EPFL

Personhood Online: Privacy, Transparency, and Inclusion for Digital Democracy

Bryan Ford, Louis-Henri Merino, Haoqian Zhang
Decentralized and Distributed Systems (DEDIS)
Swiss Federal Institute of Technology (EPFL)
dedis@epfl.ch – dedis.epfl.ch

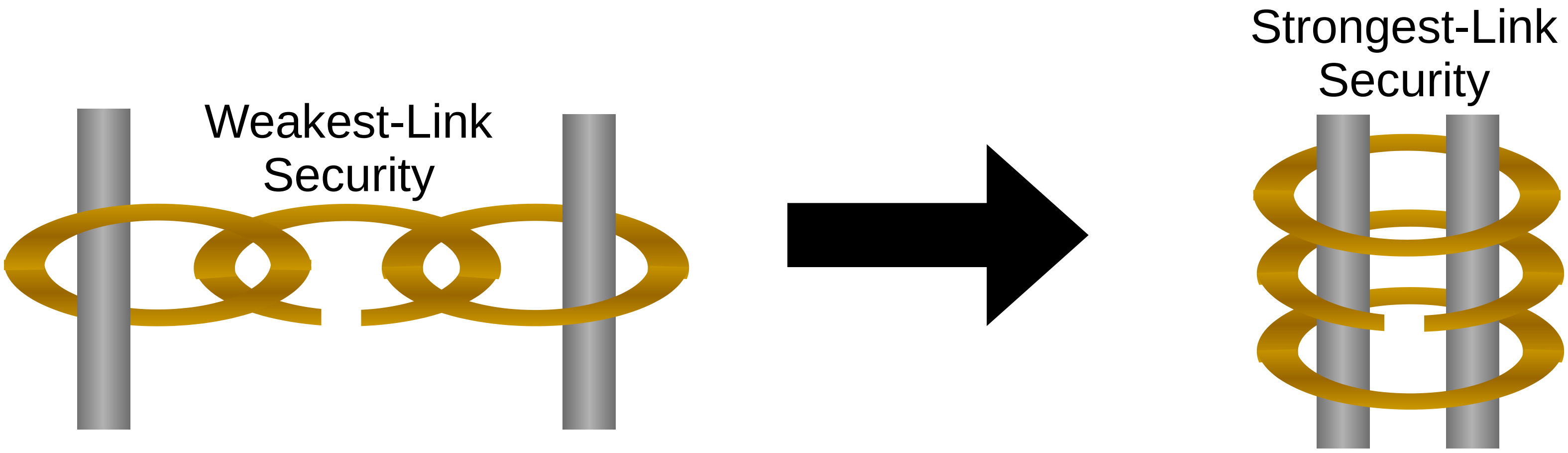
Digital Democracy Workshop – November 5, 2020

The DEDIS lab at EPFL: Mission

Design, build, and deploy secure privacy-preserving
Decentralized and Distributed Systems (DEDIS)

- **Distributed:** spread widely across the Internet & world
- **Decentralized:** independent participants, no central authority, *no single points of failure or compromise*

Overarching theme: building decentralized systems
that **distribute trust** widely with **strongest-link security**

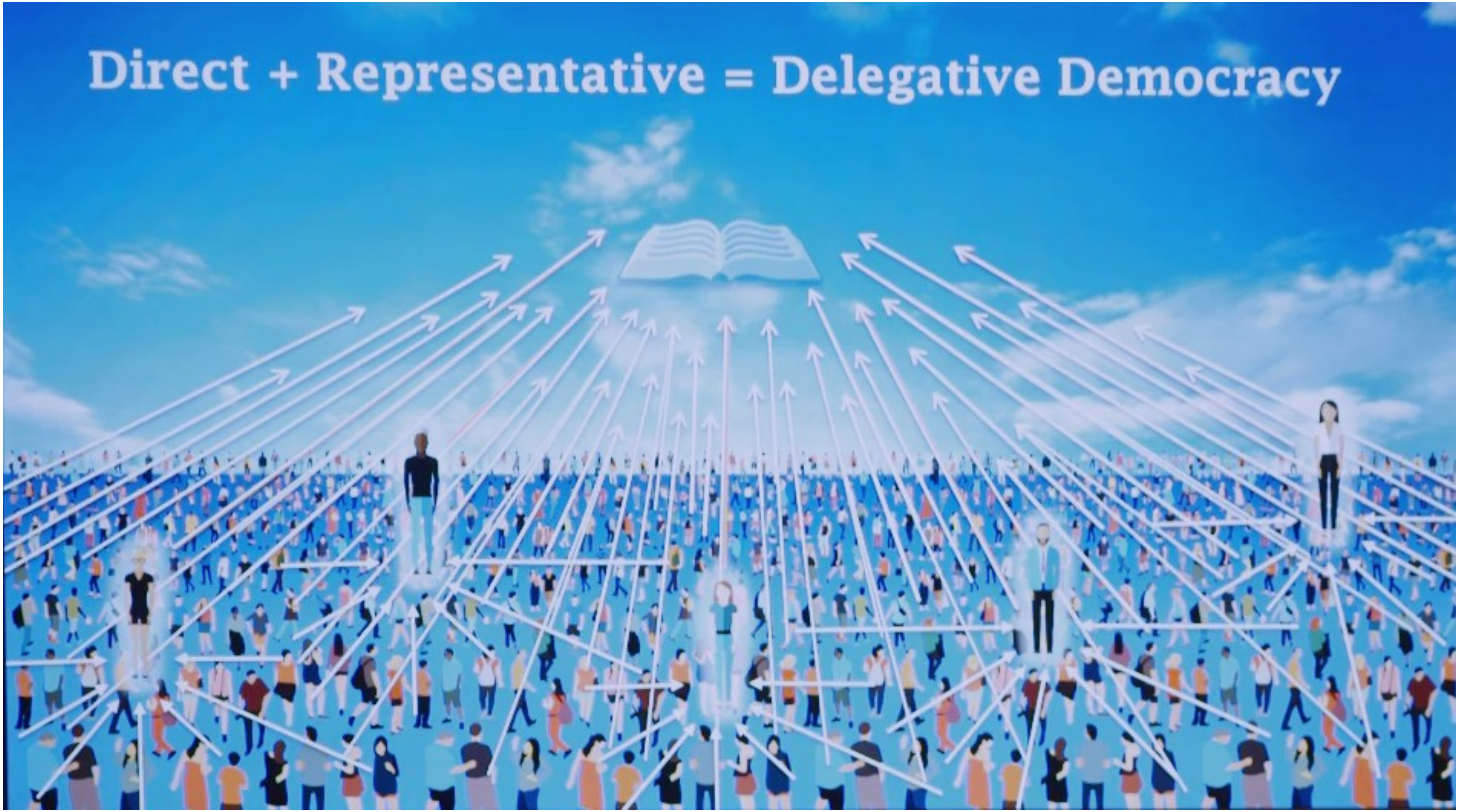


Why Digital Democracy?

Greater Convenience

[Kenneth Hacker, The Progressive Post]

Richer Participation

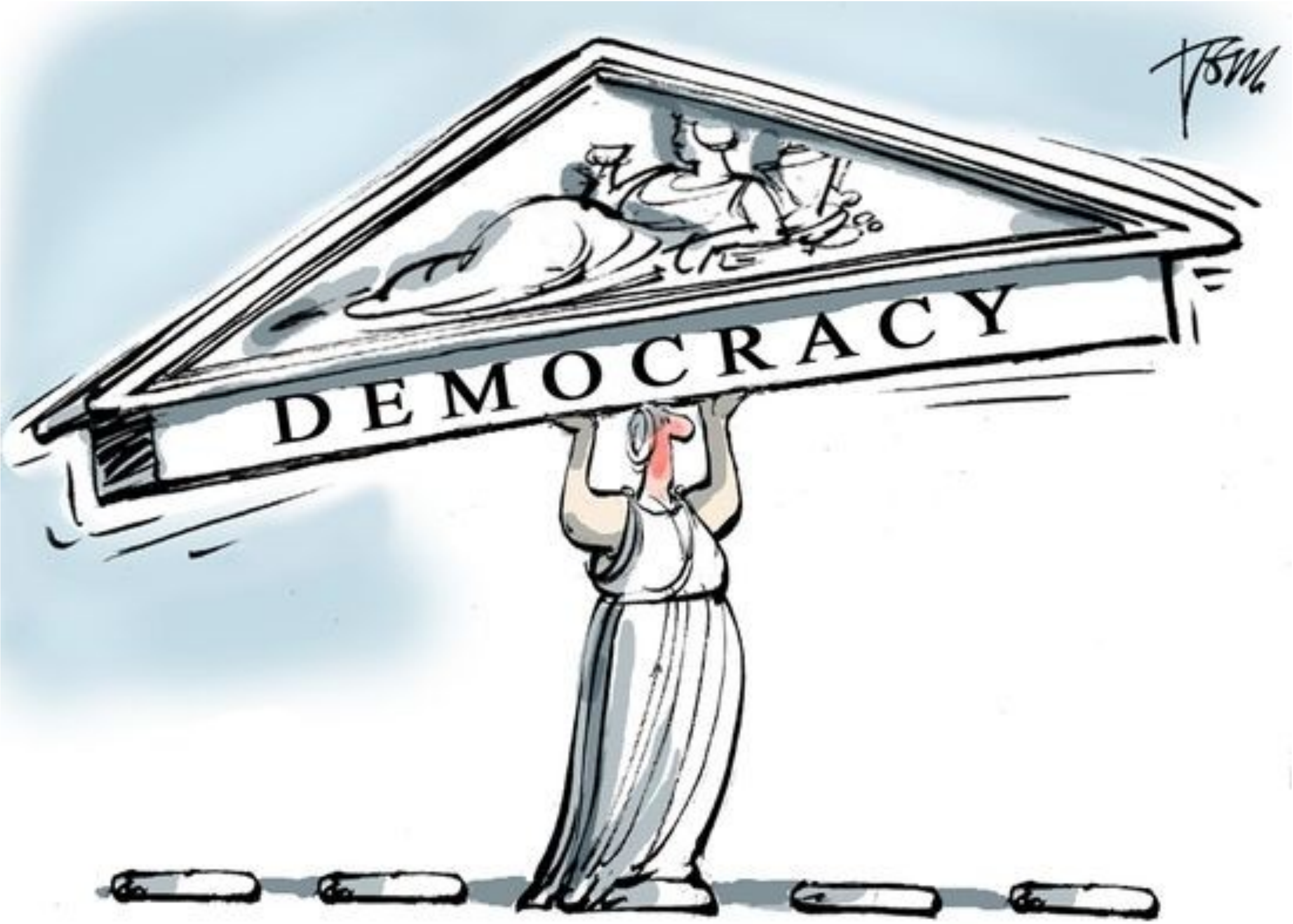


[Ehud Shapiro, Open Transcripts]

Online Self-Governance

Can digital forums and communities self-govern?

Democracy Needs a Foundation

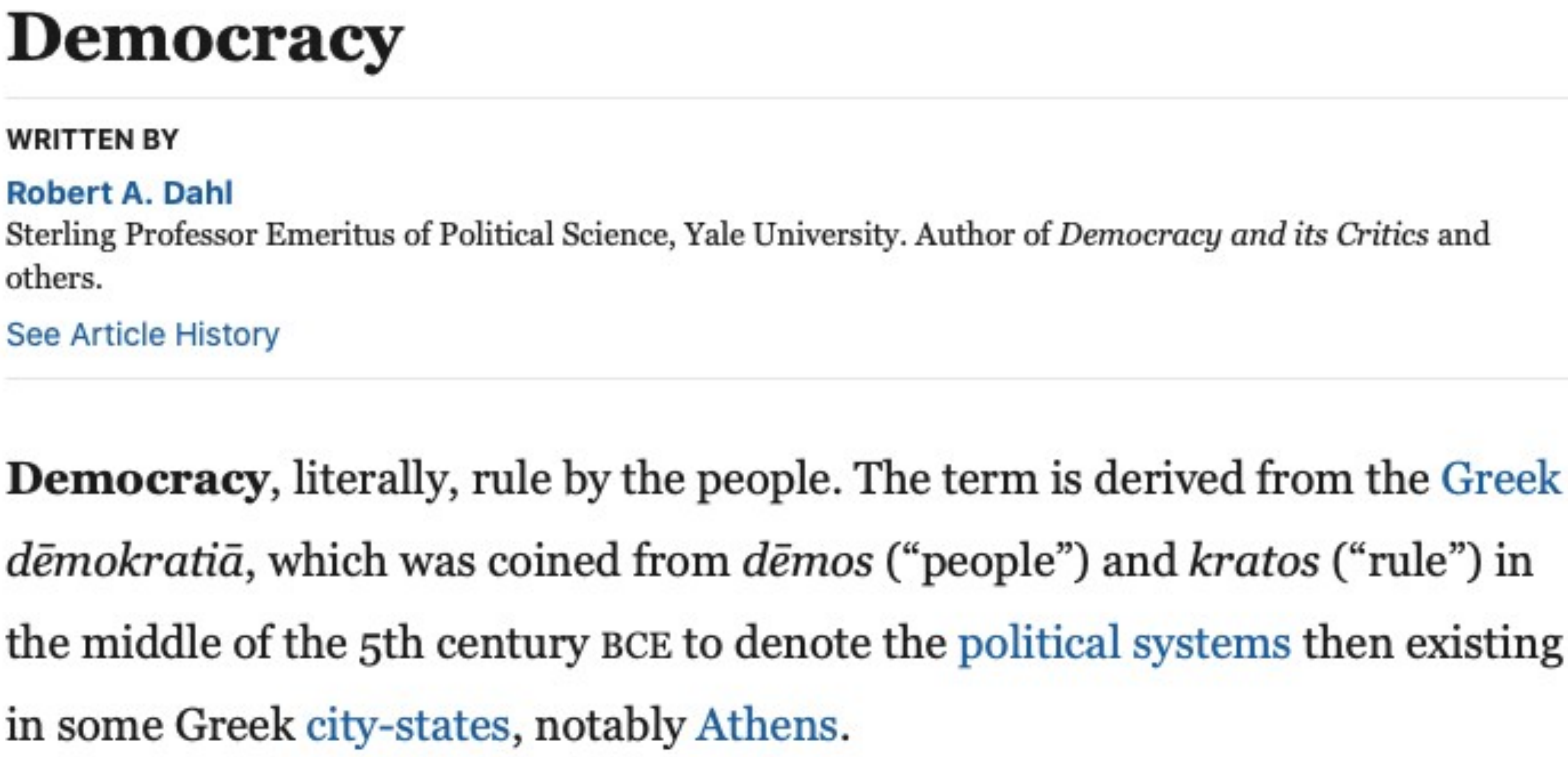


[Michalis Kountouris, Michael Cacoyannis Foundation]

Democracy’s Foundation is People

[Encyclopedia Britannica]

Democracy’s Foundation is People



Democracy

WRITTEN BY

Robert A. Dahl

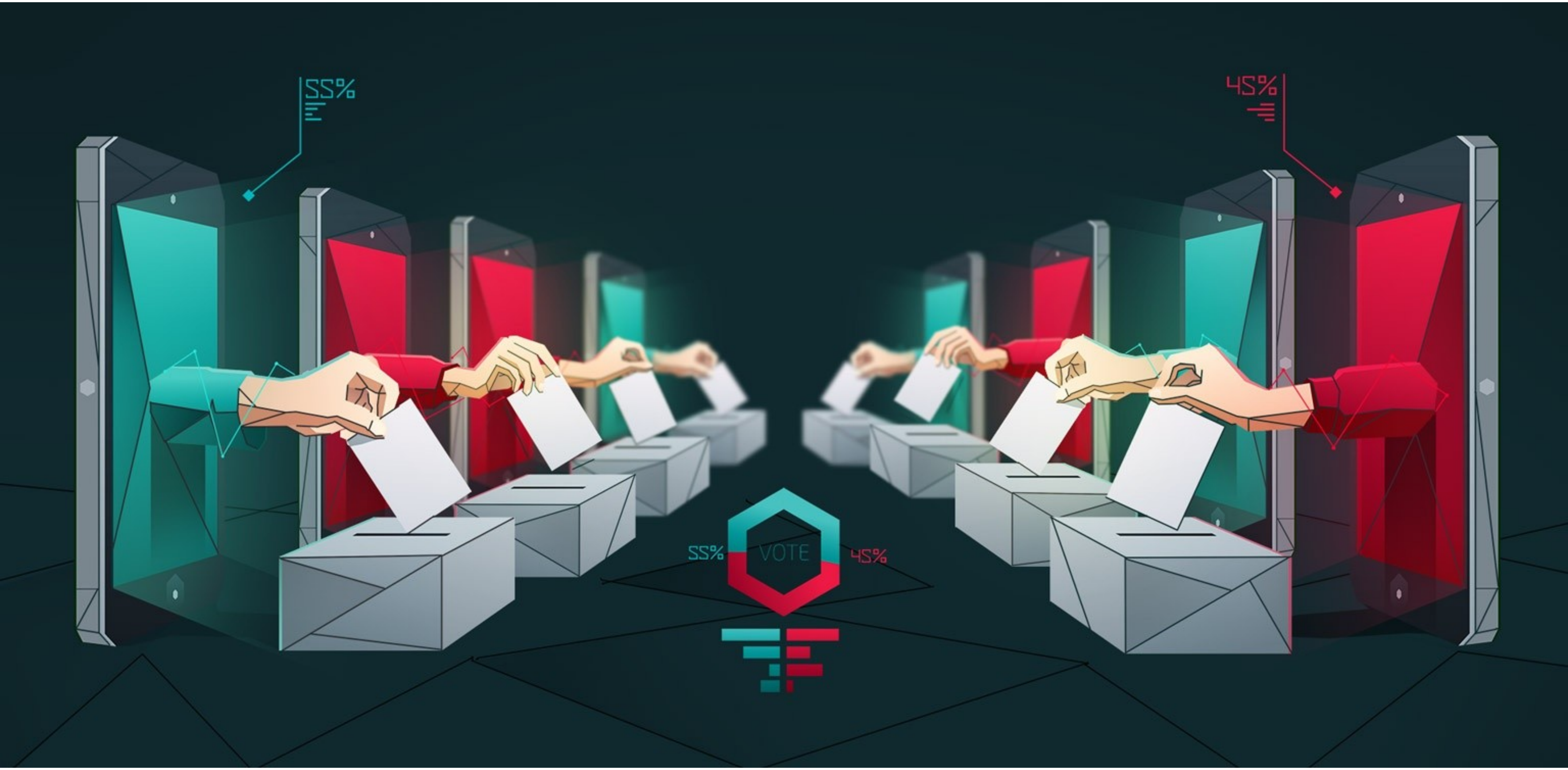
Sterling Professor Emeritus of Political Science, Yale University. Author of *Democracy and its Critics* and others.

See Article History

Democracy, literally, rule by the people. The term is derived from the Greek *dēmokratiā*, which was coined from *dēmos* (“people”) and *kratos* (“rule”) in the middle of the 5th century BCE to denote the political systems then existing in some Greek city-states, notably Athens.

[Encyclopedia Britannica]

Digital Democracy has a Problem…



[IBM/The Atlantic]

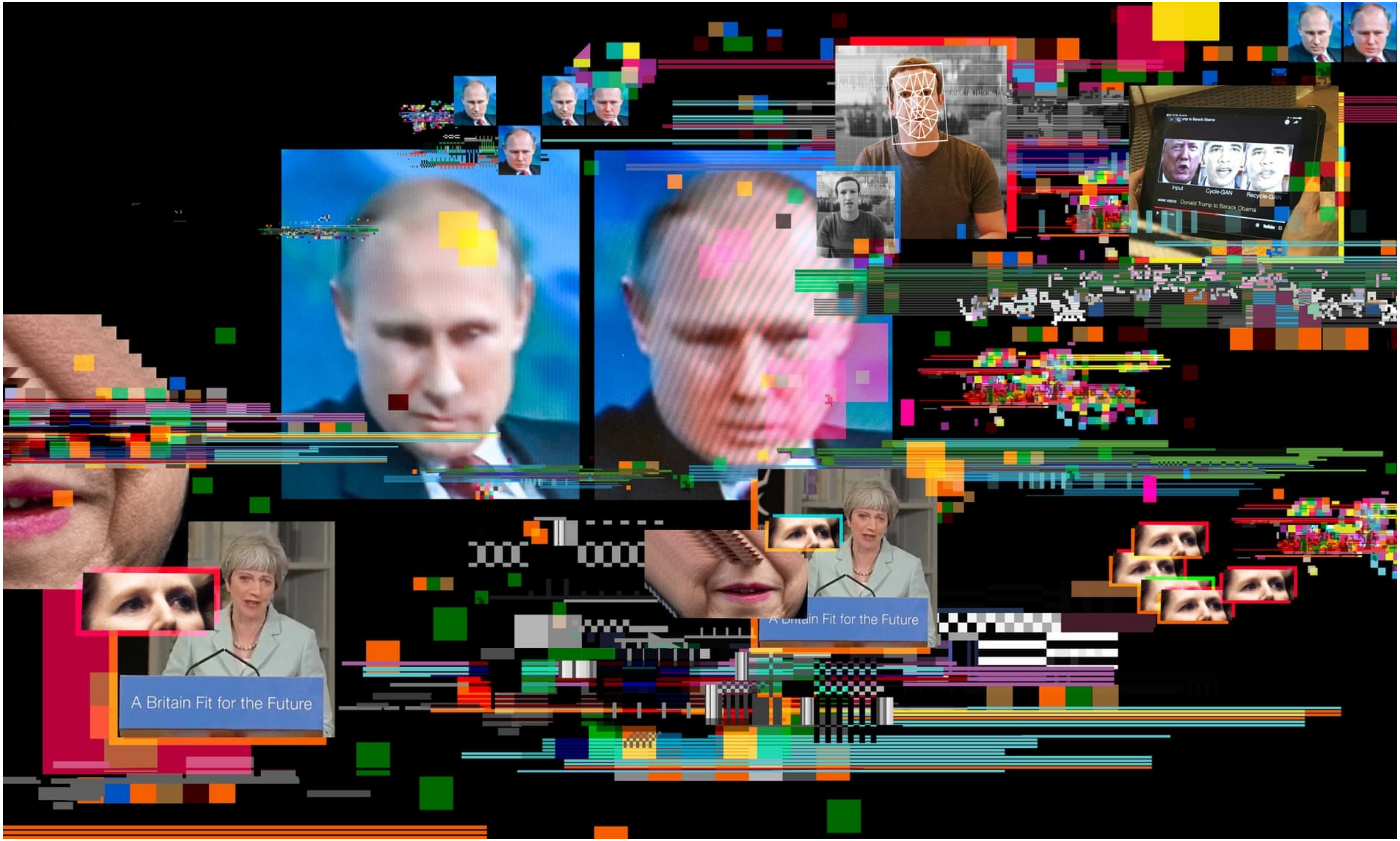
People are Physical, not Digital

[Marcus Feldthus]

People Aren’t Online, Only Profiles

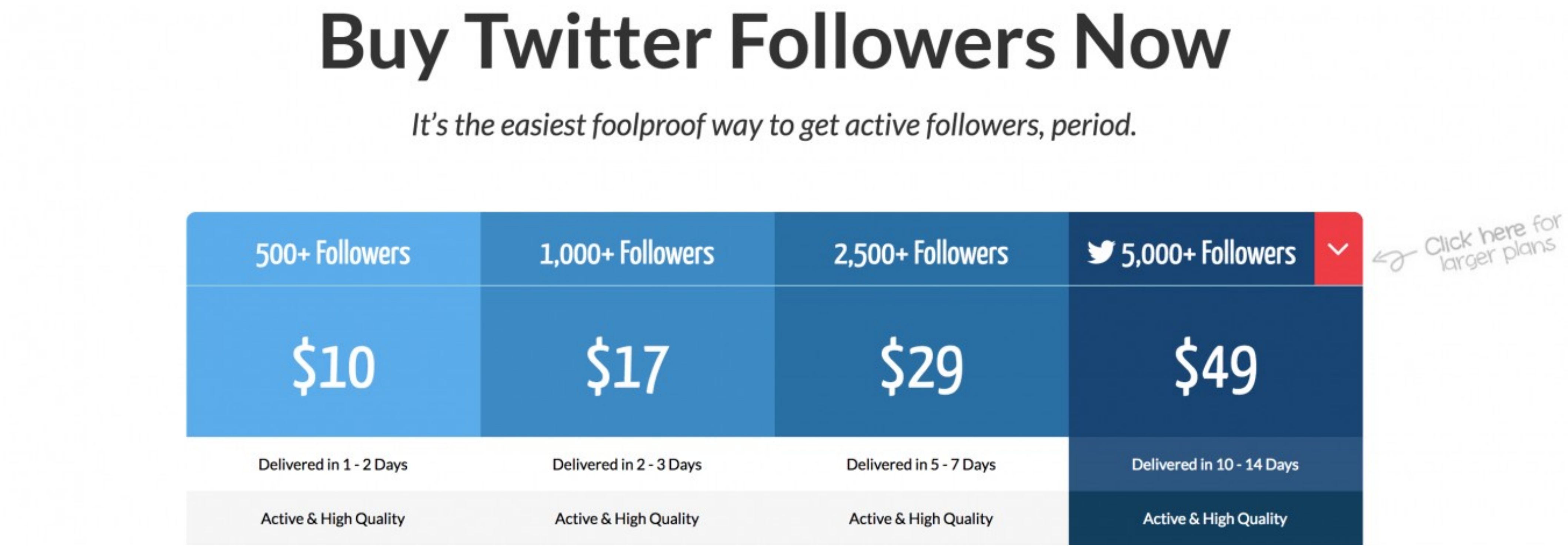
[Pixabay, The Moscow Times]

Online, the People are Fake


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

[Ian Sample, The Guardian]

Their 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

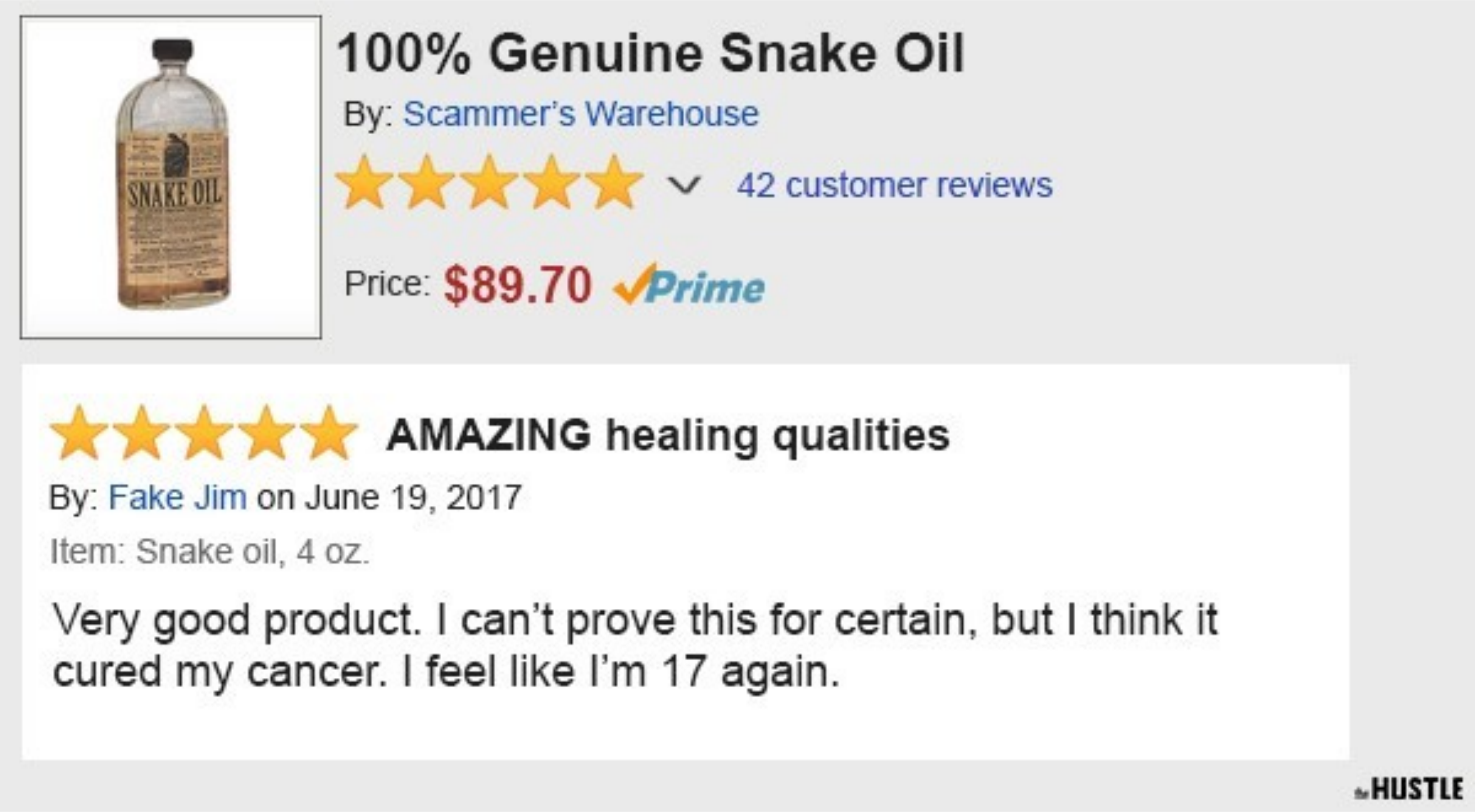
Click here for larger plans

[Ren LaForme, Poynter]

The News is Fake

[Krista Kennell, The Atlantic]

The Reviews are Fake



100% Genuine Snake Oil

By: Scammer's Warehouse

★★★★★ 42 customer reviews

Price: $89.70 ✓Prime

★★★★★ **AMAZING healing qualities**

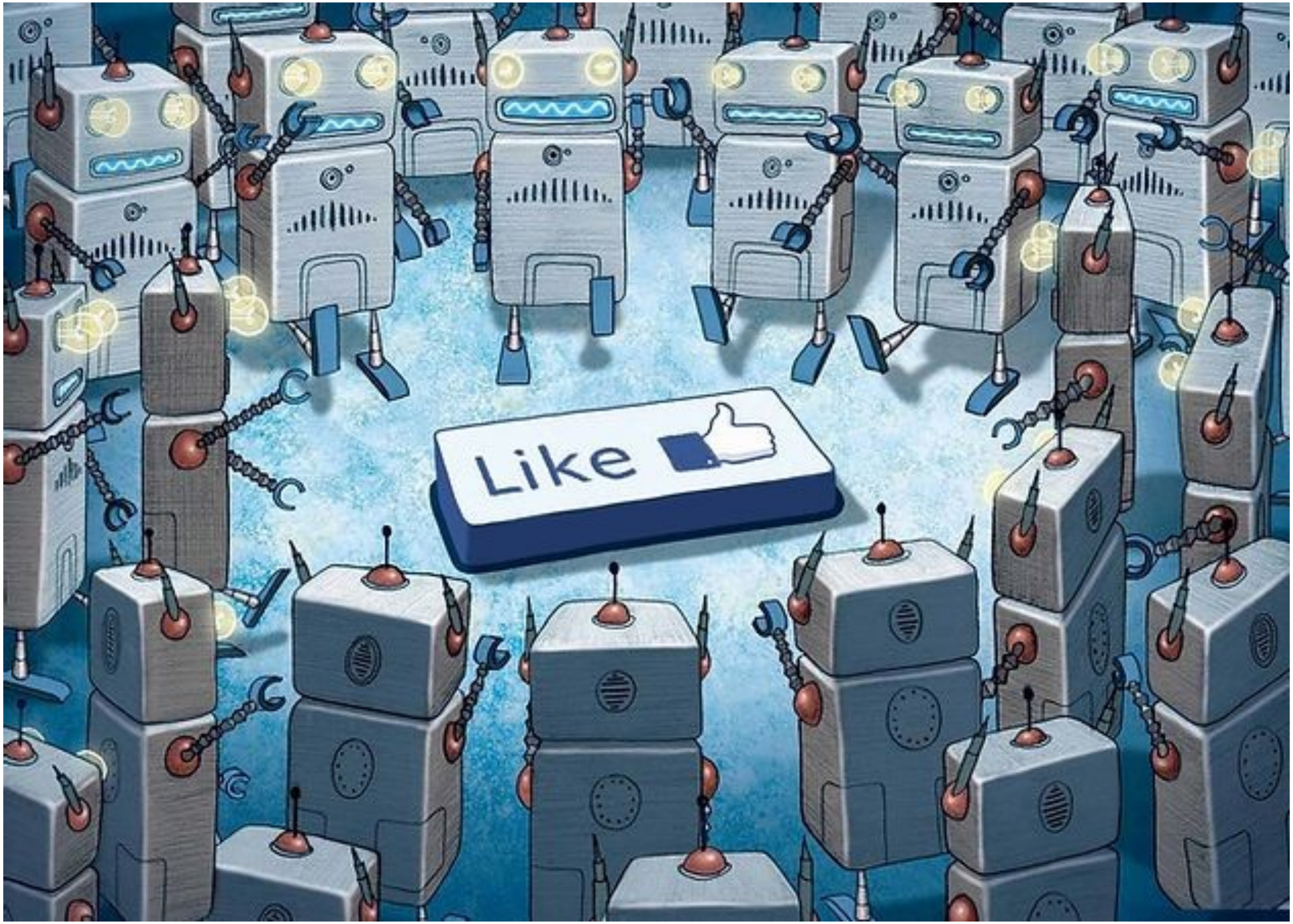
By: Fake Jim on June 19, 2017

Item: Snake oil, 4 oz.

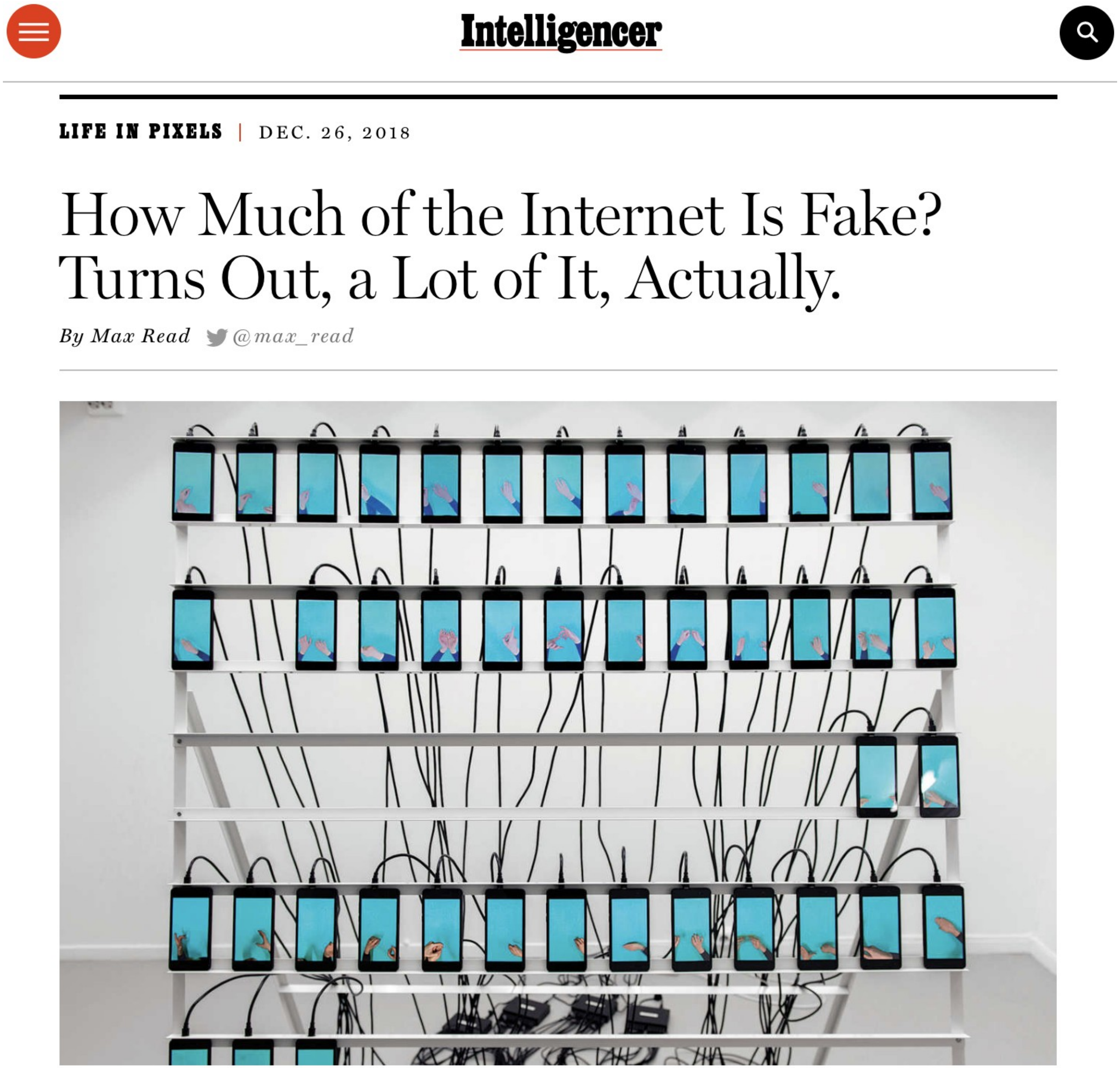
Very good product. I can't prove this for certain, but I think it cured my cancer. I feel like I'm 17 again.

[Mat Venn, Medium]

The Likes are Fake



[Rabbit Consulting Group]



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]

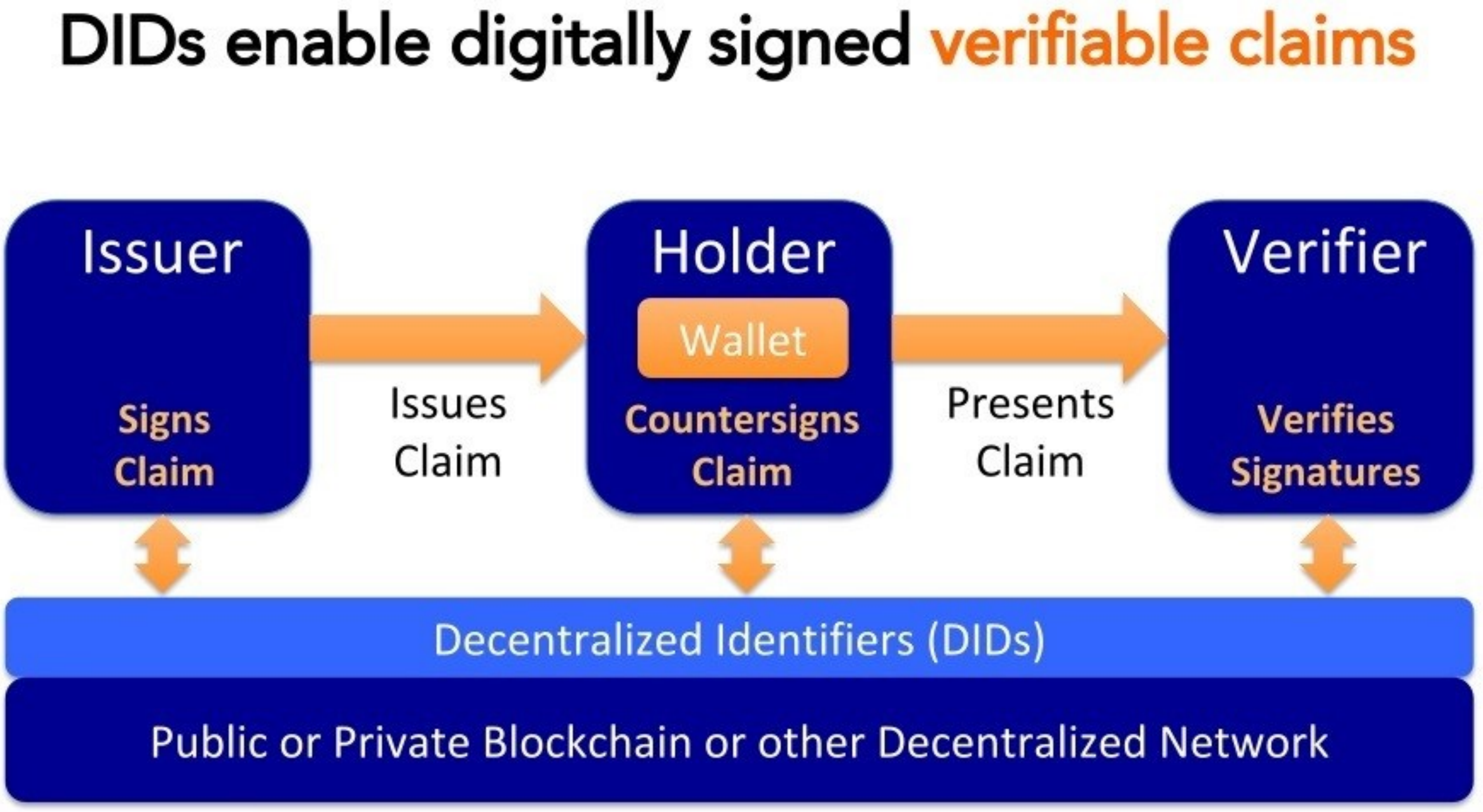
What Is the Missing Foundation?

[All About Healthy Choices]

Maybe Digital Identity – *Right?*

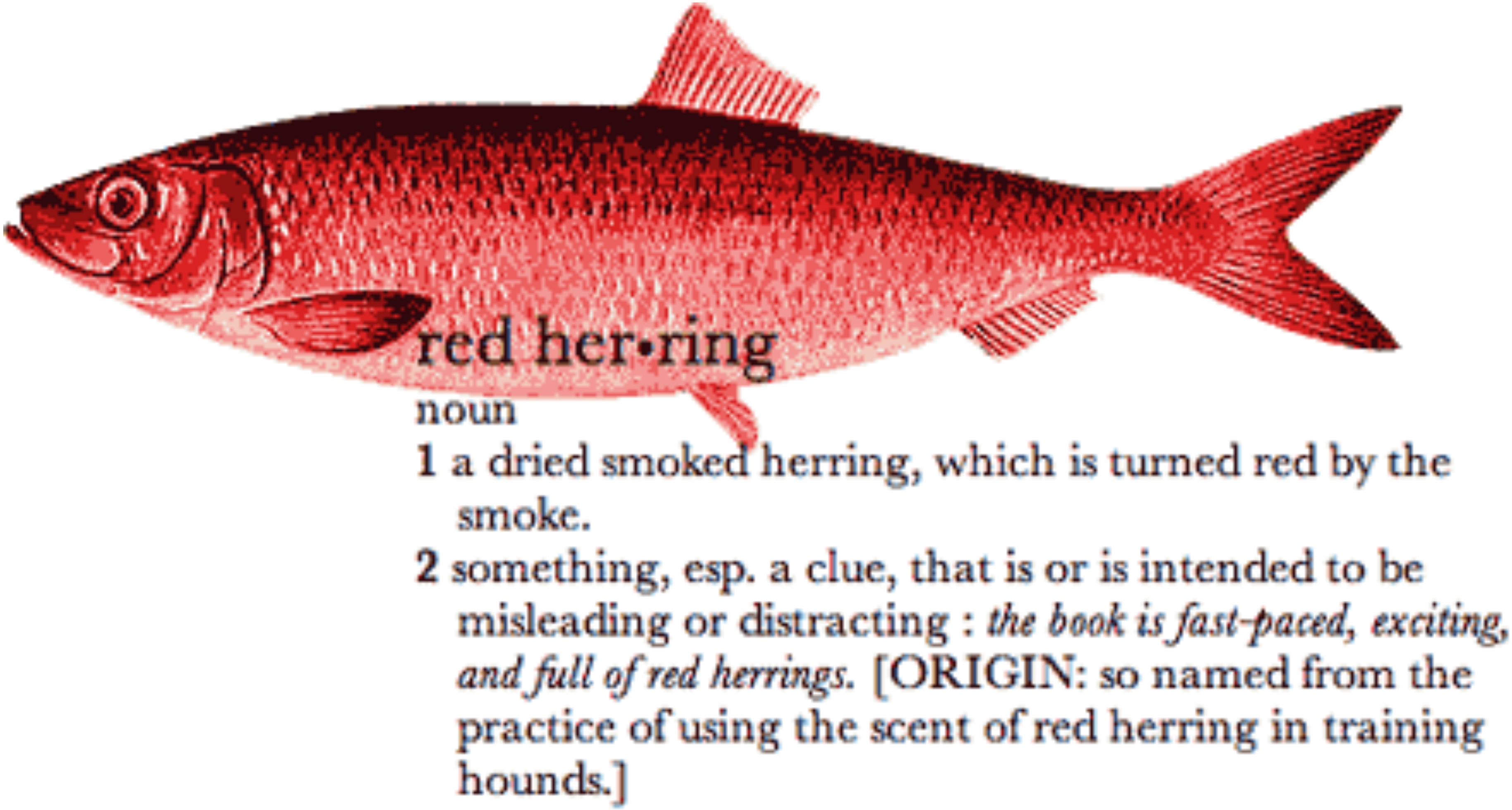
[UNCTAD]

Self-Sovereign Identity, Maybe?


DIDs enable digitally signed verifiable claims
Issuer
Signs Claim
Issues Claim
Holder
Wallet
Countersigns Claim
Presents Claim
Verifier
Verifies Signatures
Decentralized Identifiers (DIDs)
Public or Private Blockchain or other Decentralized Network

[Wikipedia]

Digital Identity is a Red Herring



red her•ring

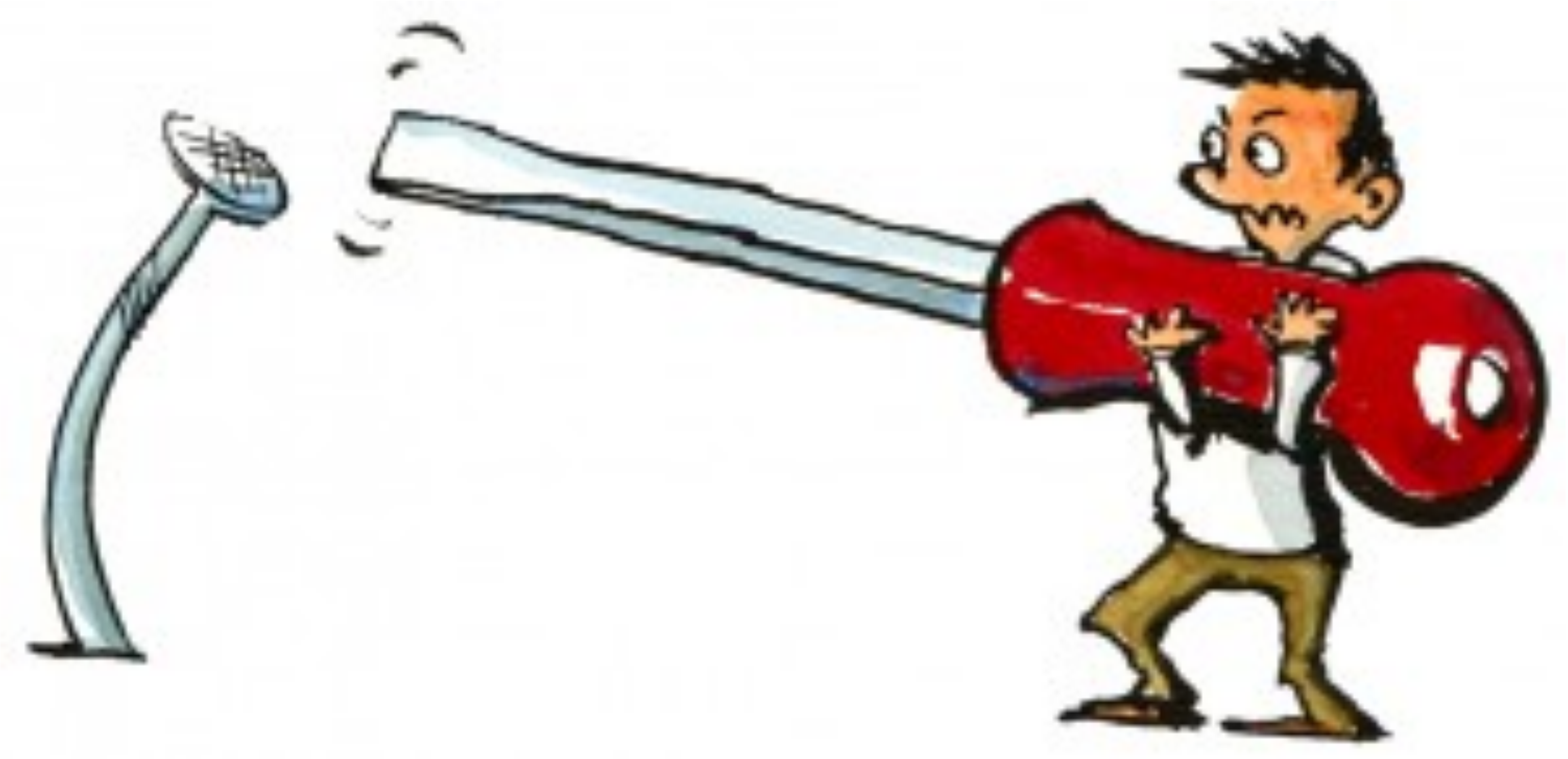
noun

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]

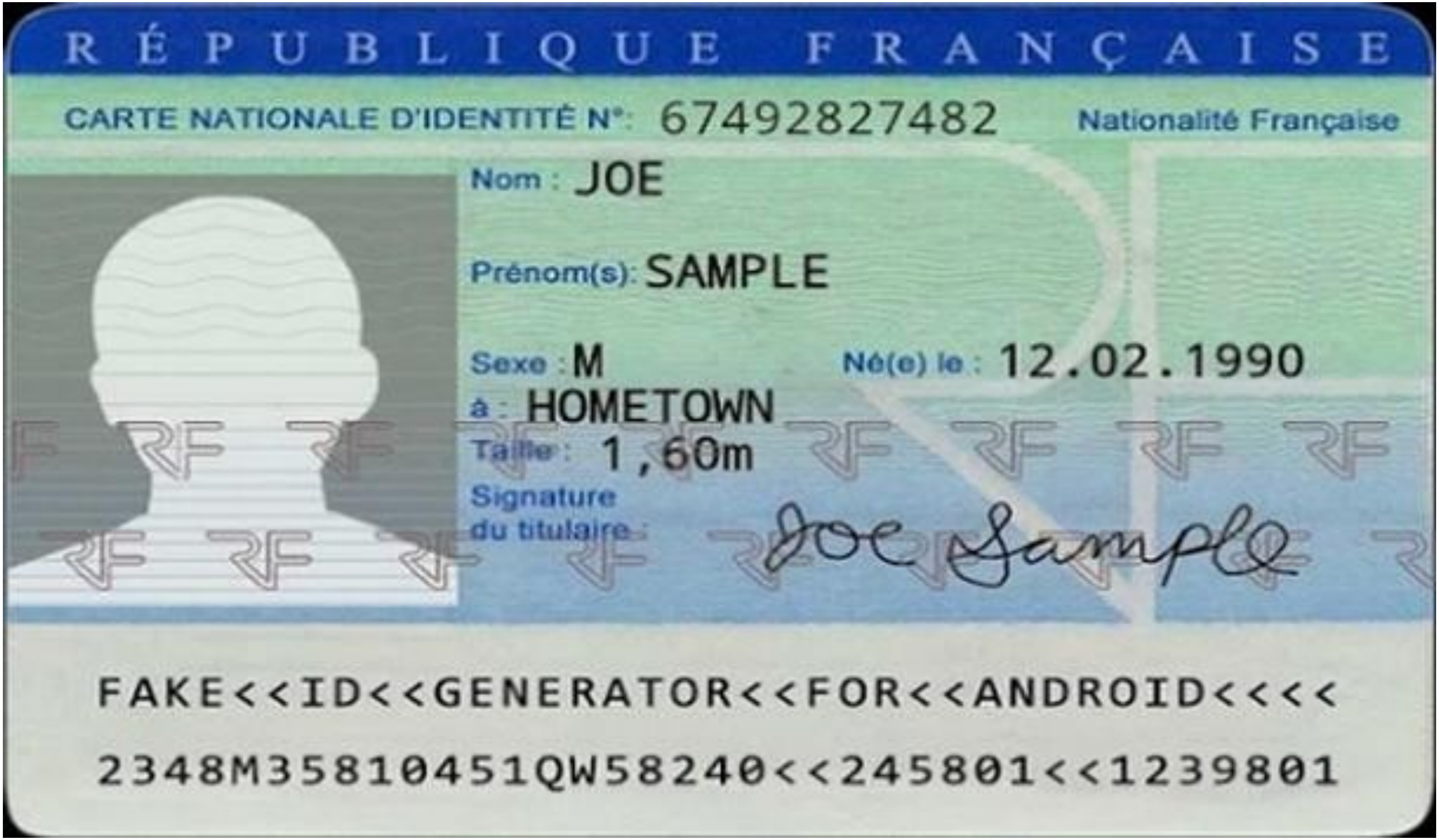
In Democracy, All People are Equal

[Tricentis]

Profiles Distinguish & Divide People

[Tom Perrett, Arkbound]

ID Documents are Forgeable



RÉPUBLIQUE FRANÇAISE

CARTE NATIONALE D'IDENTITÉ N°: 67492827482 Nationalité Française

Nom : JOE

Prénom(s): SAMPLE

Sexe : M Né(e) le : 12.02.1990

à : HOMETOWN

Taille : 1,60m

Signature du titulaire : Joe Sample

FAKE<<ID<<GENERATOR<<FOR<<ANDROID<<<<

2348M35810451QW58240<<245801<<1239801

[Android Fake ID Card Creator]

All IDs Can Be Lost, Stolen

[Andrés Aneiros]

ID Demands Exclude People

REFUGEES
TREATING REFUGEES AS THE PROBLEM IS THE PROBLEM
NO HUMAN BEING IS ILLEGAL

[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]

Proof of Personhood

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

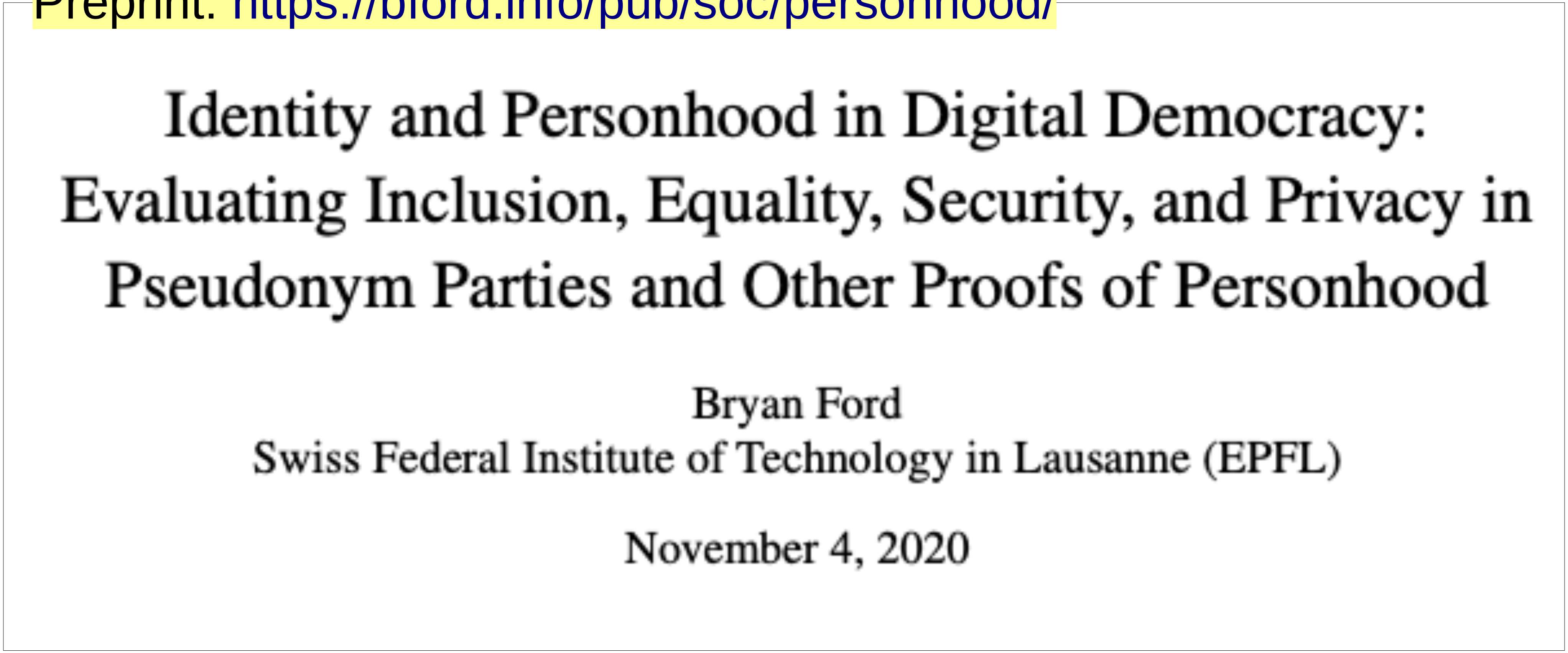
- For online forums, voting, deliberation, …

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

A Few Broad Approaches

Proofs of Identity

- ID documents, biometrics, self-sovereign ID

Proofs of Investment

- CAPTCHA, proof of work, proof of stake

Proofs of Personhood

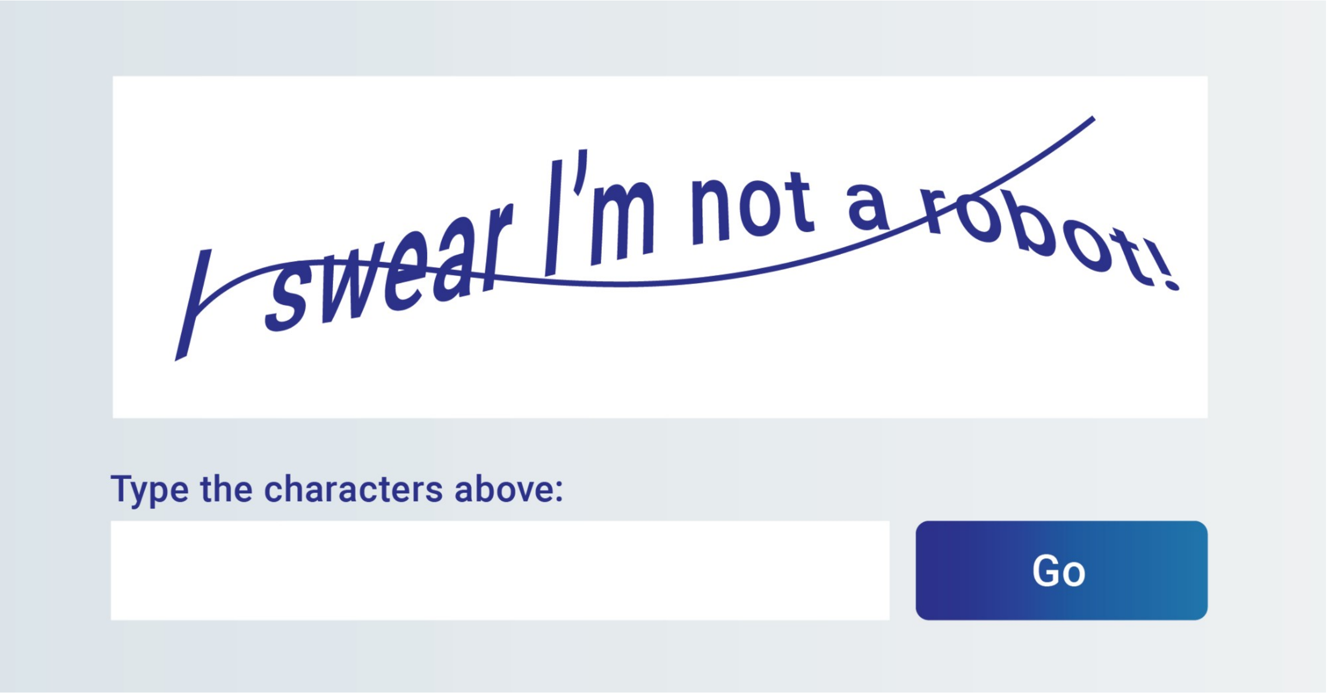
- Pseudonym parties – online or offline

Why not Proofs of Investment?

They’re 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**"

Proofs of Personhood

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

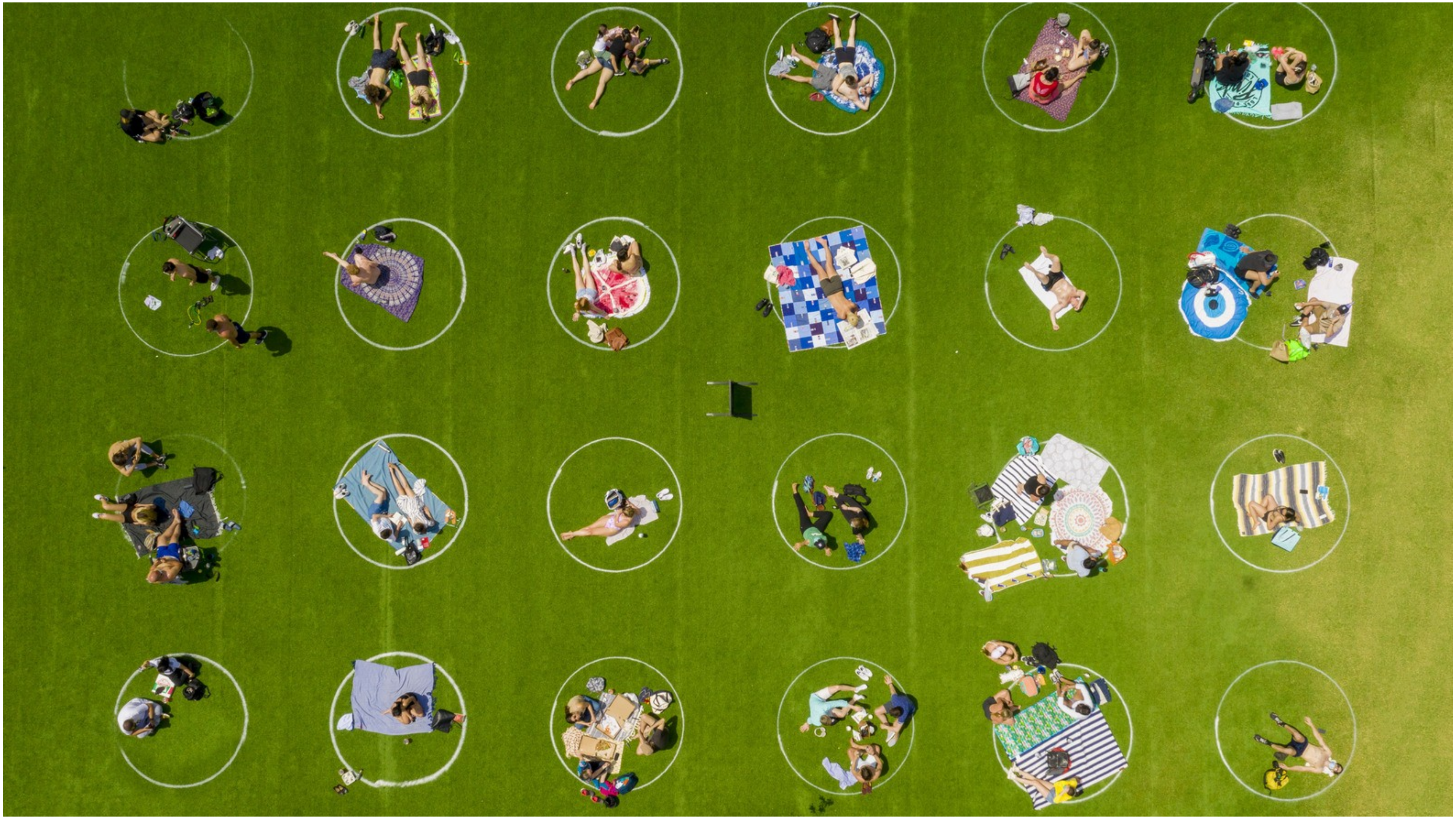
- Pseudonym Parties [Ford, 2008]
- Encointer [Brenzikofer, 2018]
- BrightID [Sanders, 2018]
- Duniter [2018]
- Idena [2019]
- HumanityDAO [Rich, 2019]
- Pseudonym Pairs [Nygren, 2019]

Pseudonym Parties

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

Pseudonym Parties

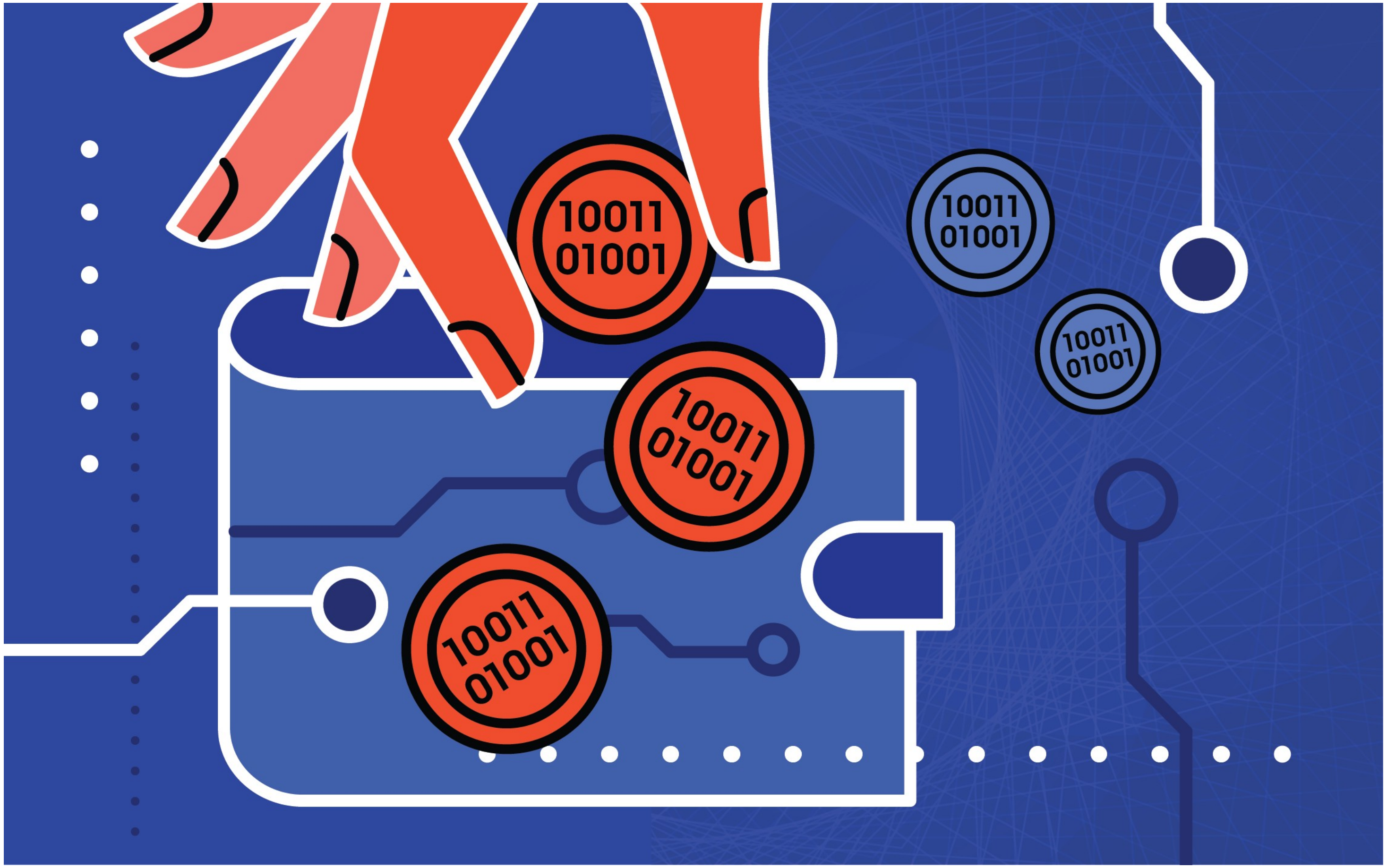
…perhaps spread out a bit more in current times



[ArchDaily]

Pseudonym Parties

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

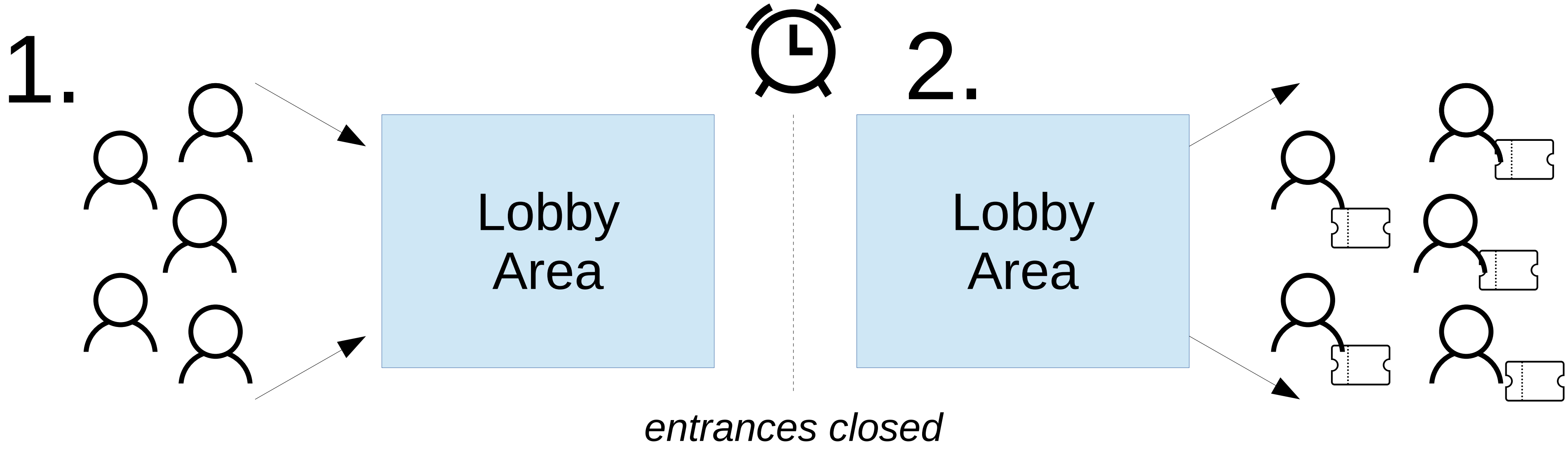


[gov.sg]

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*

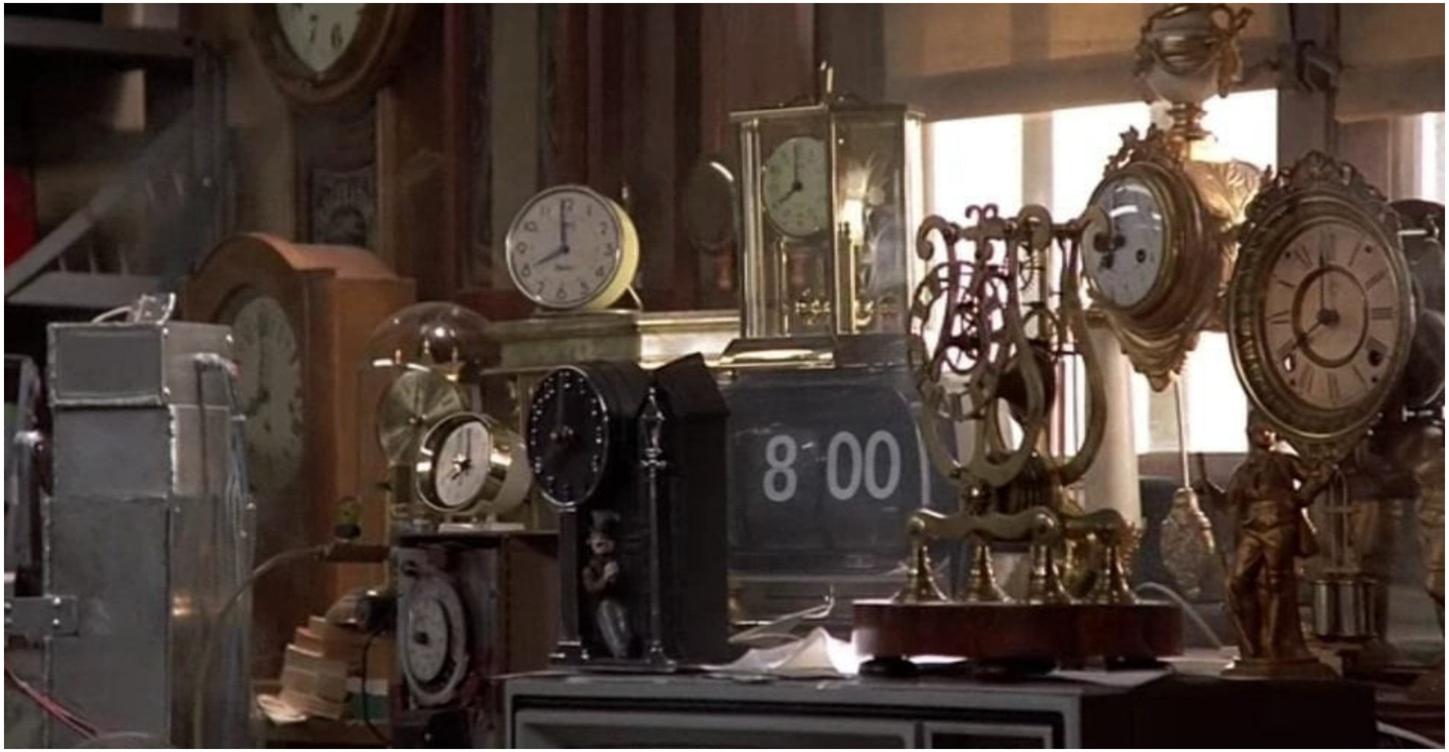


entrances closed

Regular Synchronized Events

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

- No one can physically attend two at once



Using PoP tokens

Between events, attendees might use tokens for

- Voting in online governance & deliberation
- Bypassing CAPTCHAs in online services
- Minting “basic income” in UBI cryptocurrency

Platforms might use PoP tokens for

- Counting only *unique humans* in likes, followers
- Allowing anonymous but accountable access

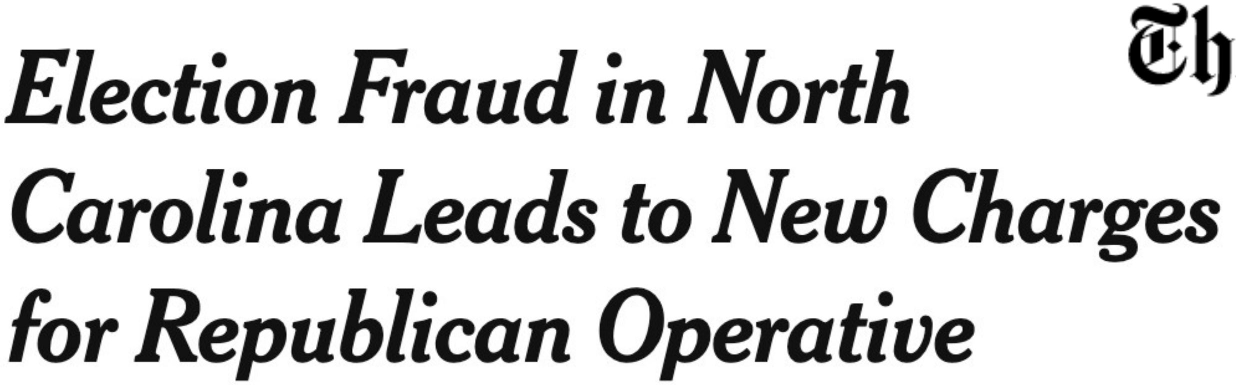
The Coercion, Vote-Buying Problem

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

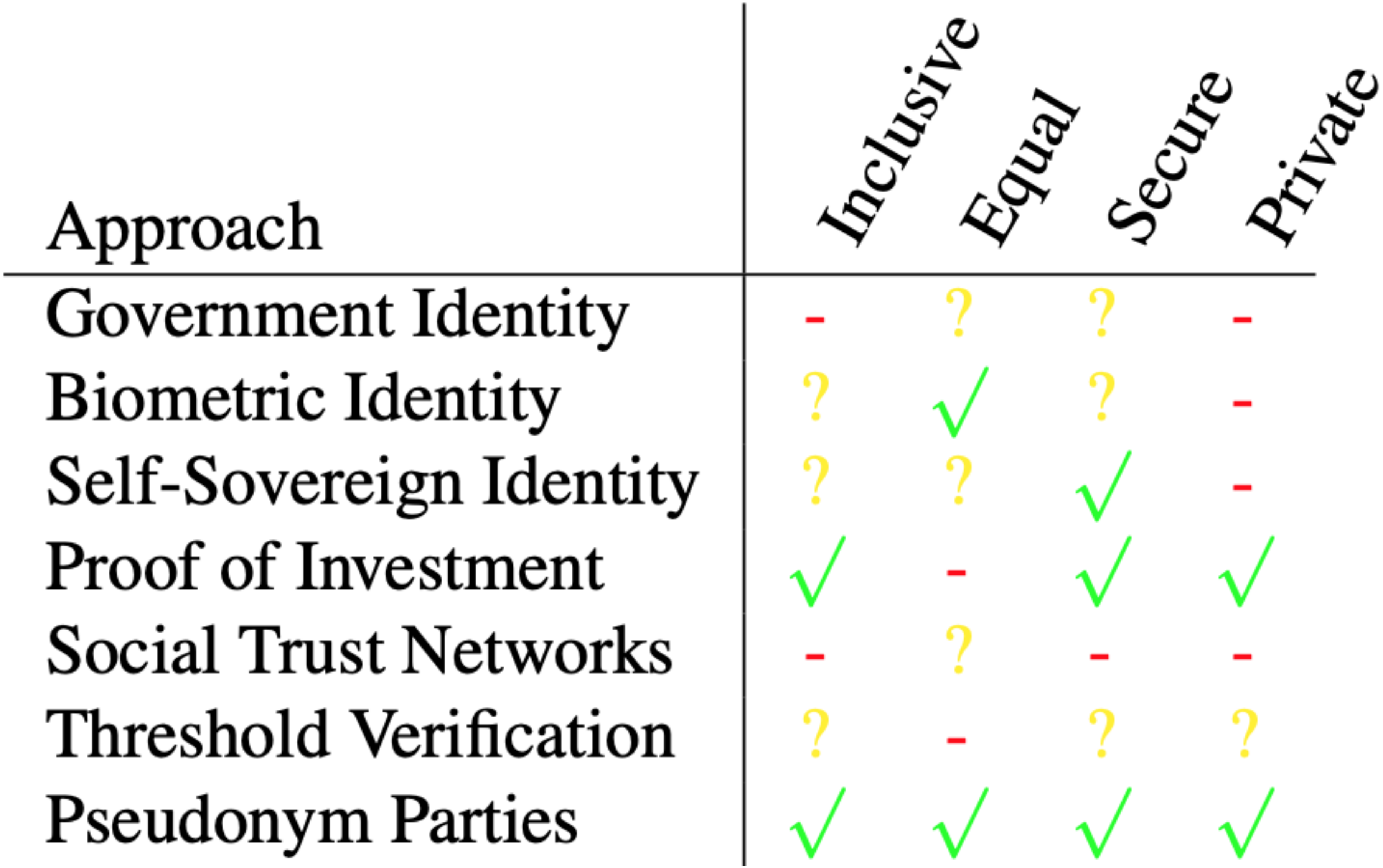
[Liz Sablich, Brookings]

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

Summary of Alternatives

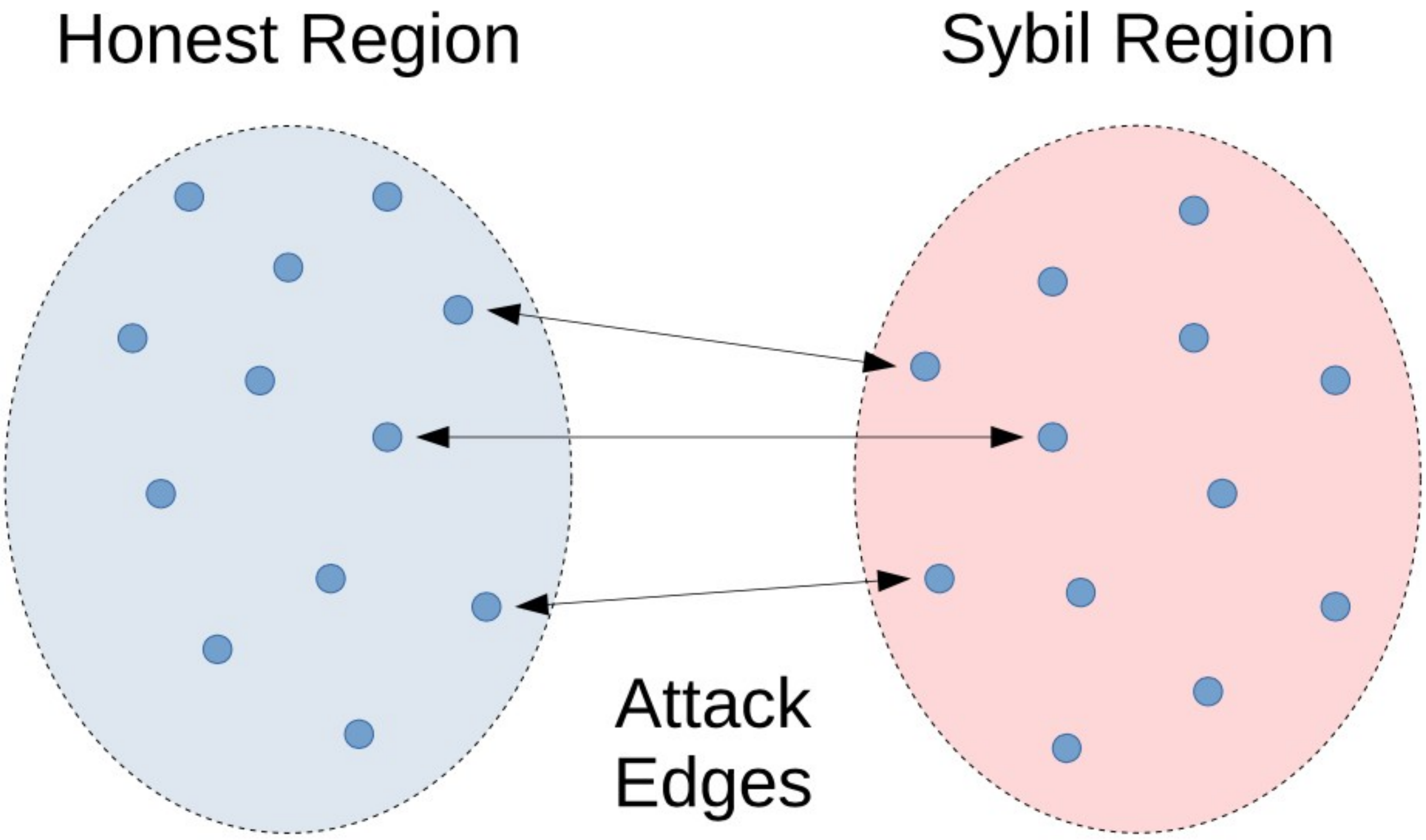


Approach	Inclusive	Equal	Secure	Private
Government Identity	-	?	?	-
Biometric Identity	?	√	?	-
Self-Sovereign Identity	?	?	√	-
Proof of Investment	√	-	√	√
Social Trust Networks	-	?	-	-
Threshold Verification	?	-	?	?
Pseudonym Parties	√	√	√	√

Social Trust Verification

Detect fake identities by social graph analysis

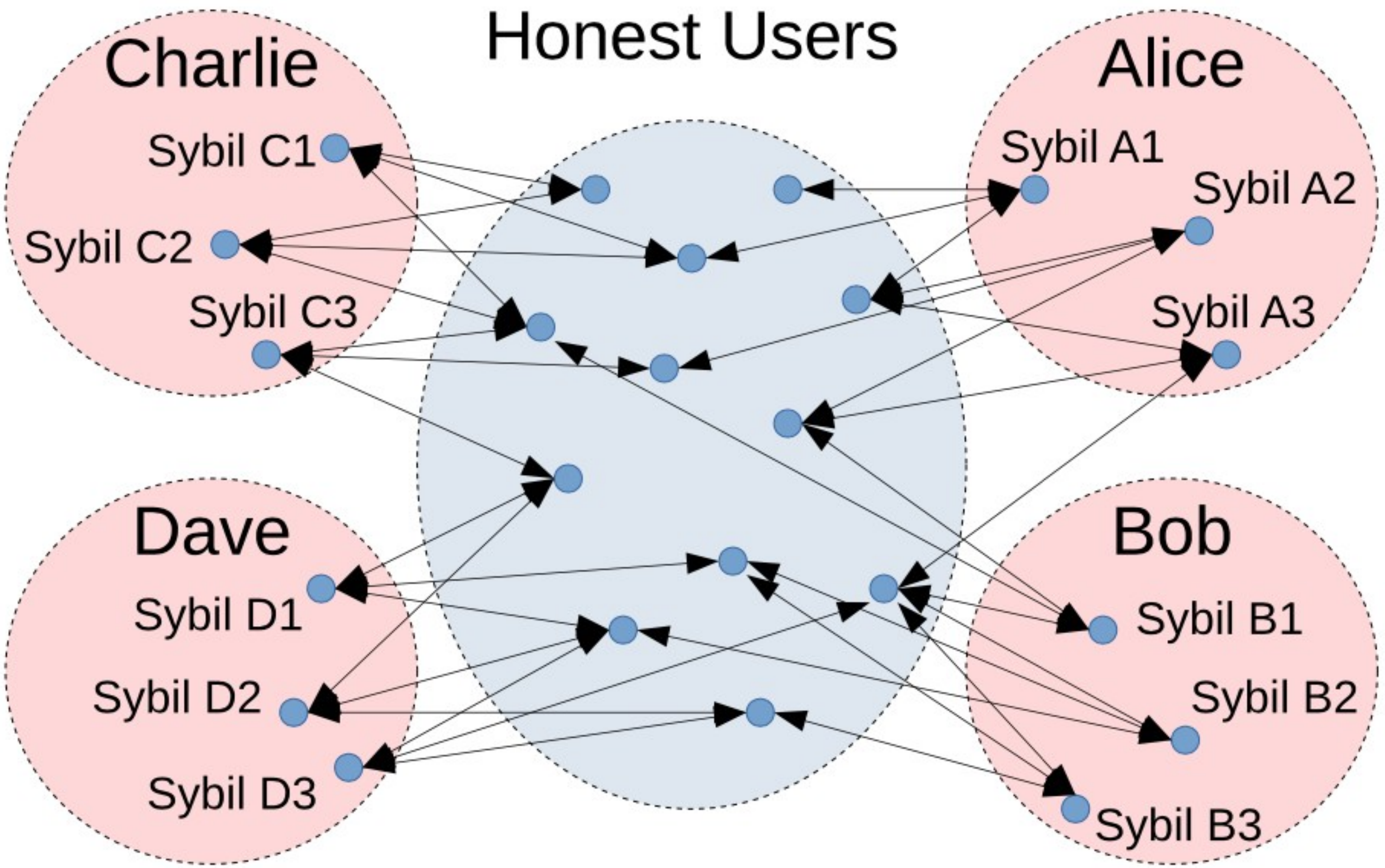
- Addresses one particular **Sybil region** attack…



Social Trust Verification

Detect fake identities by social graph analysis

- …but not other realistic scenarios, like this:



Threshold Identity Verification

Assign groups of identities to verify each other

[encointer]

Threshold Identity Verification

Unfortunately, attackers can hire “minions” to help

- From elastic hiring services like TaskRabbit
- Needs fewer minions than Sybil identities
- Attacker’s advantage grows until takeover

[Hans Haput, Vamers]

Public Spaces Key to Digital Spaces?

Occasional **public** events in **public** spaces may enable and secure our **digital online** spaces

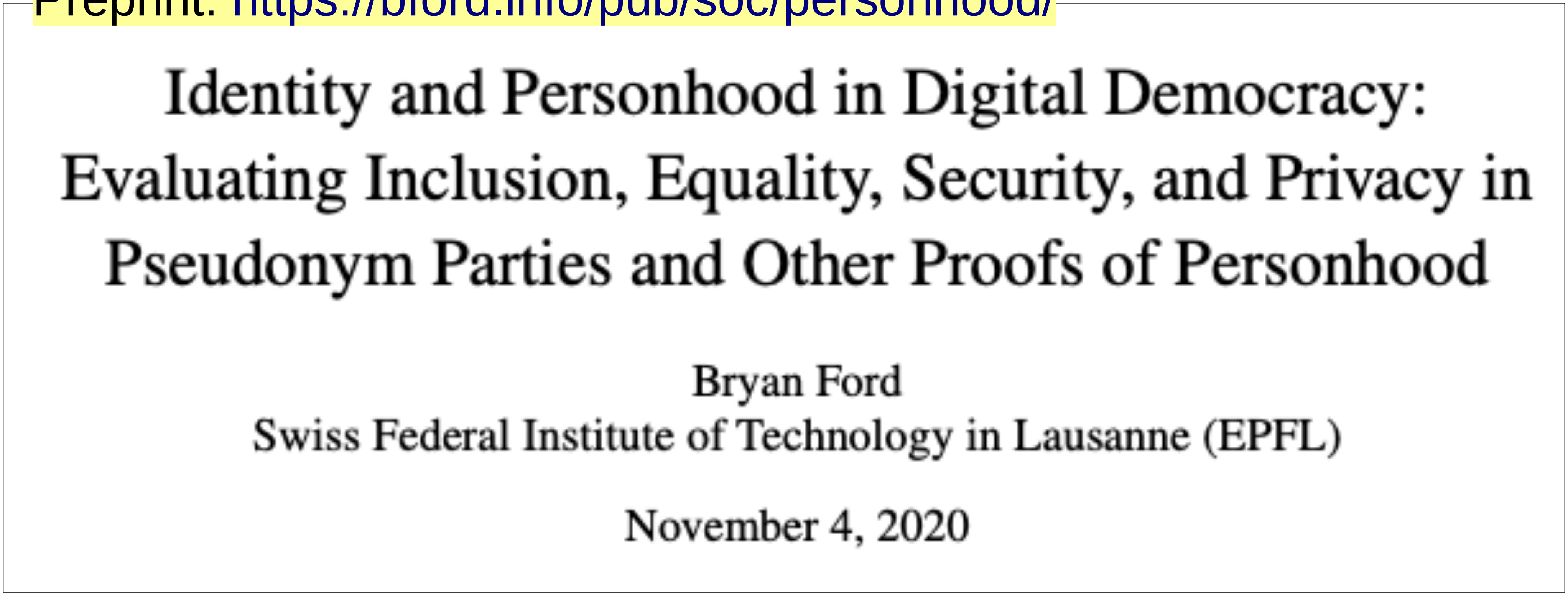
- Many questions and challenges remain

Conclusion

Digital democracy needs proof of personhood

- Must be **inclusive**, **equal**, **secure**, **private**
- Pseudonym parties & others being developed

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