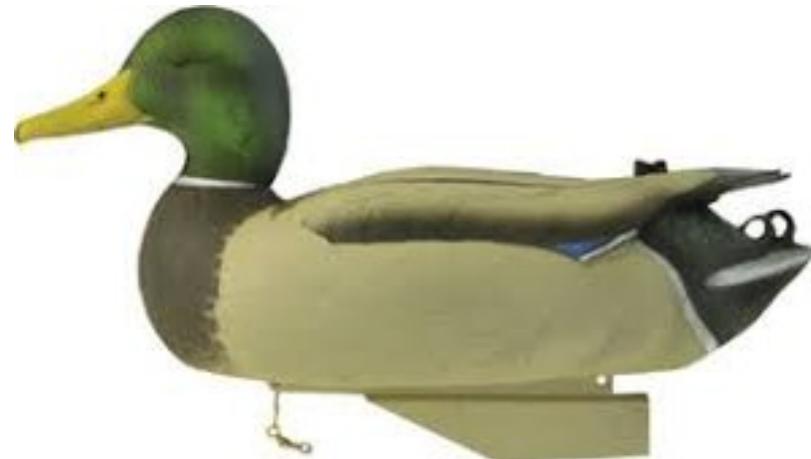
July 02, 2018 at 03:22 PM

[Philip Daian](#), [Tyler Kell](#), [Ian Miers](#), and [Ari Juels](#)

# The “fake credentials” solution [JCJ]

At **registration** time:

- Give all voters *real* and *fake* voting credentials



At **voting** time:

- Real and fake credentials both *appear* to work
- Only real credentials cast votes that *count*

# The central challenge

When, where, how do voters get credentials?

- Without being coerced at or after registration?

**Online** registration or PoP

- Unclear there's *any* plausible solution that doesn't make unrealistic/magical assumptions

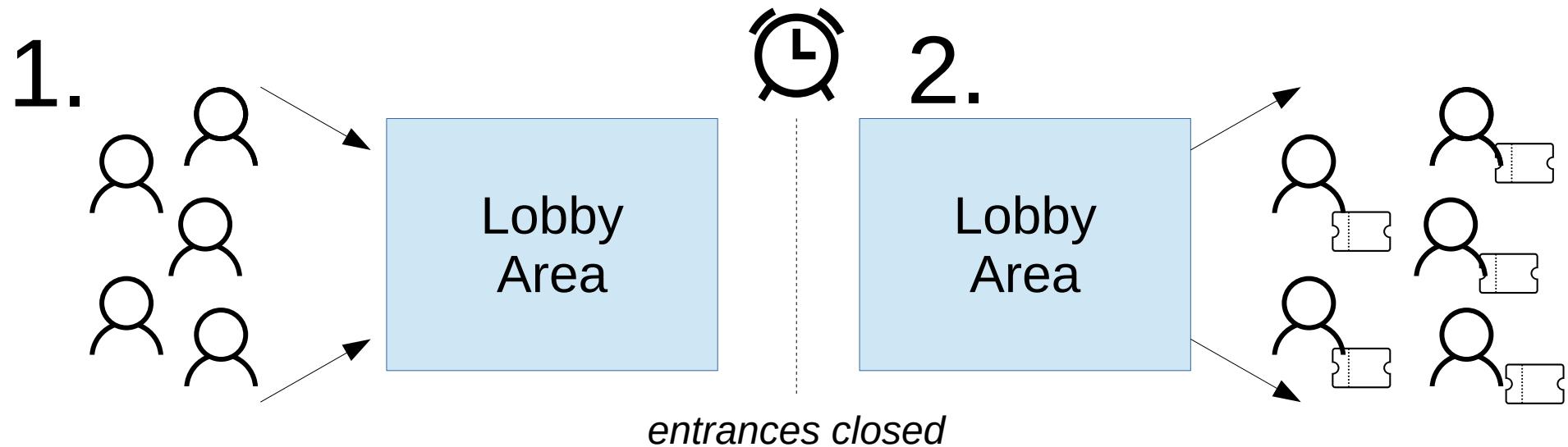
**In-person** registration or PoP

- We can leverage physical security (again)!

# PoP based on physical presence

In-person attendees get short-term *tickets*

- Not (yet) long-term PoP credentials



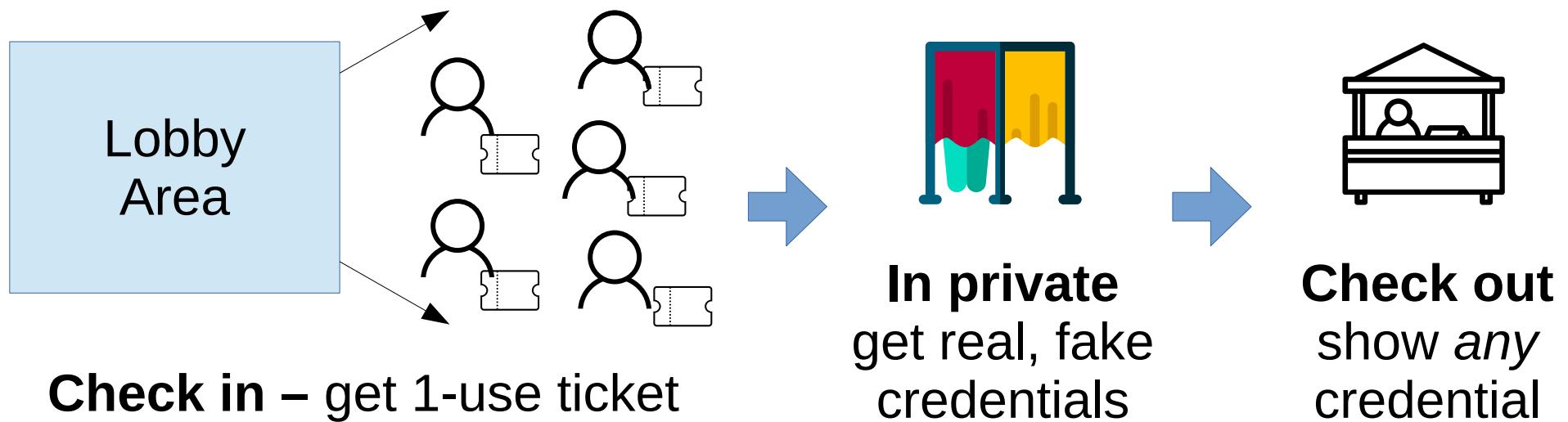
# PoP based on physical presence

In-person attendees get short-term *tickets*

- Not (yet) long-term PoP credentials

Use tickets in a supervised *privacy booth* nearby

- Create long-term real and fake PoP credentials



# Key technical & behavioral problems

The coercion problem is still far from “easy”

- What happens in the privacy booth?
- How much must voters trust what’s in it?
- How do they “know” which credential is real?
- How to ensure a coercer *can’t* learn this?
- Can voters “hide” real credential from coercer?
- Can voters understand and use the process?
- Can and will voters lie to a coercer? ...

# In-person Coercion Resistance

## **TRIP: Trust-limited Coercion-Resistant In-Person Voter Registration**

- <https://bford.info/pub/sec/trip/> (*preprint*)

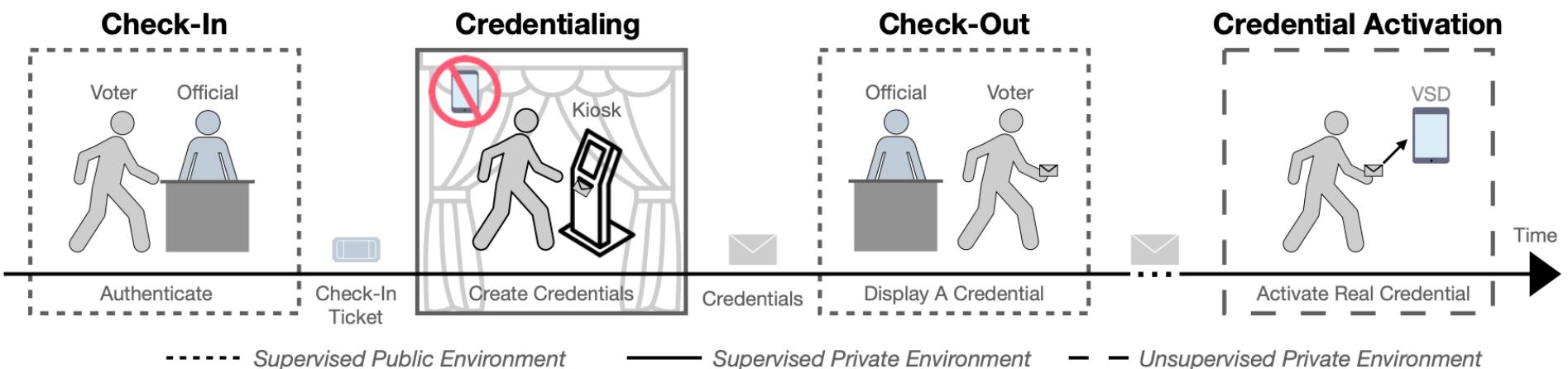
## **E-Vote Your Conscience: Perceptions of Coercion and Vote Buying, and the Usability of Fake Credentials in Online Voting**

- <https://bford.info/pub/sec/trip-usability/>  
*(published in IEEE Security & Privacy '24)*

# TRIP workflow overview

Attendees use digital kiosk in privacy booth to print real & fake *paper credentials*

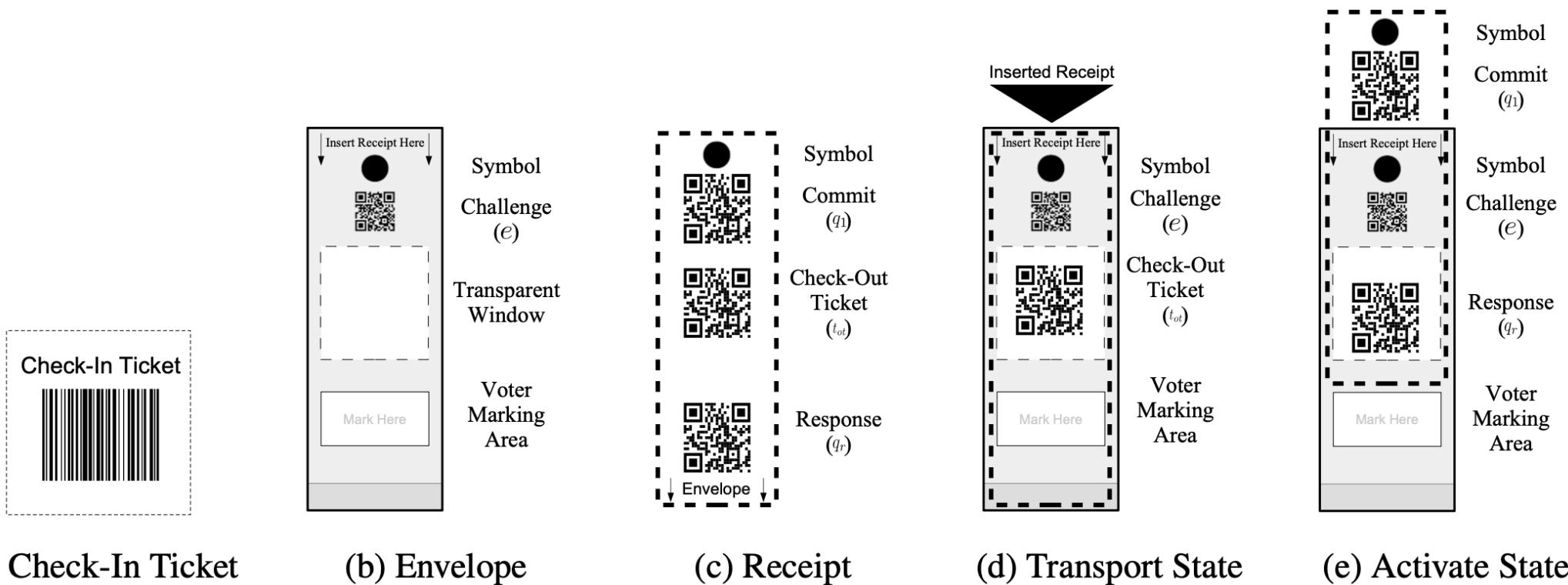
- Cheap, easy to hide from a coercer
- Attendees *not* under coercion need not trust the kiosk



# TRIP paper credential design

Kiosk prints three QR codes on a receipt printer

- *Printing sequence* determines real versus fake
- Voter observes this but can't prove it later



# Prototype kiosk setup for full study



# User study – summary of lessons

- Is the problem of voter coercion important?
  - 26% reported experience by someone they know
  - Most likely scenario: ballot selfies; source: family
- Is the TRIP kiosk usable by ordinary people?
  - SUS usability score of 70.4 → 58<sup>th</sup> percentile
- Can voters successfully use TRIP?
  - 83-95% success rate depending on metric
- Will users detect & report a malicious kiosk?
  - 30% without, 57% with, “security education”

# Next steps, goals, questions

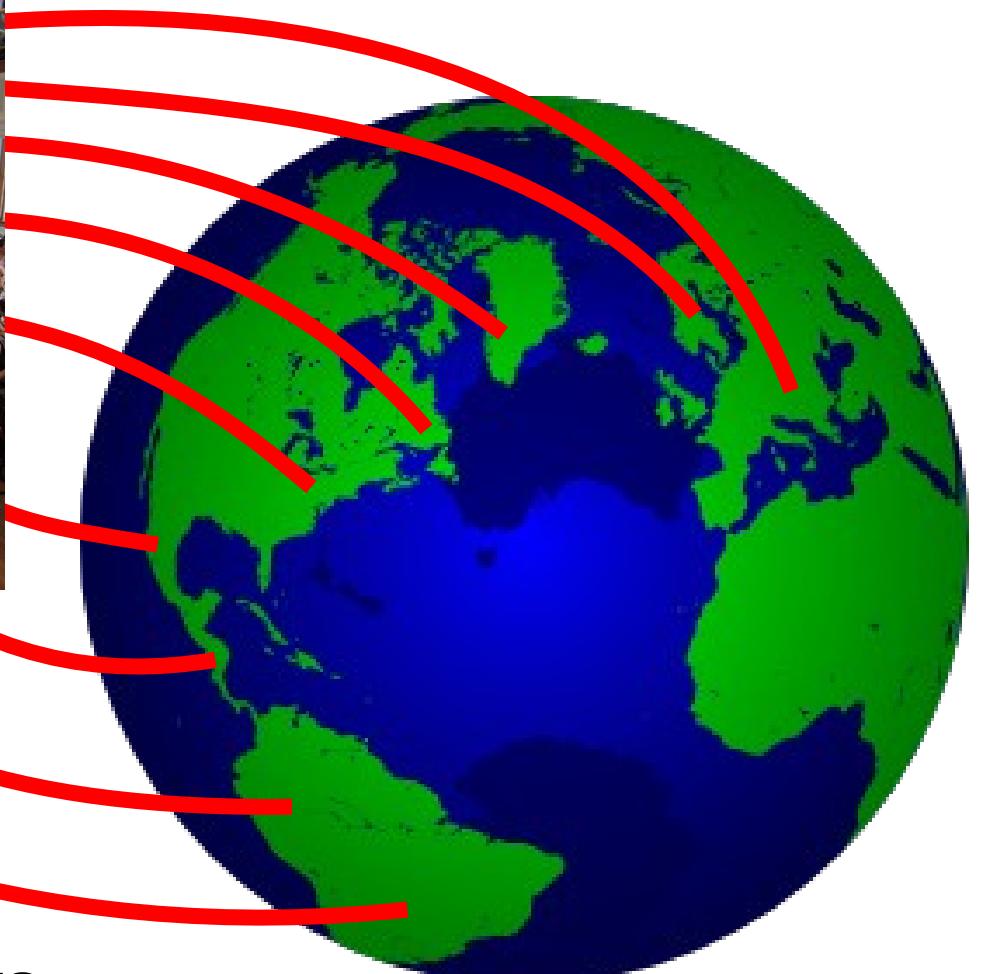
- Real series of presence-based events
  - Tentative: hybrid online/in-person seminar series
  - Participate online or at one of several/many sites
  - Only in-person participants get “voting rights”
  - Social and educational forum: *inform* participants
- User studies of proof-of-presence processes
- What participatory forum(s) to build on top?
  - Simple polls; social media; deliberative debate?
- What will make PoP compelling, sustainable?

# Talk Roadmap

- A need: sane collective decision & action
- A vision: representative global deliberation
- A foundation: proof of personhood
- A challenge: voter coercion, astroturfing
- **A program: decentralized systems for all**

# Is a true “global town hall” feasible?

For robust discussion of important global issues



→ Decisions,  
action plans that  
transparently & securely  
represent everyone's interests

# Towards a true global town hall

If **climate change** is world's most urgent problem,  
**collective action** is most urgent meta-problem.

- Must get *everyone* “at the table” on equal basis
- Hard choices require *transparency* for buy-in

I believe we *can* create distributed infrastructure  
to solve the meta-problem (then the problem)...

- Start by recognizing *how hard* meta-problem is
- We have promising pieces, but need *systems*

# Towards Real Democratic DAOs

To be truly **democratizing** our systems must be:

- Not just “decentralized” and “open to all” but...
- Facilitate true **global interaction, deliberation**
- Ensure **one person, one vote, one quota**
- Ensure **participants represent themselves**

Only **in-person approaches** appear able to offer  
**coercion-resistance, social context, education**

- Build systems, but also **get out and be human!**



# Towards Real Democratic DAOs

Further reading:



<https://bford.info/pub/>