Massachusetts Institute of Technology

Coercion-Resistant E-voting and Proof of Personhood

Louis-Henri Merino, …, Bryan Ford
Decentralized and Distributed Systems (DEDIS)
dedis@epfl.ch – dedis.epfl.ch

IC3 Winter Retreat – January 6, 2025

We’re facing **hard global** problems

Climate change

Exploding inequality

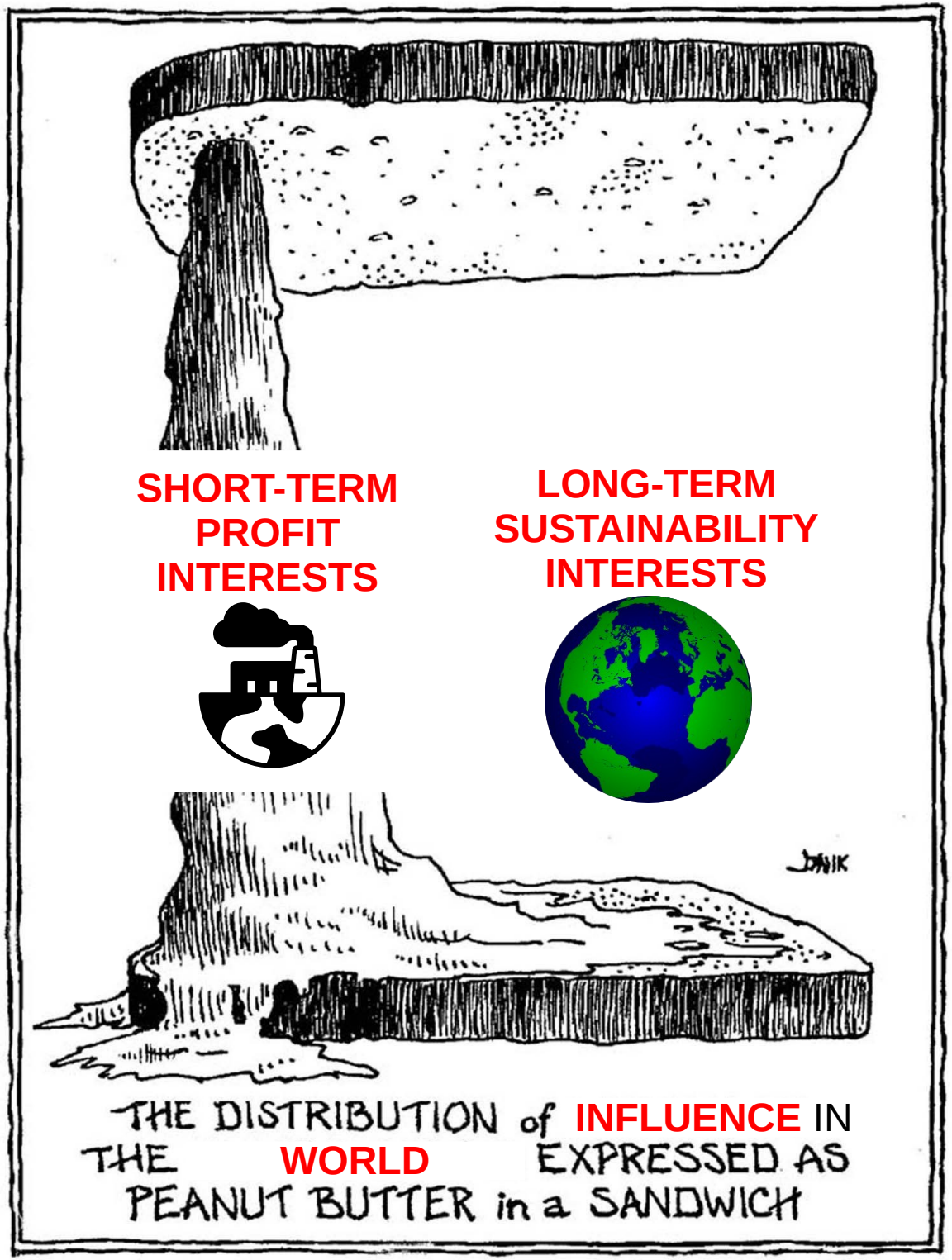
Global problems need global tools

Like **decentralized systems** … *right?*

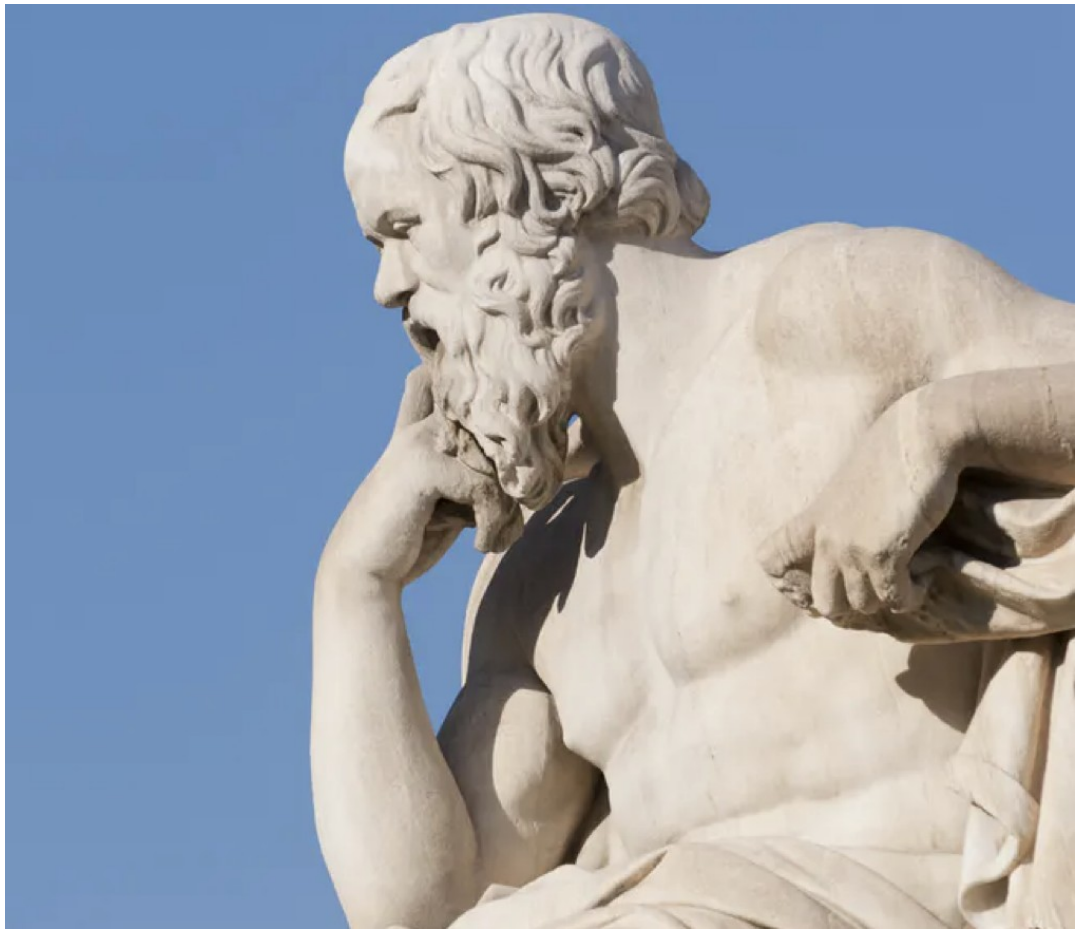
A fundamental meta-problem

“Money is power”

Real solutions can’t win votes dominated by entrenched power



Could decentralized systems…



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 & security represent *everyone's* interests

Decentralized digital democracy?

Will decentralized online systems ever be able to **self-govern** in an egalitarian, democratic fashion?

[Kenneth Hacker, The Progressive Post]

Towards a global town hall

Key requirements for *democratic decentralization*:

- 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*

Talk Outline

- **Towards democratic decentralization**
- Proof of personhood: one person, one vote
- The coercion problem in E-voting and PoP
- TRIP: in-person [fake] credential issuance
- Usability of TRIP and fake credentials
- Conclusion and ongoing/future work

Talk Outline

- Towards democratic decentralization
- **Proof of personhood: one person, one vote**
- The coercion problem in E-voting and PoP
- TRIP: in-person [fake] credential issuance
- Usability of TRIP and fake credentials
- Conclusion and ongoing/future work

Who gets how much influence?

Wealth-centric

- One dollar, one vote

[Kera]

Person-centric

- One person, one vote

[Verity Weekly]

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!

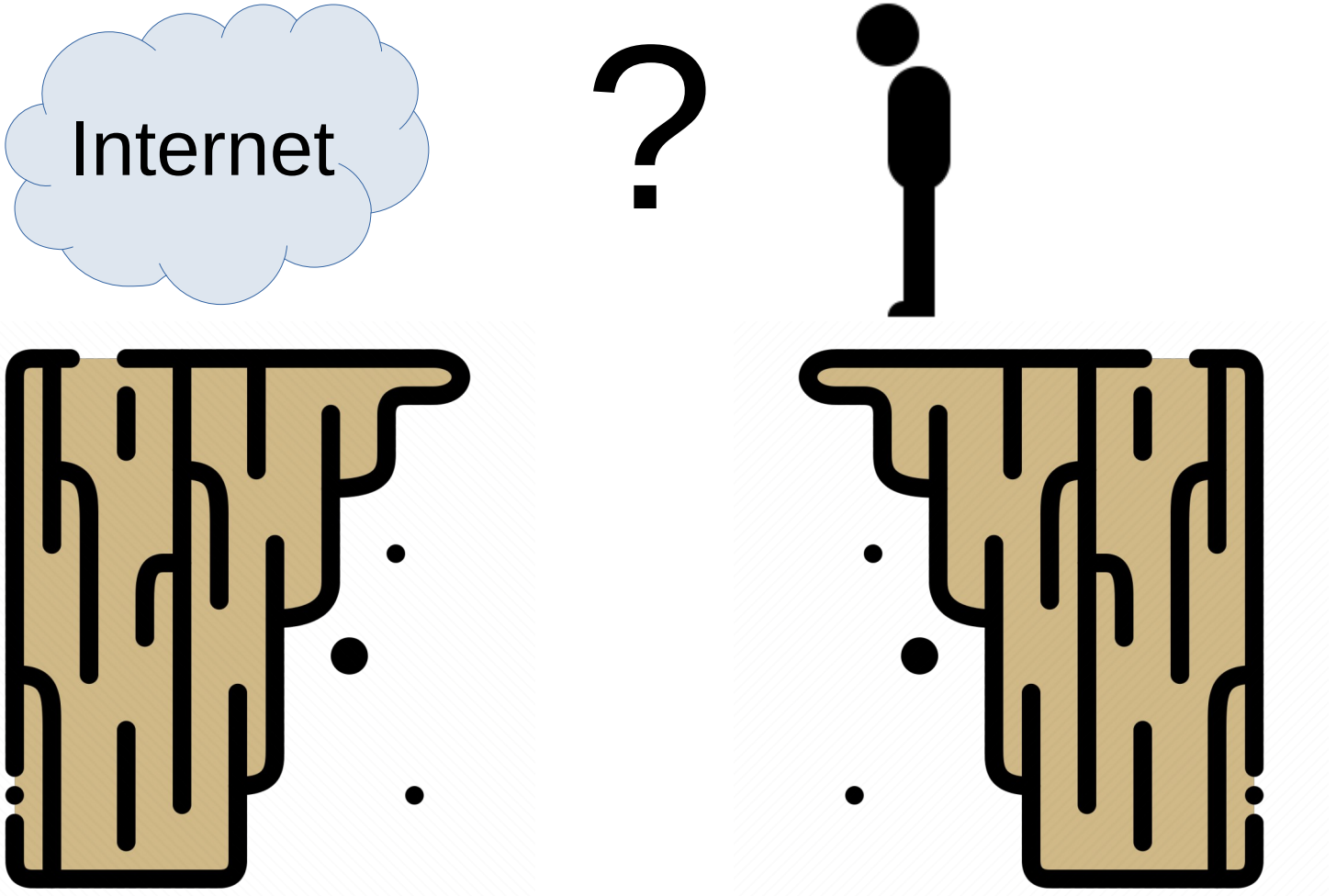
Person-centric

No guarantee
of success, but…

No other plausible
option to get
global buy-in

A Fundamental Problem

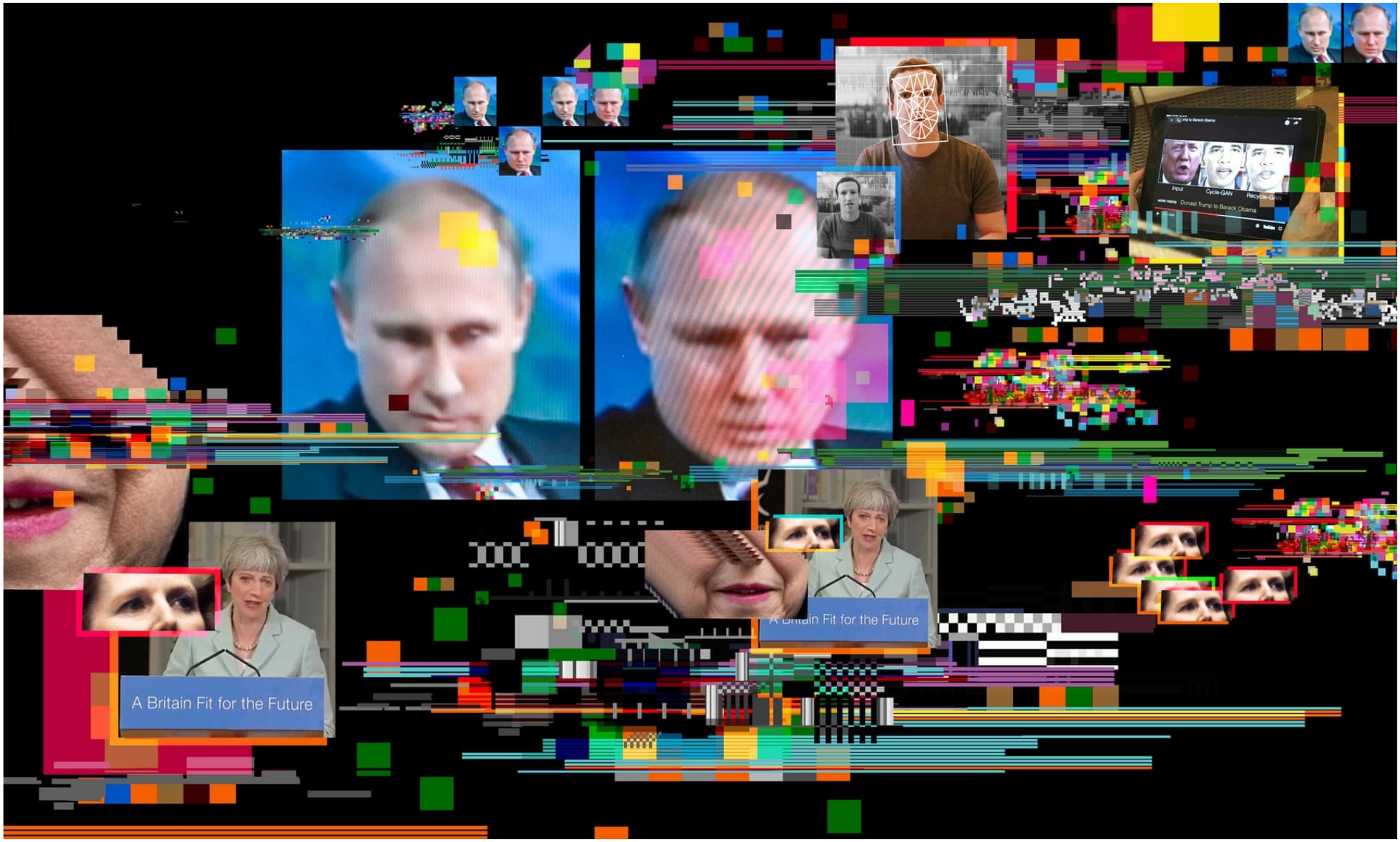
Today’s Internet doesn’t know what a “person” is



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*

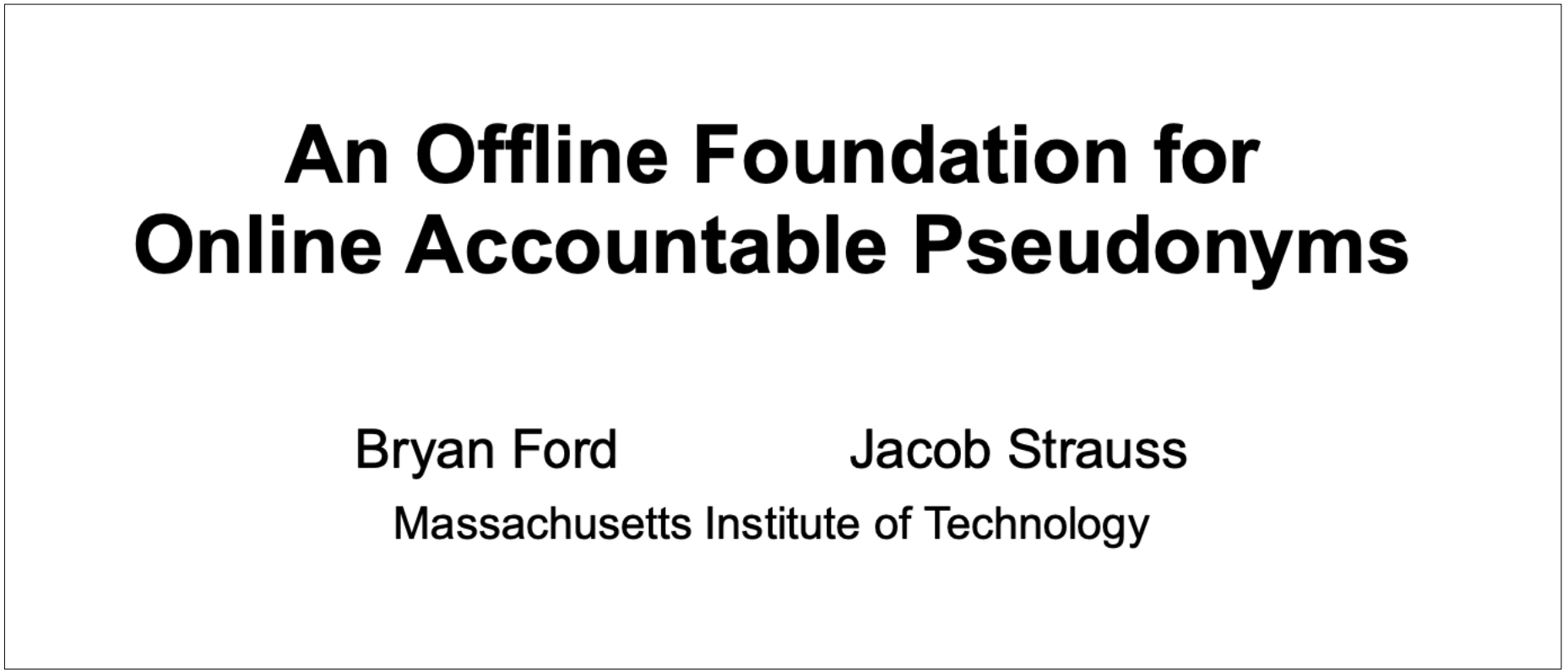
> “We must act to ensure that technology is designed and developed to serve humankind, and not the other way around”
>
> - Tim Cook, Oct 24, 2018

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]

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

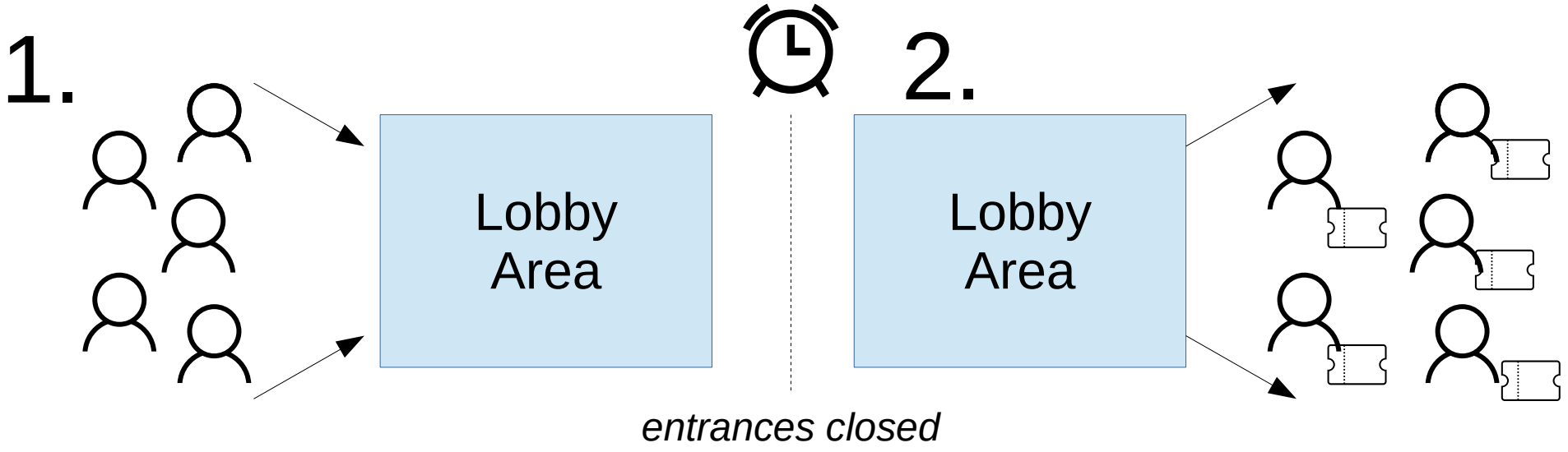
Bryan Ford Jacob Strauss

Massachusetts Institute of Technology

PoP based on physical presence

Principle: real people have only one body each

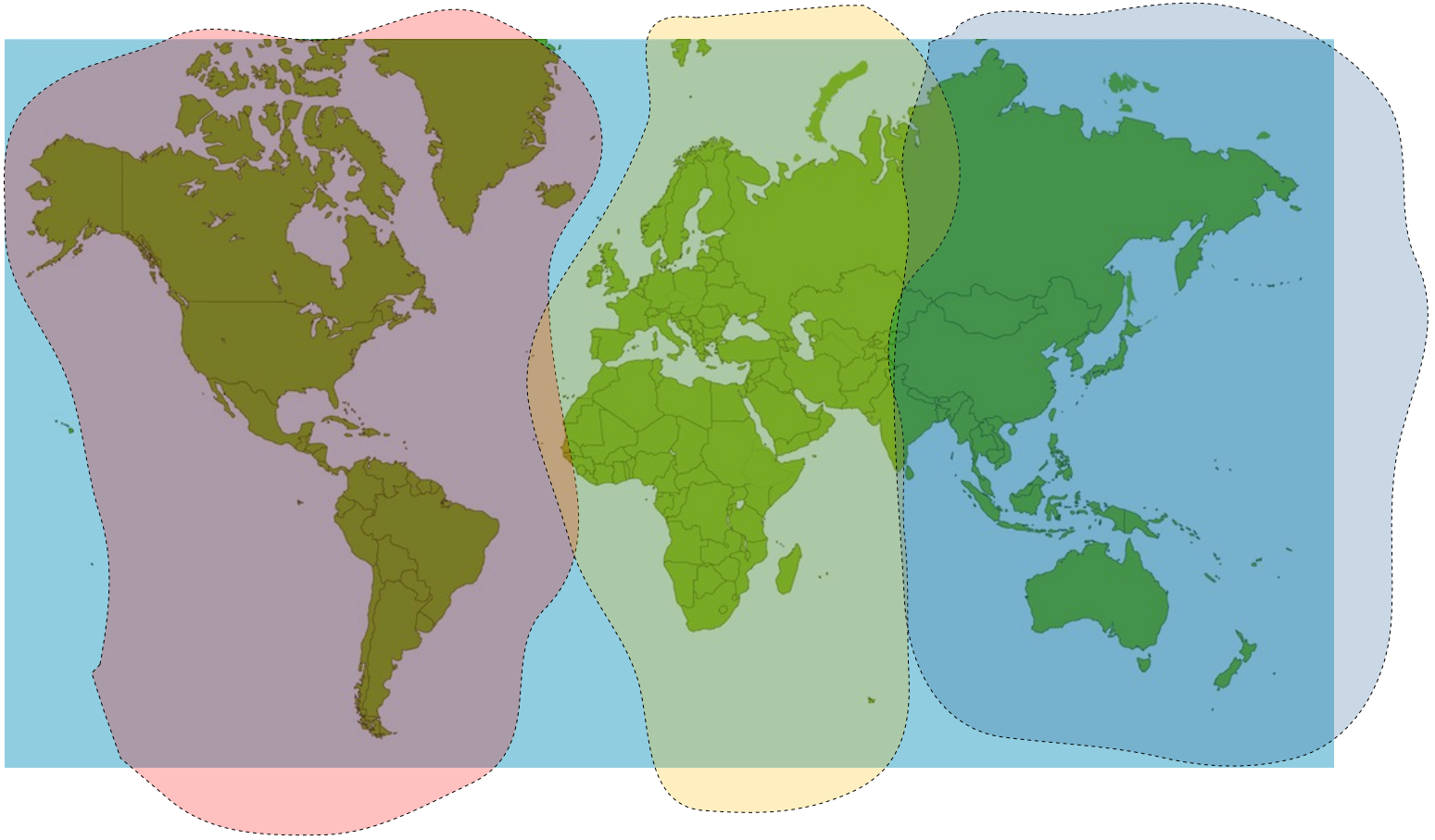
- Attendees gather in “lobby” area by a deadline
- At deadline: doors close, *no one else gets in*
- Each attendee gets one token when *leaving*



Scalable via *simultaneous* events

Potentially at many grassroots-organized events

- Even globally, in a few “timezone federations”



Some real-world precedents

People already show up regularly to concerts…

[xinhuanet]

Some real-world precedents

…political rallies and protests…

[pixabay]

Some real-world precedents

…festivals…

Some real-world precedents

…church services and other religious events…

…usually for no, or *negative*, financial reward!

A few Proof of Personhood efforts

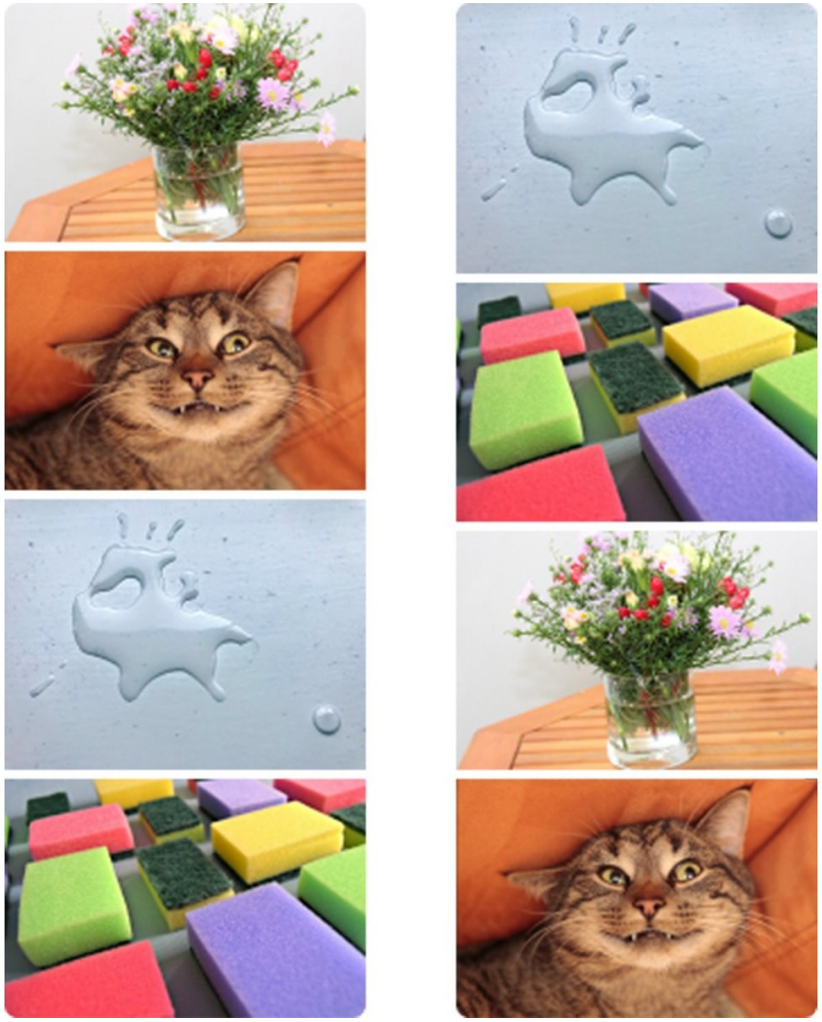
- Pseudonym Parties [Ford, 2008]
- Proof-of-Personhood [Borge et al, 2017]
- Encointer [Brenzikofer, 2018]
- BrightID [Sanders, 2018]
- Duniter [2018]
- Idena [2019]
- HumanityDAO [Rich, 2019]
- Pseudonym Pairs [Nygren, 2019]
- DFINITY Virtual People Parties [Williams, 2021]
- Worldcoin [Worldcoin, 2023]

Encointer: in-person PoP in Zurich

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

Idena: virtual pseudonym parties

- 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”, …



Talk Outline

- Towards democratic decentralization
- Proof of personhood: one person, one vote
- **The coercion problem in E-voting and PoP**
- TRIP: in-person [fake] credential issuance
- Usability of TRIP and fake credentials
- Conclusion and ongoing/future work

Towards democratic decentralization

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*

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

The coercion, vote-buying problem

Moldovan Police Accuse Pro-Russian Oligarch Of $39M Vote-Buying Scheme

The coercion, vote-buying problem

Blockchains could just make the problem worse!

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

PoP for deliberation, governance

Can PoP enable online robust self-governance?

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

But…

Whose interests do participants represent?

Collusion and coercion in PoP

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

Compressed to 0:

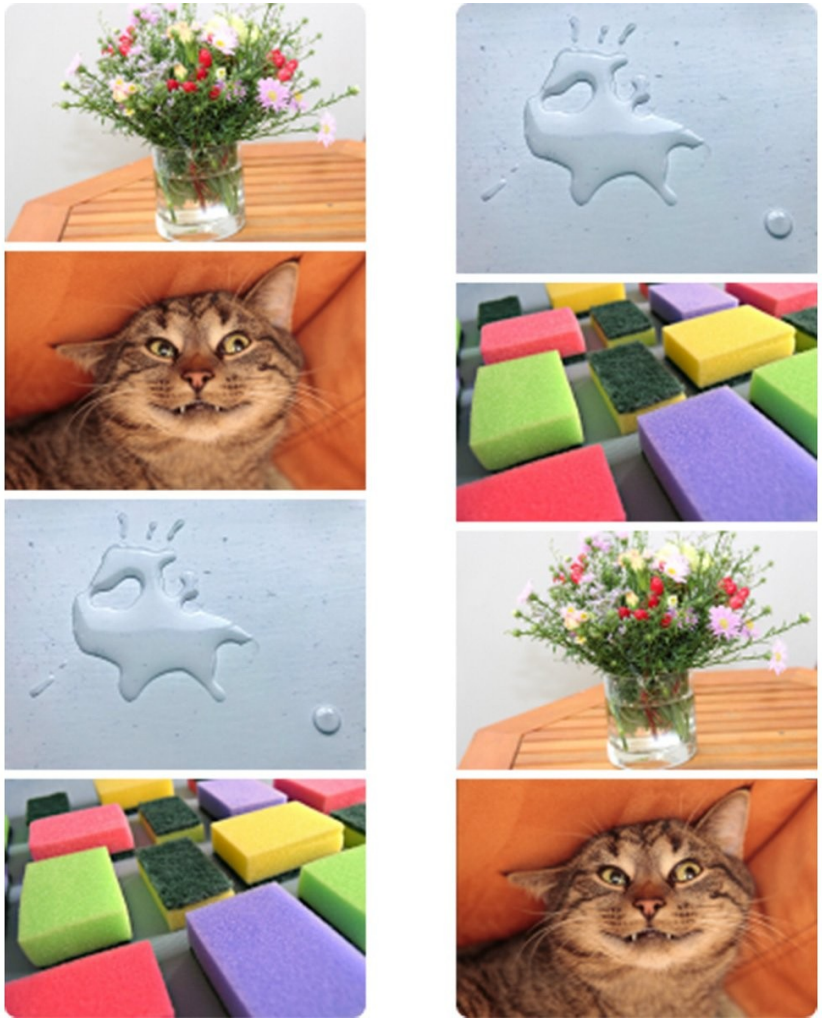
The Silent Strings of Proof of Personhood[1]

Puja Ohlhaver[2], Mikhail Nikulin[3], Paula Berman[4]

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4749892

Idena: virtual pseudonym parties

- 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

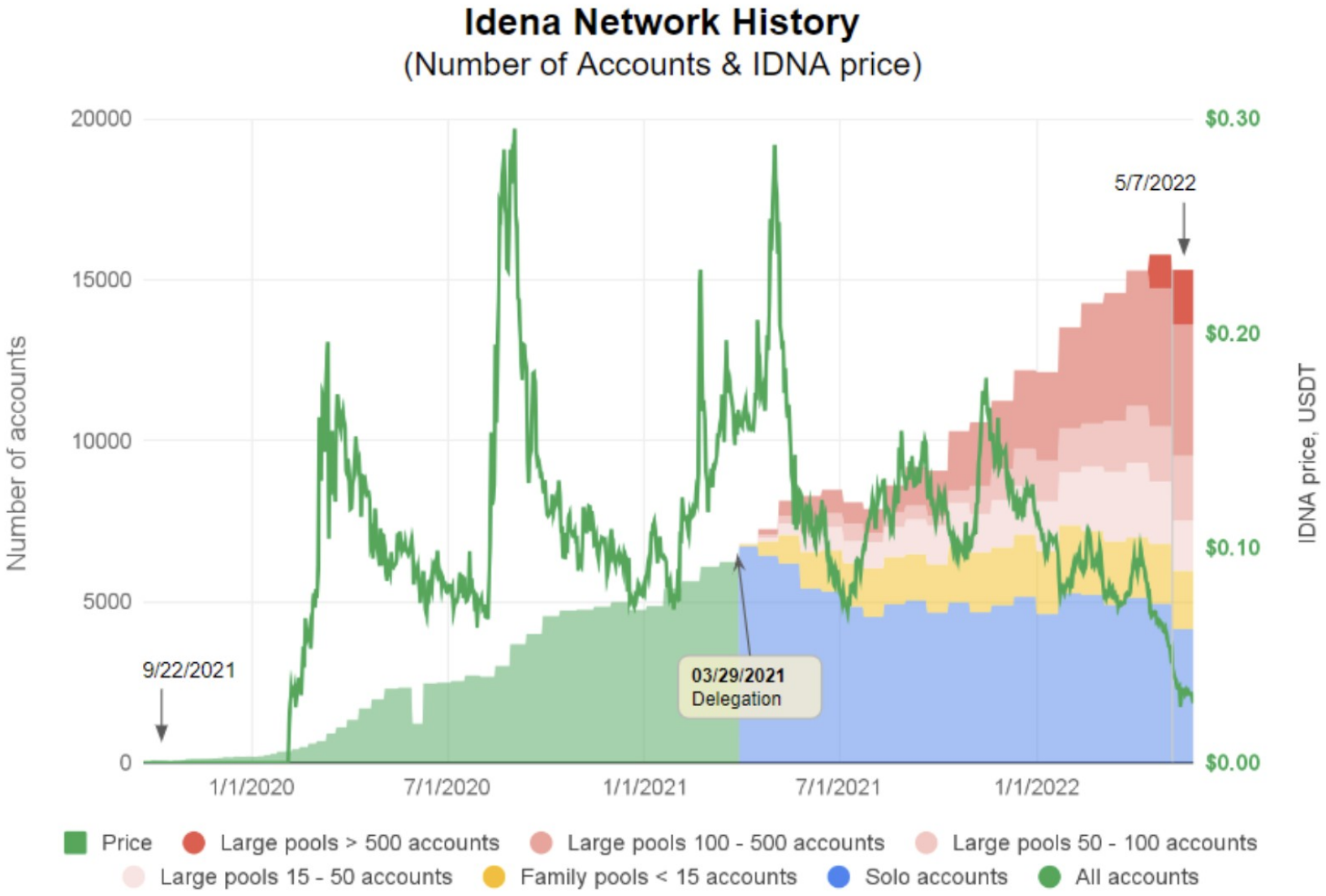


Figure 8 : Idena Network History[42]

Idena: the Puppet Pool Takeover

Talk Outline

- Towards democratic decentralization
- Proof of personhood: one person, one vote
- The coercion problem in E-voting and PoP
- **TRIP: in-person [fake] credential issuance**
- Usability of TRIP and fake credentials
- Conclusion and ongoing/future work

The “fake credentials” solution [JCJ]

At **registration** or **credentialing** 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/credentialing or PoP

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

In-person registration/credentialing or PoP

- We can leverage physical security (again)!

TRIP: in-person credentialing

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: in-person credentialing

Assume an **in-person** step for *credentialing*

- Trustworthy issuance of real & fake credentials

US-style elections with a voter registration step

- Obtain E-voting credentials while registering

Europe-style elections: automatic registration

- In-person step to opt-in to *E-voting* channel

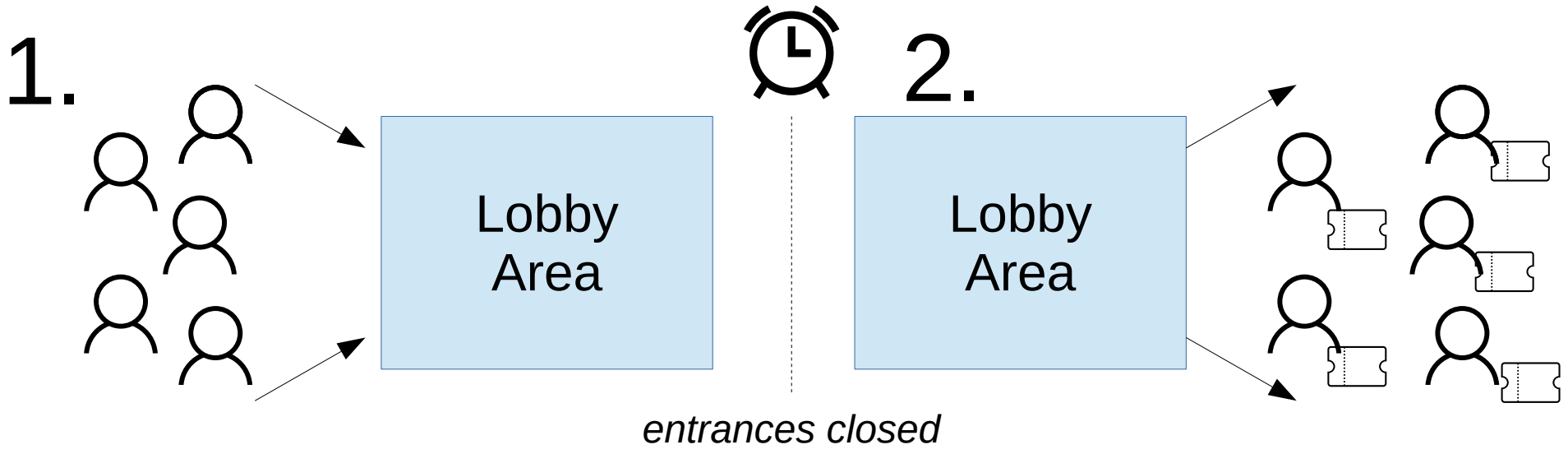
PoP via in-person pseudonym parties

- In-person credentialing at pseudonym party

PoP based on physical presence

In-person attendees get short-term *tickets*

- Not (yet) long-term PoP credentials



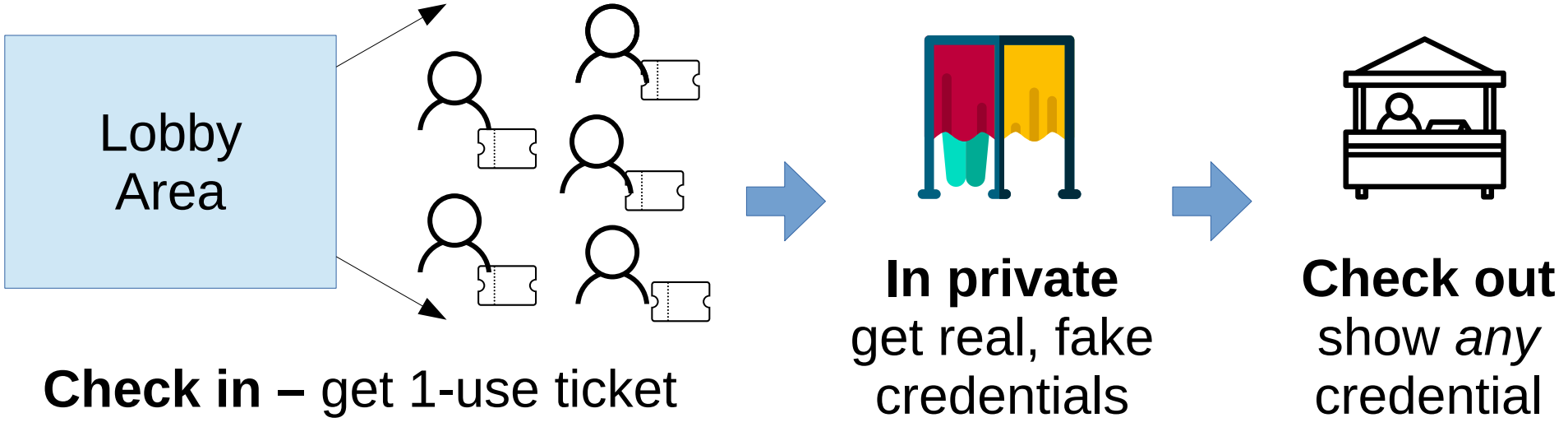
PoP based on physical presence

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

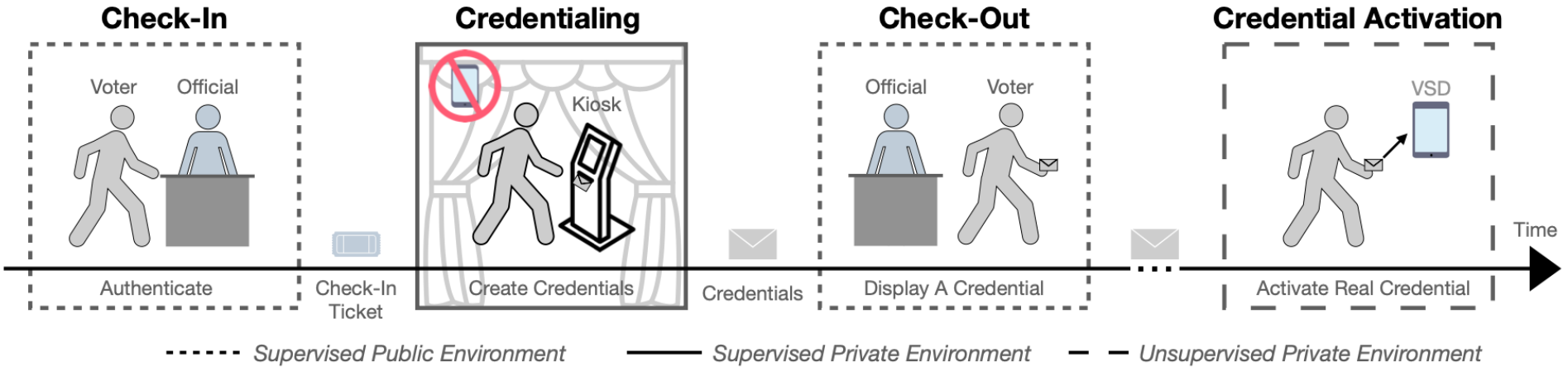
The coercion problem is still far from “easy”

- 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? …

TRIP workflow overview

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

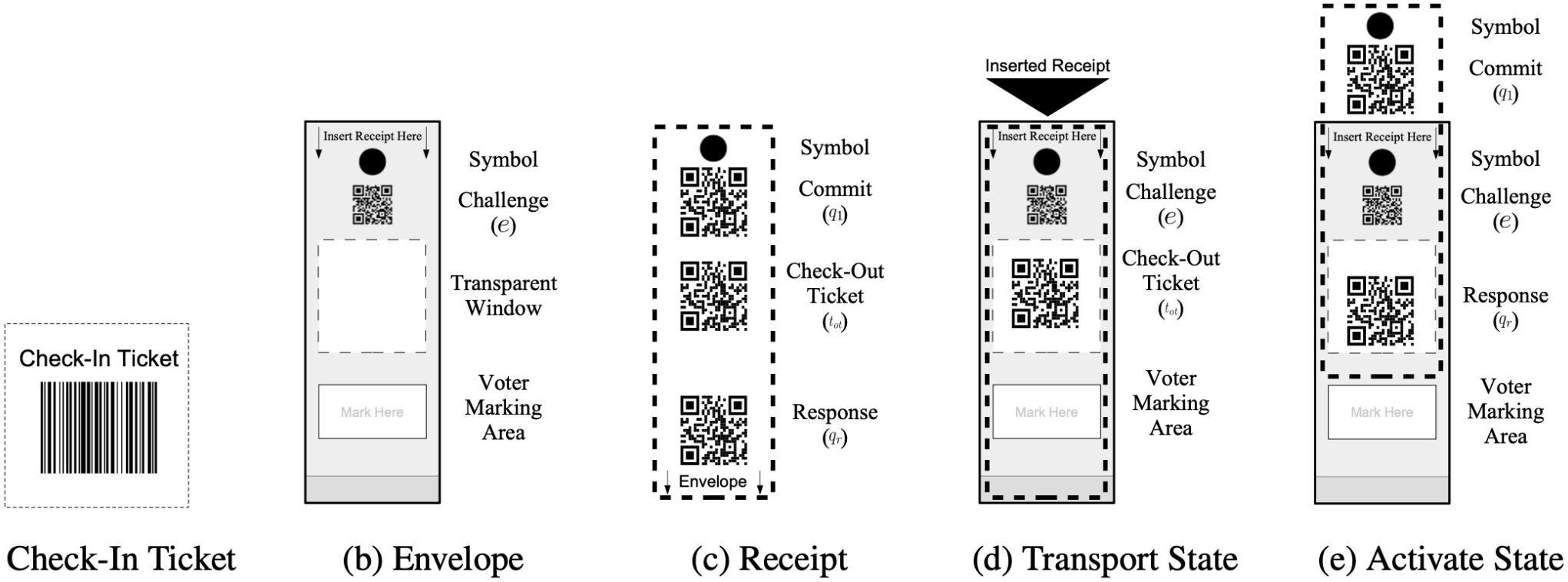
- Cheap, disposable, easy to hide from a coercer
- Attendees *not* actually under coercion need not trust the kiosk



TRIP paper credential design

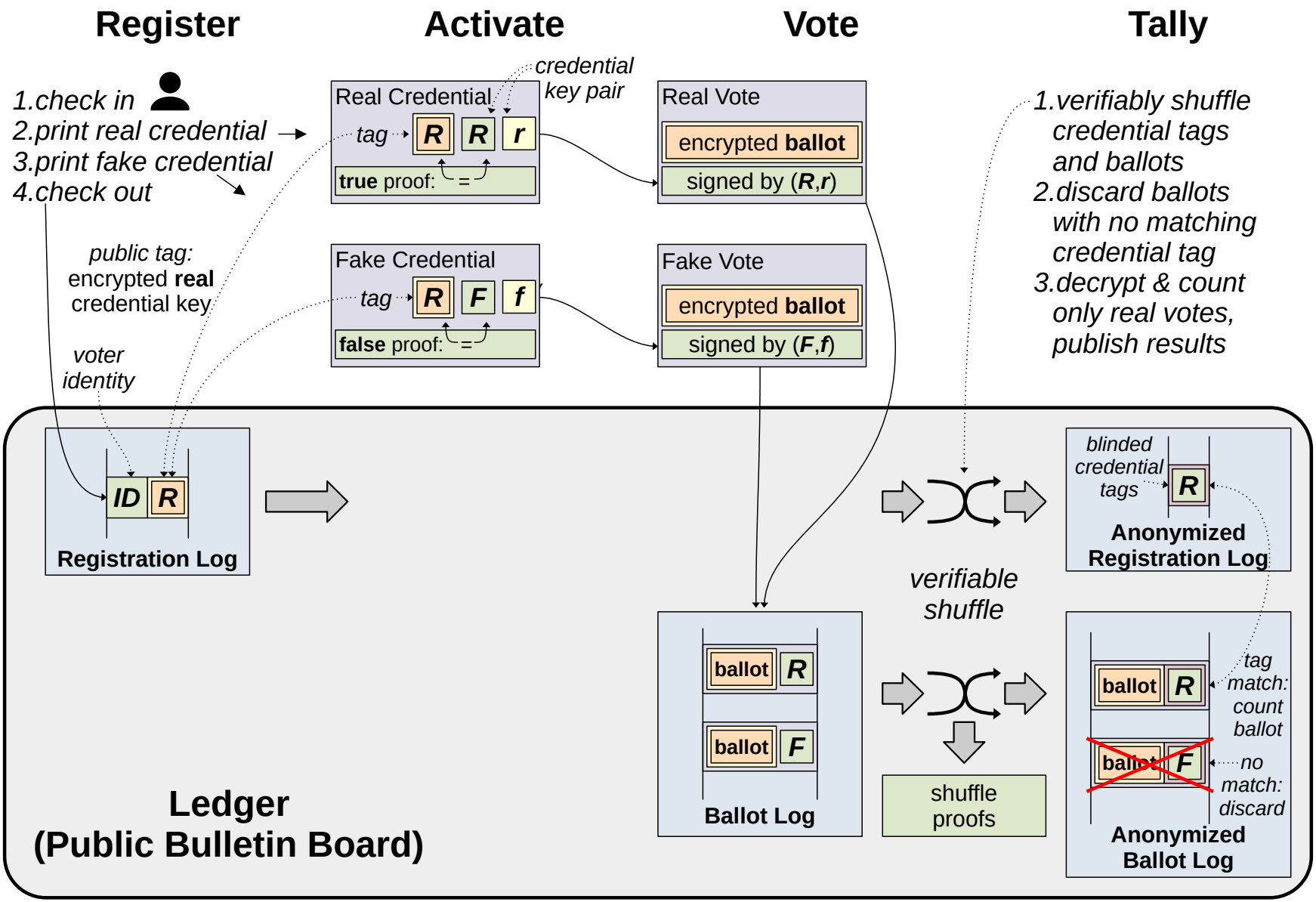
Kiosk prints three QR codes on a receipt printer

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



(a) Check-In Ticket (b) Envelope (c) Receipt (d) Transport State (e) Activate State

Coercion-resistant vote counting



Talk Outline

- Towards democratic decentralization
- Proof of personhood: one person, one vote
- The coercion problem in E-voting and PoP
- TRIP: in-person [fake] credential issuance
- **Usability of TRIP and fake credentials**
- Conclusion and ongoing/future work

Usability of fake credentials

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

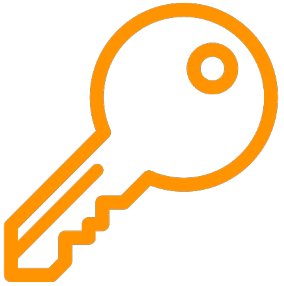
Louis-Henri Merino*, Alaleh Azhir†, Haoqian Zhang*, Simone Colombo*,
Bernhard Tellenbach‡, Vero Estrada-Galiñanes*, Bryan Ford*
*EPFL †MIT ‡Armasuisse

[IEEE Symposium on Security & Privacy 2024]

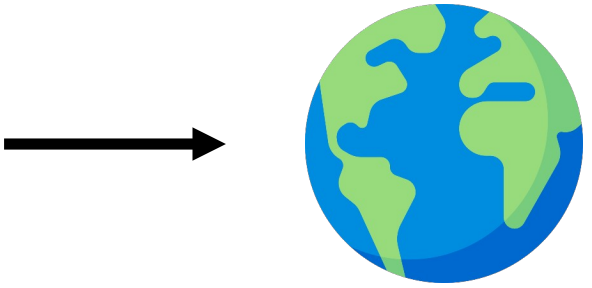
Prototype kiosk setup for user study

Perceptions of fake credentials

96% understood its use



76% create at least one fake credential



53% would create in reality

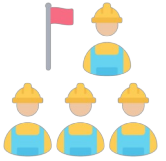
Reported coercion incidents

26%

report experiencing or knowing of someone who has experienced at least one form of voter coercion

Reported Sources

Spouse

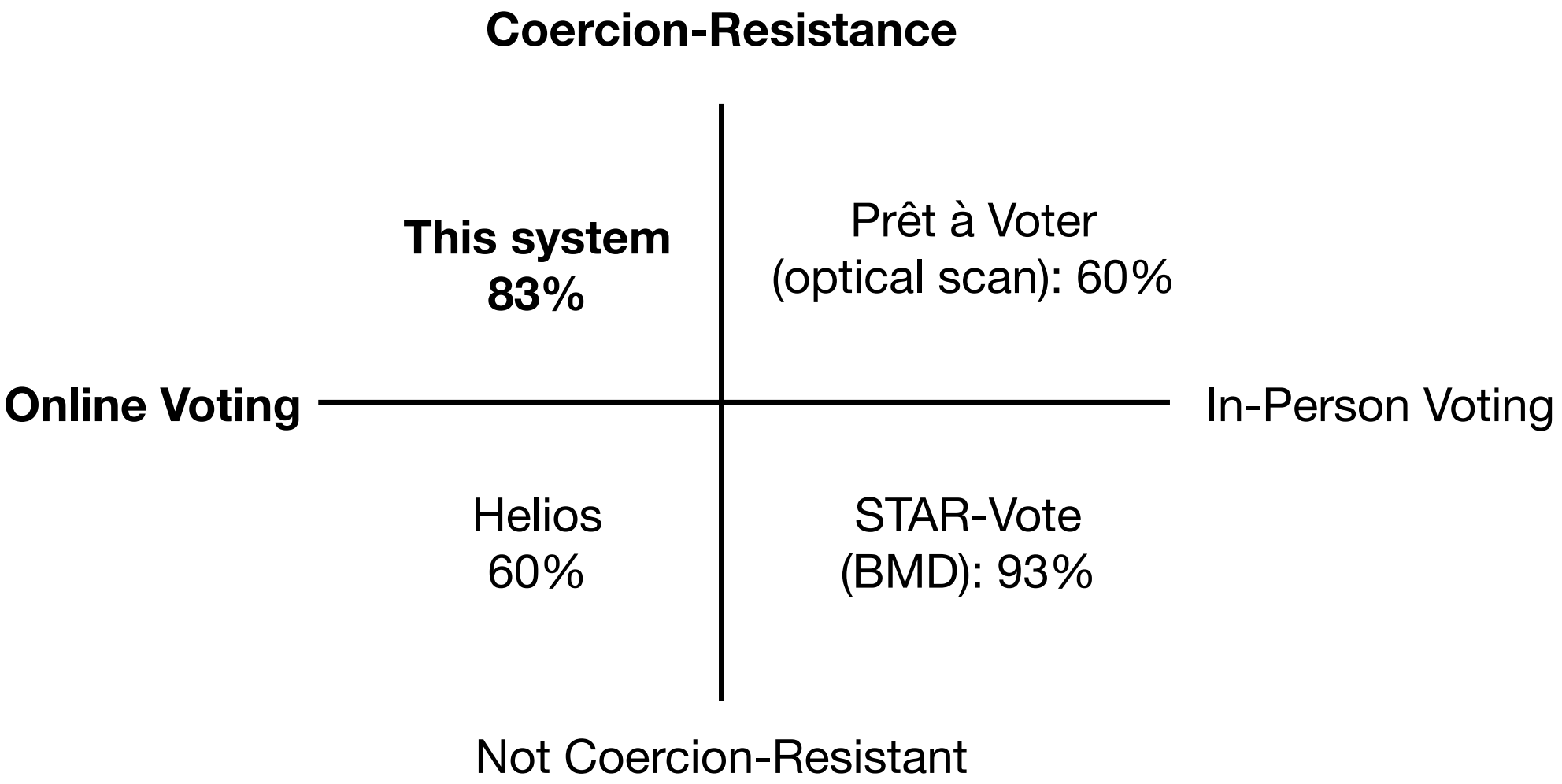


Labor Unions

Colleagues

Party Members

Usability score comparison



Talk Outline

- Towards democratic decentralization
- Proof of personhood: one person, one vote
- The coercion problem in E-voting and PoP
- TRIP: in-person [fake] credential issuance
- Usability of TRIP and fake credentials
- **Conclusion and ongoing/future work**

Is a true “global town hall” feasible?

For robust discussion of important global issues

→ Decisions, action plans that transparently & security represent *everyone’s* interests

Towards democratic decentralization

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!**

EPFL

Coercion-resistant E-voting and Proof of Personhood

Further reading:

https://bford.info/pub/