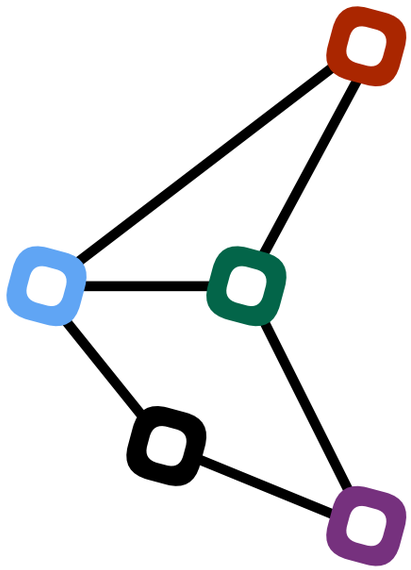
EPFL dedis



Decentralized and Distributed Systems Laboratory (DEDIS)

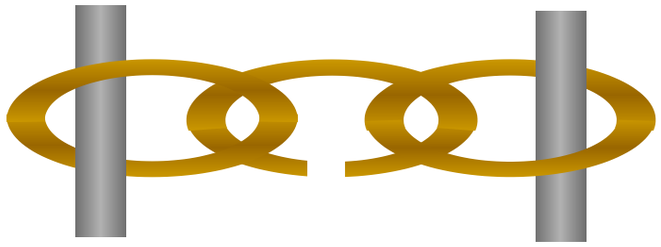
Prof. Bryan Ford
Dr. Vero Estrada-Galiñanes
dedis@epfl.ch – dedis.epfl.ch

EDIC Orientation – September 5, 2023

A Fundamental Challenge

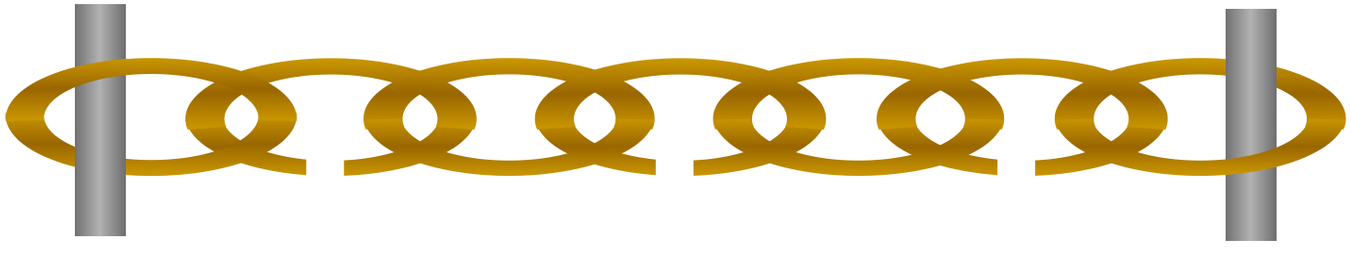
In today's IT systems, security is an afterthought

- Designs embody "weakest-link" security



Scaling to bigger systems → weaker security

- Greater chance of any "weak link" breaking

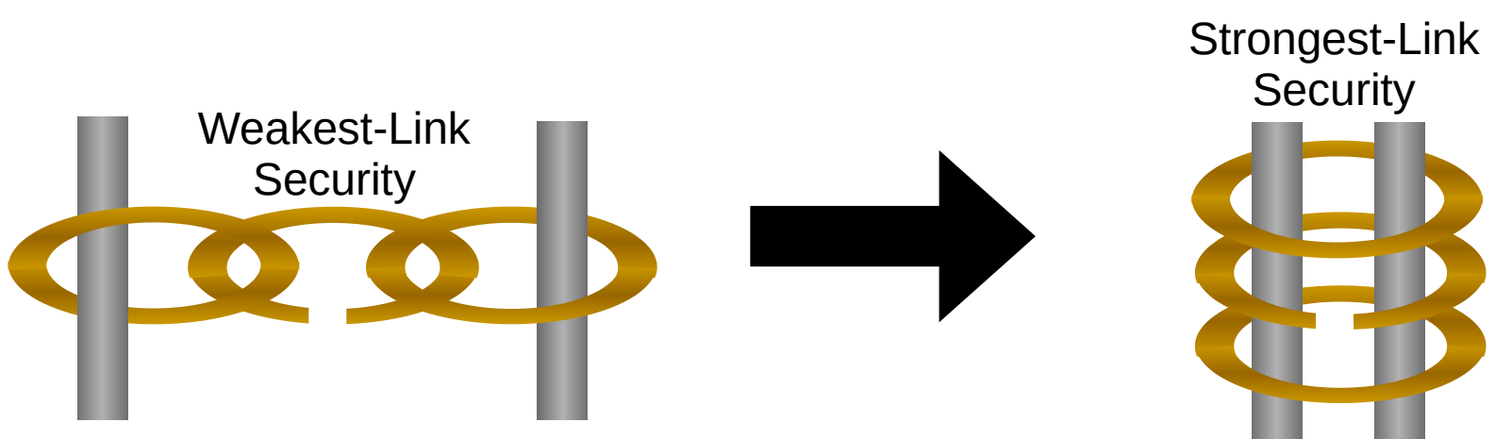


The DEDIS lab at EPFL: Mission

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**



Sample of DEDIS research topics

- Privacy and anonymity technologies
- Blockchains and cryptocurrencies
- Digital identity, personhood, and democracy

Sample of DEDIS research topics

- **Privacy and anonymity technologies**
- Blockchains and cryptocurrencies
- Digital identity, personhood, and democracy

Privacy and anonymity

- Private information retrieval (PIR) enables a client to fetch a record from a database while hiding from the database server(s) which specific record(s) the client retrieves.
- **PROBLEM:** Unauthenticated PIR is inadequate for applications where data integrity matters

How does the client knows that the record is authentic?

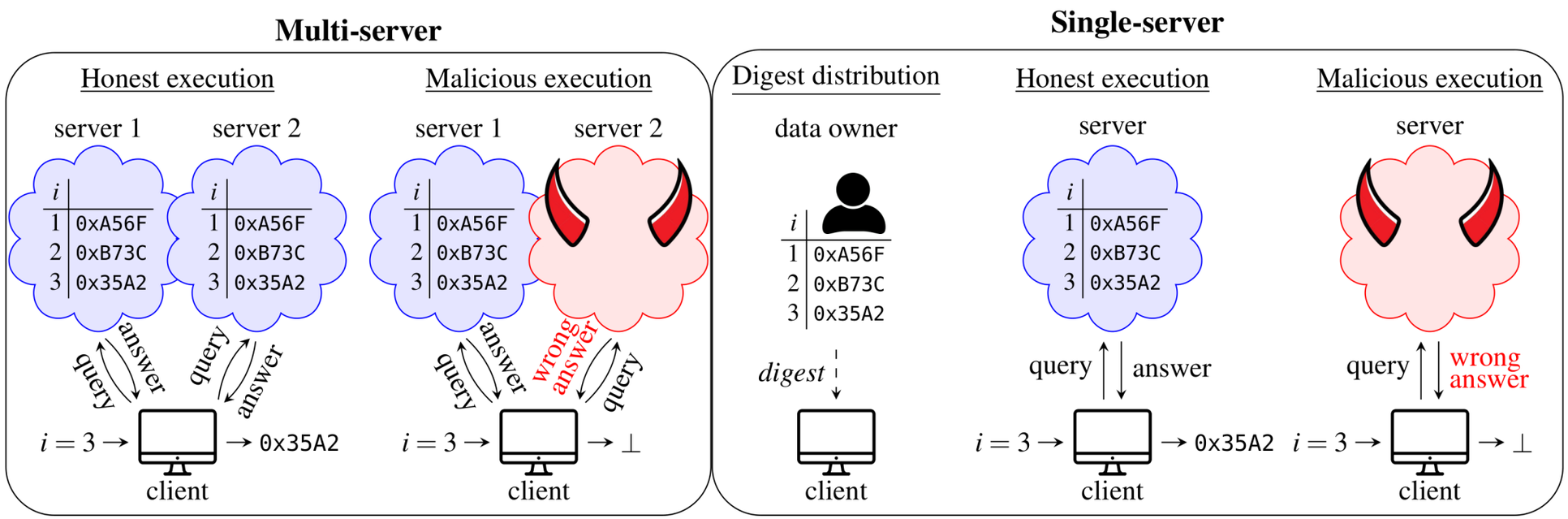
How does the client detects misbehavior and aborts?

Applications: Why integrity matters in PIR?

- Public-key servers: Fetching a false public key
- Domain name systems: Recovering the wrong IP address
- Online certificate status protocol: Trick the client into trusting a revoked certificate
- Content library: Recover malware-infected files

Authenticated Private Information Retrieval

- DEDIS lab project presented in [USENIX Security ‘23]



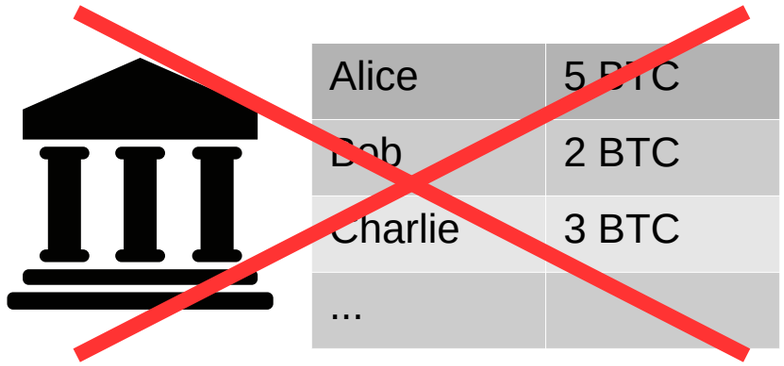
Sample of DEDIS research topics

- Privacy and anonymity technologies
- **Blockchains and cryptocurrencies**
- Digital identity, personhood, and democracy

(credit: Tony Arcieri)

Distributed Ledgers

Problem: we don't want to trust any designated, centralized authority to maintain the ledger



Alice	5 BTC
Bob	2 BTC
Charlie	3 BTC
...	

Solution: “everyone” keeps a copy of the ledger!

- Everyone checks everyone else's changes to it

Alice's copy

Alice	5 BTC
Bob	2 BTC
Charlie	3 BTC
...	

Bob's copy

Alice	5 BTC
Bob	2 BTC
Charlie	3 BTC
...	

Charlie's copy

Alice	5 BTC
Bob	2 BTC
Charlie	3 BTC
...	

Applications of Distributed Ledgers

Can represent a distributed electronic record of:

- Who owns how much **currency**? (Bitcoin)
- Who owns a name or a digital work of art?
- What are the terms of a **contract**? (Ethereum)
- When was a **document** written? (notaries)
- What is the **provenance** of a part? (supply chain)
- Who **are** you? (self-sovereign identity)
- Who used **data** for what purpose? (access logs)
- …

Limitations of Today’s Blockchains

Public/permissionless (e.g., Bitcoin, Ethereum)

- Slow, weak consistency, low total throughput
- Limited privacy: leaky, can’t keep secrets
- User devices must be online, well-connected
- Mining is inefficient, insecure, re-centralizing

Private/permissioned (e.g., HyperLedger, R3, …)

- Weak security – single points of compromise

DEDIS Blockchain Research

Working to make tomorrow's blockchains:

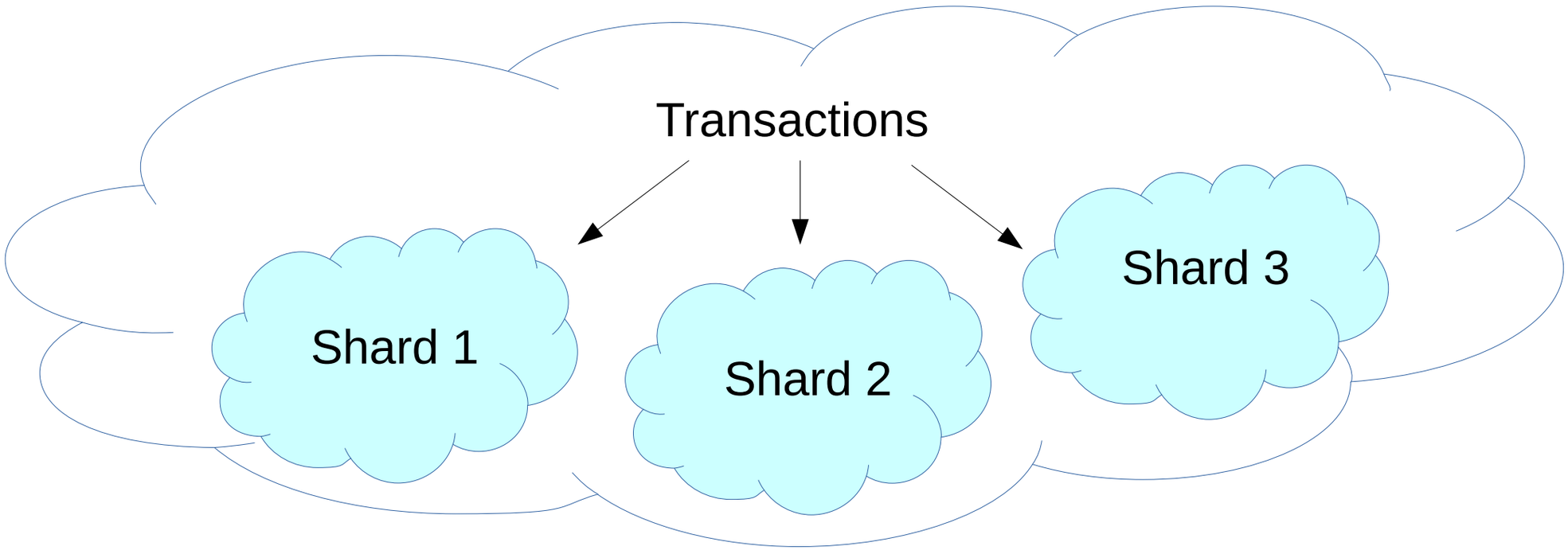
- **Fast:** responsive in seconds, not minutes/hours
- **Scalable:** support high transaction volumes
- **Private:** keeping confidential data secure
- **Available:** blockchain records usable offline
- **Powerful:** private analysis of encrypted data

DEDIS next-generation blockchain infrastructure already available, in use by multiple partners

Horizontal Scaling via Sharding

OmniLedger: A Secure Scale-Out Ledger [S&P 18]

- Break large collective into smaller subgroups
- Builds on scalable bias-resistant randomness protocol (IEEE S&P 2017)
- 6000 transactions/second: competitive with VISA



FAST - SCALABLE

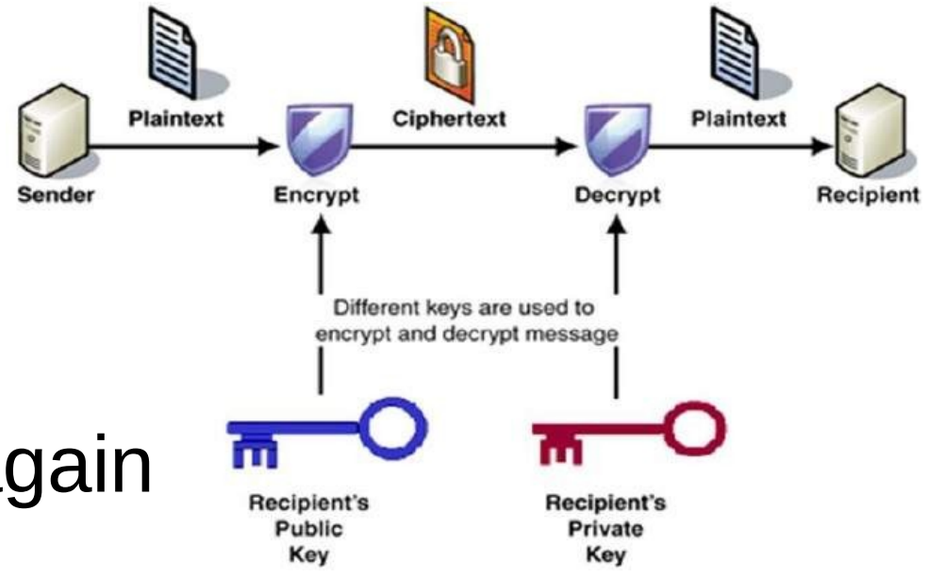
The Privacy Problem in Blockchains

In current blockchains, secrets (keys, passwords) must be held “off-chain” by private parties

- Just a hash on-chain → document might be lost
- Encrypted on-chain → encrypted to whom?
  - Decided at encryption, *cannot be changed/revoked*

Current blockchains can’t manage secrets, because they would leak to *all* participants

- Weakest-link security again

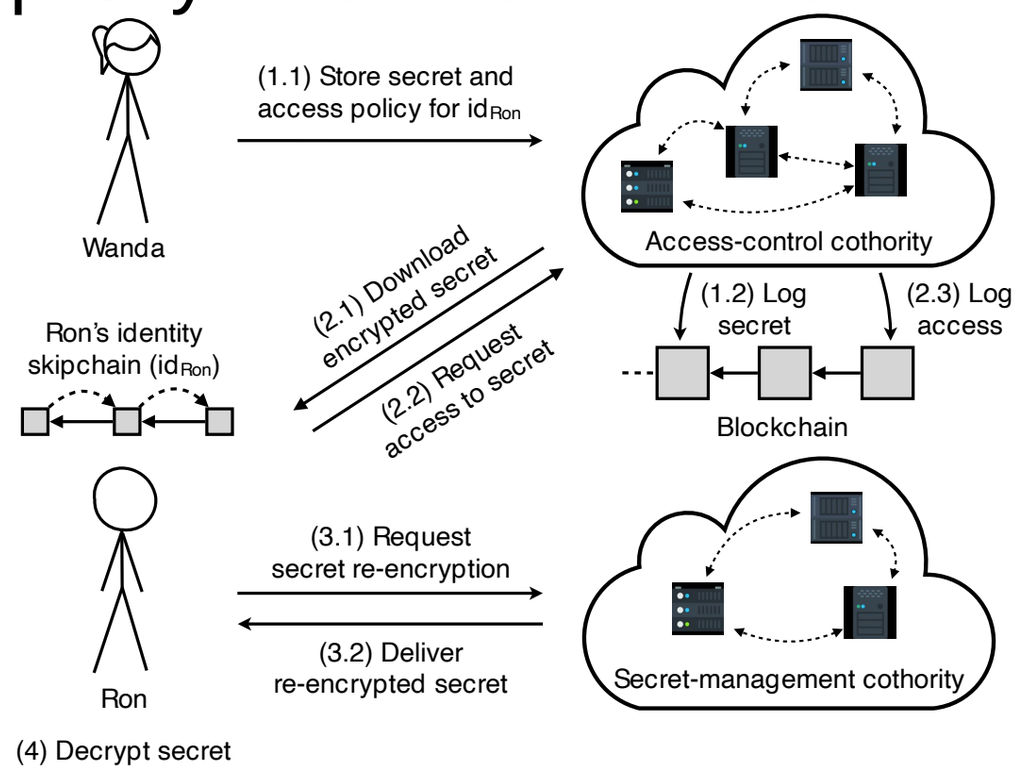


On-Chain Secrets

“CALYPSO: Private Data Management for Decentralized Ledgers” [VLDB ‘21]

Encrypt(*) secrets *care-of the blockchain itself*, under a specific access policy or smart contract

- Threshold of trustees mediate all accesses
- Enforce policies, access recording
- Ensure data both *hidden* and *disclosed* when policy requires
- Can *revoke* access if policy/ACLs change



(*) with post-quantum security if desired

Resilience and Digital Sovereignty

Today's clouds & blockchains expose users to non-transparent risks with **no geographic limit**

- Failures, attacks *anywhere* can compromise the availability, security, privacy of critical systems

Even if data at rest is stored in designated locality, **access to it** via applications often still vulnerable

- Example: can't access data/applications due to naming or ID system failure [Google, Dec 2020]

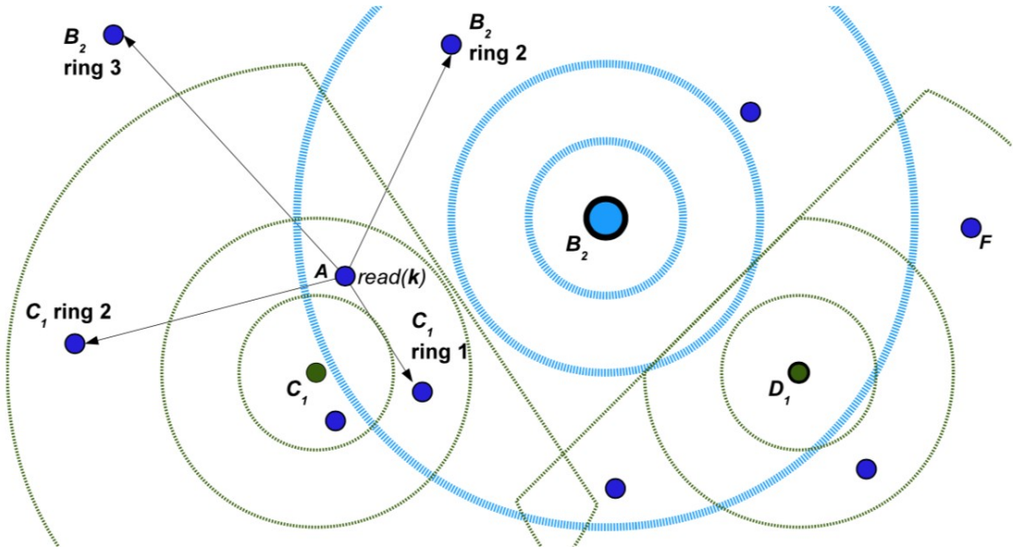
AVAILABLE

Resilient Data & Access Sovereignty

"Limiting Lamport Exposure to Distant Failures"

Immunize distributed systems from distant failures

- When users & data located in region of interest, guarantees access availability even if the region is **fully disconnected** from rest of world
- Also immunizes **performance** from slowdowns by distant systems



AVAILABLE

Sample of DEDIS research topics

- Privacy and anonymity technologies
- Blockchains and cryptocurrencies
- **Digital identity, personhood, and democracy**

Decentralized Digital Democracy

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

[Kenneth Hacker, The Progressive Post]

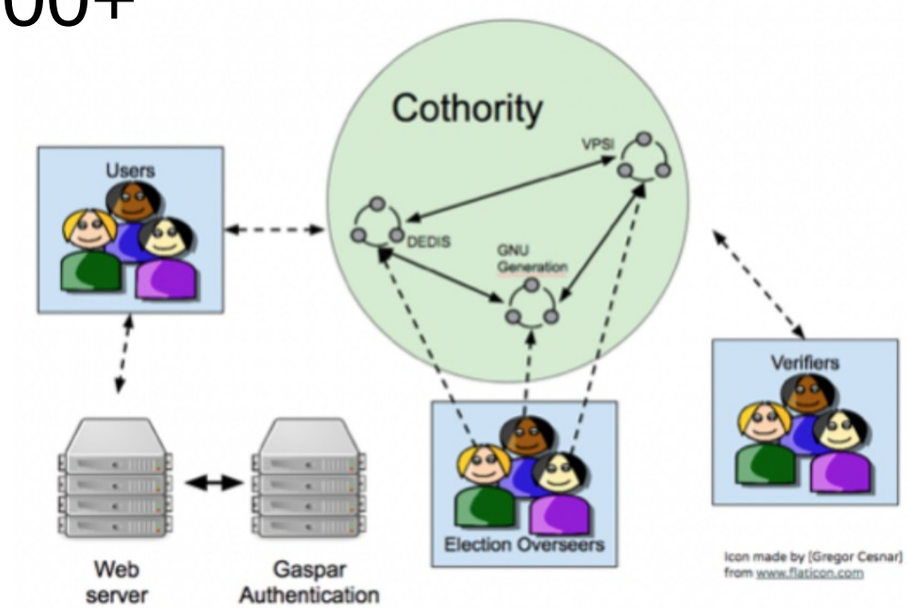
Institutional E-voting at EPFL

Prototyped blockchain-based e-voting system

- State-of-the-art cryptographic security/privacy
- Validated, approved for deployment within EPFL community of 10,000+

Exploring next-generation e-voting technologies

- In contact with Geneva, Swiss Post e-voting efforts



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

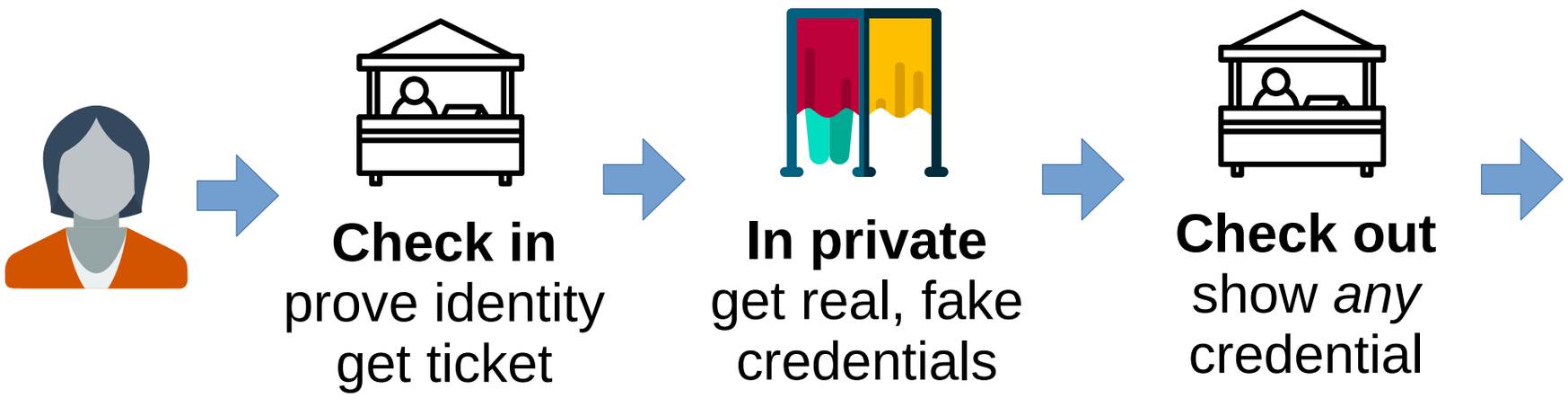
Election Fraud in North Carolina Leads to New Charges for Republican Operative

July 30, 2019

TRIP: Coercion-Resistant Signup

Voter periodically registers/renews *in person*

- Gets verifiable *real* and *fake* credentials
- Fake credentials cast votes that *don't count*
- Voter learns difference (in privacy booth) but *can't prove it to anyone*



Contrasting Influence Foundations

Wealth-centric

- One dollar, one vote

[Kera]

Person-centric

- One person, one vote

[Verity Weekly]

Contrasting Influence Foundations

Wealth-centric

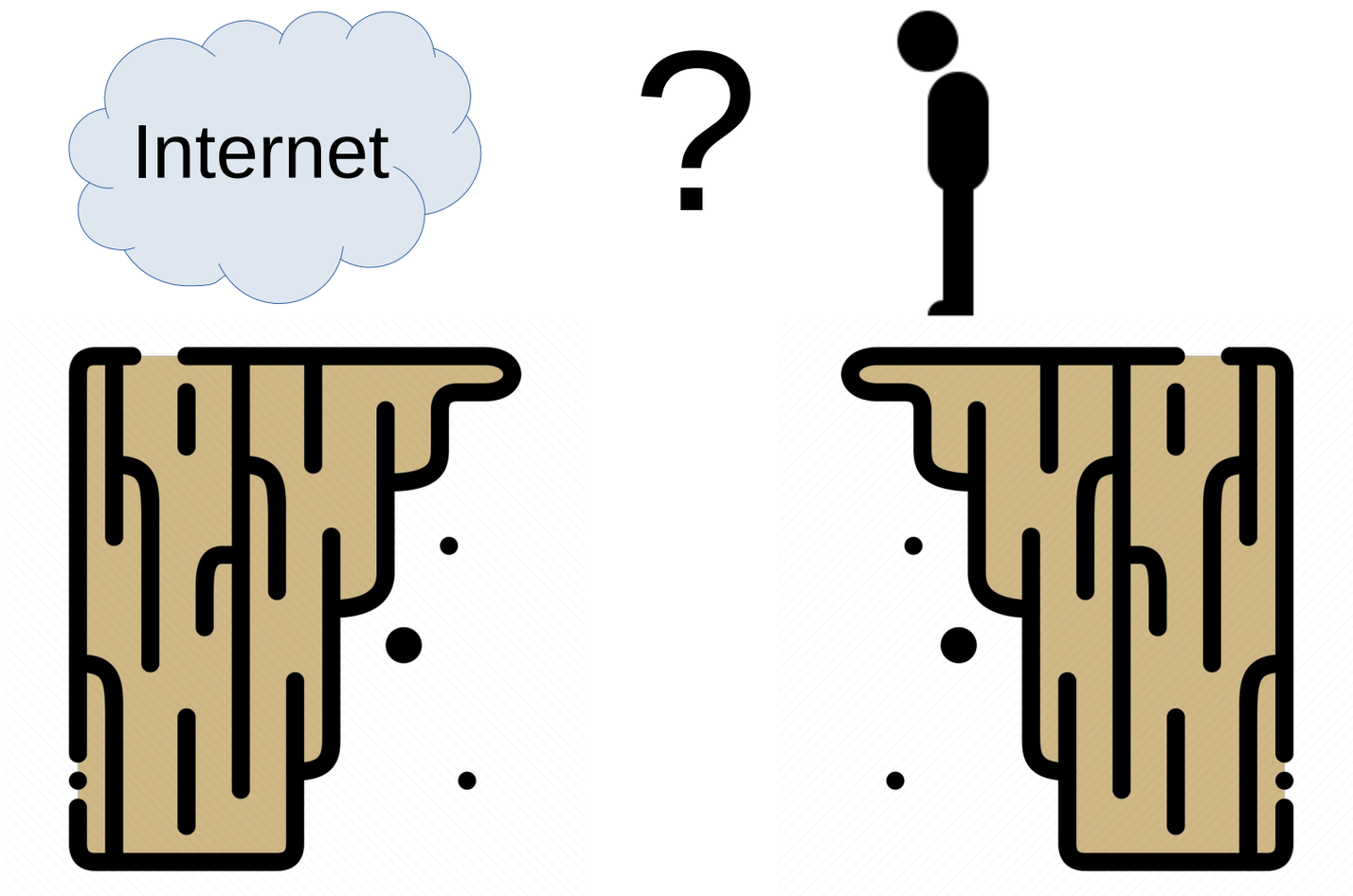
Largely Solved

Person-centric

Largely Unsolved

A Fundamental Problem

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



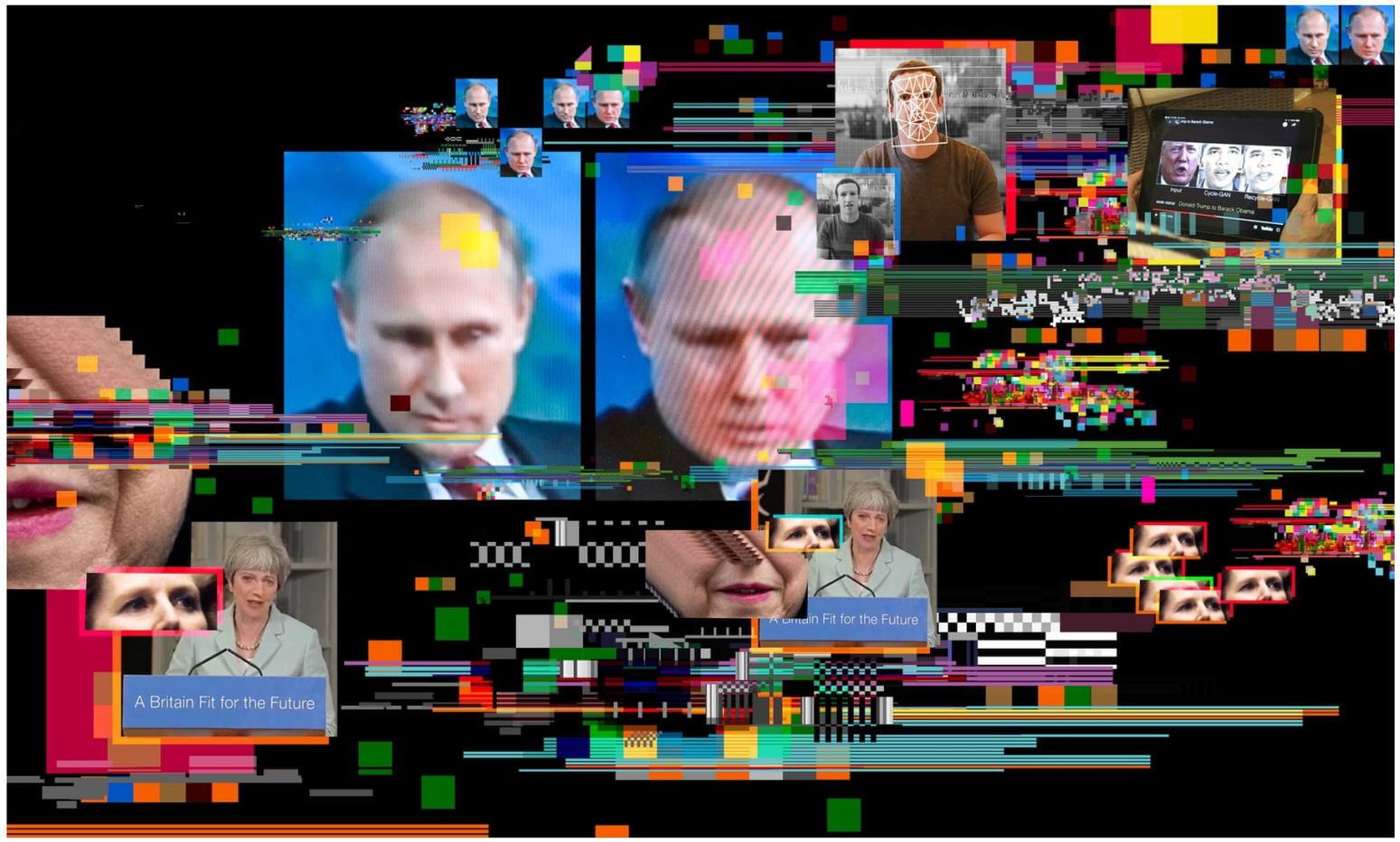
A Fundamental Problem

Services know “people” only as accounts, profiles

[Pixabay, The Moscow Times]

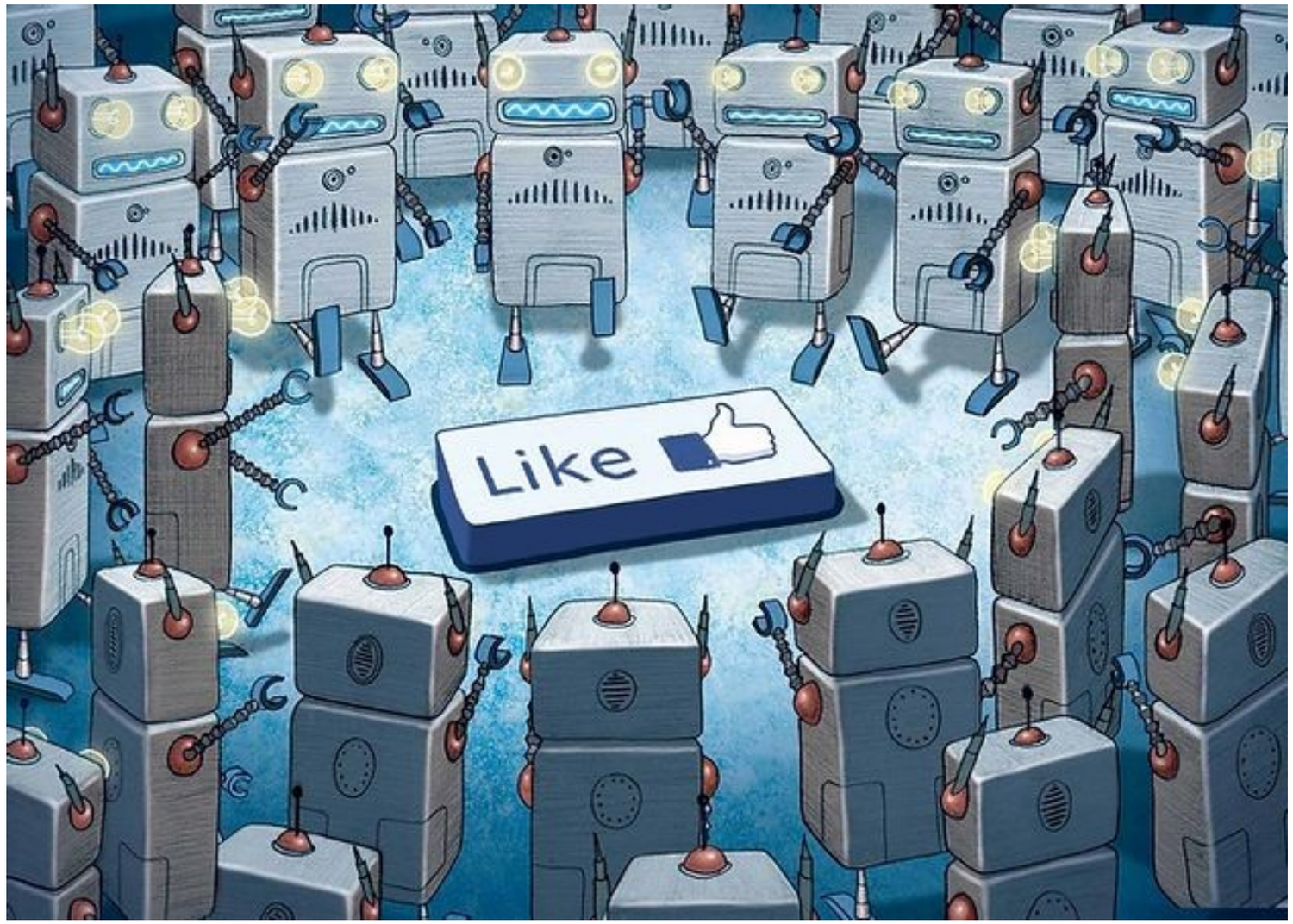
A Fundamental Problem

Profiles are cheap, discardable, easily faked



[Ian Sample, The Guardian]

Likes are fake



[Rabbit Consulting Group]

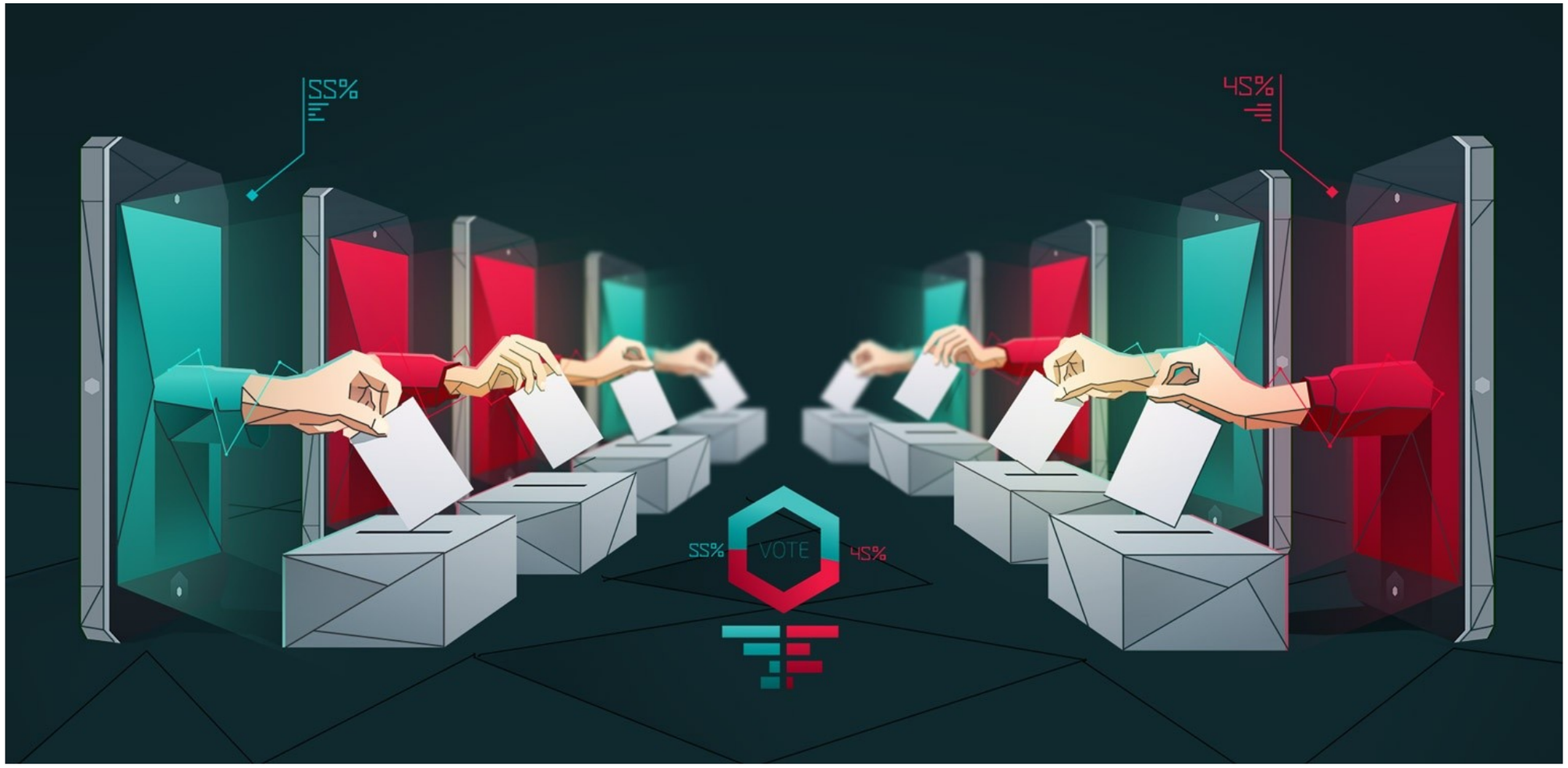
Followers are fake

[Ren LaForme, Poynter]

Reviews are fake

[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*

Online society: missing a foundation?

[All About Healthy Choices]

Decentralized Systems for **People**

How to distribute **voting power** in open systems?

Today's public blockchains: **investment-based**

- **Proof of Work:** waste more energy mining → more voting power & rewards
- **Proof of Stake:** buy, stake more existing coin → more voting power & rewards

DEDIS is building **person-centric blockchains**

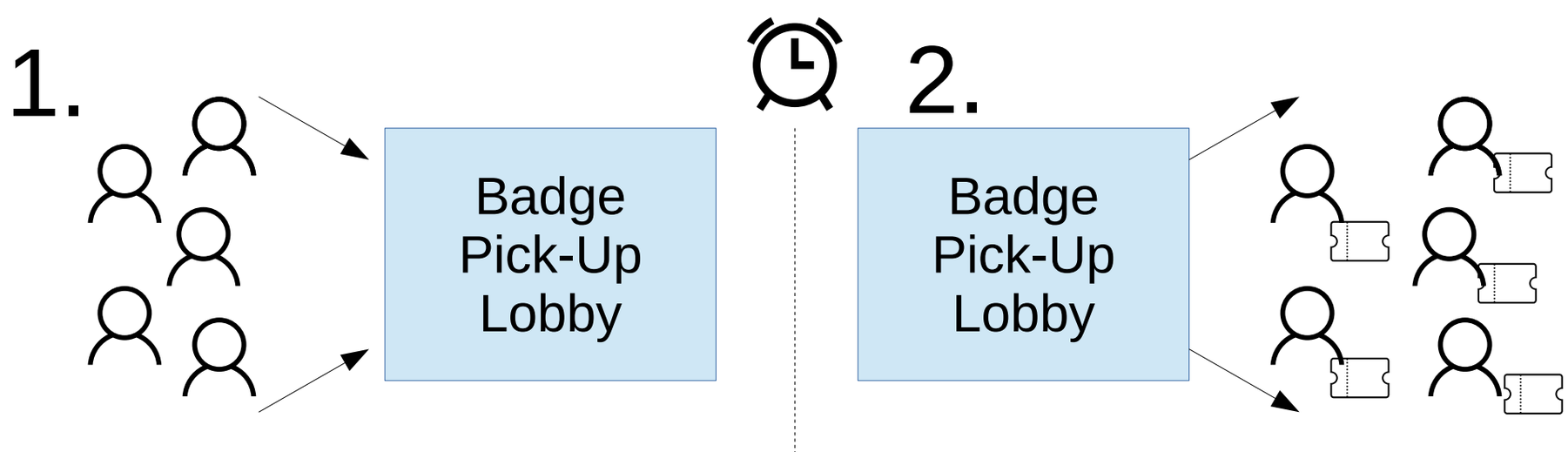
- **Proof of Personhood:** one person, one vote, one quota of rewards, *independent of investment*

One Approach: Pseudonym Parties

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*

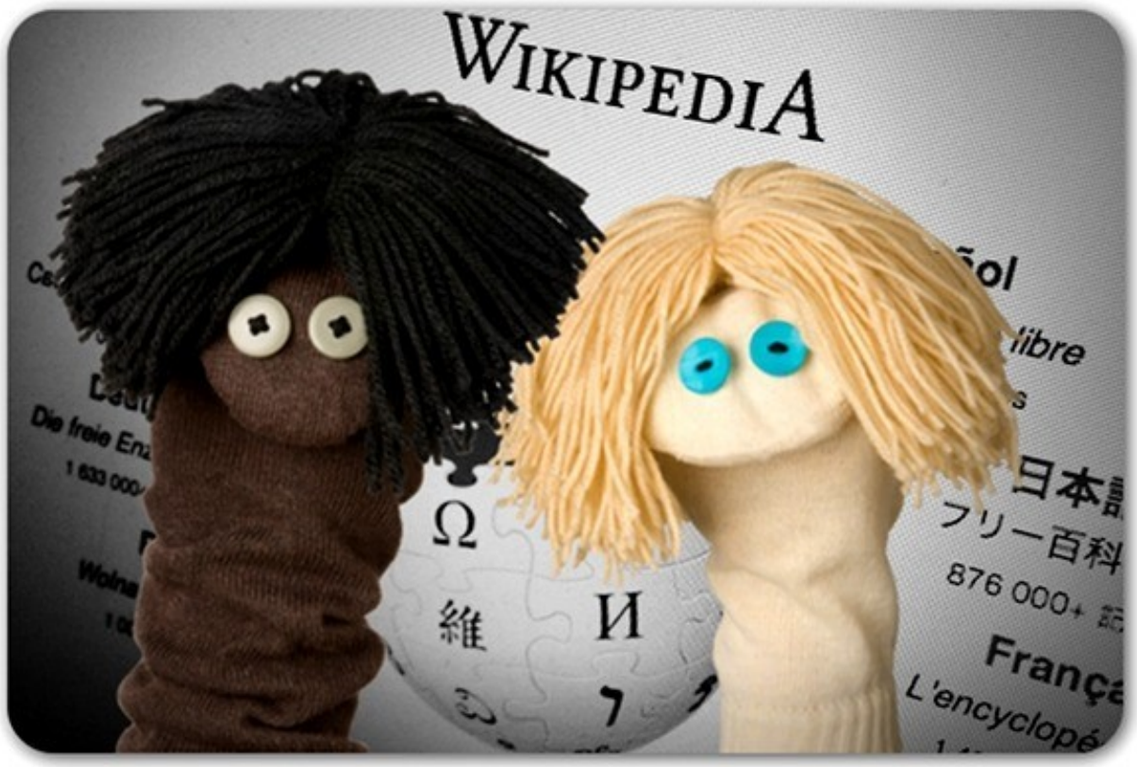
- Attendees file out from lobby to “main event”
- Get *one* QR code each scanned at lobby exit



What is
Proof of Personhood
[potentially]
useful for?

Crowdsourcing w/o Sock Puppets

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



Crypto Universal Basic Income

Enable everyone to “print money” at an equal rate

Old-fashioned governance… online

DEDIS research topics: summary

The DEDIS lab builds experimental systems in:

- Privacy and anonymity technologies
- Blockchains and cryptocurrencies
- Digital identity, personhood, and democracy

…and other topics!