Proof of Personhood: Introduction and Challenges

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

July 27, 2021

Proof of Personhood: talk outline

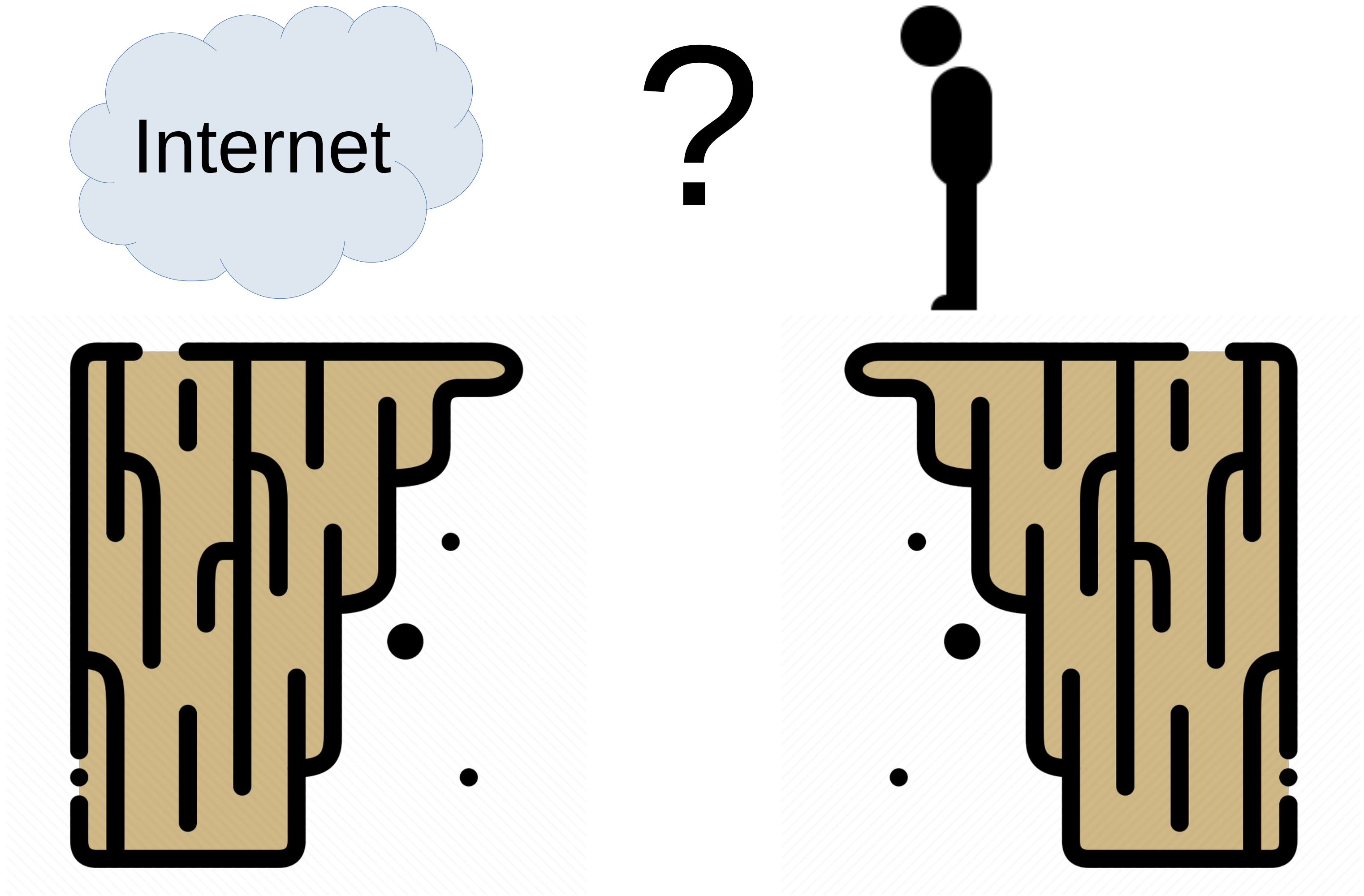
- Problem: why tech ~~doesn't~~ *can't* serve people
- History: whence came "proof of personhood"
- Goals: inclusion, equity, security, privacy
- Uses: what might we do with PoP tokens?
- Challenges: why it's (really, really) hard

Proof of Personhood: talk outline

- **Problem: why tech ~~doesn't~~ *can't* serve people**
- History: whence came "proof of personhood"
- Goals: inclusion, equity, security, privacy
- Uses: what might we do with PoP tokens?
- Challenges: why it's (really, really) hard

The Fundamental Problem

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



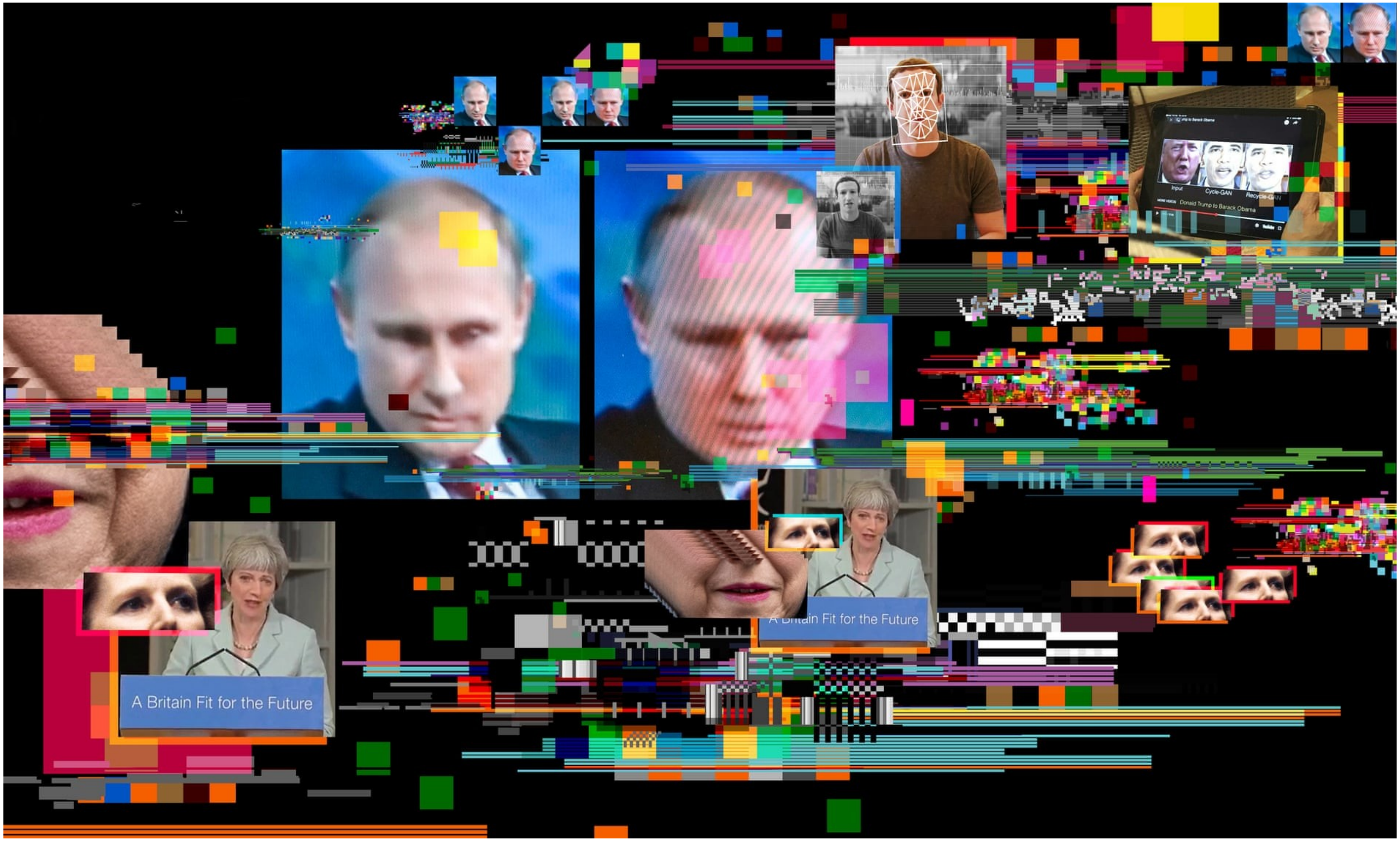
The Fundamental Problem

Services know “people” only as accounts, profiles

[Pixabay, The Moscow Times]

The Fundamental Problem

Profiles are cheap, discardable, easily faked


A Britain Fit for the Future
A Britain Fit for the Future
Input
Cycle-GAN
Recycle-GAN
Donald Trump to Barack Obama

[Ian Sample, The Guardian]

The Fundamental Problem

Profiles are cheap, discardable, easily faked

"On the Internet, nobody knows you're a dog."

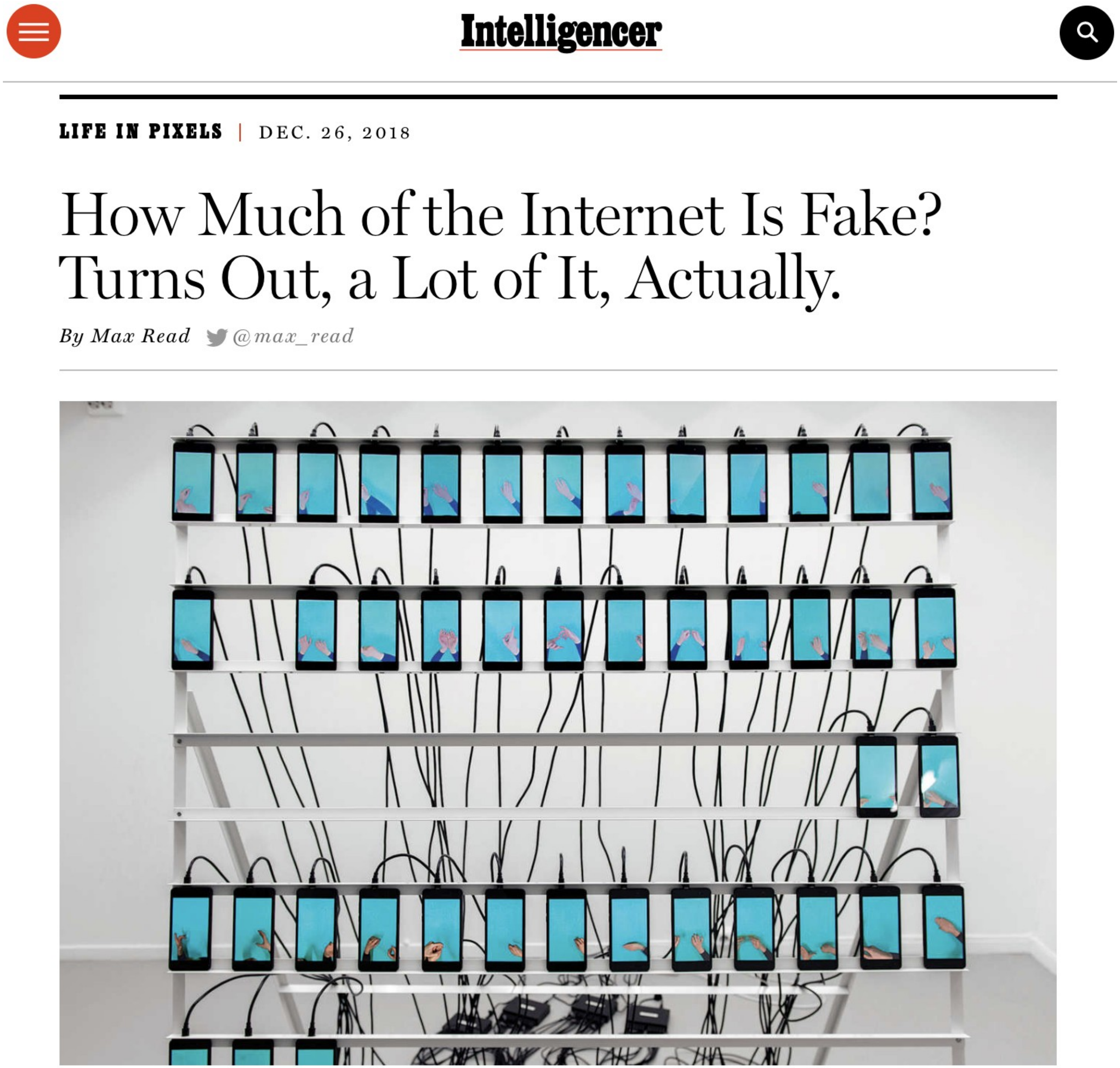
Upside:
inclusion, privacy

Downside:
are "people" really *people*?

The Fundamental Problem

Services can’t count *anything* “one per person”

[imdb]



Intelligencer

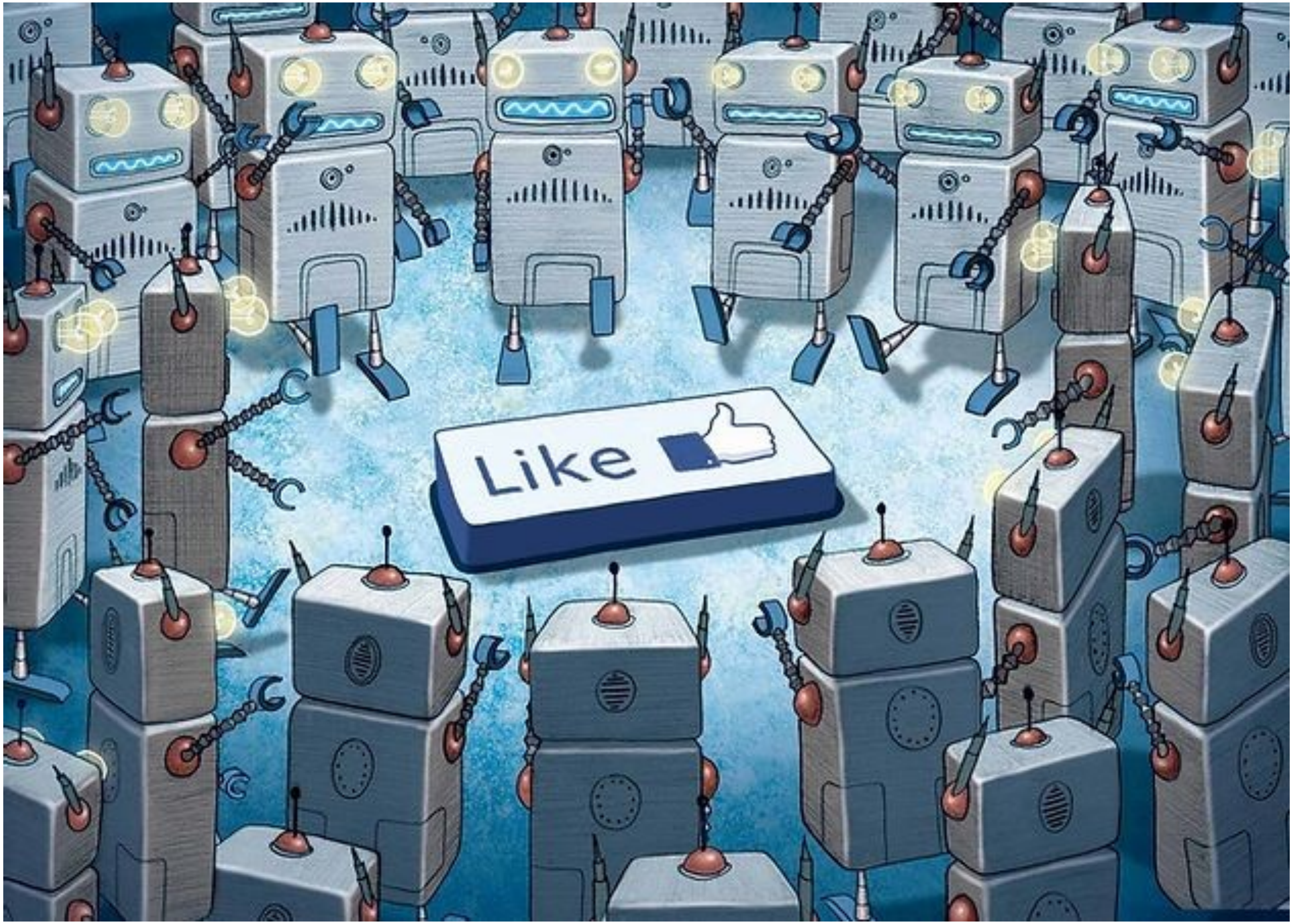
LIFE IN PIXELS | DEC. 26, 2018

How Much of the Internet Is Fake? Turns Out, a Lot of It, Actually.

By Max Read *@max_read*

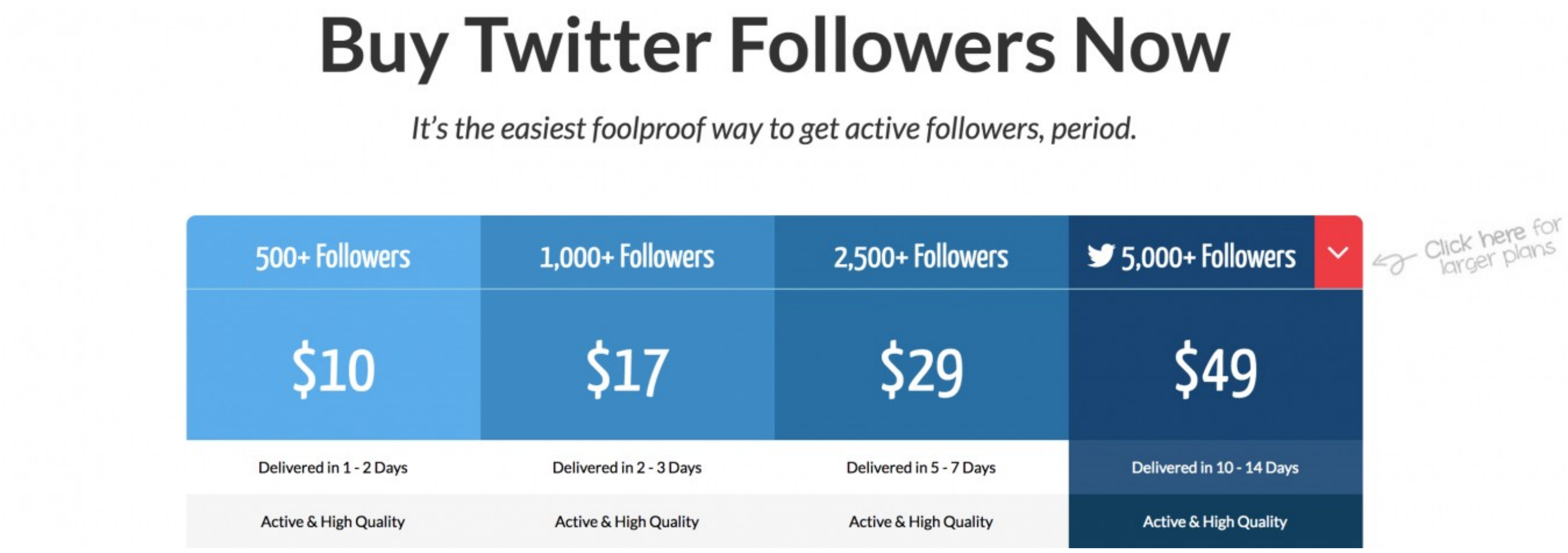
[Ayatgali Tuleubek, Intelligencer]

Likes are fake



[Rabbit Consulting Group]

Followers are fake



Buy Twitter Followers Now

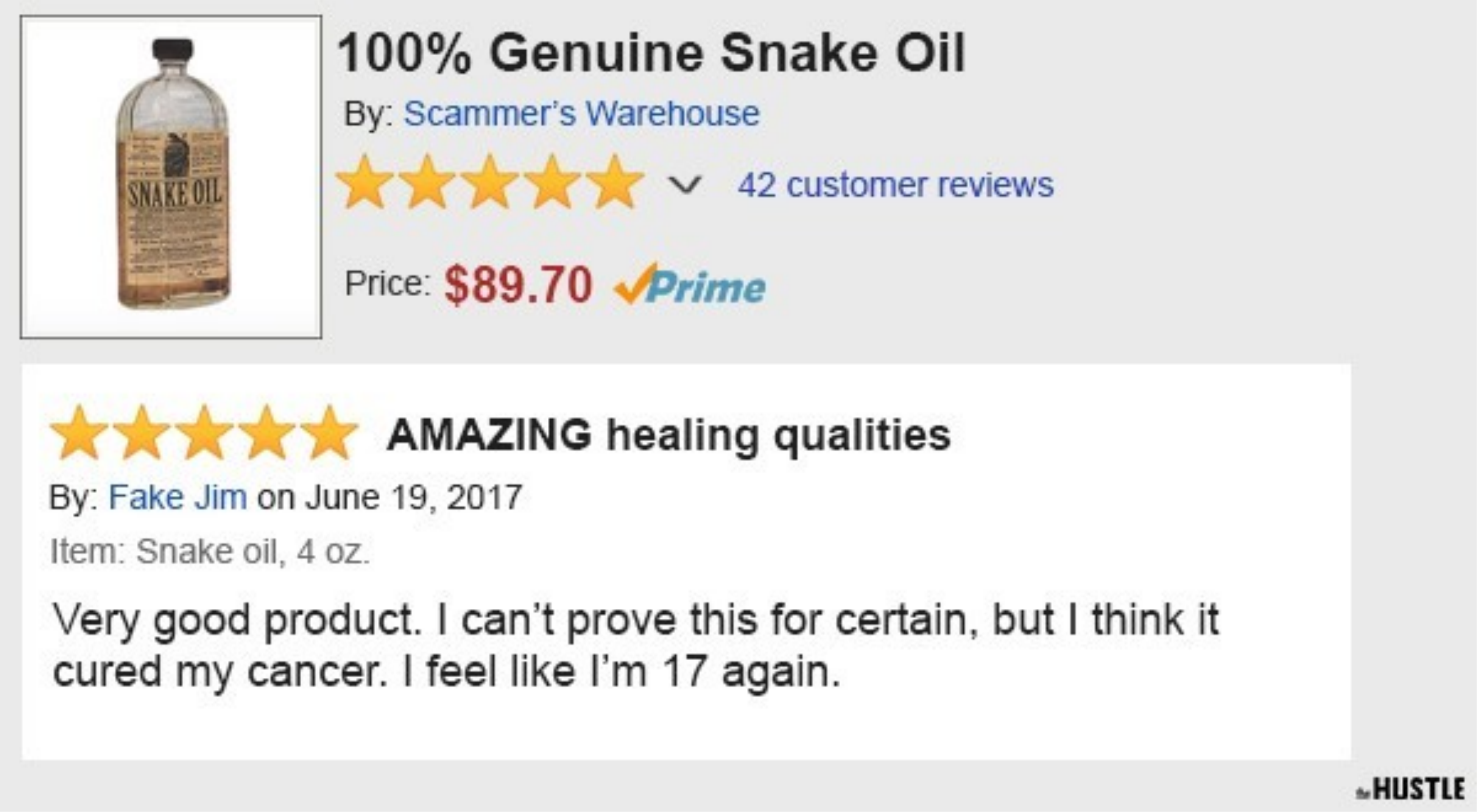
It's the easiest foolproof way to get active followers, period.

500+ Followers	1,000+ Followers	2,500+ Followers	5,000+ Followers
$10	$17	$29	$49
Delivered in 1 - 2 Days	Delivered in 2 - 3 Days	Delivered in 5 - 7 Days	Delivered in 10 - 14 Days
Active & High Quality	Active & High Quality	Active & High Quality	Active & High Quality

Click here for larger plans

[Ren LaForme, Poynter]

Reviews are fake



100% Genuine Snake Oil

By: Scammer's Warehouse

★★★★★ 42 customer reviews

Price: $89.70 ✓Prime

★★★★★ AMAZING healing qualities

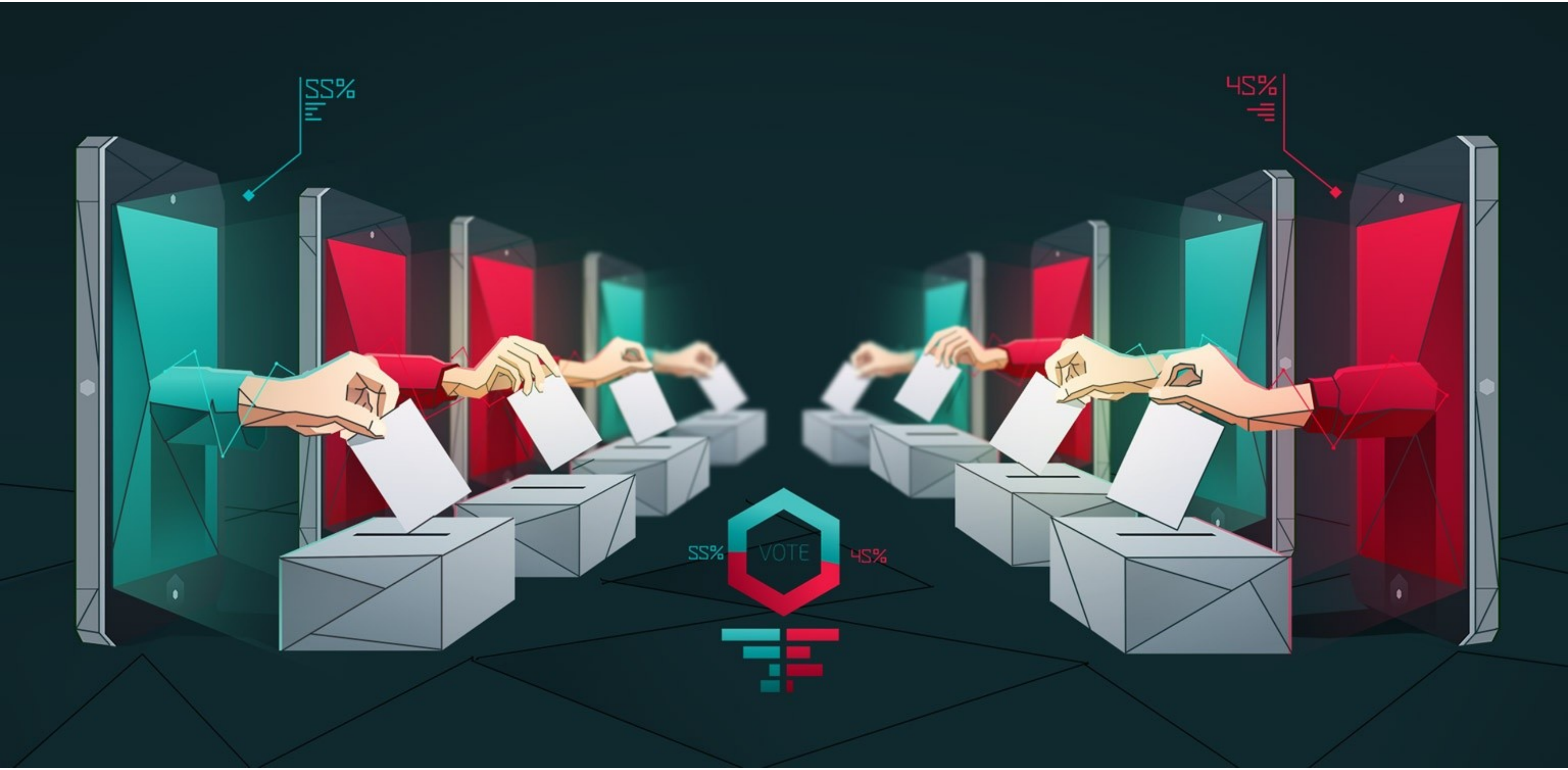
By: Fake Jim on June 19, 2017

Item: Snake oil, 4 oz.

Very good product. I can't prove this for certain, but I think it cured my cancer. I feel like I'm 17 again.

[Mat Venn, Medium]

Votes are fake



[IBM/The Atlantic]

As a result…

Online communities *can't self-govern*…

…any way that tries to treat people *equally*

As a result…

Communities can’t self-govern content or “truth”

[Krista Kennell, The Atlantic]

As a result…

Instead, companies, governments, unaccountable oversight boards must “govern” online behavior

Democracy, “one person one vote”, isn’t an option

Online society: missing a foundation?

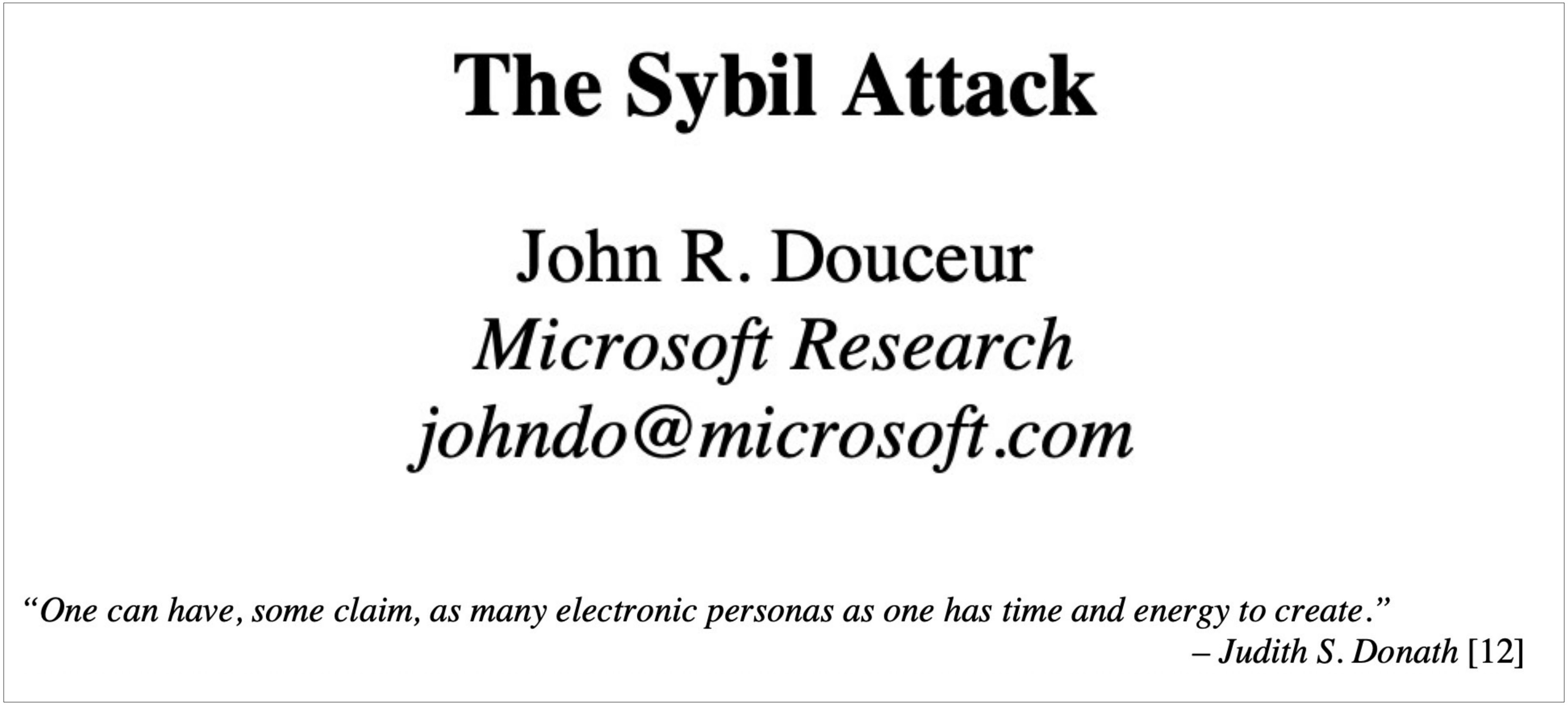
[All About Healthy Choices]

Proof of Personhood: talk outline

- Problem: why tech ~~doesn't~~ *can't* serve people
- **History: whence came "proof of personhood"**
- Goals: inclusion, equity, security, privacy
- Uses: what might we do with PoP tokens?
- Challenges: why it's (really, really) hard

Proof of Personhood: Literature

- Douceur, “**The Sybil Attack**” [2002]
  - Explored the difficulty & generality of the problem



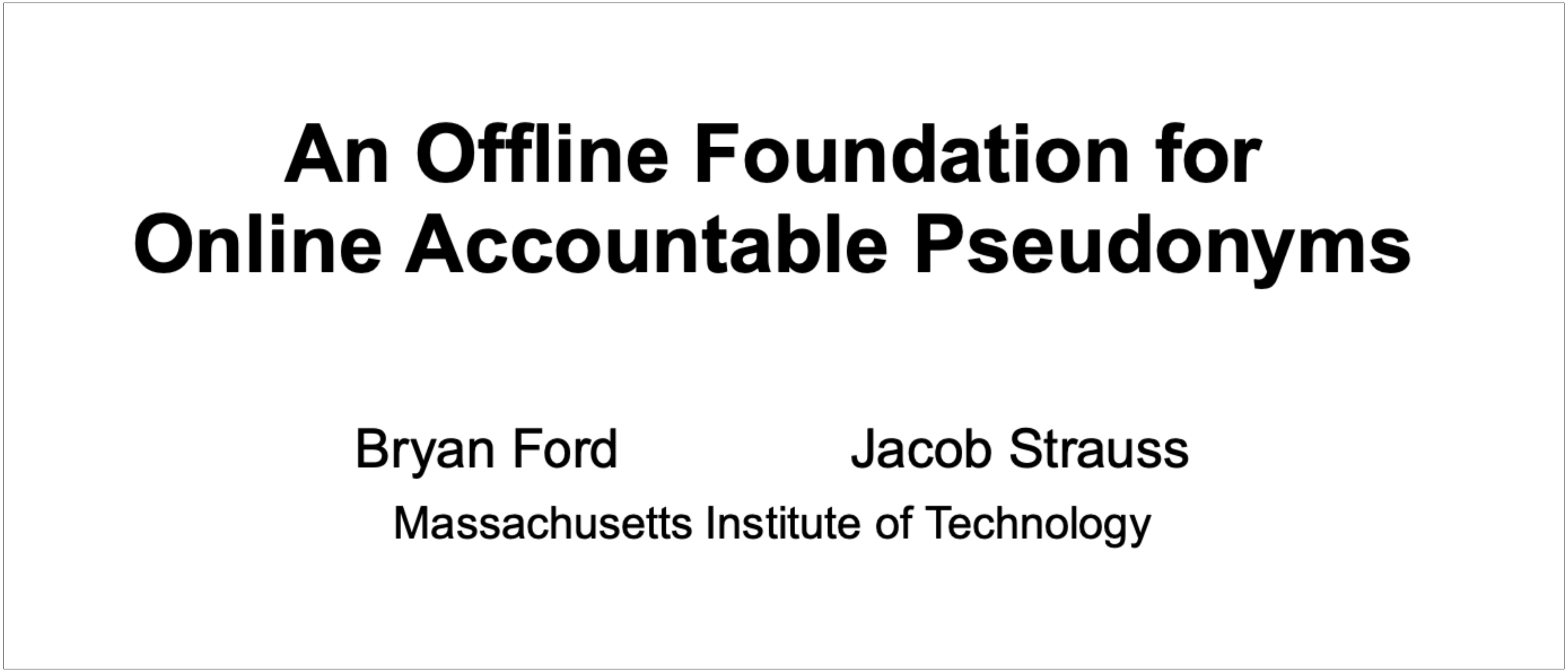
The Sybil Attack

John R. Douceur
Microsoft Research
johndo@microsoft.com

“One can have, some claim, as many electronic personas as one has time and energy to create.”
– Judith S. Donath [12]

Proof of Personhood: Literature

- 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 Jacob Strauss

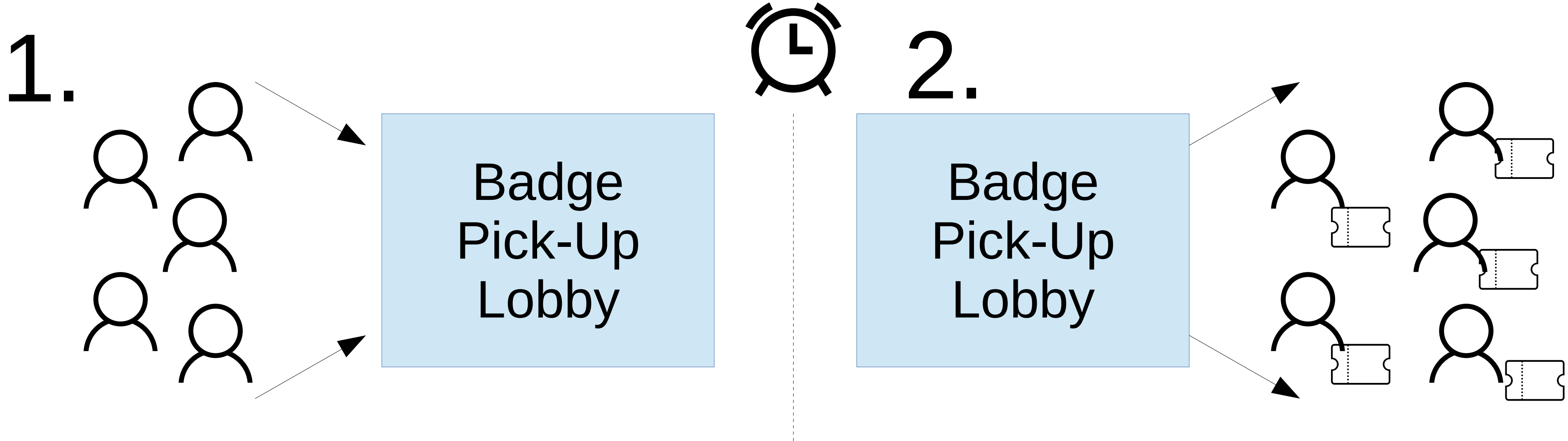
Massachusetts Institute of Technology

Pseudonym Parties: Basic Idea

To get a token, attendees must arrive and enter a closed or cordoned-off *lobby* by a set deadline

At deadline, entrance doors closed: *no re-entry*

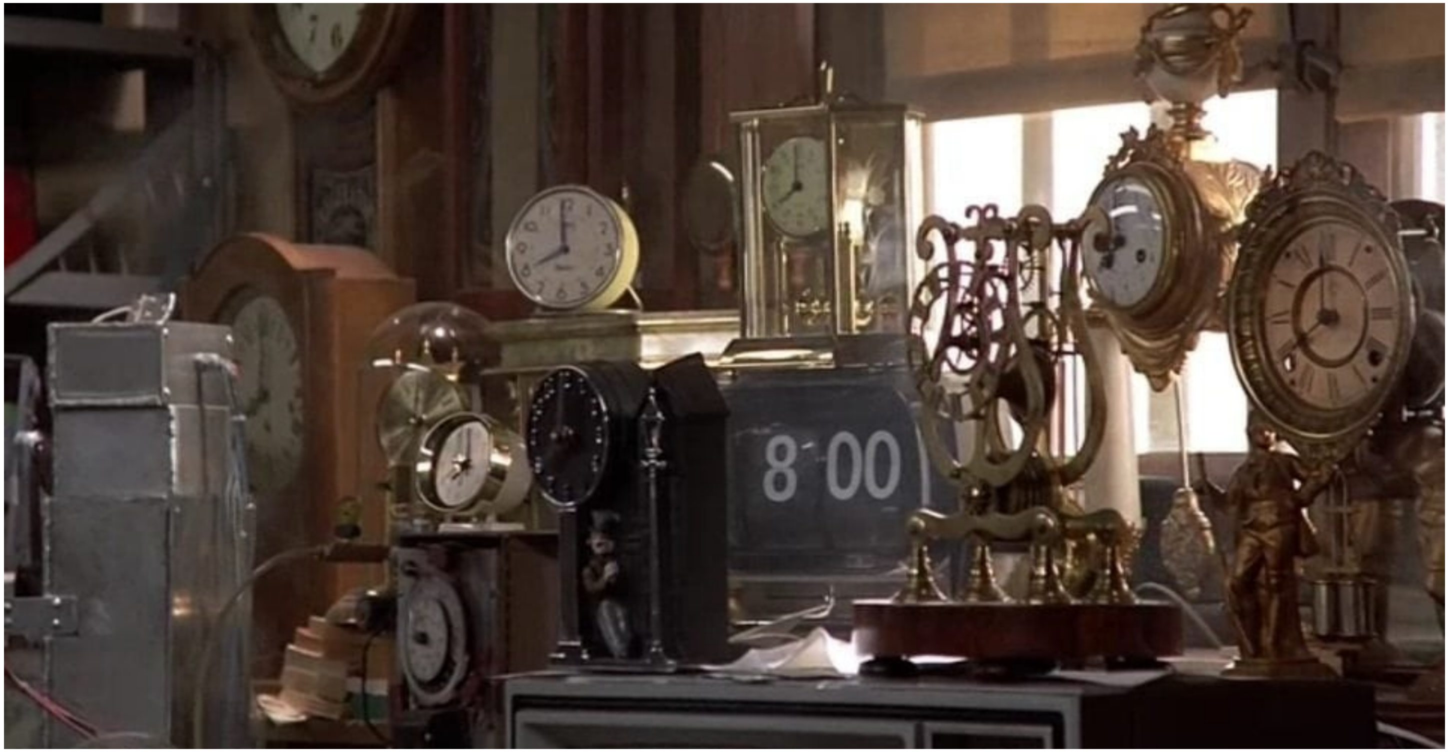
- Attendees file out from lobby to “main event”
- Get *one* QR code each scanned at lobby exit



Pseudonym Parties: Scaling

Federation of PoP groups might hold *concurrent* events with *simultaneous* arrival deadlines

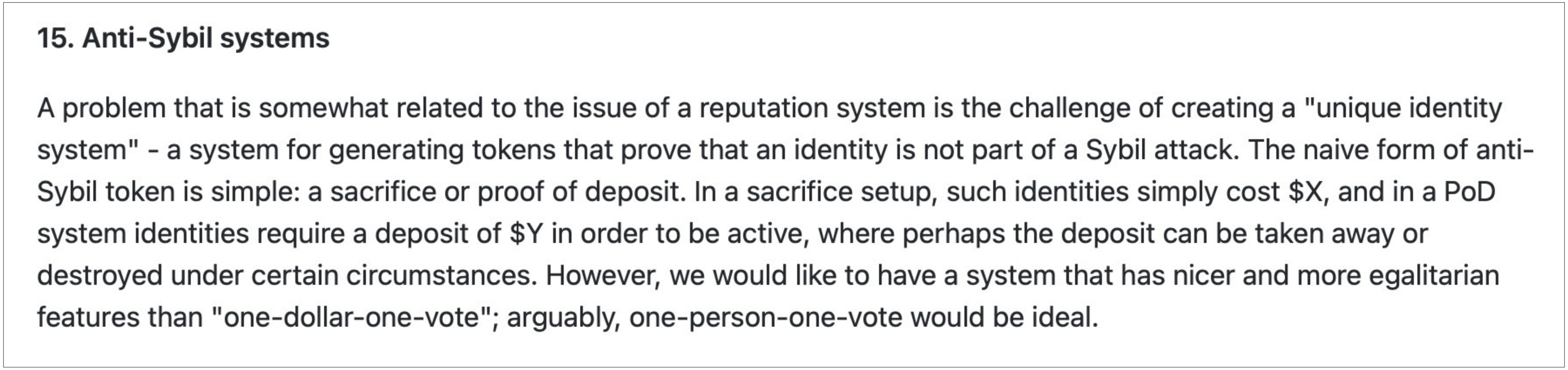
- No one can physically attend two at once



Proof of Personhood: Literature

Buterin, “**Problems**” [2014]

- proposed a “unique identity system” ideally satisfying a one-person-one-vote property



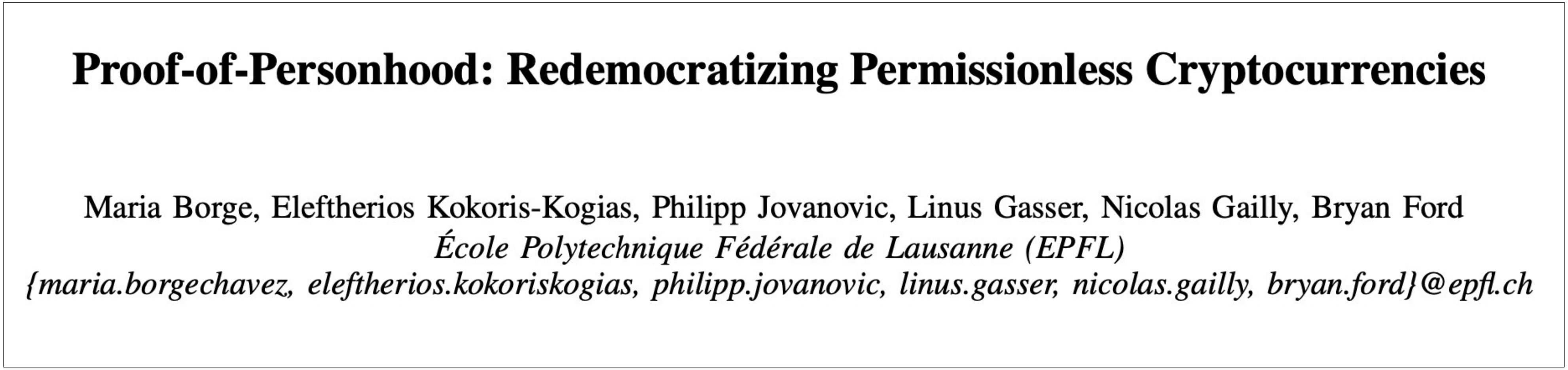
15. Anti-Sybil systems

A problem that is somewhat related to the issue of a reputation system is the challenge of creating a "unique identity system" - a system for generating tokens that prove that an identity is not part of a Sybil attack. The naive form of anti-Sybil token is simple: a sacrifice or proof of deposit. In a sacrifice setup, such identities simply cost $X, and in a PoD system identities require a deposit of $Y in order to be active, where perhaps the deposit can be taken away or destroyed under certain circumstances. However, we would like to have a system that has nicer and more egalitarian features than "one-dollar-one-vote"; arguably, one-person-one-vote would be ideal.

Proof of Personhood: Literature

Borge et al, “**Proof-of-Personhood: Redemocratizing Permissionless Cryptocurrencies**” [2017]

- Introduced the term & cryptocurrency use-case



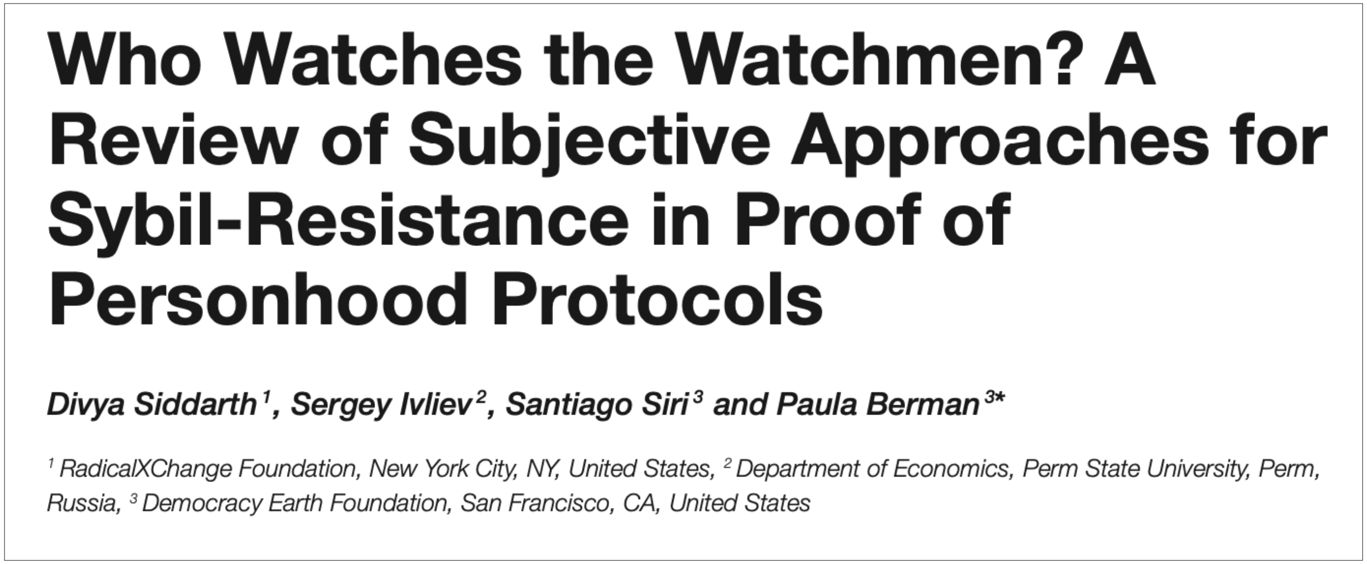
Proof-of-Personhood: Redemocratizing Permissionless Cryptocurrencies

Maria Borge, Eleftherios Kokoris-Kogias, Philipp Jovanovic, Linus Gasser, Nicolas Gailly, Bryan Ford
École Polytechnique Fédérale de Lausanne (EPFL)
{maria.borgechavez, eleftherios.kokoriskogias, philipp.jovanovic, linus.gasser, nicolas.gailly, bryan.ford}@epfl.ch

Proof of Personhood: Literature

Siddarth et al, “**Who Watches the Watchmen?**” [2020]

- First broad survey of many emerging approaches



Who Watches the Watchmen? A Review of Subjective Approaches for Sybil-Resistance in Proof of Personhood Protocols

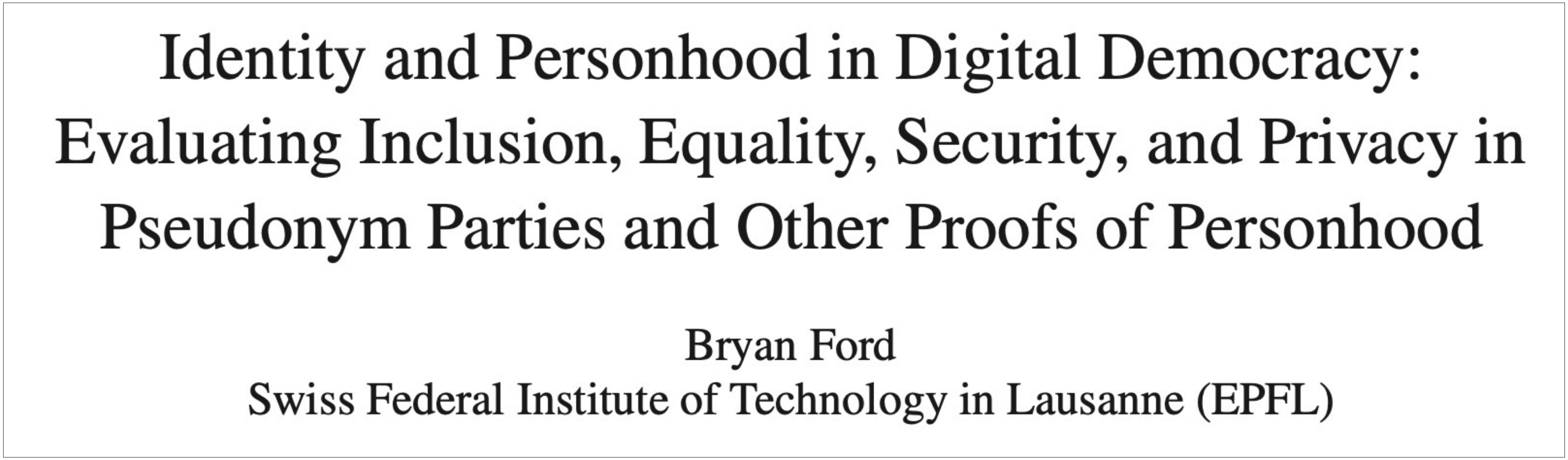
Divya Siddarth[1], Sergey Ivliev[2], Santiago Siri[3] and Paula Berman[3]*

[1] RadicalXChange Foundation, New York City, NY, United States, [2] Department of Economics, Perm State University, Perm, Russia, [3] Democracy Earth Foundation, San Francisco, CA, United States

Proof of Personhood: Literature

Ford, “**Identity and Personhood in Digital Democracy**” [2020]

- Comparative analysis of different approaches



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)

Some Known Approaches

- **Documented Identity**
  - Government-assigned ID attributes, CanDID
- **Biometric Identity**
  - India’s Aadhaar, UNHCR WFP, UniqueID
- **Physical Presence:** in-person participation
  - Election ink, Pseudonym parties, Encointer
- **Online Presence:** remote participation
  - Idena, Pseudonym pairs
- **Trust Networks:** PGP “Web of Trust” model
  - HumanityDAO, Upala, Circles UBI, GPIs

Proof of Personhood: talk outline

- Problem: why tech ~~doesn't~~ *can't* serve people
- History: whence came "proof of personhood"
- **Goals: inclusion, equity, security, privacy**
- Uses: what might we do with PoP tokens?
- Challenges: why it's (really, really) hard

Proof of Personhood: Goals

How should we “measure success” in an approach to proof of personhood?

I propose four main judgment criteria:

- **Inclusion:** can all *real people* participate?
- **Equality:** do they get equal power, rewards?
- **Security:** can it withstand powerful attacks?
- **Privacy:** what must people disclose or prove?

10 millimetres (mm) millimètres = 1 centimetre (cm) centimètre (cm)
100 centimetres (cm) centimètres = 1 metre (m) mètre
1000 metres (m) mètres = 1 kilometre (km) kilomètre

Inclusion

Ideal: enable every *real, live* person to participate

Reality: there are always barriers – what are they?

- Must **have**: passport, birth certificate, etc.? smartphone? money? time? mobility? friends?
- Must **prove**: citizenship? biometric sample? presence at an event? social trust/reputation?

All *can* exclude… How often? How to handle?

Equality

Ideal: every person gets *exactly* the same rights

- One vote per person, one quota of rewards, ...

Can a clever, determined, or rich abuser (still) get several active “personhood tokens” at once?

- Accumulation: get one nym “trusted”, repeat…
- Identity proxies: phone numbers, credit cards…
- Coercion: can the rich “buy” the participation, rewards, voting rights of poorer participants?

Security

Can a clever, determined, or rich abuser steal tokens, or synthesize a large number of fakes?

- e.g., by exploiting single points of compromise?
  - Biometrics (e.g., Aadhaar): one compromised registration authority could register many fakes
- e.g., by using powerful AI-driven deep fakery?
  - Synthesize “evidence”: talking heads, showing “ID cards”, video “chatting”, whole crowds at “event”…

Long-term security will need to rely on *transparency* plus *overwhelmingly redundant evidence.*

Privacy

What does a person need to *show* or *prove* to obtain (full) participation? How sensitive is it?

- Documents: name, age, gender, citizenship?
- Social media profiles? Friends, followers?

Can *using* personhood tokens violate privacy?

- Would like to “present” a token to many sites without leaking *any* cross-site trackable ID

Proof of Personhood: talk outline

- Problem: why tech ~~doesn't~~ *can't* serve people
- History: whence came "proof of personhood"
- Goals: inclusion, equity, security, privacy
- **Uses: what might we do with PoP tokens?**
- Challenges: why it's (really, really) hard

A Few Applications of Personhood

A far-from-exhaustive list:

- Replace CAPTCHAs for abuse rate-limiting
- Automatic website login with 1-per-person nym
- Social media: 1-per-person like/follow counts
- Cryptocurrencies with universal basic income
- Democratic online governance structures

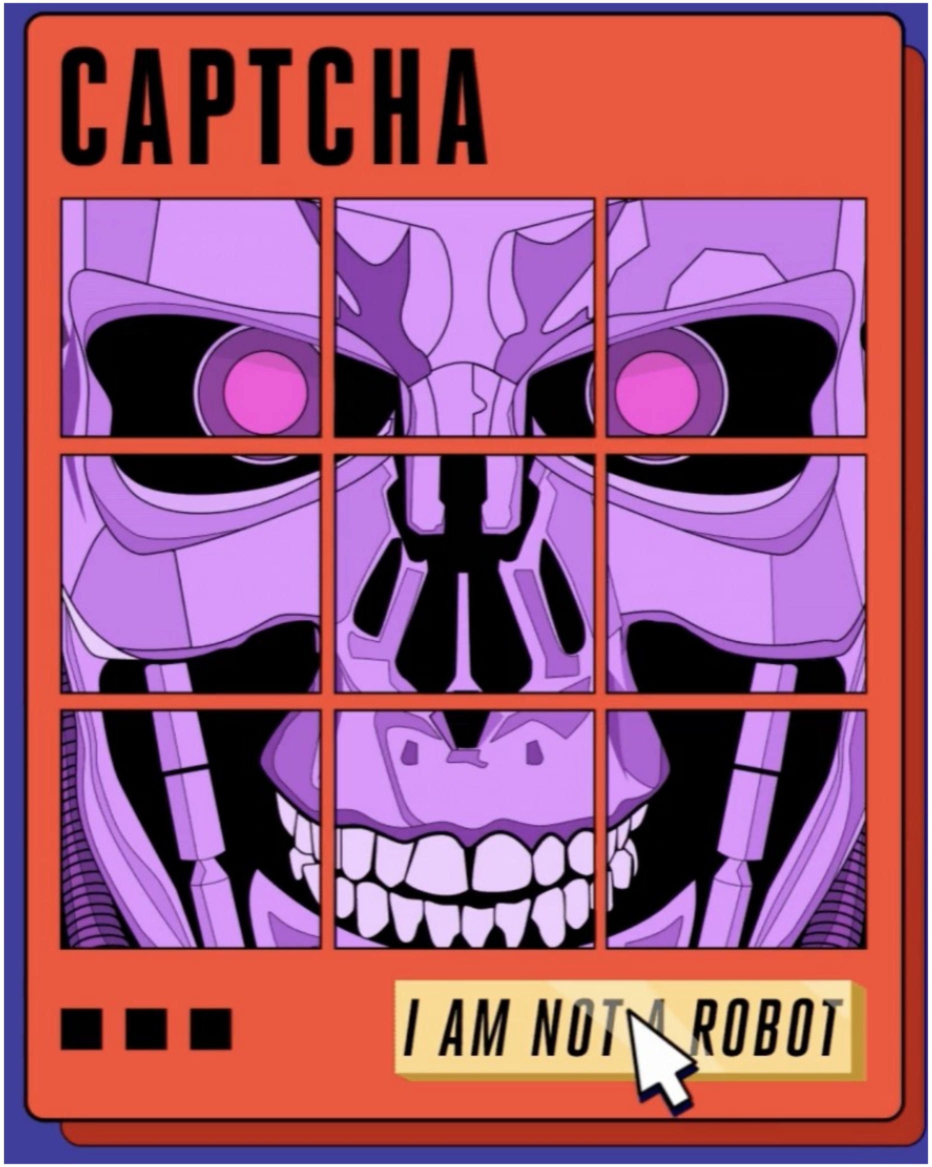
CAPTCHAs

Get harder and harder, because…AI

- Humans will eventually lose (often do already)

Personhood tokens *could* perhaps be both:

- More abuse-limiting
- More inclusive



[The Verge]

Pseudonymous Single Sign-On

Participating websites could allow “one-click registration + login” with 1-per-person pseudonym

- Next time you visit website, get same account
- No need to disclose any identity information
- If you abuse, website can block your account

Sign In As Pseudonym

Crowdsourcing w/o Sock Puppets

Websites like Wikipedia could become (again) editable “by default” without sock puppet abuse

News…With Comments, Again

News websites could bring back their reader comments sections, without becoming toxic

Crypto Universal Basic Income

Enable everyone to “print money” at an equal rate

Online voting, self-governance

[Kenneth Hacker, The Progressive Post]

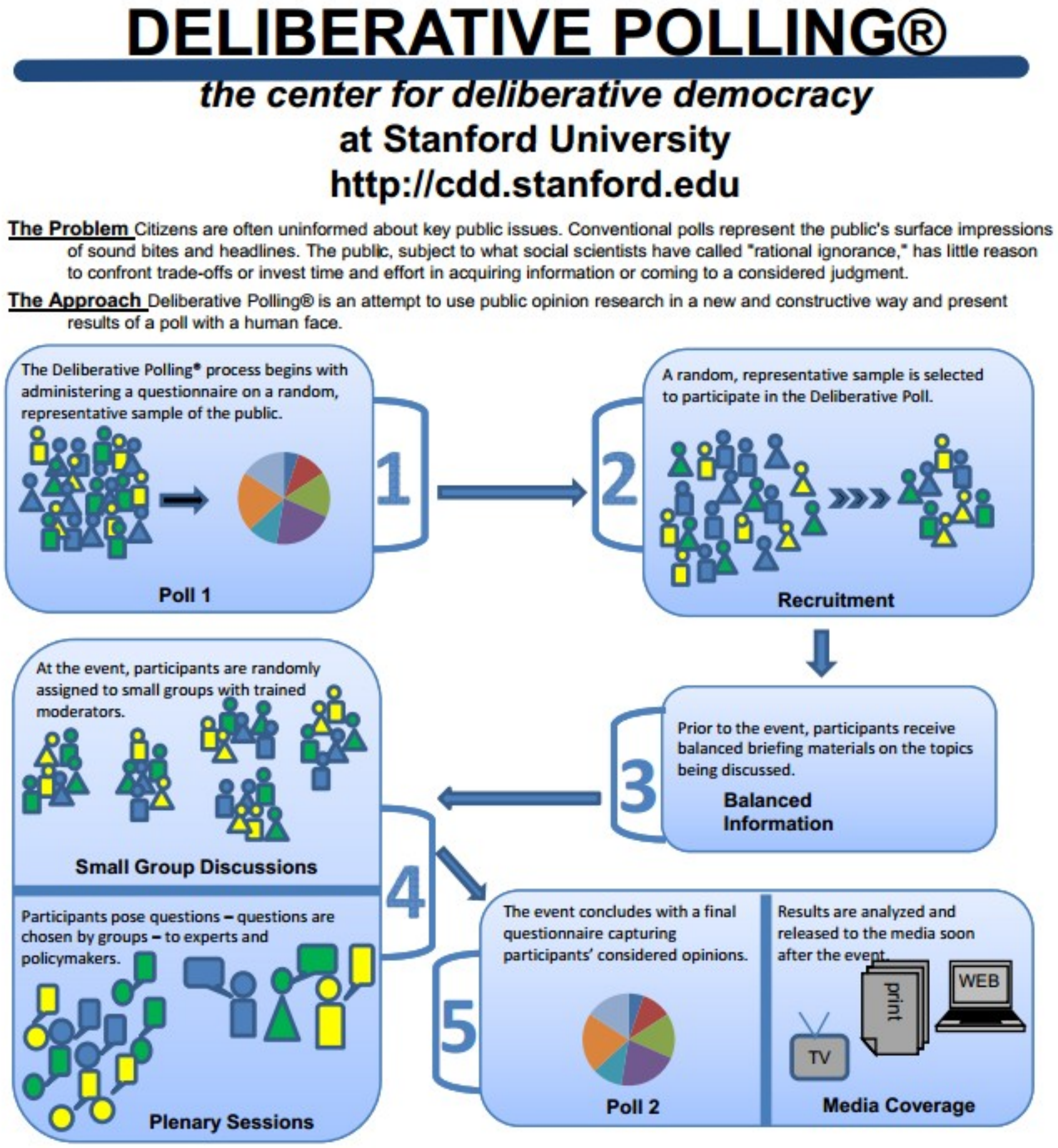
Rich participatory structures

Direct + Representative = Delegative Democracy

[Ehud Shapiro, Open Transcripts]

Sortition-based Polling, Deliberation

Statistically random samples of *real people*



DELIBERATIVE POLLING®

the center for deliberative democracy
at Stanford University
http://cdd.stanford.edu

The Problem Citizens are often uninformed about key public issues. Conventional polls represent the public's surface impressions of sound bites and headlines. The public, subject to what social scientists have called "rational ignorance," has little reason to confront trade-offs or invest time and effort in acquiring information or coming to a considered judgment.

The Approach Deliberative Polling® is an attempt to use public opinion research in a new and constructive way and present results of a poll with a human face.

1 Poll 1: The Deliberative Polling® process begins with administering a questionnaire on a random, representative sample of the public.

2 Recruitment: A random, representative sample is selected to participate in the Deliberative Poll.

3 Balanced Information: Prior to the event, participants receive balanced briefing materials on the topics being discussed.

4 Small Group Discussions: At the event, participants are randomly assigned to small groups with trained moderators.

Plenary Sessions: Participants pose questions – questions are chosen by groups – to experts and policymakers.

5 Poll 2: The event concludes with a final questionnaire capturing participants' considered opinions.

Media Coverage: Results are analyzed and released to the media soon after the event.

Proof of Personhood: talk outline

- Problem: why tech ~~doesn't~~ *can't* serve people
- History: whence came "proof of personhood"
- Goals: inclusion, equity, security, privacy
- Uses: what might we do with PoP tokens?
- **Challenges: why it's (really, really) hard**

A Few Key Challenges

- Inclusion: required time, mobility, abilities
- Equality: are identity proxies 1 per person?
- Security: compromised devices (esp biometric)
- Security: how to prove *absence* of alter egos?
- Security: resisting deep fakery
- Security: handling coerced/bought participation
- Privacy: what must people reveal, or prove?
- Privacy: reusable but non-trackable tokens

Alter Egos

Can you ask Clark Kent to prove that he's *not* also Superman? By what evidence? Should you?

Personas or Alter Egos are Normal

[The Face]

Work, Home, Hobby, Secret Identities

[Fast Company]

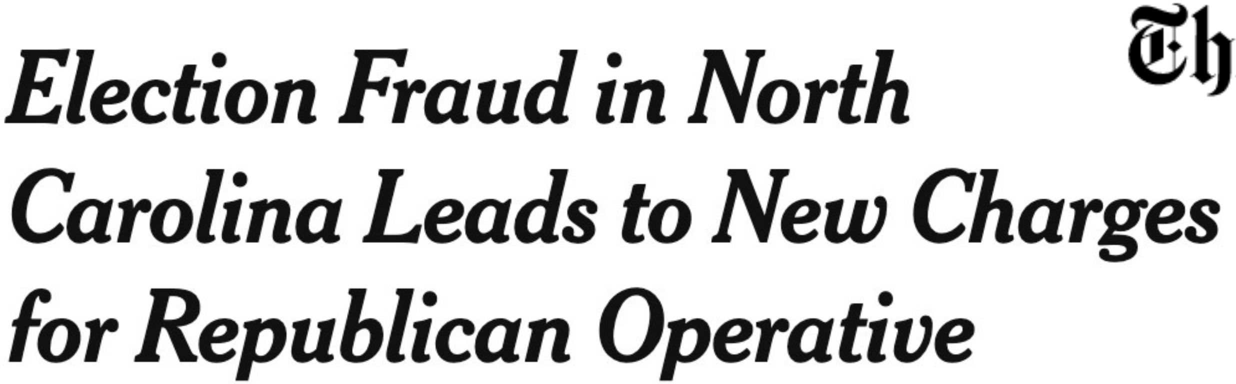
The Coercion, Vote-Buying Problem

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!

The New York Times



Election Fraud in North Carolina Leads to New Charges for Republican Operative

July 30, 2019

Conclusion

Proof of personhood promises to fill in a missing foundation enabling technology to serve *people*

- Be able to allocate or count “one per person”
- Meaningful voting, reputation, self-governance

Exciting to see an explosion of different approaches and pragmatic experiments

- They need inclusion, equality, security, privacy
- Many open questions & challenges remain