EPFL

Who – Or What – Will Our Distributed Metaverse Serve?

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

INRIA – July 7, 2022

We're facing **hard global** problems

Climate change

COVID-19 pandemic

Exploding inequality

Global problems need global tools

Like the Internet…or the Metaverse?

What is "the Metaverse"?

NEAL STEPHENSON

Snow Crash

LEDA

We already inhabit "a metaverse"

Some of us already have done so for decades…
since the era of USENET and MUDs

Mental immersion doesn't require VR goggles!

The metaverse is…

An alternate digital universe that *we build!*
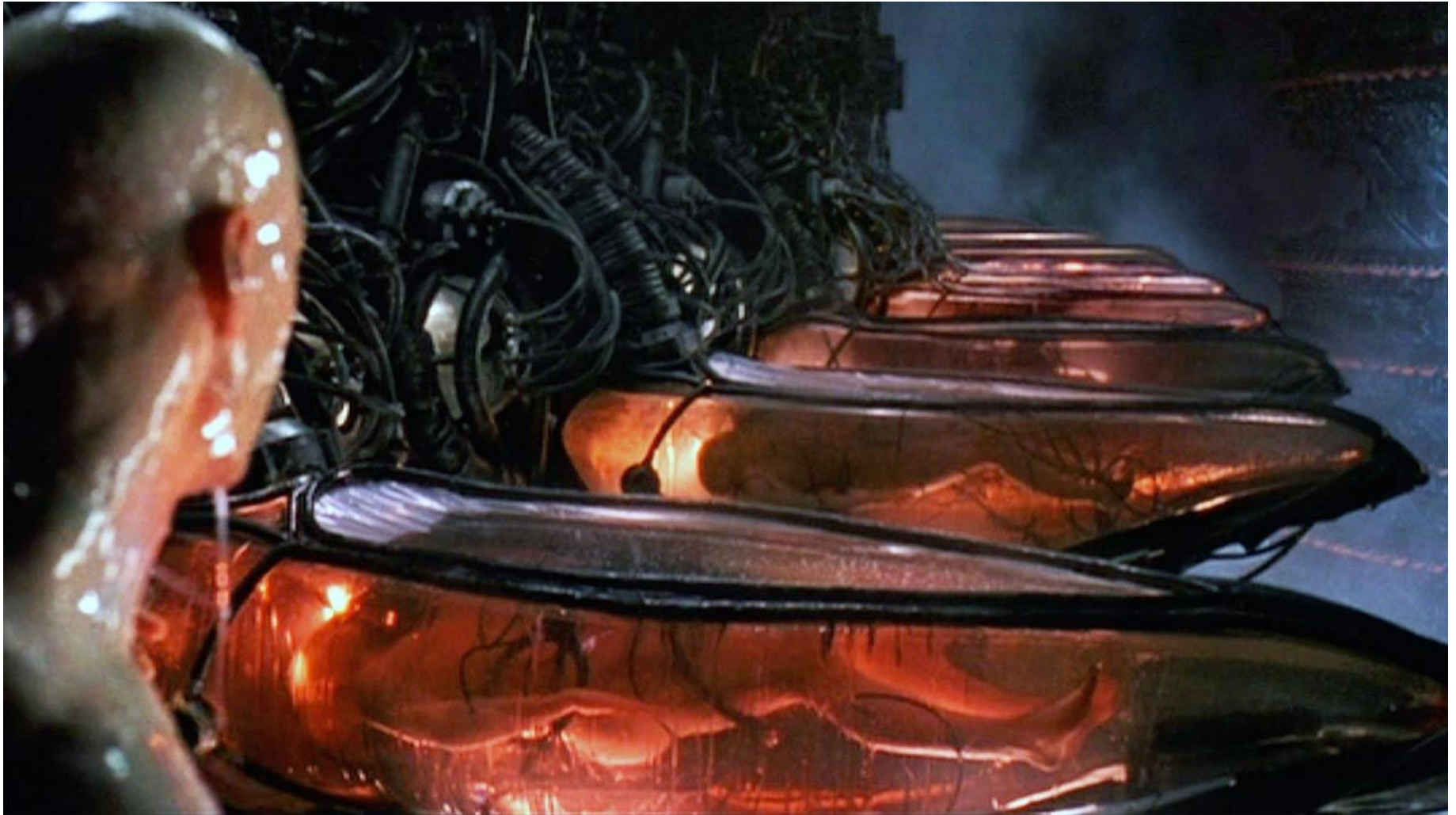
- An **engineered** virtual reality

We – at least collectively – have *choice* of

- How it should be designed
- For whom it should be designed
- What purposes it should serve
- To whom it should be accountable

Will a metaverse empower us?

Or will it enslave us?

It's still our choice, *for now*…

Will the metaverse be…

Distributed? *Of course.* It must **scale** globally.

That's the *easy* part…and mostly solved already

Centralized Distributed Systems

…are what Google, Facebook, etc., are good at.

Much systems research is performance-centric:
push packets, run apps XX% fasters/lighter/etc.

As academic researchers,
do the big tech companies need our help?

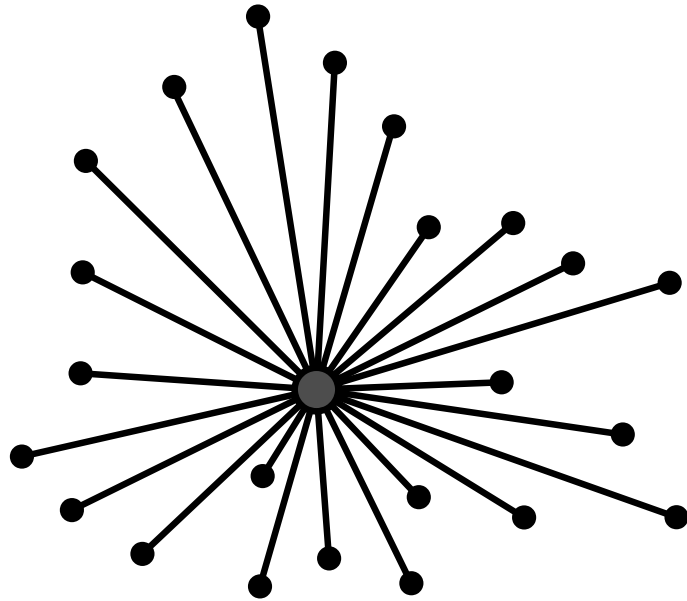Is optimizing already-usable systems "research"?

Will the metaverse be…
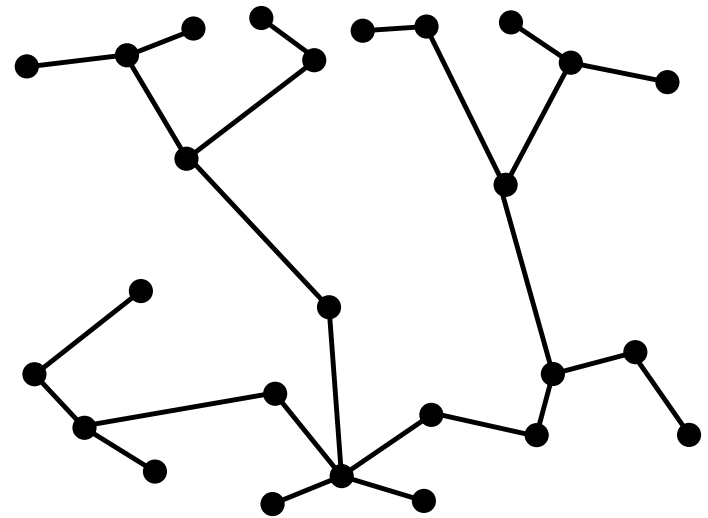
Decentralized? That's a harder question.

- Should it be decentralized? How? Why?
- What does "decentralized" even mean?

How is a system "decentralized"?

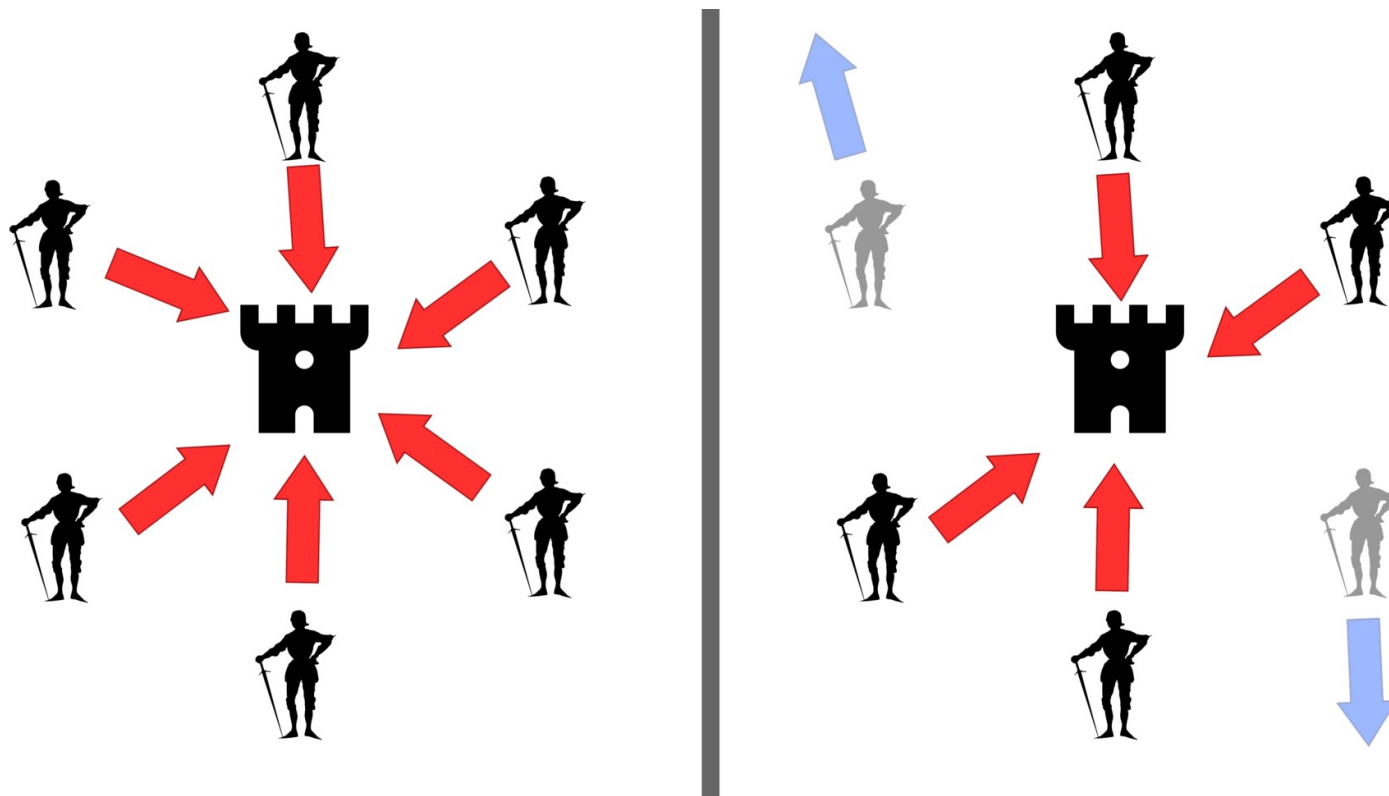- By **network topology** – no central "hub"?

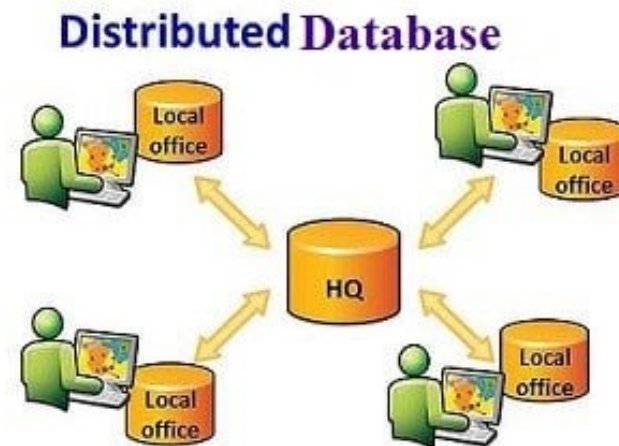CENTRALIZED   DECENTRALIZED

How is a system "decentralized"?

- By **network topology** – no central "hub"?
- By **trust** – no central fully-trusted entity?

How is a system "decentralized"?

- By **network topology** – no central "hub"?
- By **trust** – no central fully-trusted entity?
- By **data distribution** – no central database?

Centralized Database

Local office · Local office · Local office · Local office · HQ

Distributed Database

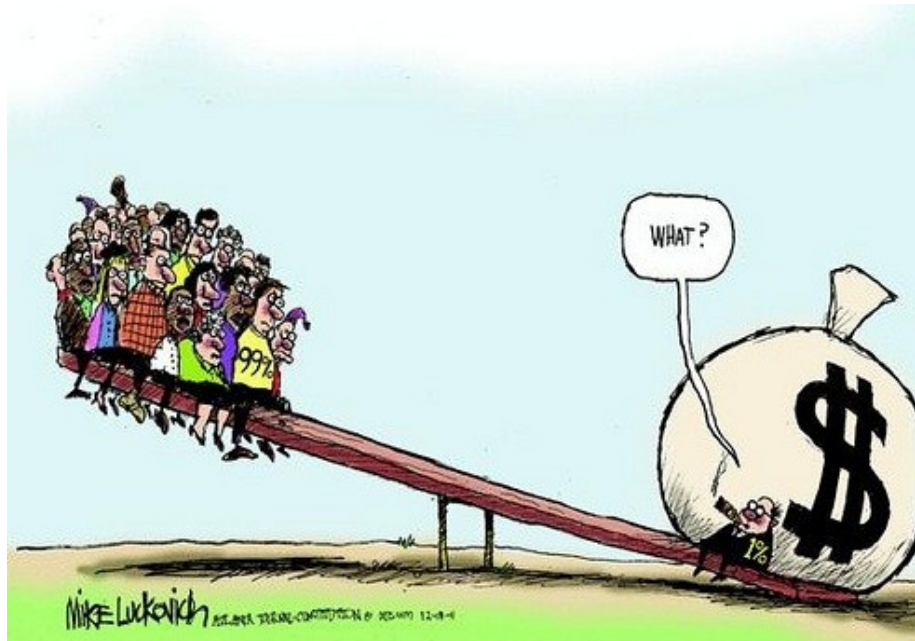Local office · Local office · Local office · Local office · HQ

How is a system "decentralized"?

- By **network topology** – no central "hub"?
- By **trust** – no central fully-trusted entity?
- By **data distribution** – no central database?
- By **power & control** – no one "owns" most?

For the many, or the few?

How will power, control, influence be distributed?

Will residents be *voting citizens* or *the product*?

How to Pick Research Problems

What are the most important research problems
in distributed and decentralized systems?

I claim: those that help ensure our digital metaverse

- **serves** people instead of **exploiting** them

- serves **everyone** – not just **a few elites**

Those that **help us solve** critical global challenges
like climate change, rather than contributing to them

Three Key Problem Areas
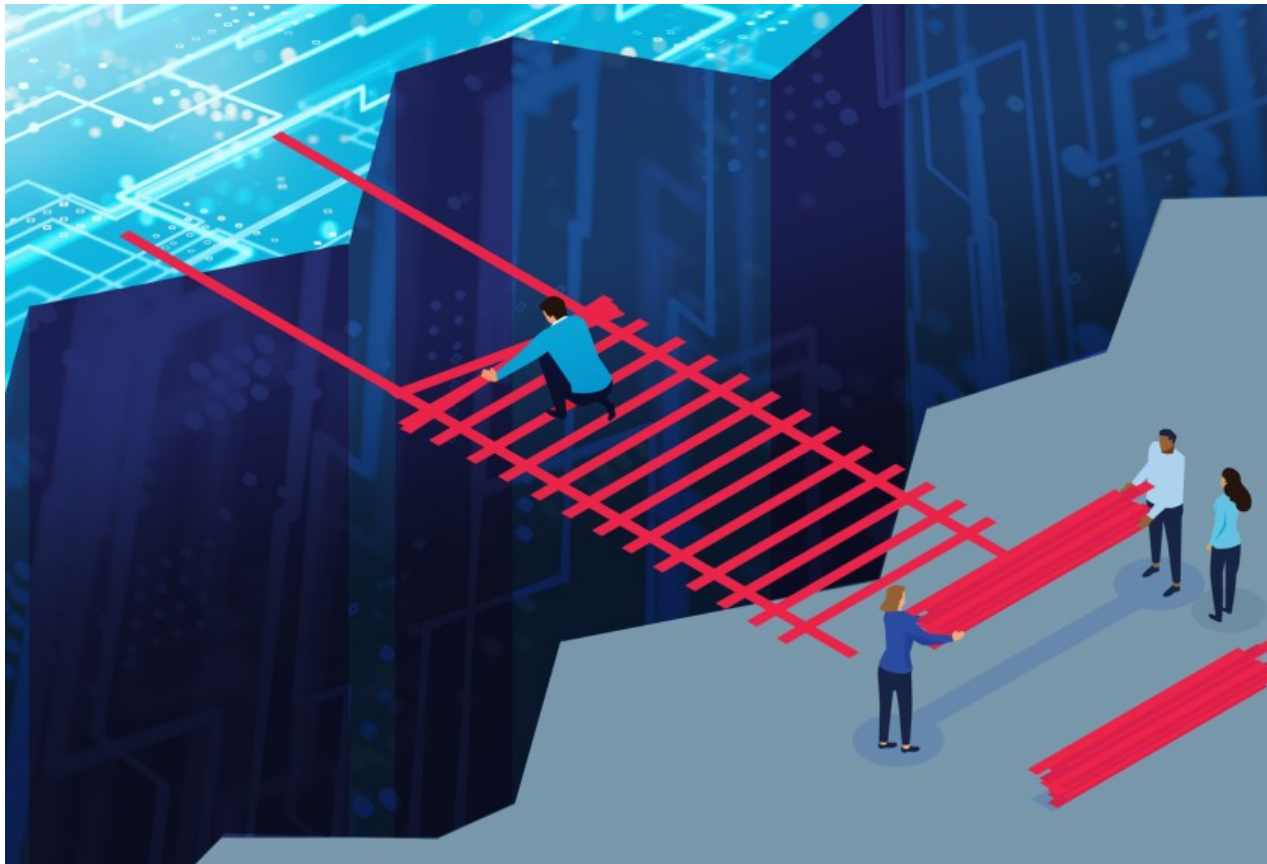
What does this mean more concretely?

A metaverse that **serves people** must:

1) Be **inclusive** of everyone, everywhere

2) Serve **real people**, not fake accounts

3) Preserve **freedoms** of self-determination

Let's look at technical problems in each area...

Problem 1: Inclusion

How to build distributed/decentralized systems that reliably "cross the digital divide"?

Problem 1: Inclusion

How to make our systems usable by to those:

- With old, slow, resource-limited devices?

- Access only to shared devices?

- Slow, expensive, or intermittent connectivity?

- Wartime conditions, unstable/repressive states?

How can such users remain **first-class citizens**, not trapped in a *purgatory of indirect processes*?

Guaranteed Local Accessibility?

Observation:

Local connectivity often faster/cheaper/defensible when **global** connectivity is slow or unavailable

Can we build systems that **guarantee** localized accessibility, usability under global disconnection?

- Strong synergy with edge systems research – but *not just (or mainly) about optimization!*
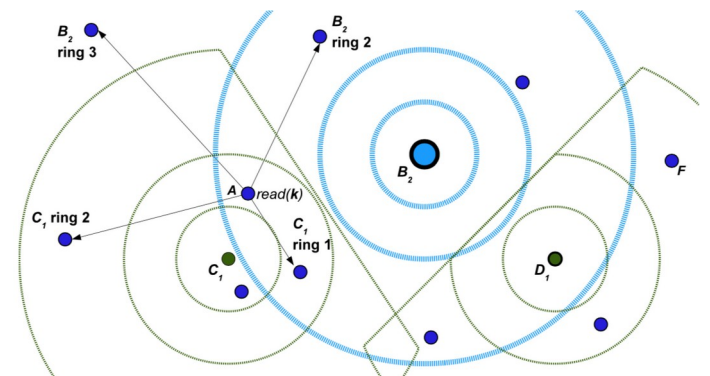
Guaranteed Local Accessibility?

Workshop paper:
"Immunizing Systems from Distant Failures by Limiting Lamport Exposure" [HotNets '21]

Conference paper:

unpublished 8 years & counting

Preprint (arXiv:1405.0637):
"Crux: Locality-Preserving Distributed Services"

Problem 1: Inclusion

Other interesting questions in this area:

- How can systems guarantee "first-class" status to users of old/slow/shared devices?

- How can systems guarantee local operation *at any scale* while globally disconnected?

- What kind of distributed application model, system API, "app store" can protect inclusion?

- How can we evaluate, benchmark, formalize, and reason about inclusion-related properties?

Problem 2: Personhood

Who will be the "voting citizens" of the metaverse?

- How many votes will each **real person** wield?
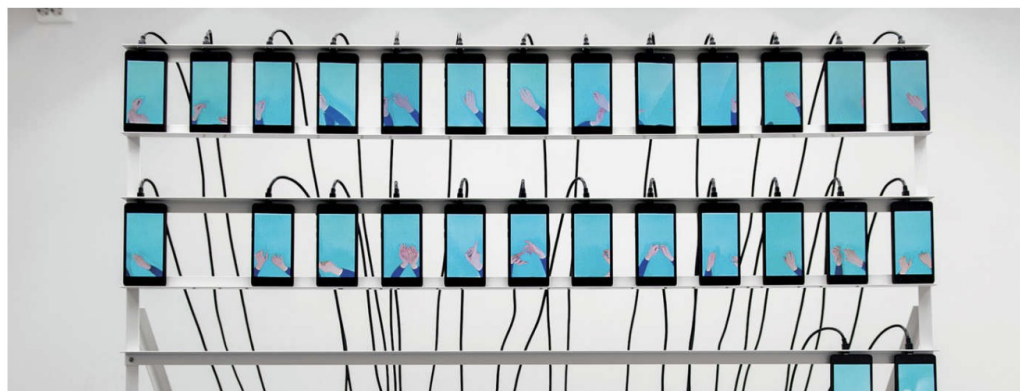- How many votes will **fake accounts** control?

The Fundamental Problem

Today's Internet doesn't know what a "person" is

People aren't digital, only profiles are

[Pixabay, The Moscow Times]

Membership and Influence

If a society can't decide – or secure – its membership and influence foundations → chaos

Contrasting Influence Foundations

Wealth-centric

- One dollar, one vote

Person-centric

- One person, one vote

[Kera]

[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

Without any basis for personhood...

Companies, governments, opaque algorithms, private oversight boards "govern" online behavior

Democracy, "one person one vote", isn't an option

Contrasting Influence Foundations

Wealth-centric

decision-making led us to adopt global policies benefitting the few toward the detriment of the rest of us…

Person-centric

decision-making at a *global* scale may be the only way to reach policies in the long-term interest of us all.

What Is the Missing Foundation?

[All About Healthy Choices]

Proof of Personhood

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

- For online forums, voting, deliberation, …

Key desirable properties:

- **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!

Proofs of Personhood

How can we potentially 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]
- Genuine Personal Identifiers [SocInfo 2020]
- Who Watches the Watchmen? [Frontiers 2020]
- Identity and Personhood in Digital Democracy [Ford 2020]

A Categorization of Approaches

Differentiated by the *basis* for resisting fakes:

- **Identity:** based on a documented history trail
  - Government identity, KYC, self-sovereign identity
- **Biometrics:** inequality comparison of templates
  - Aadhaar in India, WFP Kenya, WorldCoin
- **Social trust:** graph-based reputation, analysis
  - PGP tradition, SybilLimit, BrightID, GPIs, …
- **Physical presence:** one body, one vote/token
  - Indelible ink (India), pseudonym parties, Encointer

Some Alternatives Compared

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

Problem 2: Personhood

Some related questions in this area:

- Can biometric identity (Aadhaar, Worldcoin) be inclusive, decentralized, privacy-preserving?

- Can reputation & recommendation systems offer [provable] metrics of *real value to people*?

- Can we create [crypto]currencies or CBDCs that empower people, limit wealth inequality?

- Can participatory sites (wikis, crowdsourcing) allow anonymity while ensuring accountability?

Problem 3: Freedoms

Can systems protect users' basic freedoms of self-determination even under pressure/coercion?

- Not just bots but *real people* can be bought!

- More climate change, inequality, etc.
  → global conflict → authoritarian pressures

Strong synergy with privacy technologies (PETS), but it's *not just (or even mainly) about privacy*

- Privacy is *necessary* but not *sufficient*

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
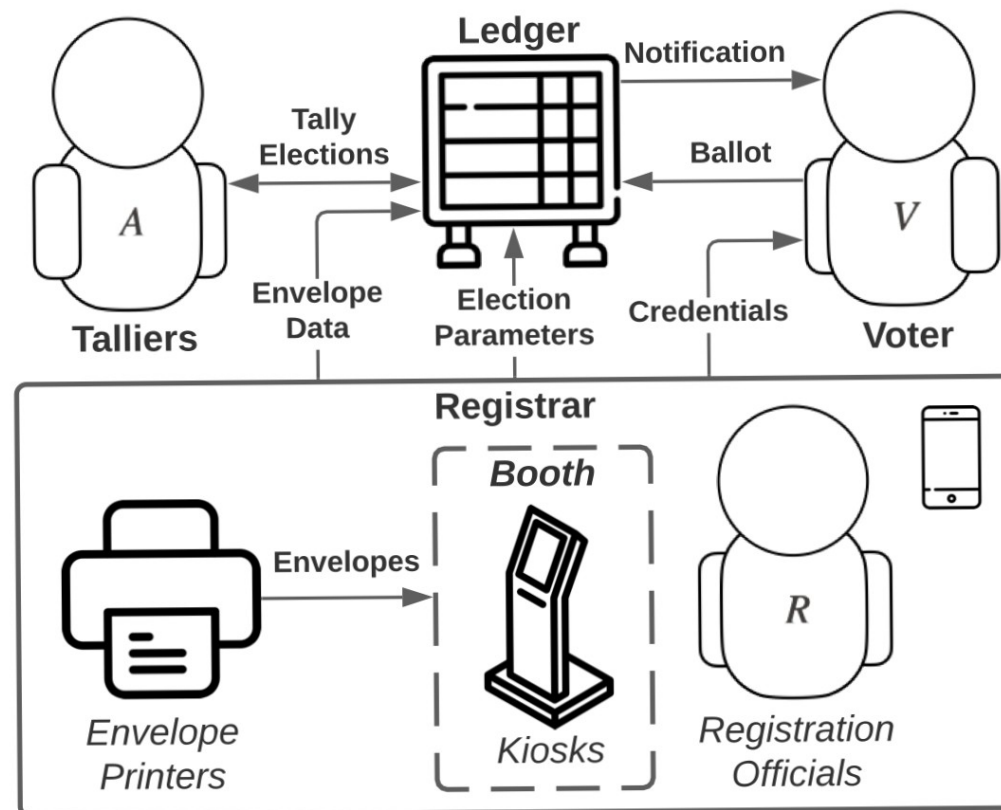
The New York Times

July 30, 2019

Coercion-resistant E-Voting

In-progress work:

"TRIP: Trustless Coercion-Resistant In-Person Voter Registration" [arXiv:2202.06692]

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

Problem 3: Freedoms

Other interesting questions in this area:

- Can systems help protect victims of wartime conditions, migrants/refugees, stateless…?

- Can online deliberation, reputation, value systems be made resistant to astroturfing?

- Can we build coercion-resistant (deniable?) storage systems for sensitive/personal data?

- Can [crypto]currencies and wallets be made resistant to coercion or use under duress?

Conclusion

The "Metaverse" is already here (& distributed)

But will our metaverse **serve people**?

- Will it serve *everyone*? (**inclusion**)
- Will it serve *real people*? (**personhood**)
- Will it *empower* people*? (**freedoms**)

If our research isn't addressing today's key global challenges, is it just contributing to the problem?