Digital Personhood: Towards Technology that Securely Serves People

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

VISP Distinguished Lecture – October 13, 2021

Talk Outline

- Is the Internet “democratizing”? Can it be?
- Self-governance foundations: money vs people
- Identity: a siren song of digital surveillance
- Digital personhood: equality with privacy online
- Applications: governance, social media, crypto
- Conclusion: towards digital self-governance

We’re facing **hard global** problems

Climate change

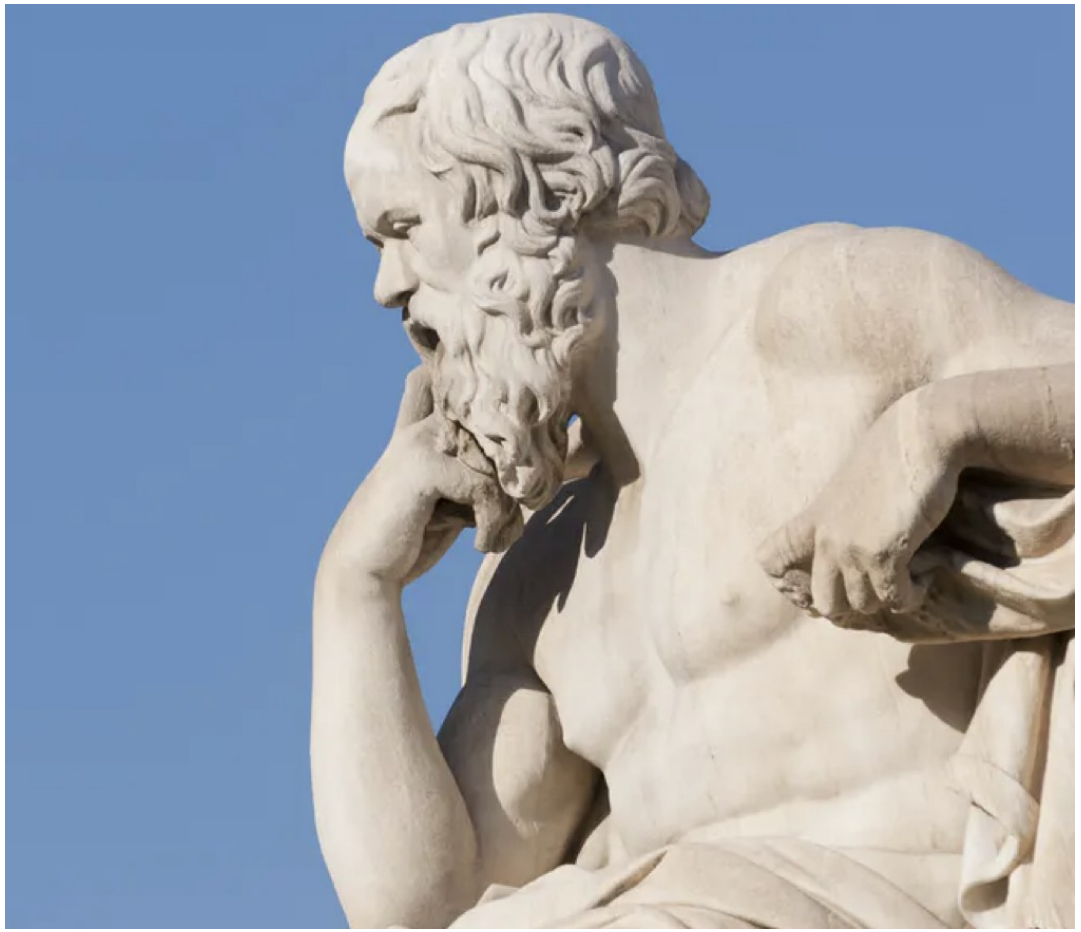
COVID-19 pandemic

Exploding inequality

Global problems need global tools

Like the Internet … *right?*

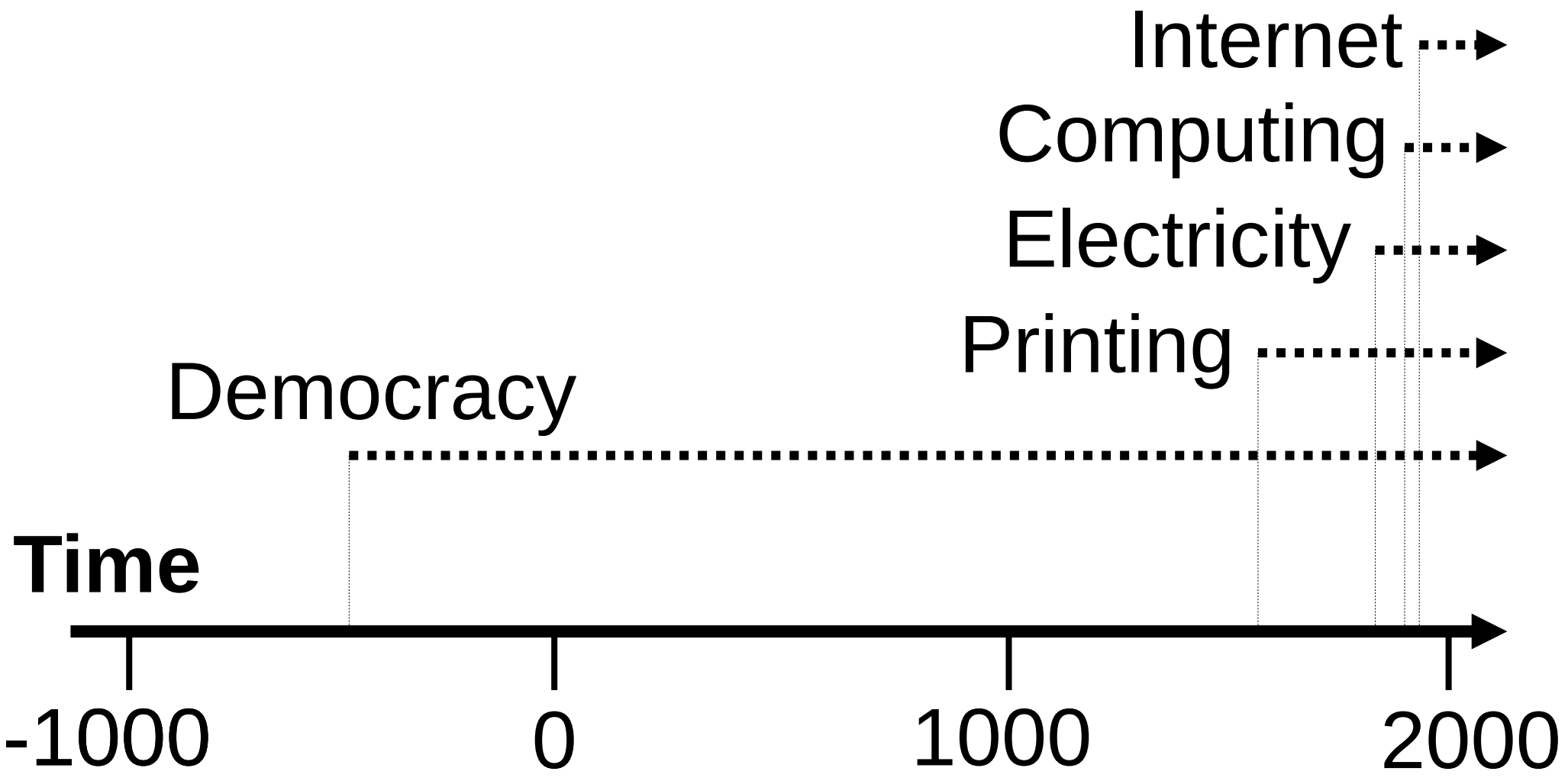
Is networked computing…



Helping us find *wise* solutions?

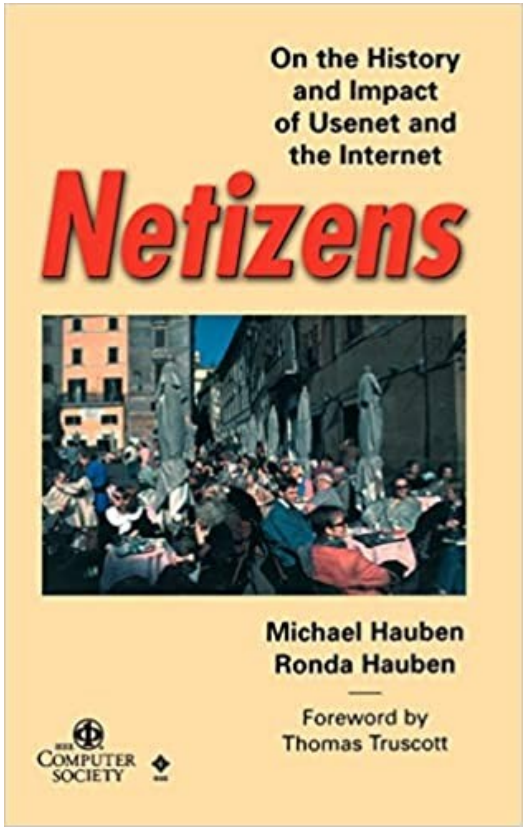
In *everyone's* collective interest?

A few transformative technologies



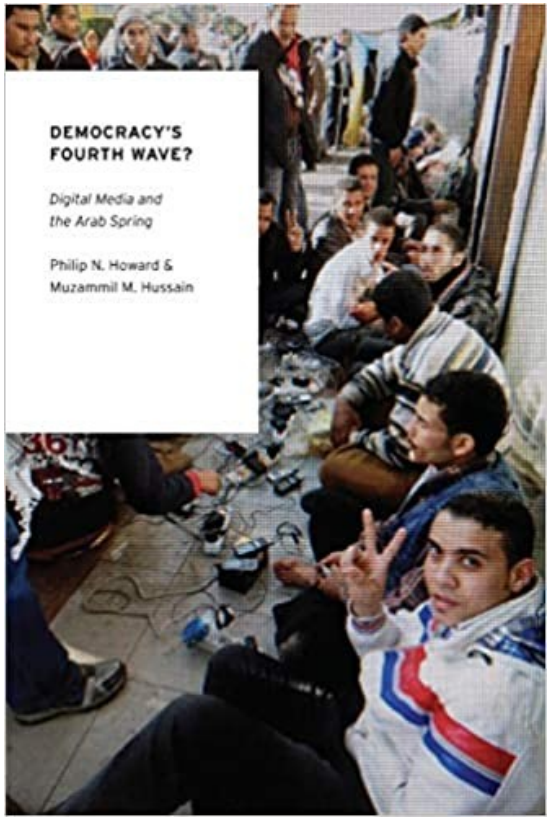
Is the Internet “Democratizing”?

1997



Chapter 18
“The Computer as a Democratizer”

2013



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

Is the Internet “Democratizing”?

2016

How Social Media Helps Dictators

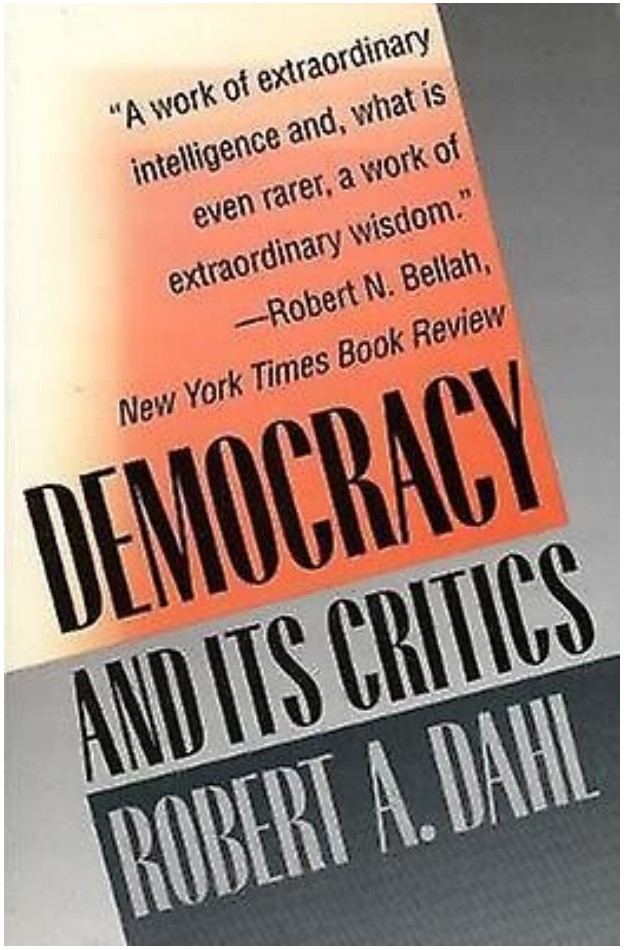
It's been hailed as "liberation technology." But it has a darker side.

By Erica Chenoweth

Why democracy…and what *is* it?

Council of Europe,
“Democracy”

Robert Dahl,
“Democracy & its critics”



Why democracy…and what *is* it?

Council of Europe,
"Democracy"

Key criteria:

- Individual autonomy
- Equality

Robert Dahl,
"Democracy & its critics"

Key criteria:

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

So is the Internet “Democratizing”?

So is the Internet “Democratizing”?

- Giving “everyone” a voice & a platform

- Equality?
- Enlightened understanding?
- Effective participation?

Can we **make** the Internet more "democratizing"?

Problems I wish more CS research focused on:

- **Equality:** giving all *equal* voice, rights, benefits
  - Not domination of loudest voice or fattest wallet
- **Inclusion:** ensure computing serves *all* people
  - Including those with old hardware, poor connectivity
- **Autonomy:** put people, communities in *control*
  - Not vendors, platforms, app stores, algorithms

Talk Outline

- Is the Internet “democratizing”? Can it be?
- **Self-governance foundations: money vs people**
- Identity: a siren song of digital surveillance
- Digital personhood: equality with privacy online
- Applications: governance, social media, crypto
- Conclusion: towards digital self-governance

Online Self-Governance

Can digital forums and communities self-govern?

Foundations of Self-Governance

Key question: what foundation do we build on?

[Tes]

Membership and Influence

Any collective organization process must define:

- **Membership:** whose input *counts* in the collective process, i.e., who gets any power?
- **Influence:** how *much* power does each member wield in self-governance processes?

Membership is a binary property, in or out

Influence is numeric, may be multidimensional

Contrasting Influence Foundations

Wealth-centric

- One dollar, one vote

[Kera]

Person-centric

- One person, one vote

[Verity Weekly]

Contrasting Influence Foundations

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

Membership and Influence

If an organization can’t decide – or secure – its membership and influence foundations → chaos

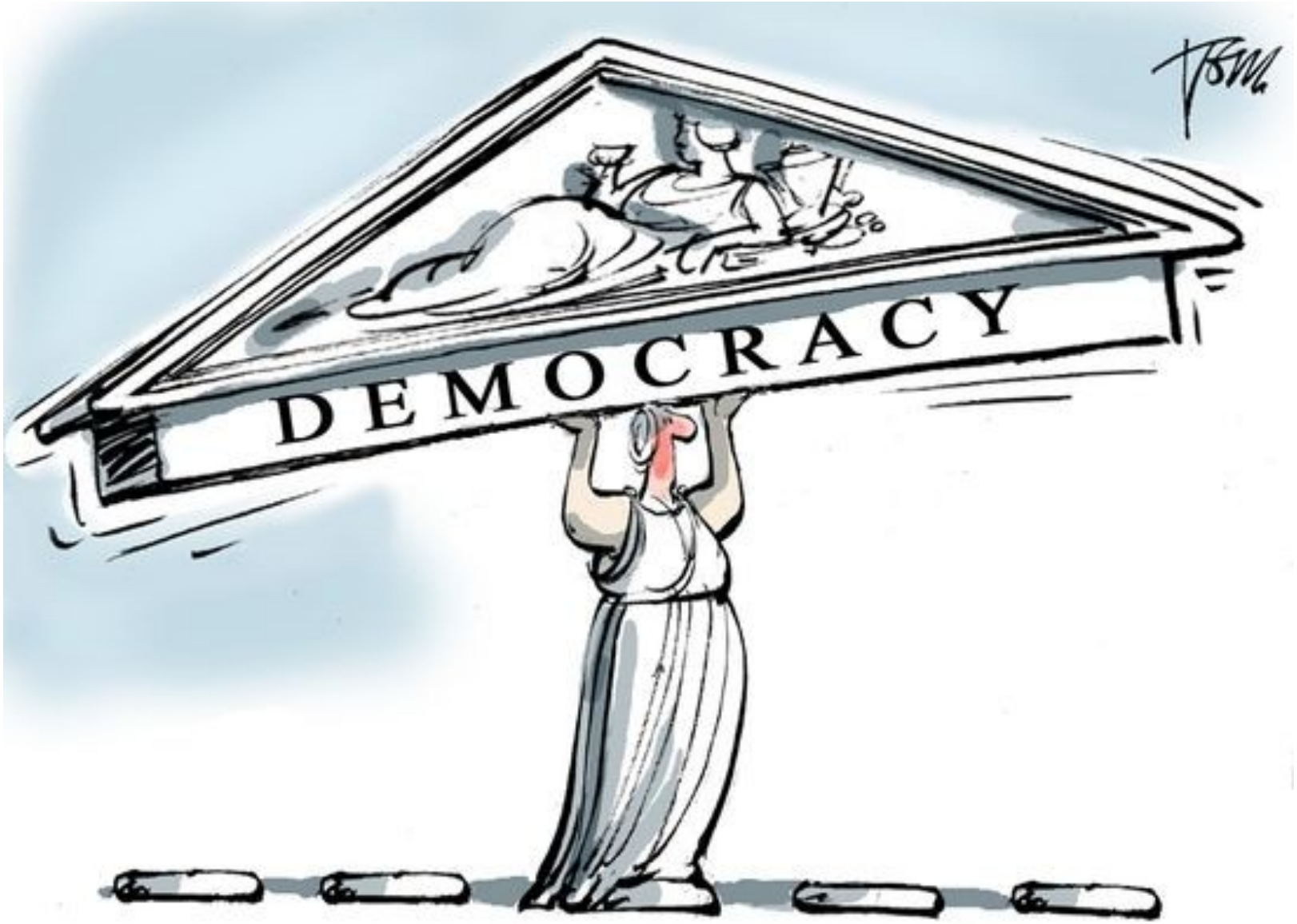
Digitalization of Self-Governance

As our lives and self-governance shifts online…

- **Wealth-centric:** many technology solutions
- **Person-centric:** solutions are more elusive

[Infinity Economics]

Democracy Needs a Foundation

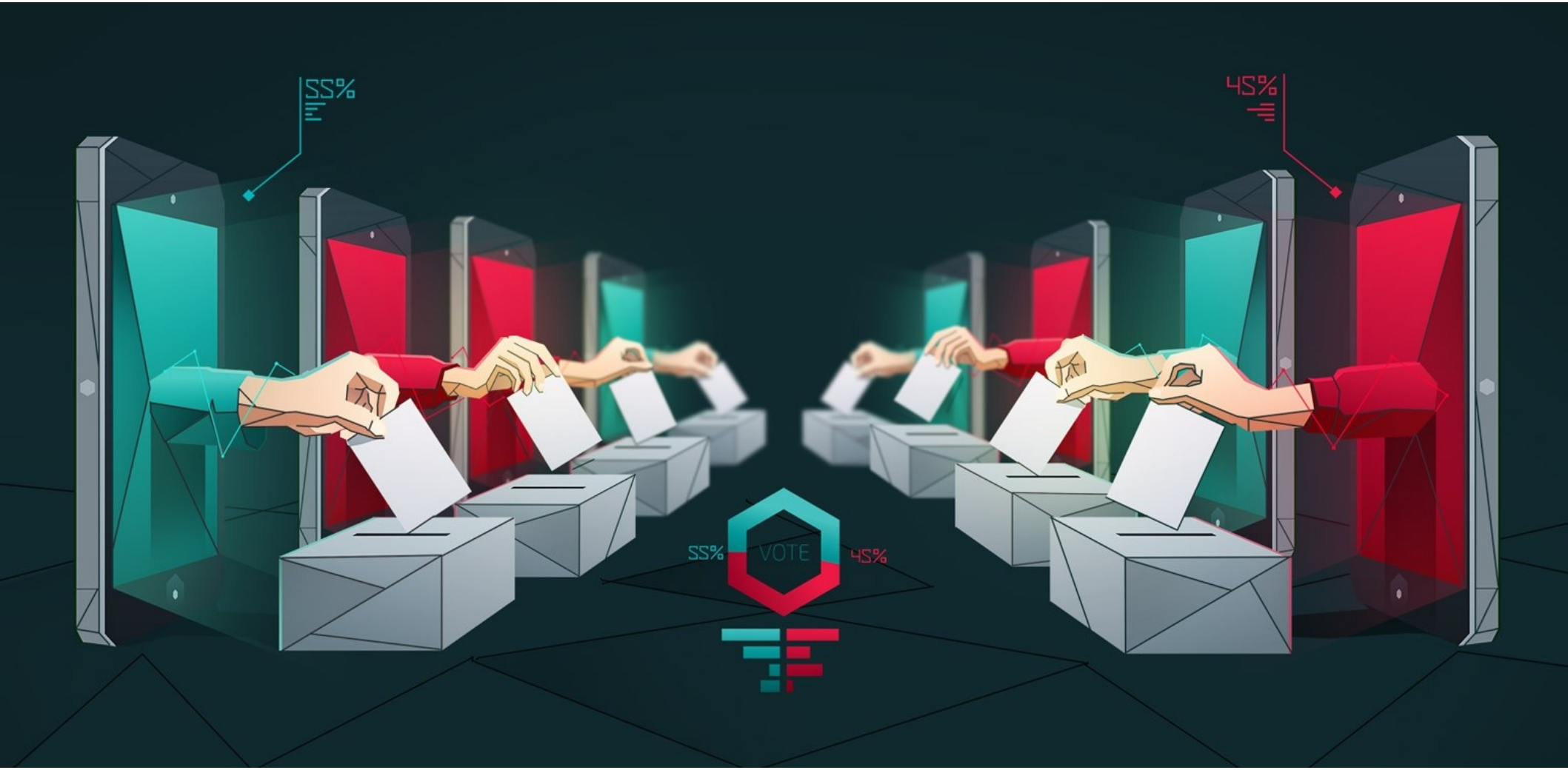


[Michalis Kountouris, Michael Cacoyannis Foundation]

Democracy’s Foundation is People

[Encyclopedia Britannica]

Digital Democracy has a Problem…



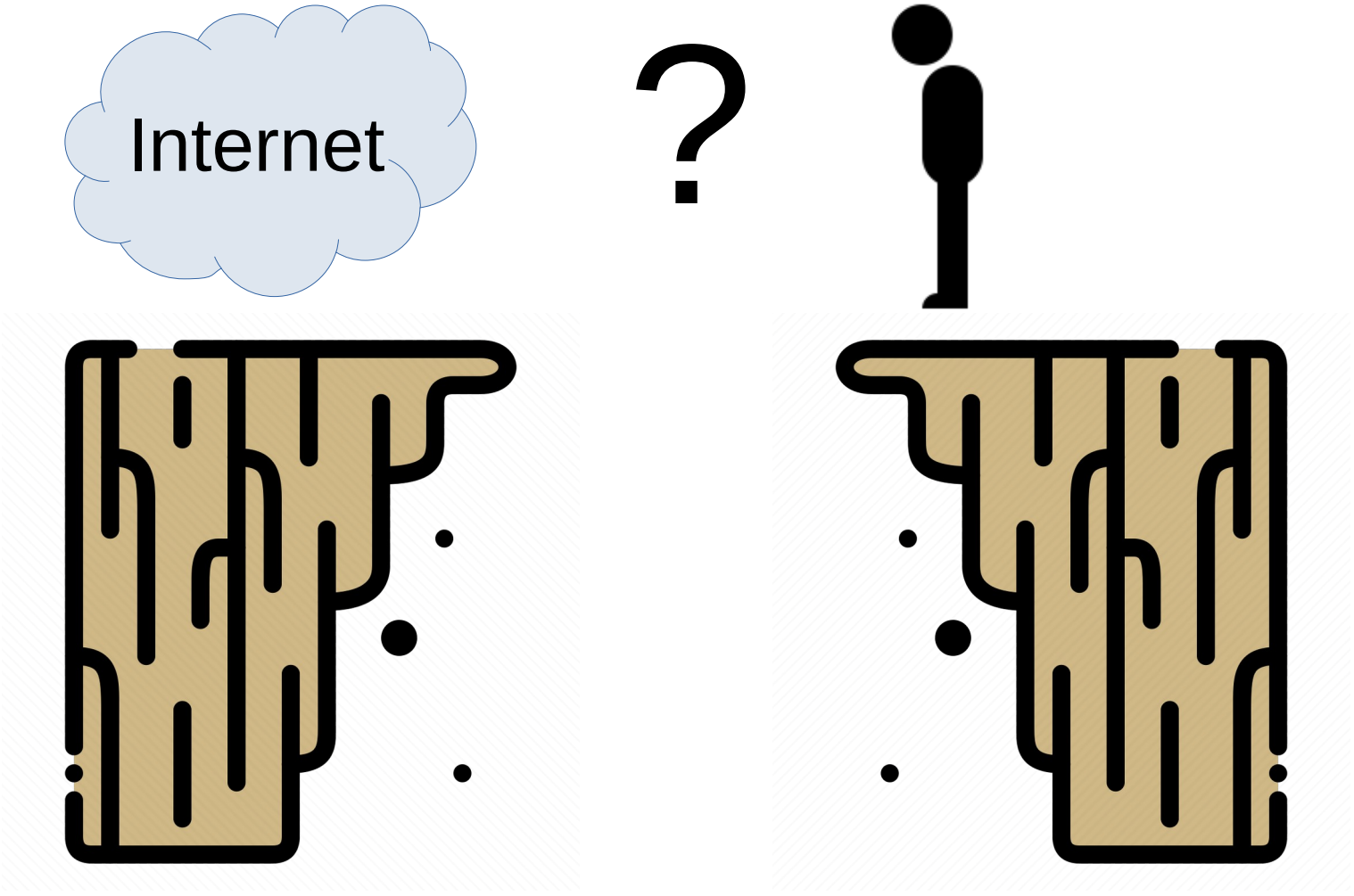
[IBM/The Atlantic]

People are Physical, not Digital

[Marcus Feldthus]

The Fundamental Problem

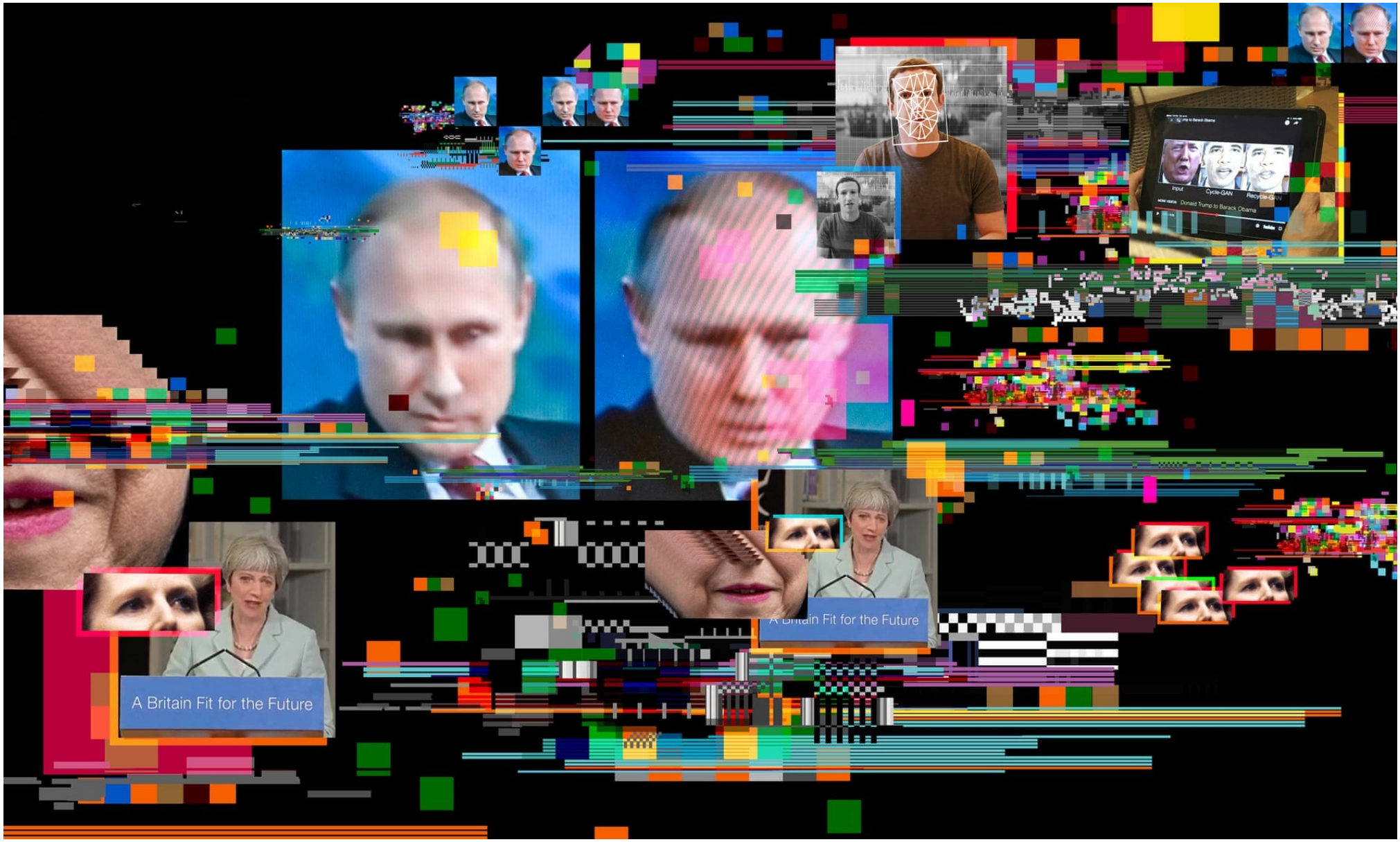
Today’s Internet doesn’t know what a “person” is



People aren’t digital, only profiles are

[Pixabay, The Moscow Times]

Online, the People are Fake



[Ian Sample, The Guardian]

Online, the People are Fake

Profiles are cheap, discardable, easily faked

Upside:
inclusion, privacy

Downside:
are “people” really *people*?

Online, the People are Fake

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

[imdb]

Their Followers are Fake

[Ren LaForme, Poynter]

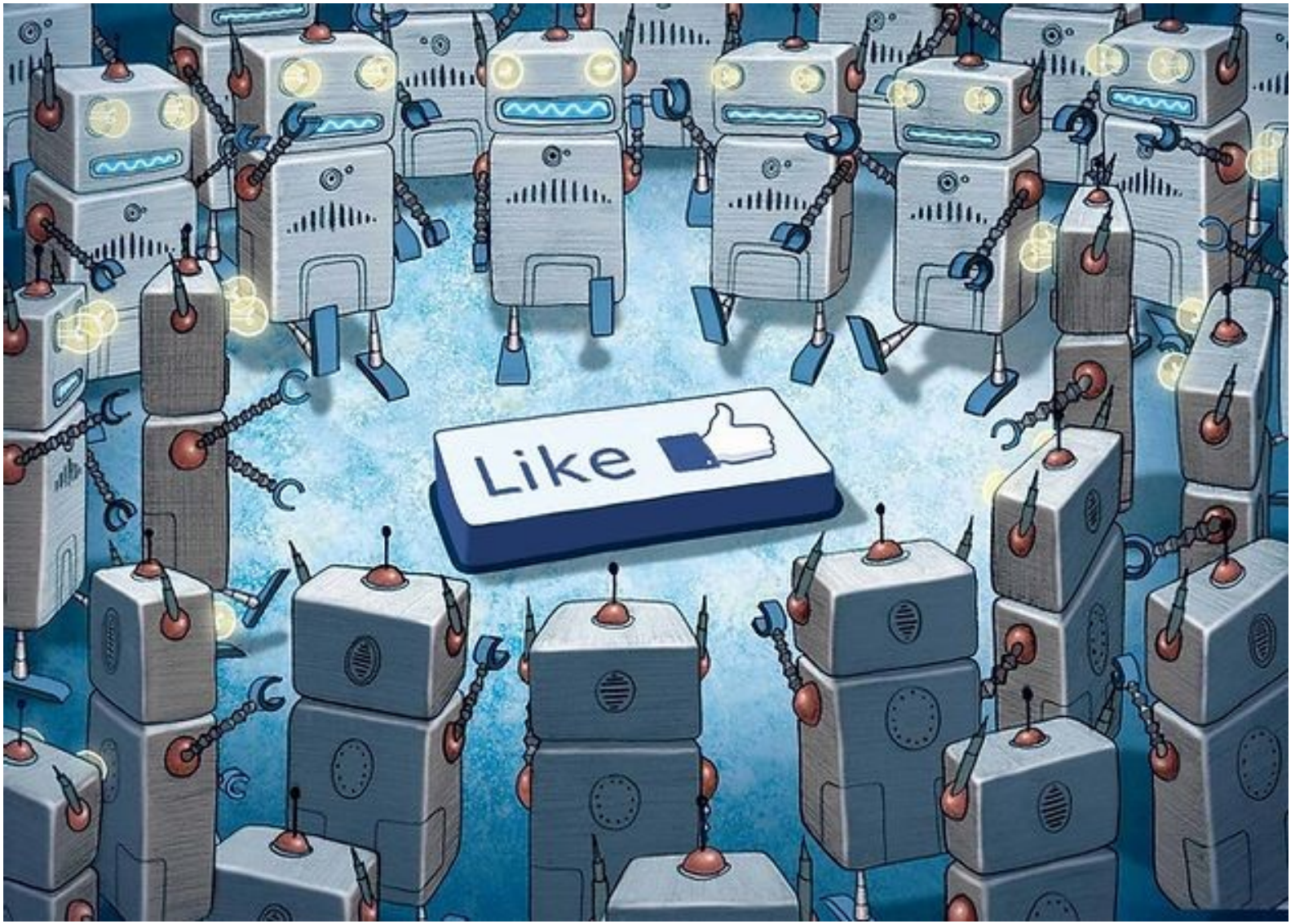
The News is Fake

[Krista Kennell, The Atlantic]

The Reviews are Fake

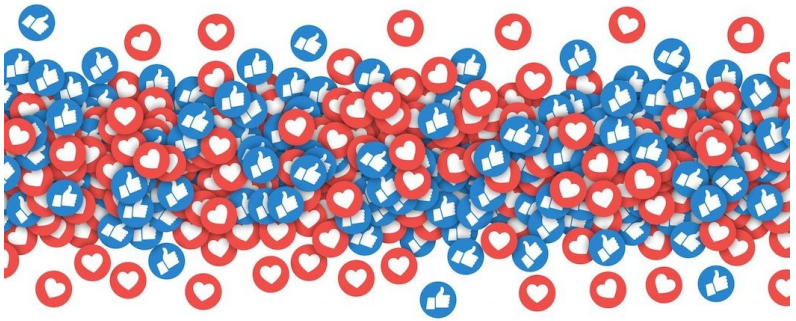
[Mat Venn, Medium]

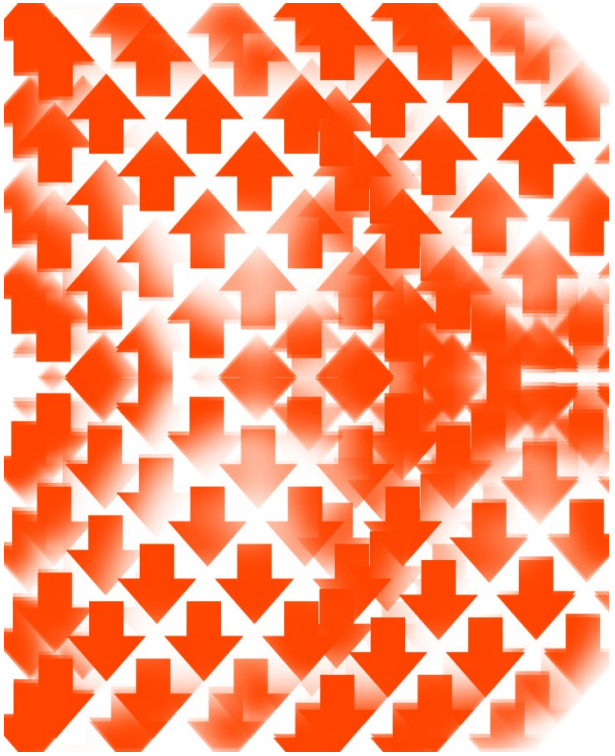
The Likes are Fake

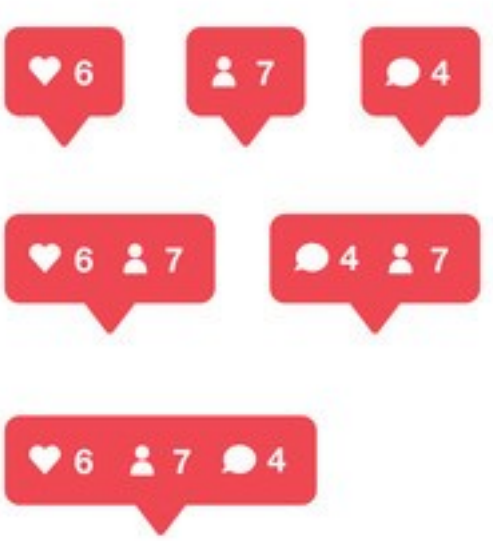


[Rabbit Consulting Group]

The Sybil Attack Problem







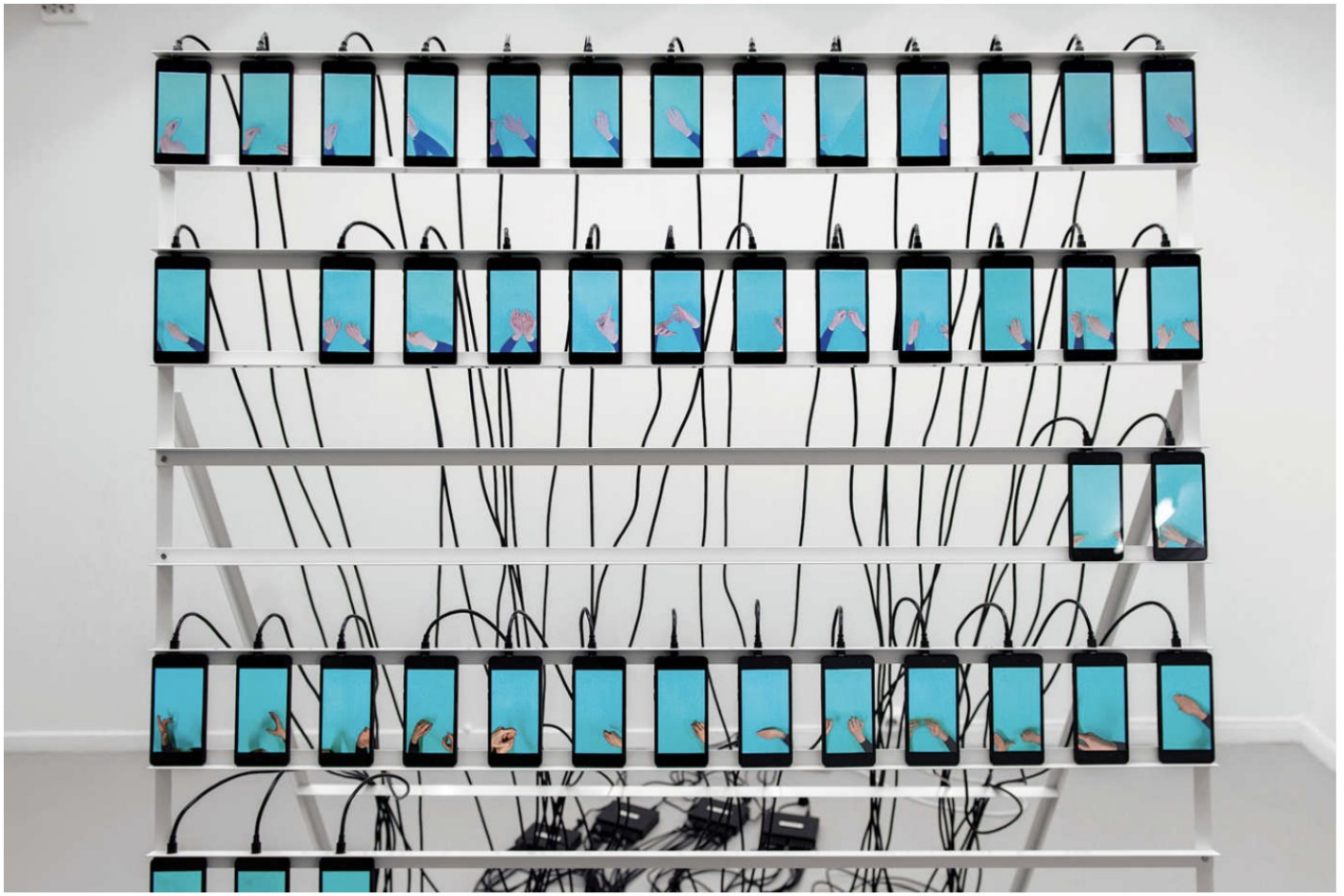
Likes,
Followers,
Upvotes,
Downvotes,
Reviews…

Are they by *real* or *fake* people?

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]

As a result…

Companies, governments, opaque algorithms, private oversight boards “govern” online behavior

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

What Is the Missing Foundation?

[All About Healthy Choices]

Requirements for Digital Democracy

Can we build digital organizations of *people*?

- **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

Talk Outline

- Is the Internet “democratizing”? Can it be?
- Self-governance foundations: money vs people
- **Identity: a siren song of digital surveillance**
- Digital personhood: equality with privacy online
- Applications: governance, social media, crypto
- Conclusion: towards digital self-governance

Identity – The Missing Foundation?

[UNCTAD]

Digital Identity is a Red Herring

red her•ring

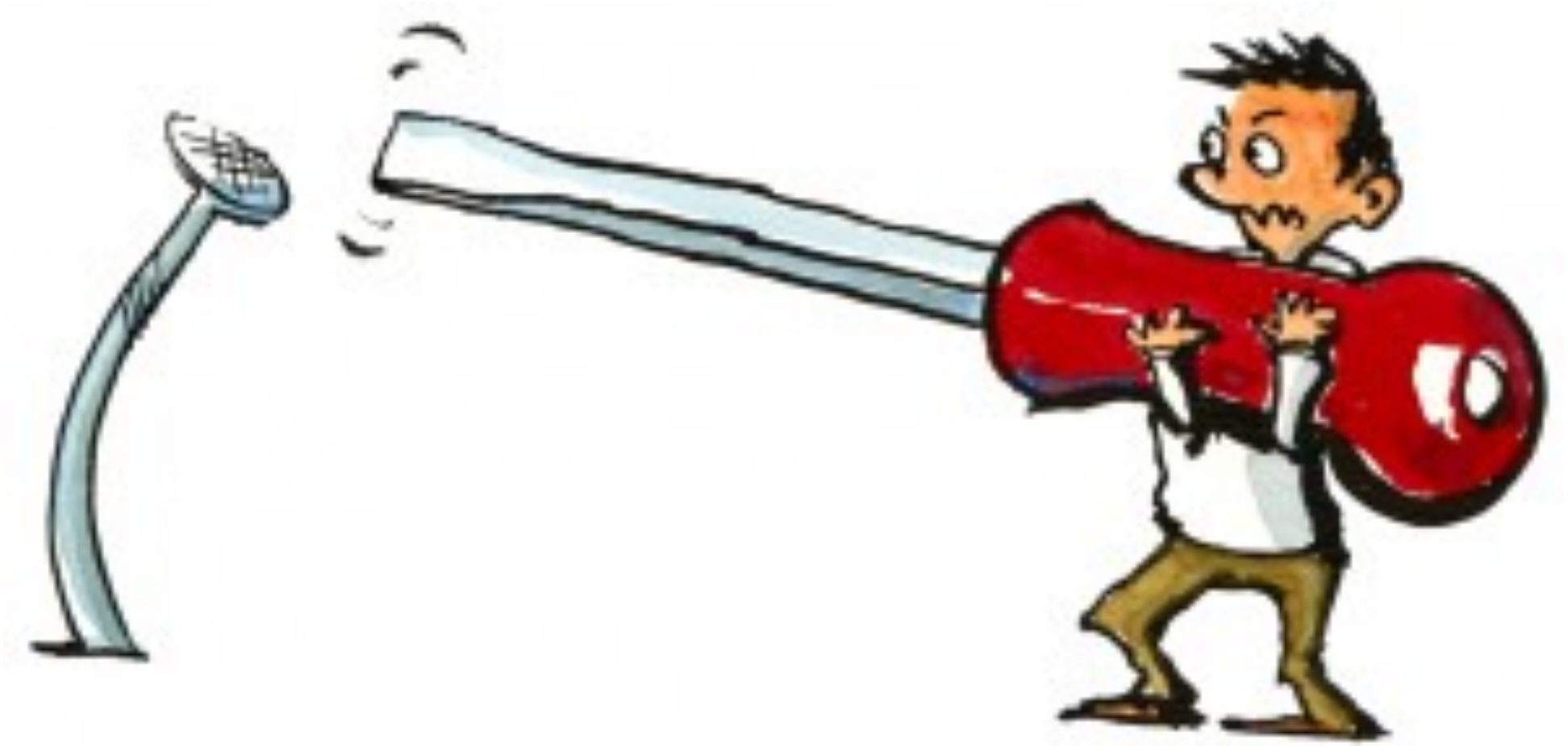
noun

1 a dried smoked herring, which is turned red by the smoke.

2 something, esp. a clue, that is or is intended to be misleading or distracting : *the book is fast-paced, exciting, and full of red herrings.* [ORIGIN: so named from the practice of using the scent of red herring in training hounds.]

[Darin Stevenson, Medium]

At Best It’s the Wrong Tool



[Frits Ahlefeldt]

At Worst It’s a Siren’s Song

[Herbert James Draper, Wikipedia]

Digital identities are just more profiles

[UK Government Digital Service]

Profiles are for *distinguishing* people

[Tom Perrett, Arkbound]

Democracy is about *equality* of people

[Tricentis]

Approaches to Digital Identity

- Social Media Identities
  - Expect tech platforms to detect fakes, abuses
- Proofs of Investment: economic entry costs
  - CAPTCHAs, proof of work, proof of stake
- Documented Identity: “Know Your Customer”
  - Government-issued ID, self-sovereign ID
- Biometric Identity
  - India’s Aadhaar, World Food Programme

Approaches to Digital Identity

- **Social Media Identities**
  - Expect tech platforms to detect fakes, abuses
- Proofs of Investment: economic entry costs
  - CAPTCHAs, proof of work, proof of stake
- Documented Identity: “Know Your Customer”
  - Government-issued ID, self-sovereign ID
- Biometric Identity
  - India’s Aadhaar, World Food Programme

Social Media and Fake Detection

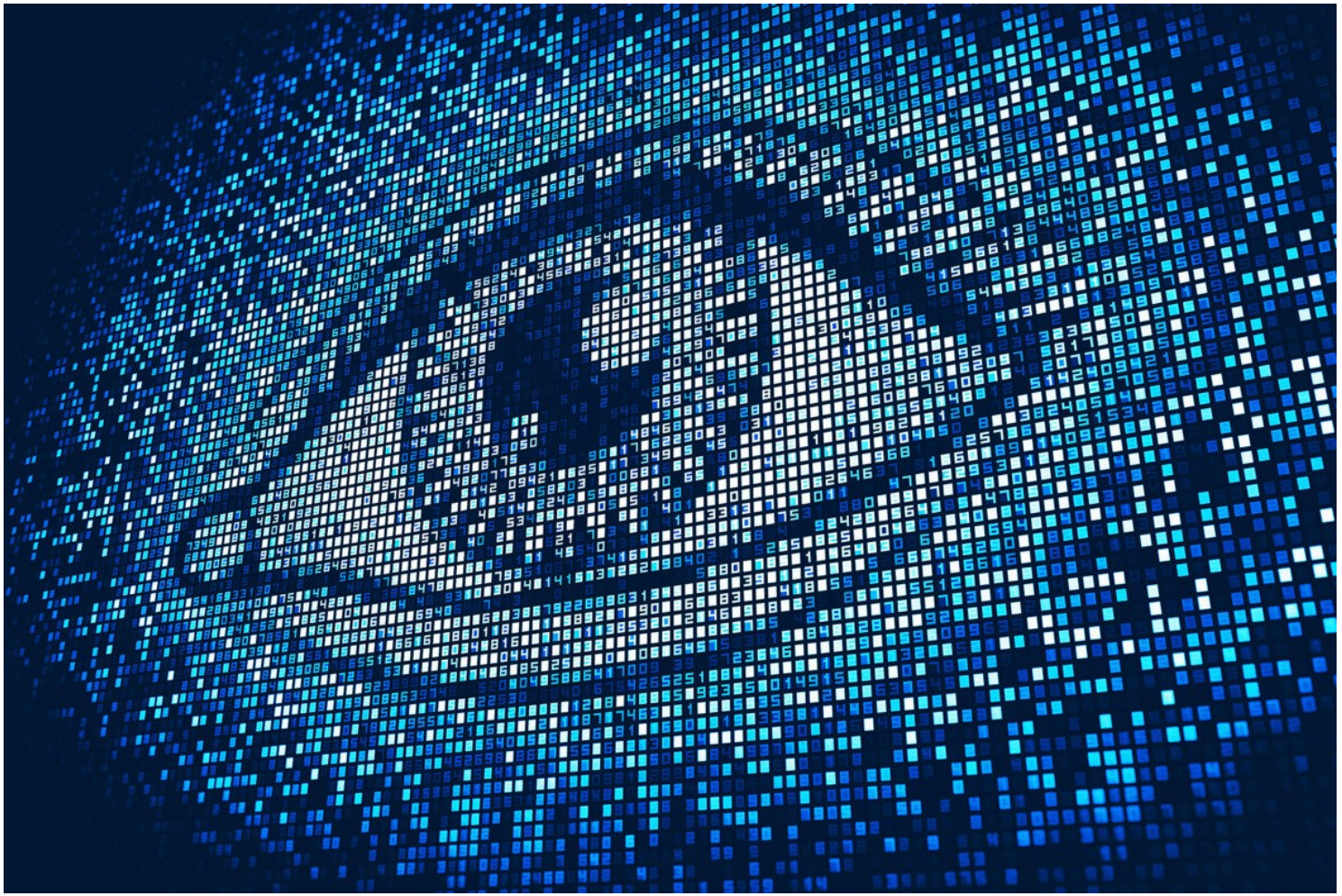
Social media: make signup easy, but detect fakes

- Relies on user reports, moderator teams, AI/ML

[fakenewsai.com]

Problems With Fake Detection

Problem 1: platforms must see, watch everything



[Harvard Gazette]

Problems With Fake Detection

Problem 2: opaque & unaccountable processes

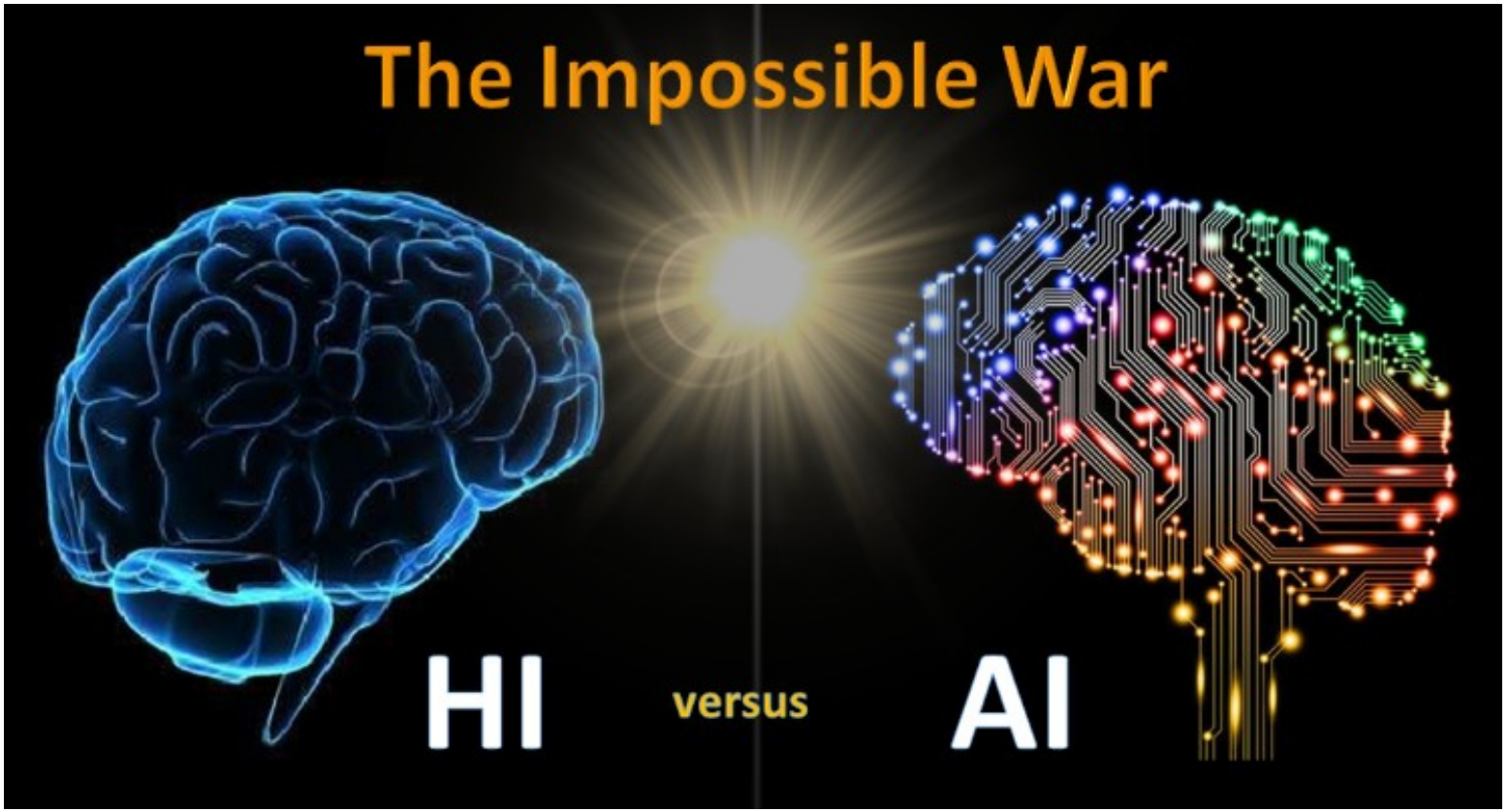
- AI can be wrong, biased, bigoted, racist, …

[TechRepublic]

Problems With Fake Detection

Problem 3: the bad guys also have AI

- AI defenses against AI attacks → humans lose

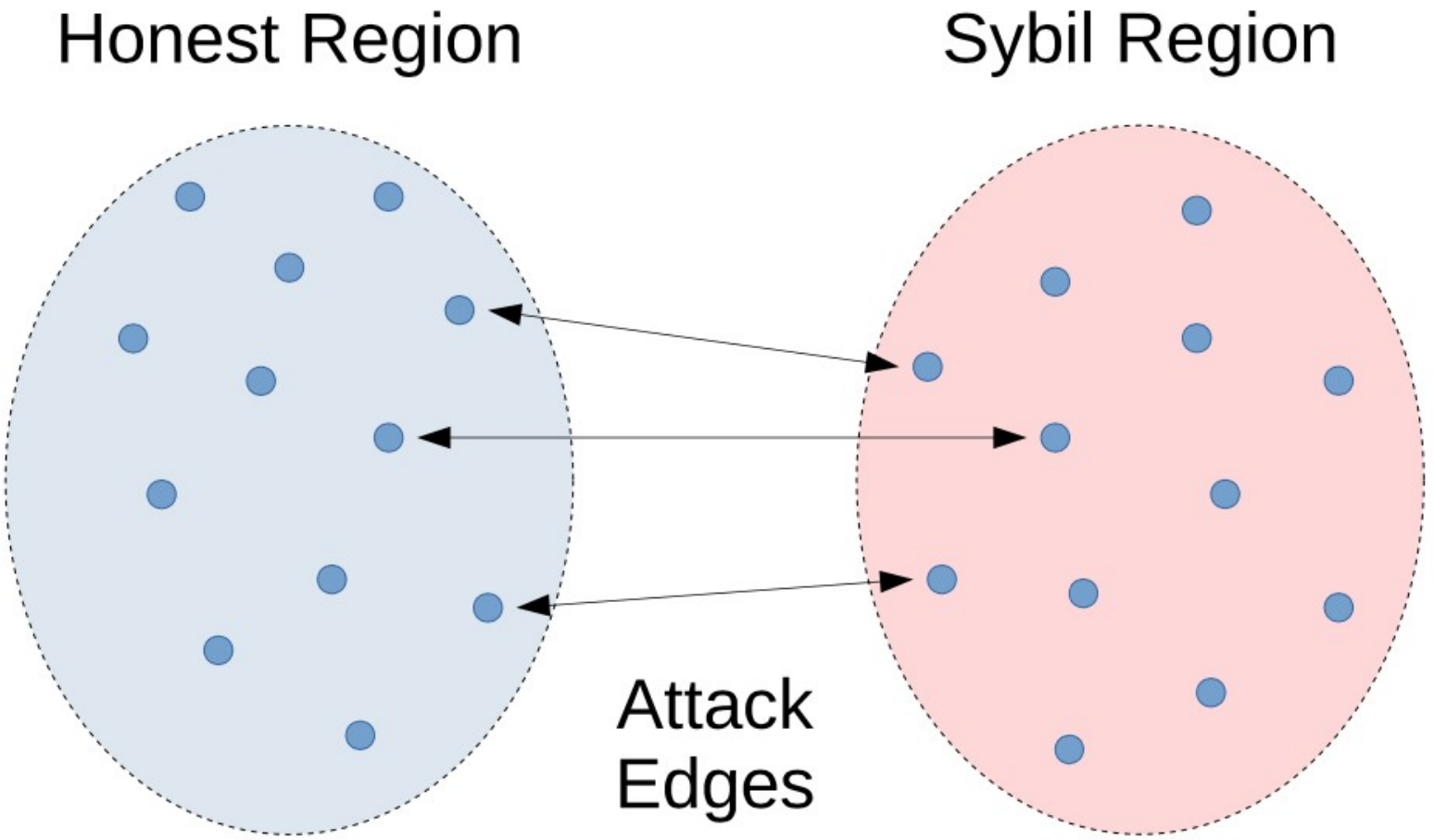


[the-gep.com]

Social Trust Graph Algorithms

Detect fake identities by social graph analysis

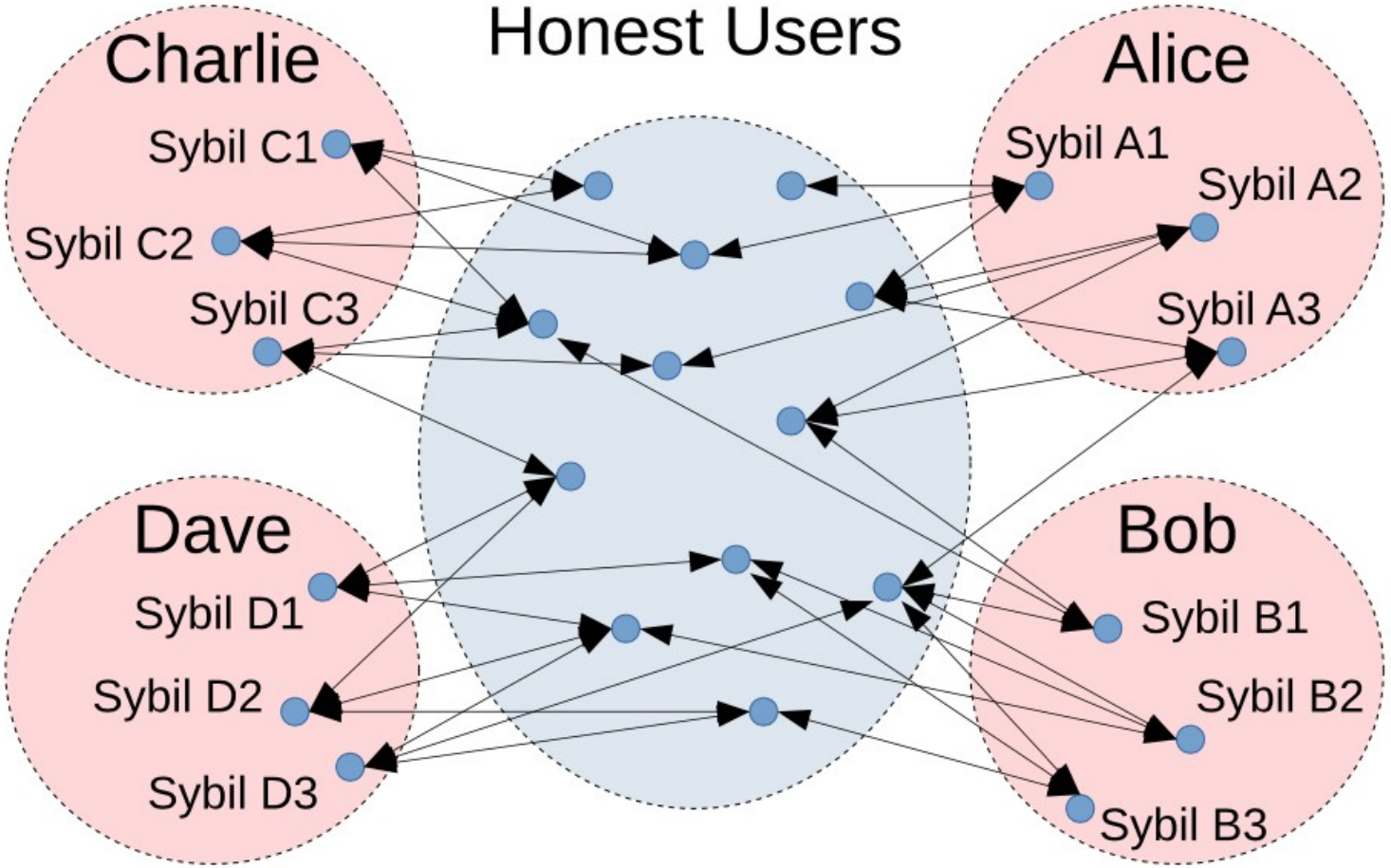
- Addresses one particular **Sybil region** attack…



Social Trust Graph Algorithms

Detect fake identities by social graph analysis

- …but not other realistic scenarios, like this:



Approaches to Digital Identity

- Social Media Identities
  - Expect tech platforms to detect fakes, abuses
- **Proofs of Investment: economic entry costs**
  - CAPTCHAs, proof of work, proof of stake
- Documented Identity: “Know Your Customer”
  - Government-issued ID, self-sovereign ID
- Biometric Identity
  - India’s Aadhaar, World Food Programme

Technological “Proofs of Investment”

Secure, permissionless, and privacy-preserving!

[Paul Gregoire, The Big Smoke]

CAPTCHAs: Invest Human Time

[Prince & Isasi, Cloudflare]

- Getting harder due to AI recognition attacks
- Excludes many real people with disabilities
- Fails equality test: just solve more CAPTCHAs!

Proof of Work: Invest Computation

[Getty Images, BBC News]

- Fails equality test: just buy & burn more energy!

Proof of Stake: Invest Currency

[BitcoinWiki]

- Buy existing cryptocurrency, *stake* it for some time
- Earn rewards proportional to amount of stake
- Fails equality test: just buy & stake more currency!

Proofs of Investment

[Economist]

Suitable for [digital] democracy only if our goal is "**one dollar, one vote**"

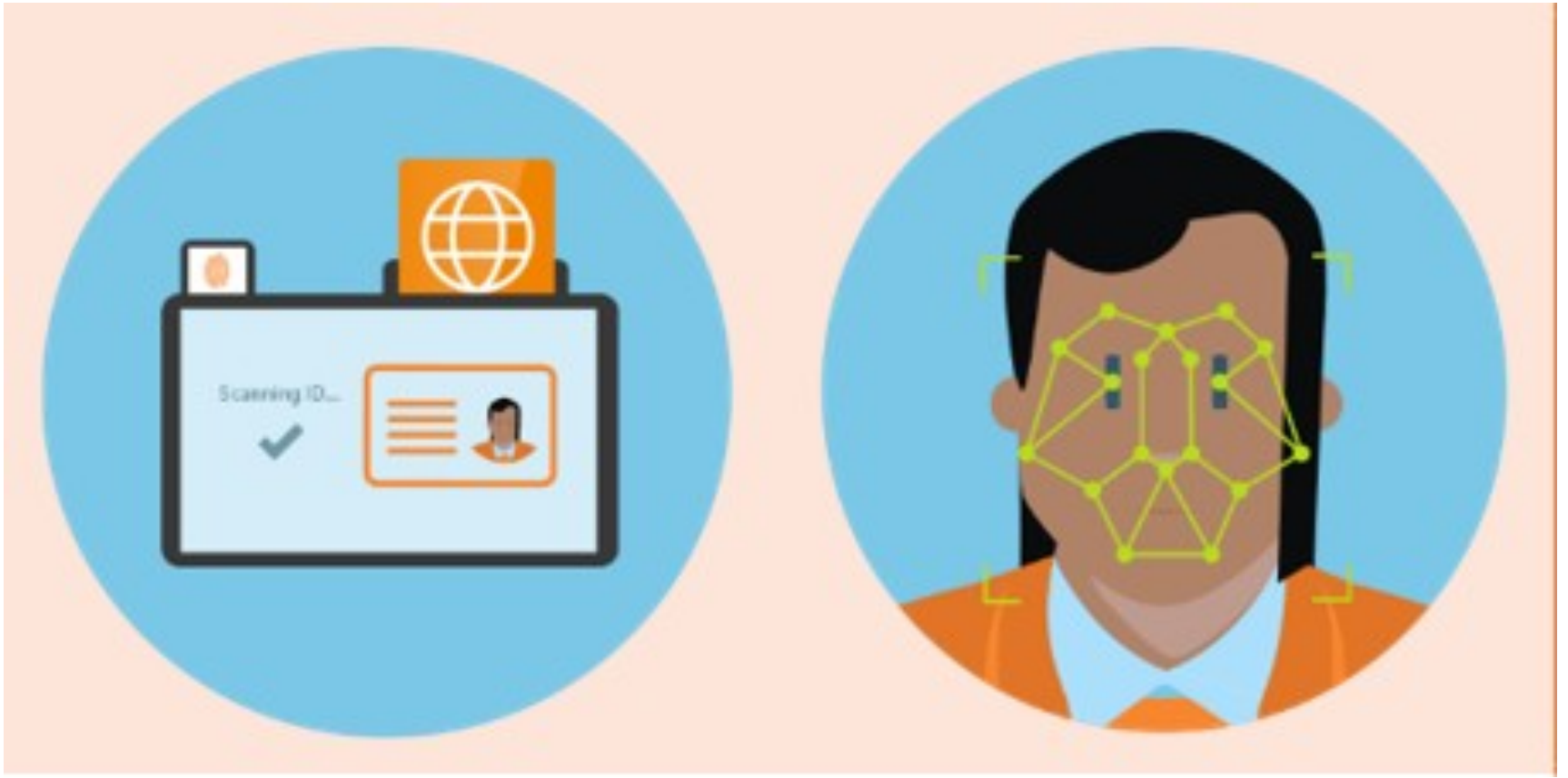
Approaches to Digital Identity

- Social Media Identities
  - Expect tech platforms to detect fakes, abuses
- Proofs of Investment: economic entry costs
  - CAPTCHAs, proof of work, proof of stake
- **Documented Identity: “Know Your Customer”**
  - Government-issued ID, self-sovereign ID
- Biometric Identity
  - India’s Aadhaar, World Food Programme

Identity Verification Services

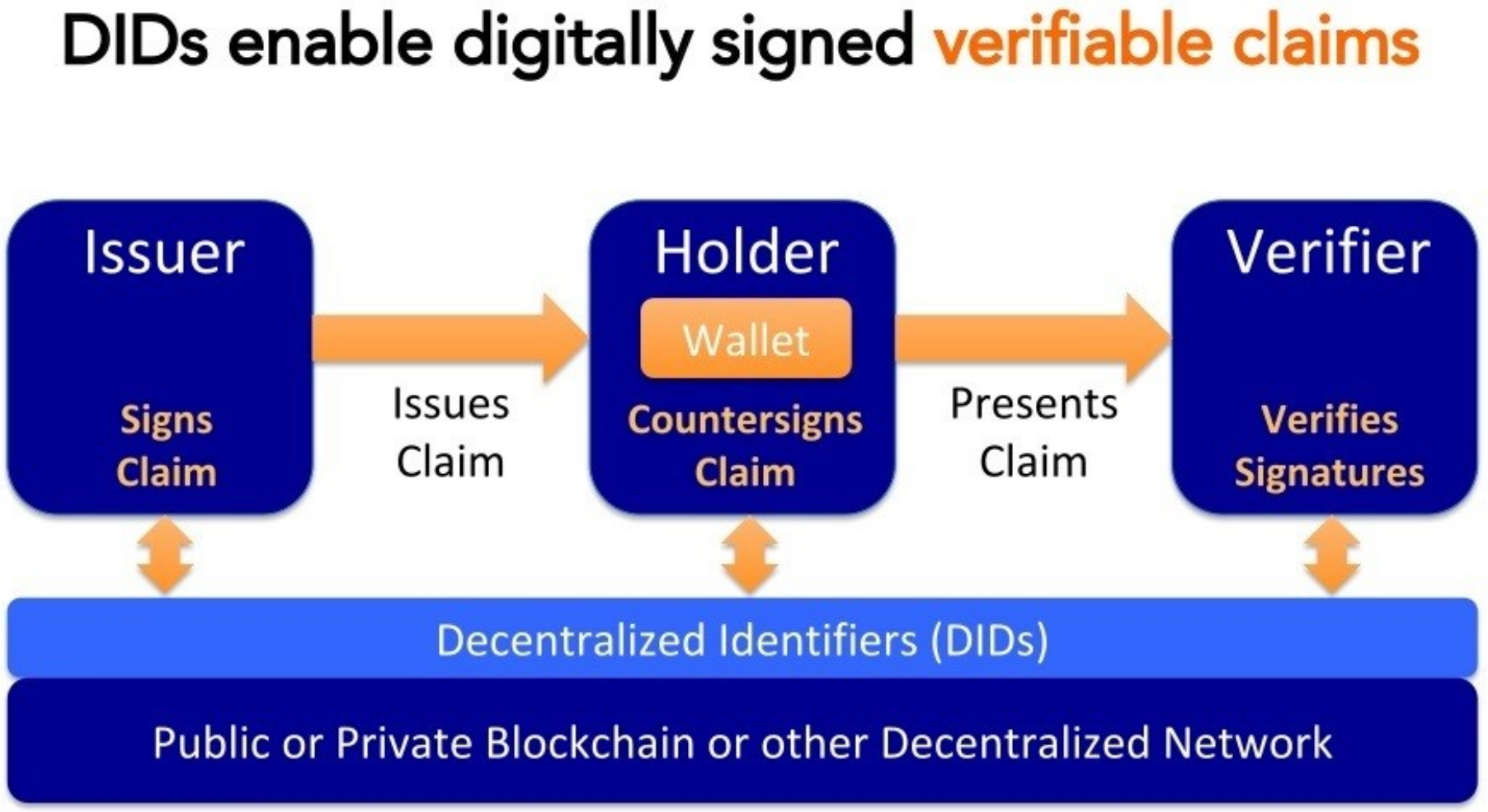
Online verification of traditional identity documents

- Problem: bad guys have AI, deep fakes, …



[Thales]

Self-Sovereign Identity, Maybe?



[Wikipedia]

ID Documents are Forgeable

[Android Fake ID Card Creator]

All IDs Can Be Lost, Stolen

[Andrés Aneiros]

ID Demands Exclude People

[Fikrie Merican]

ID Demands Invade Privacy

[Charles J. Sykes, Hoover Institution]

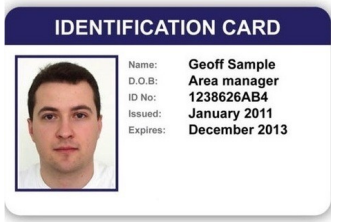
Personas or Alter Egos are Normal

[The Face]

Work, Home, Hobby, Secret Identities

[Fast Company]

Digital Identity: the KYC Approach



Key Advantages:

- Many businesses, governments working on it
- Leverages existing “document-trail” identities

Key Disadvantages:

- Identity documents not hard to fake, steal, buy
  - SSN $1, Fake ID $20, fake passport $1000, …
- Identity authorities are single points of compromise
  - Attacker needs to break *only one* to create many Sybils
- Exclusionary: undocumented/unlucky lose out
  - Migrants, refugees, homeless, stateless, …

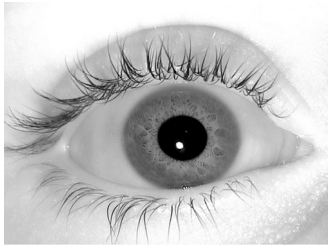
Approaches to Digital Identity

- Social Media Identities
  - Expect tech platforms to detect fakes, abuses
- Proofs of Investment: economic entry costs
  - CAPTCHAs, proof of work, proof of stake
- Documented Identity: “Know Your Customer”
  - Government-issued ID, self-sovereign ID
- **Biometric Identity**
  - India’s Aadhaar, World Food Programme

Are Biometrics a Solution?

Key Advantages:

- Technically scalable, workable in principle
  - India Aadhaar, UNHCR World Food Program, …



Key Disadvantages:

- Requires not just *authentication* (1-to-1 comparison) but *biometric identity* (1-to-billions comparison)
  - 0.01% FAR → 100,000 false positives *per user* in India
- Privacy: must collect in massive queryable database
  - Biometrics are passwords you can’t change when leaked
- One compromised device can enroll many Sybils

Biometric identity: a cautionary tale

“Aadhaar Failures: A Tragedy of Errors” - Khera

[EPW]

Approaches to Digital Identity

- ~~Social Media Identities~~
  - Expect platforms to detect fakes, abuses
- ~~Proofs of Investment~~
  - CAPTCHAs, proof of work, proof of stake
- ~~Documented Identity~~: "Know Your Customer"
  - Government-issued ID, self-sovereign ID
- ~~Biometric Identity~~
  - India's Aadhaar, World Food Programme

Identity: a failed digital foundation

No known digital **identity** approach appears to be

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

Perhaps we should focus on verifying **people** rather than on verifying their **identities**?

Maybe the cart is pulling the horse

Digital **identity** first requires digital **personhood**

Talk Outline

- Is the Internet “democratizing”? Can it be?
- Self-governance foundations: money vs people
- Identity: a siren song of digital surveillance
- **Digital personhood: equality with privacy**
- Applications: governance, social media, crypto
- Conclusion: towards digital self-governance

Proof of Personhood

A mechanism to verify **people**, not **identities**

- For online forums, voting, deliberation, …

Key goals:

- **Inclusion**: any *real human* may participate
- **Equality**: one person, one vote
- **Security**: protect both individuals & collective
- **Privacy**: free expression, association, identity
  - Including freedom of multiple unlinkable personas!

Proof of Personhood

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

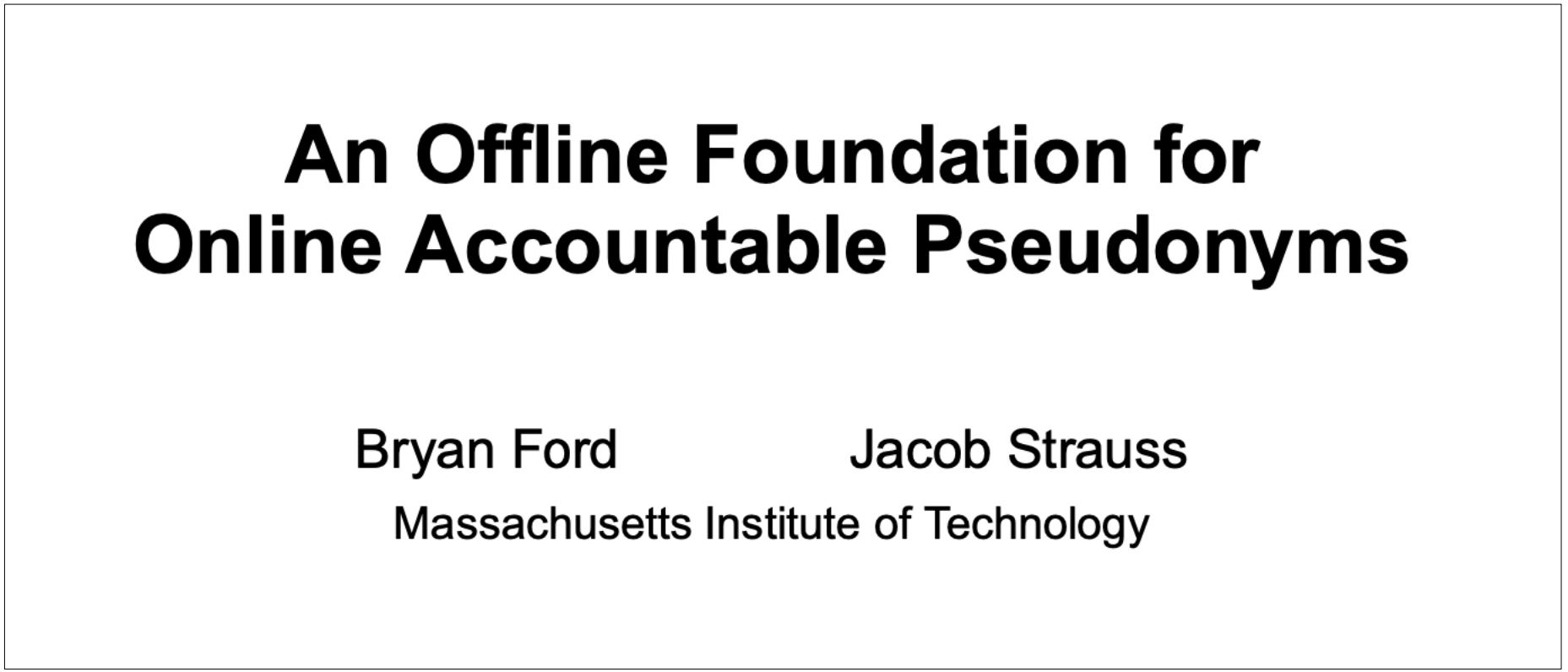
Proofs of Personhood

Can we achieve “one person, one vote” online?

- 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]

Pseudonym Parties

- 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

In case we may have forgotten…

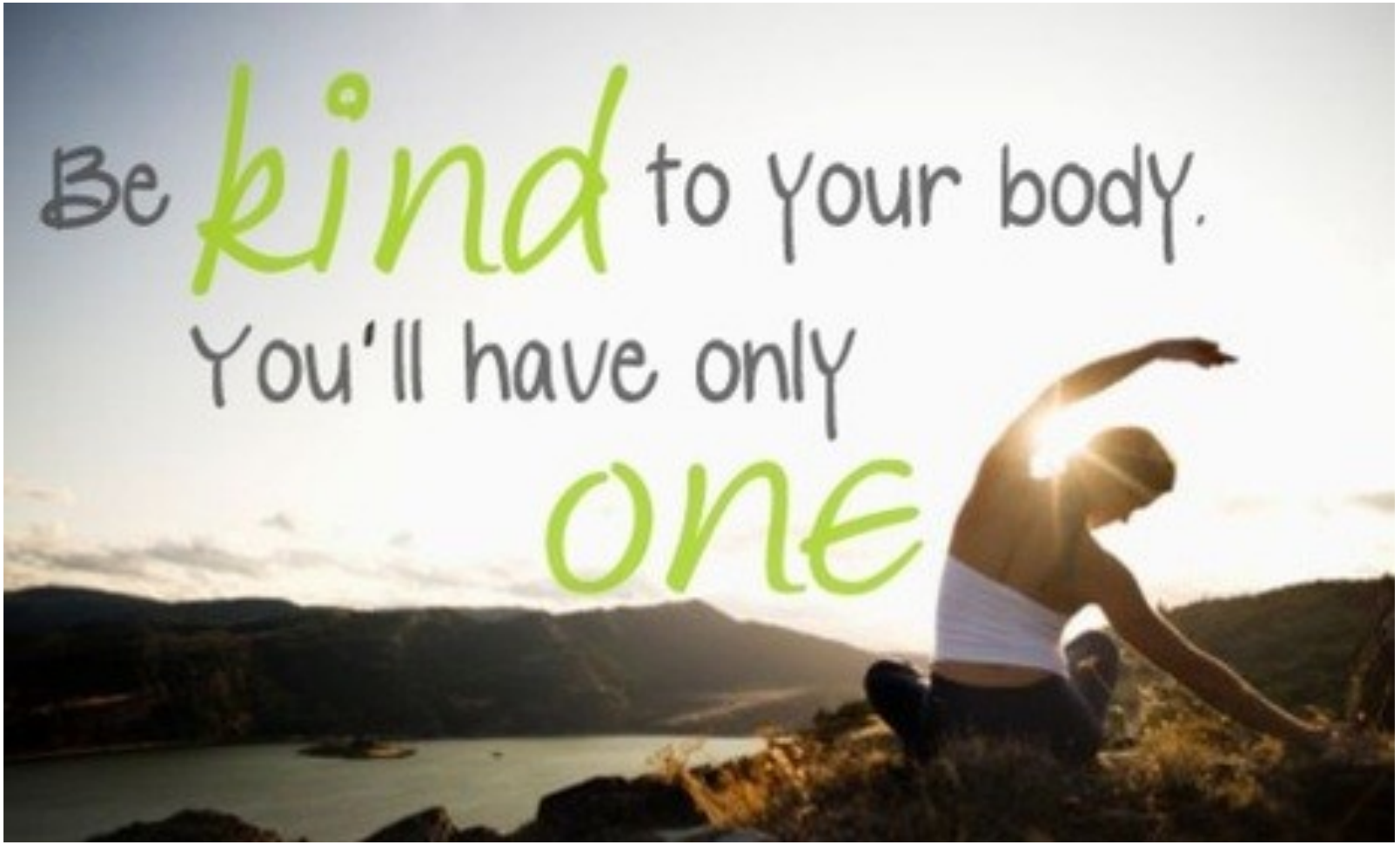
Real people have **real bodies** in the **real world**

[Silvana Denker, People]

Maybe we should use them … once in a while?

A “digital security” principle

Real people have **only one body** each



[Wisdom in Waves]

A “digital security” principle

Real people can be in **only one place at a time**

- (unless you’re John Malkovich)

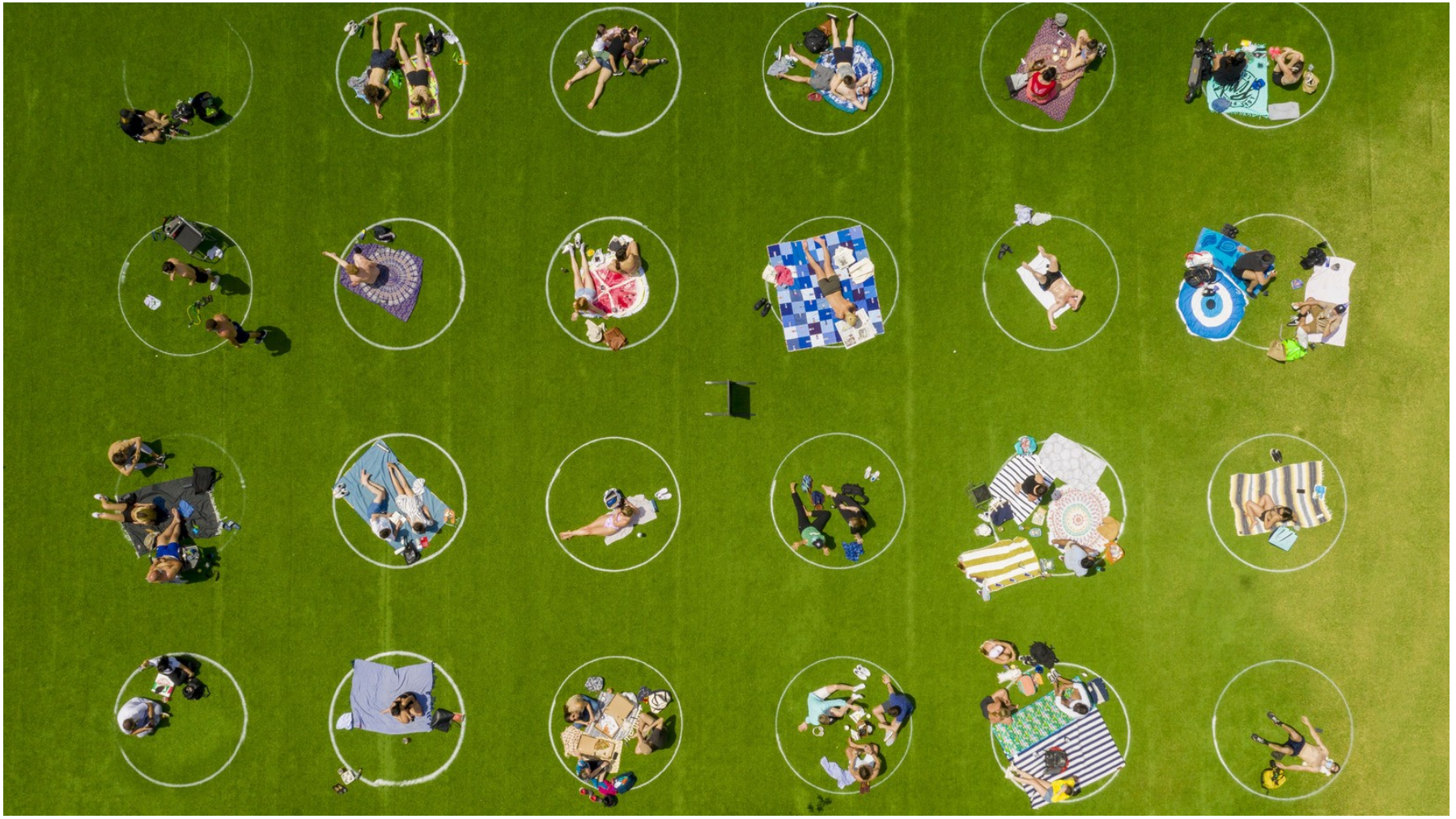
[Rolling Stone]

Pseudonym Parties

Periodic **in-person** events, like *Landsgemeinde*

Pseudonym Parties

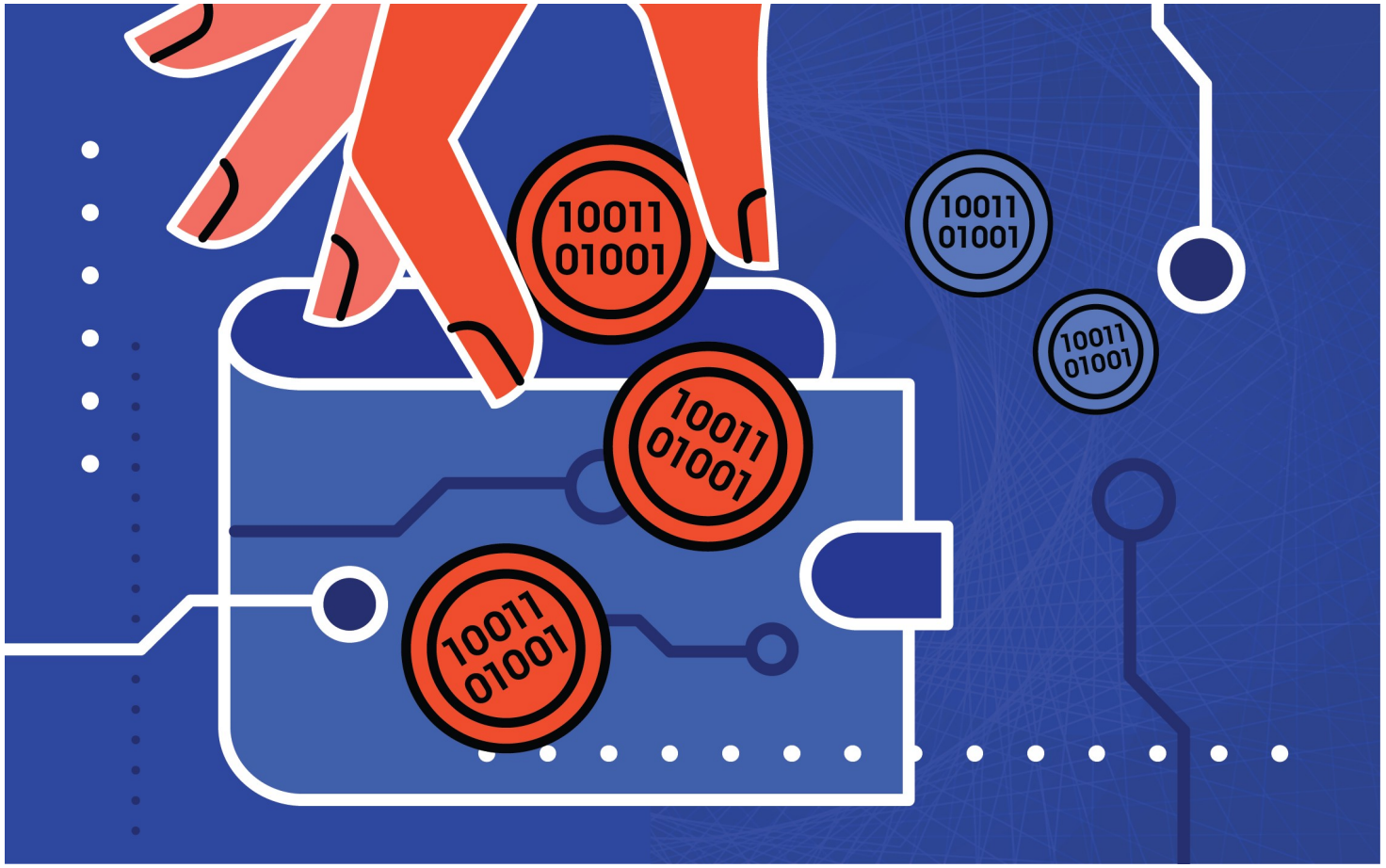
…perhaps spread out a bit more in current times



[ArchDaily]

Pseudonym Parties

Used not for making decisions immediately but only giving each attendee *one digital PoP token*

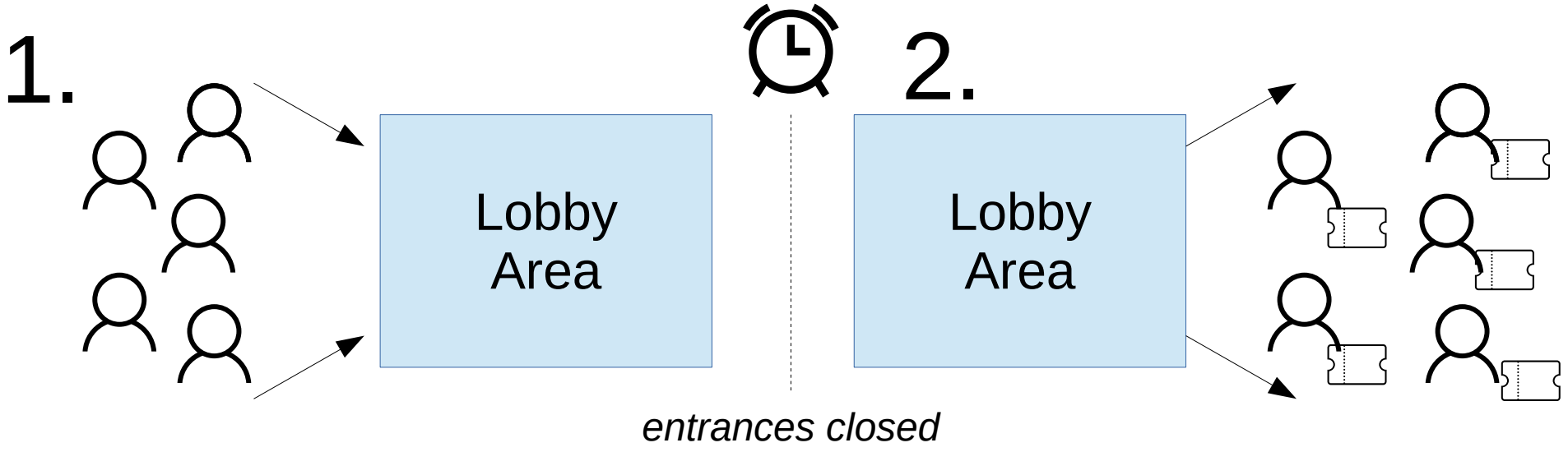


[gov.sg]

One Person, One Token

How to ensure each person gets *only one* token?

- Attendees gather in **lobby** area by a deadline
- At deadline entrances close, *no one else gets in*
- Each attendee gets one token *while leaving*



Precedent: Election Ink or Stain

Indelible stain that takes a few days to wear off

- Track record: used for 50+ years in India
- Some cost, some security/privacy issues

Yes, you need to *get there*…

But there could be many locations to go

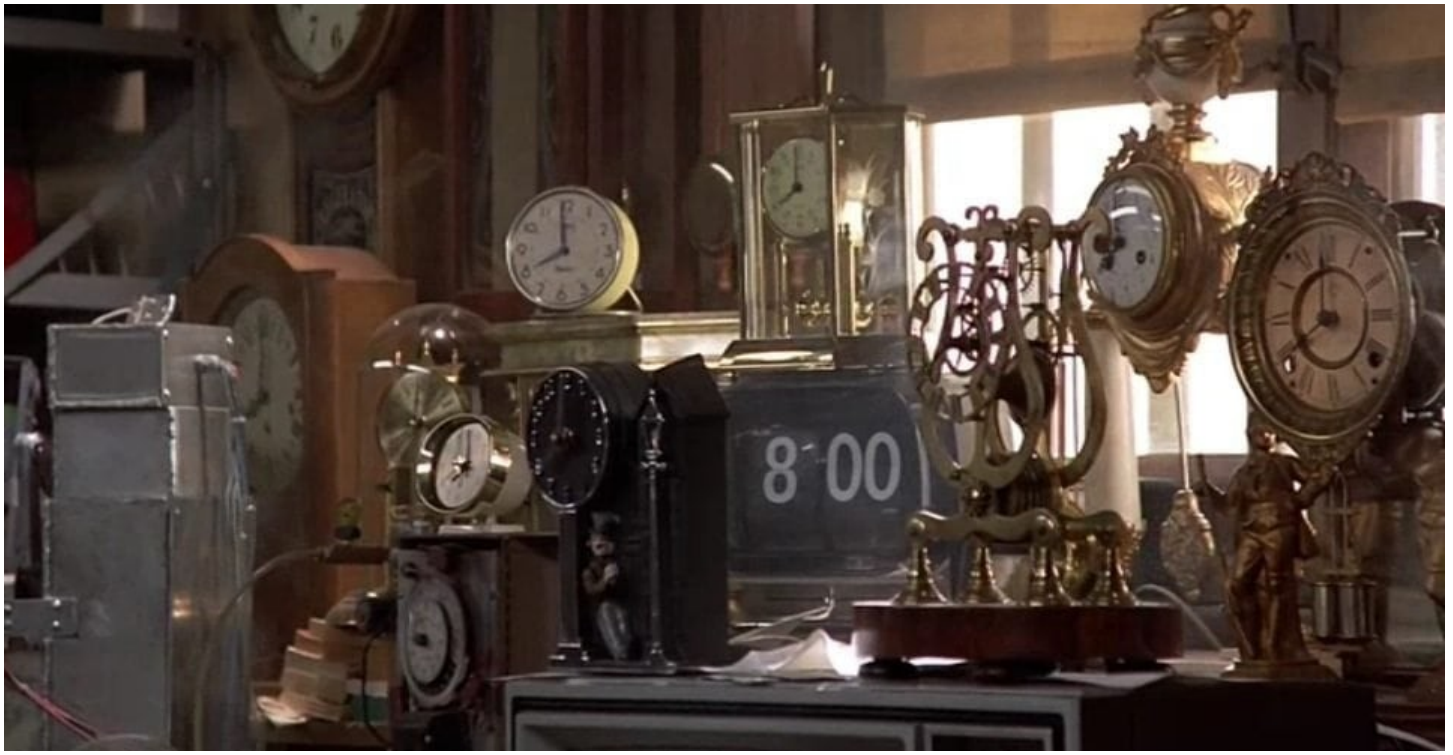
- In principle every city, town, street corner

[encointer]

Regular Synchronized Events

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

- No one can physically attend two at once



You choose which event to attend

Events could be organized around concerts...

[xinhuanet]

You choose which event to attend

…or political rallies and protests…

[pixabay]

You choose which event to attend

…or festivals…

You choose which event to attend

…or humanitarian aid distributions…

You choose which event to attend

…or in the atriums of hospitals or other care facilities for those less mobile…

[friendsofcrh.ca]

You choose which event to attend

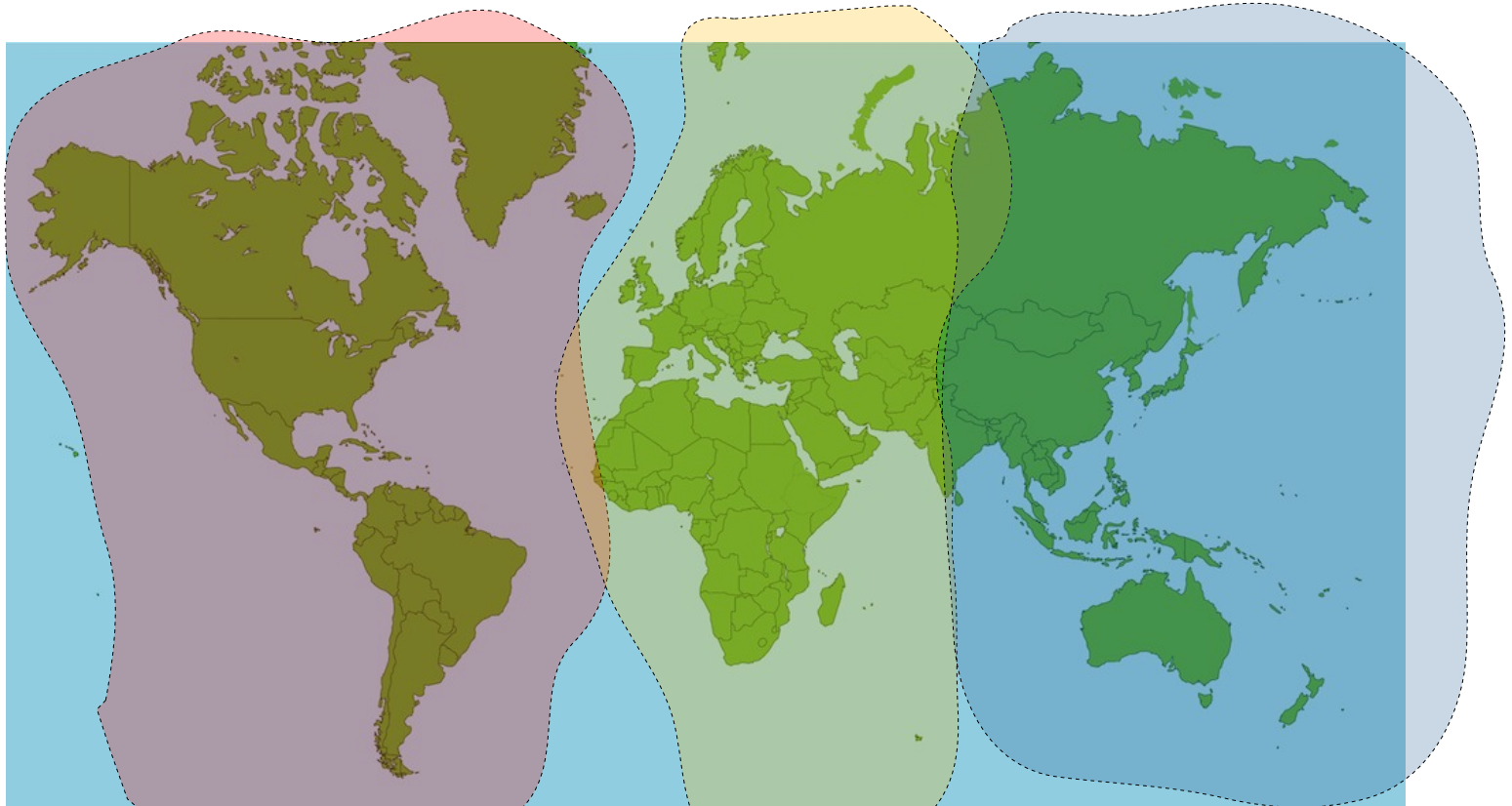
…or religious occasions…

People have many reasons to gather *anyway*

The Timezone Challenge

A convenient time somewhere is 4 AM elsewhere

- Solution 1: varying times → “fair” inconvenience
- Solution 2: ~3 large synchronization regions



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

Anti-Coercion with Fake Tokens

Each attendee gets brief time in a **privacy booth**

- Out of any coercer's control or surveillance

[Liz Sablich, Brookings]

Anti-Coercion with Fake Tokens

Each attendee gets both **real** & **decoy** tokens

- Give decoy tokens to kids, sell them
- Both “work” – but only real ones **count**
- Only the **true voter** knows which is which

Ongoing progress in DEDIS lab

Semester projects to build & test PoP prototypes:

- Fall 2020: 10 undergrads, 2 PhDs – [report]
- Spring 2021: 10 undergrads, 2 PhDs – [report]
- Fall 2021: 12 undergrads, 4 PhDs – WIP

Also driving & inspiring DEDIS research in:

- Privacy-preserving blockchains [CALYPSO]
- Resilient locality-sensitive computing [Limix]
- Robust asynchronous consensus [QSC]
- Coercion-resistant E-voting [Votegral]

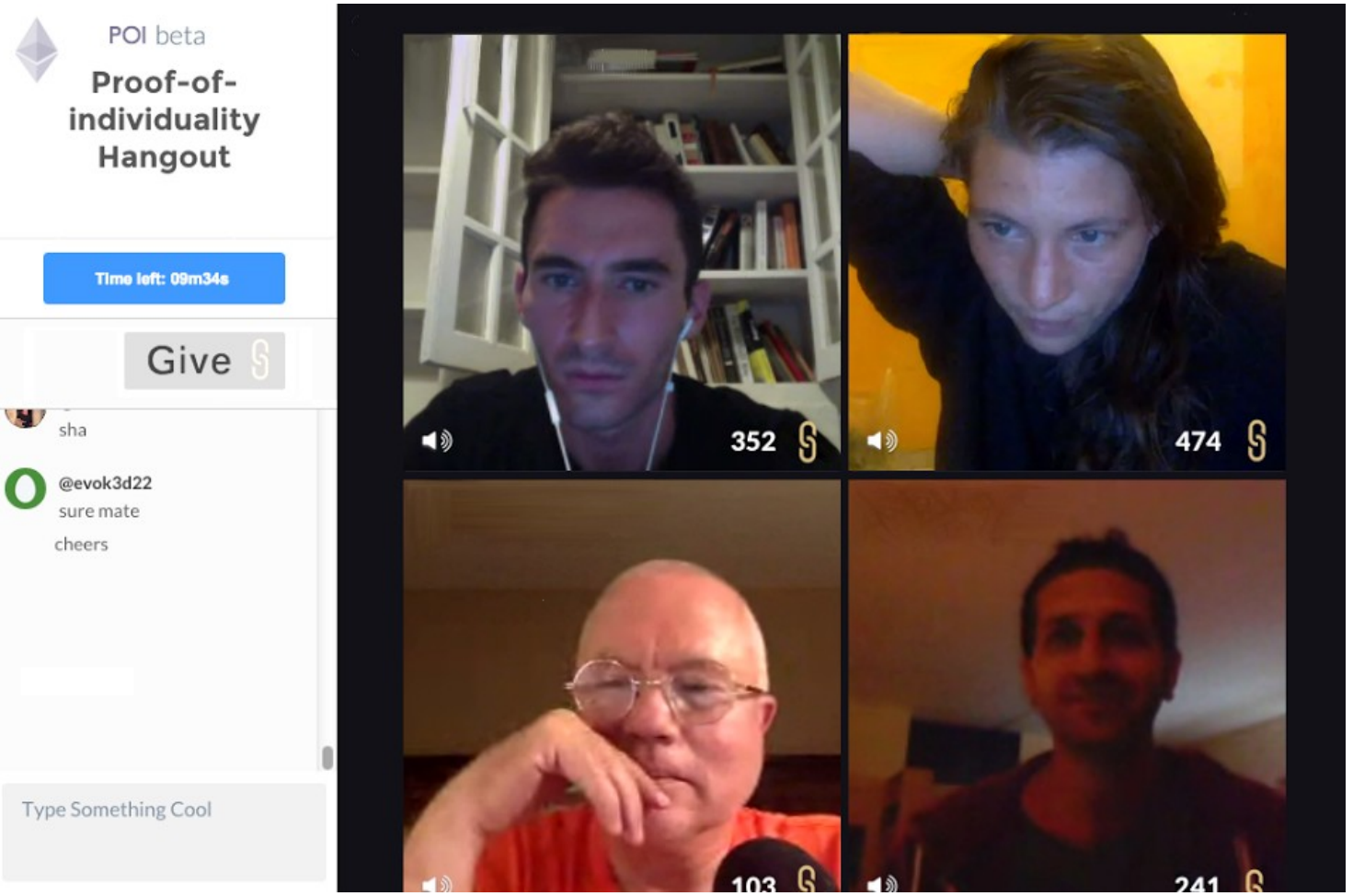
Other approaches being explored

Encointer: assignments to meet in random groups

[encointer]

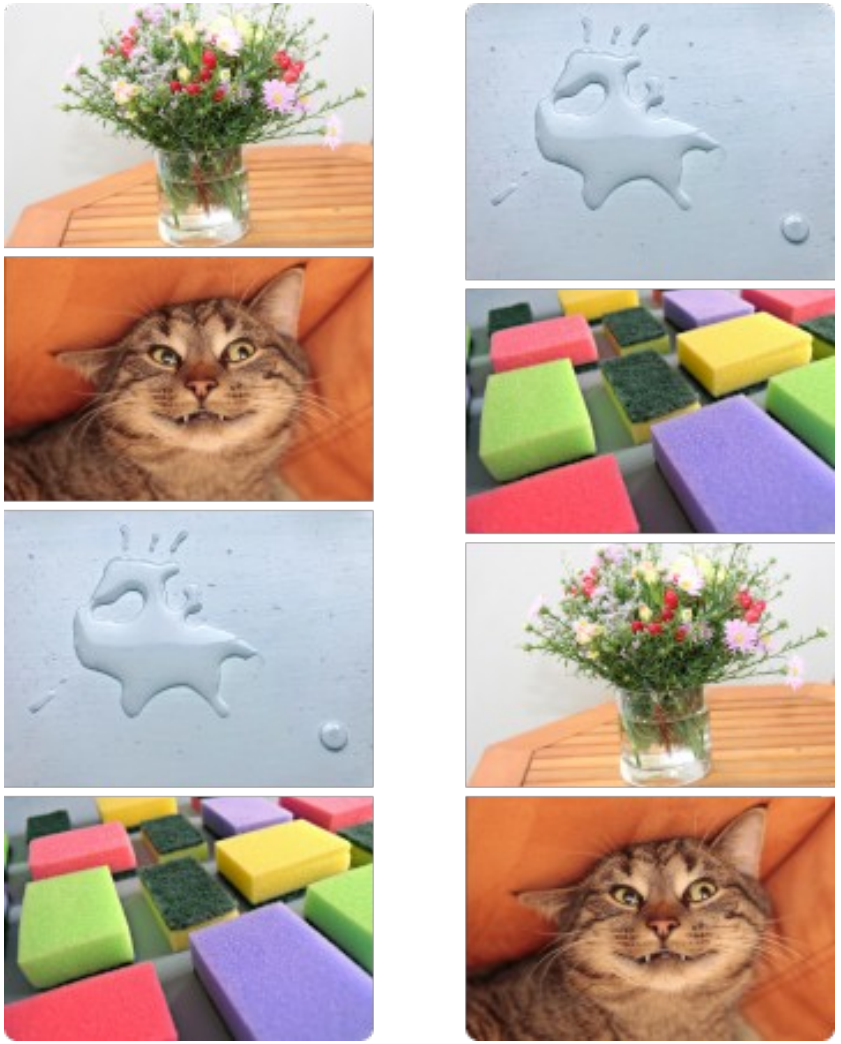
Other approaches being explored

Proof-of-Individuality using online video interaction



Other approaches being explored

Idena: using “AI-hard” FLIP challenges



Other approaches being explored

Personhood based on *anonymized* existing IDs

- Crypto-Book: anonymized social media identity
  - “Building Privacy-Preserving Cryptographic Credentials from Federated Online Identities” [Maheswaran et al, CODASPY 2016]
- CanDID: anonymized government identity
  - “CanDID: Can-Do Decentralized Identity with Legacy Compatibility, Sybil-Resistance, and Accountability”
  - [Maram et al, IEEE S&P 2021]

Summary of Alternatives

Approach	Inclusive	Equal	Secure	Private
Government Identity	-	?	?	-
Biometric Identity	?	√	?	-
Self-Sovereign Identity	?	?	√	-
Proof of Investment	√	-	√	√
Social Trust Networks	-	?	-	-
Threshold Verification	?	-	?	?
Pseudonym Parties	√	√	√	√

Talk Outline

- Is the Internet “democratizing”? Can it be?
- Self-governance foundations: money vs people
- Identity: a siren song of digital surveillance
- Digital personhood: equality with privacy online
- **Applications: governance, social media, crypto**
- Conclusion: towards digital self-governance

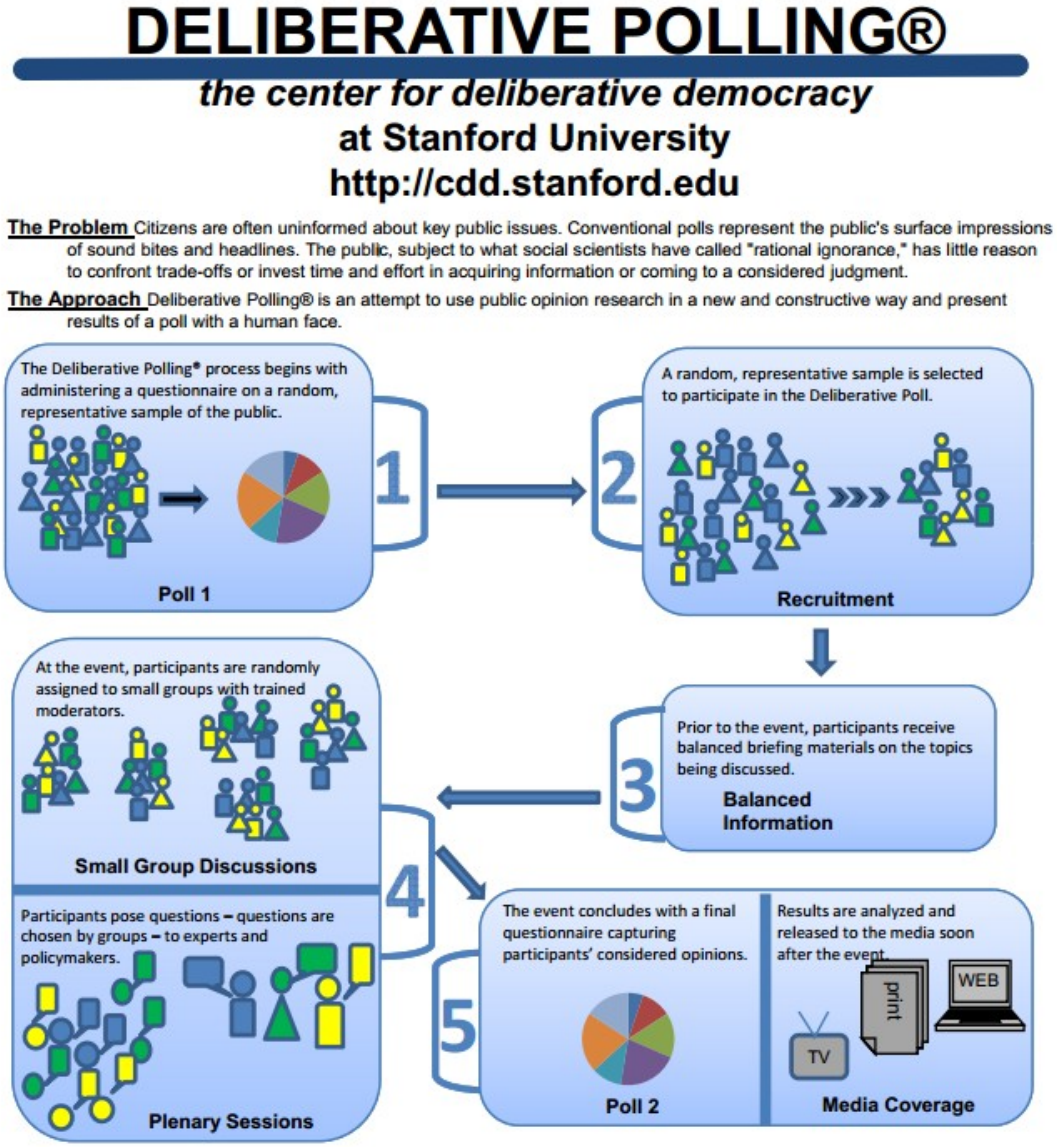
Old-fashioned governance…online

Online Participatory Democracy

Mass online deliberation, liquid democracy, …

Sortition-based Polling, Deliberation

Statistically random samples of *real people*



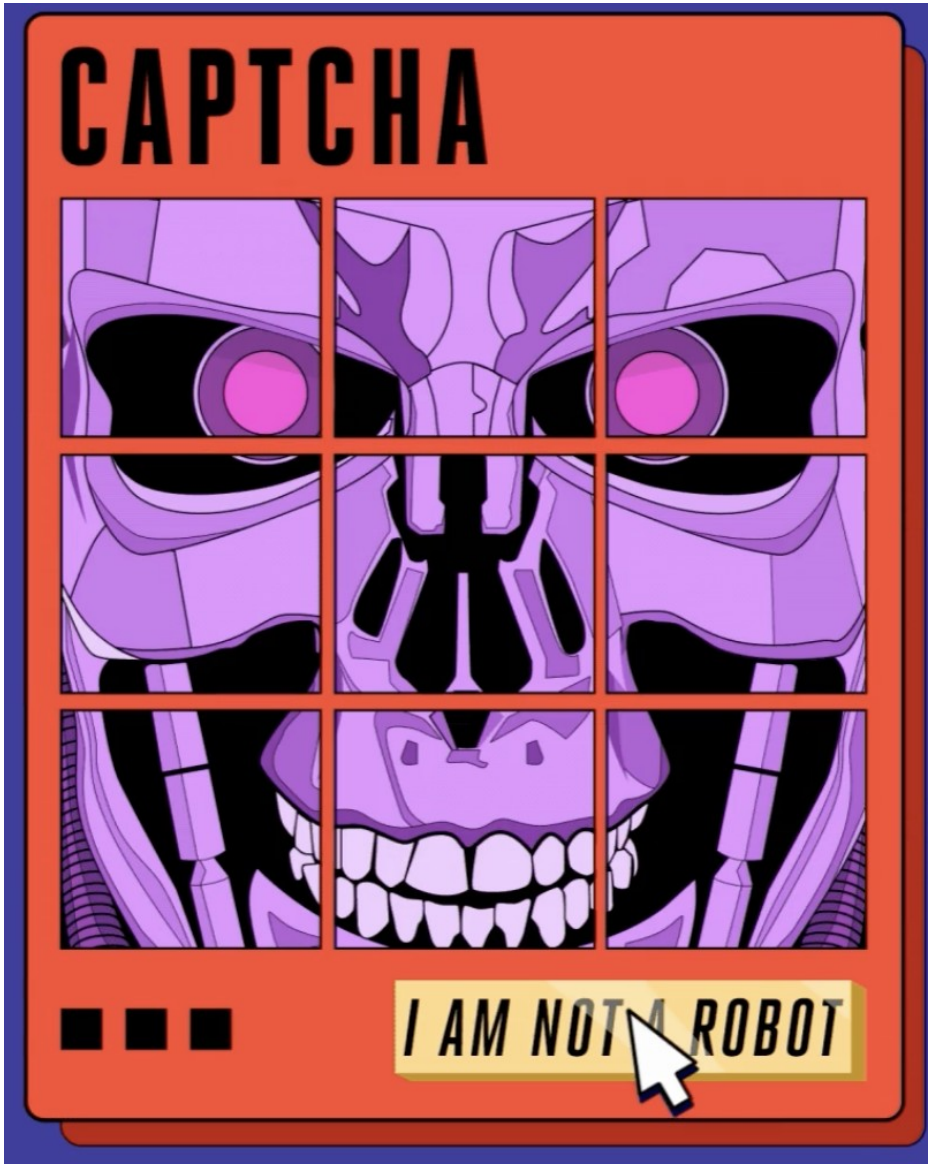
Replacing CAPTCHAs

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 **a Person**

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

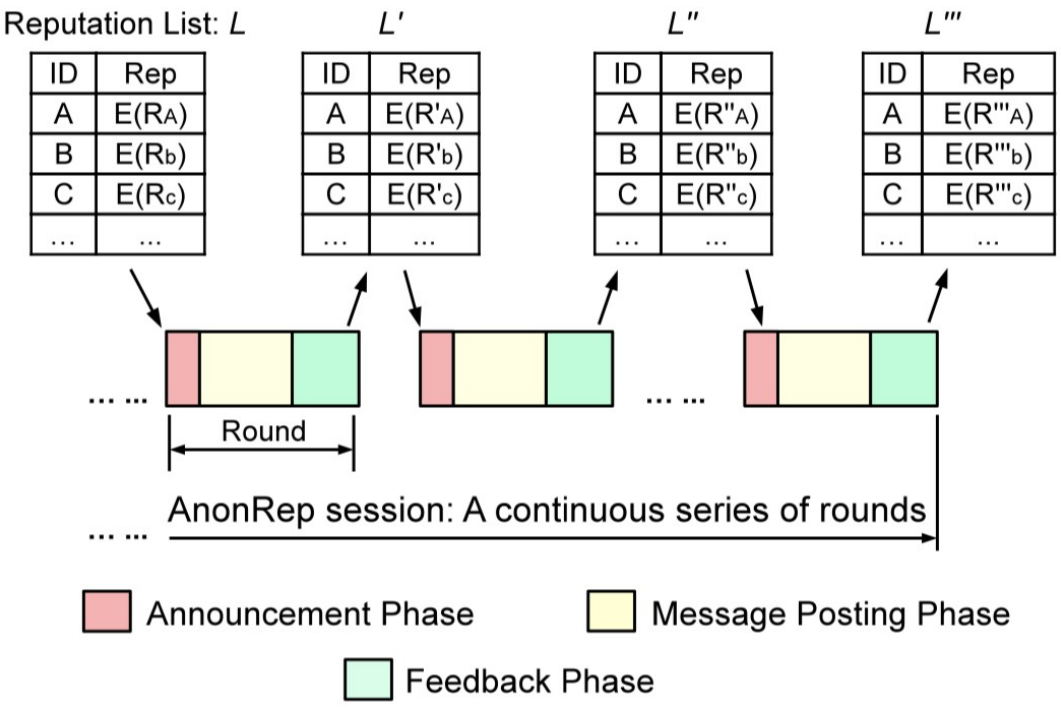
Accountable Anonymity at Scale

Can we satisfy the usually-competing goals of:

- Fully protecting self-expression via **anonymity**
- Limiting & mitigating abuse via **accountability**

Secure anonymous reputation, moderation, …

- e.g., AnonRep [NSDI ‘16]



Talk Outline

- Is the Internet “democratizing”? Can it be?
- Self-governance foundations: money vs people
- Identity: a siren song of digital surveillance
- Digital personhood: equality with privacy online
- Applications: governance, social media, crypto
- **Conclusion: towards digital self-governance**

Towards Formal Digital Personhood

A new type of *social contract* for the digital world?

Cost: you must regularly invest effort to *show up*

Reward: rights and protections in the digital world

- Right to privacy, anonymity, *and* to protection from anonymous abuse (you can reliably block/filter)
- Right to freedom of speech, *and* to protection from unfair amplification of others' speech
- Right to equal economic opportunity to create money in new permissionless cryptocurrencies
- Right to inclusion, systems that *stay decentralized*

Conclusion

Can we make the Internet truly "**democratizing**"?

- Not just "a platform" where loudest/richest wins
- Can it ensure **equality**, **inclusion**, **autonomy**?

Digital personhood: towards equality online

- "One person, one vote" – *without* identification
- Multiple emerging offline & online approaches
- Many applications – *if* we can make it work