



# Privacy-Preserving Personhood-Based Credentials

Ksandros Apostoli, Simone Colombo, Bryan Ford  
Decentralized and Distributed Systems (DEDIS)  
Swiss Federal Institute of Technology (EPFL)  
[dedis@epfl.ch](mailto:dedis@epfl.ch) – [dedis.epfl.ch](https://dedis.epfl.ch)

IC3 Winter Retreat – January 16, 2022

# We're facing hard global problems



Climate change



COVID-19 pandemic

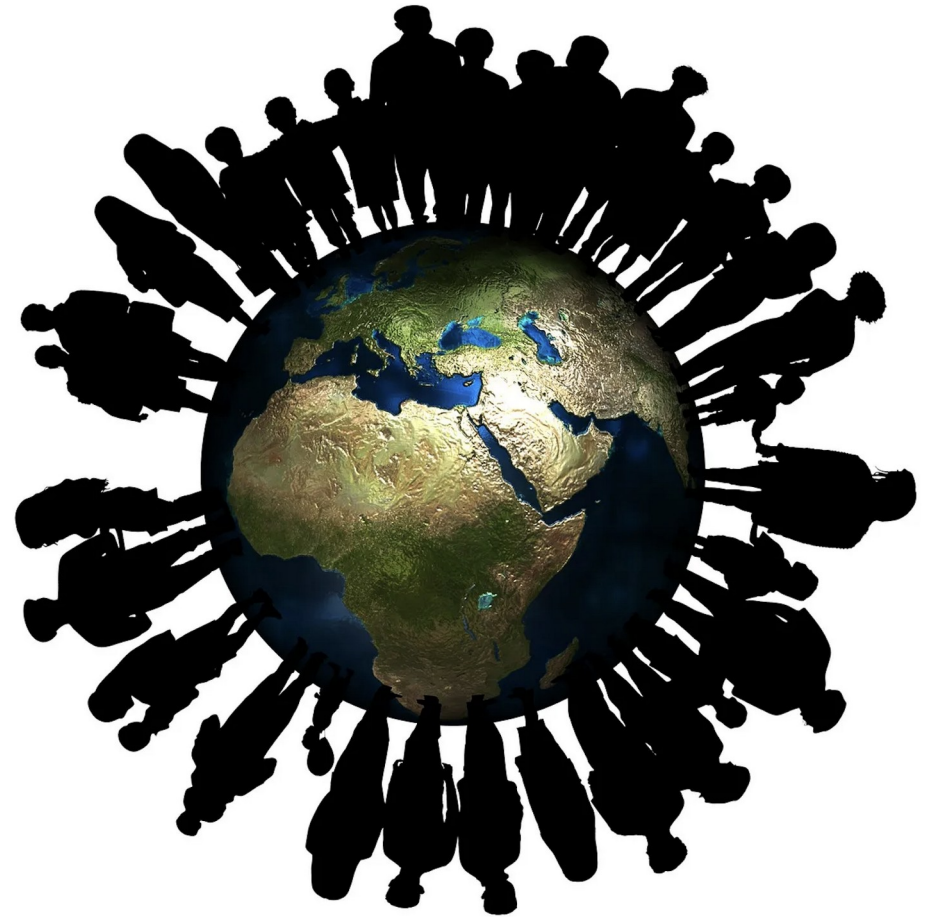


Exploding inequality

# Will decentralized technologies...



Help us find  
*wise* solutions?



Serve *everyone's*  
collective interest?

# Whom do our systems represent?

Most systems today:

## Wealth-centric stake

- One dollar, one vote



[Kera]

What we urgently need:

## Person-centric stake

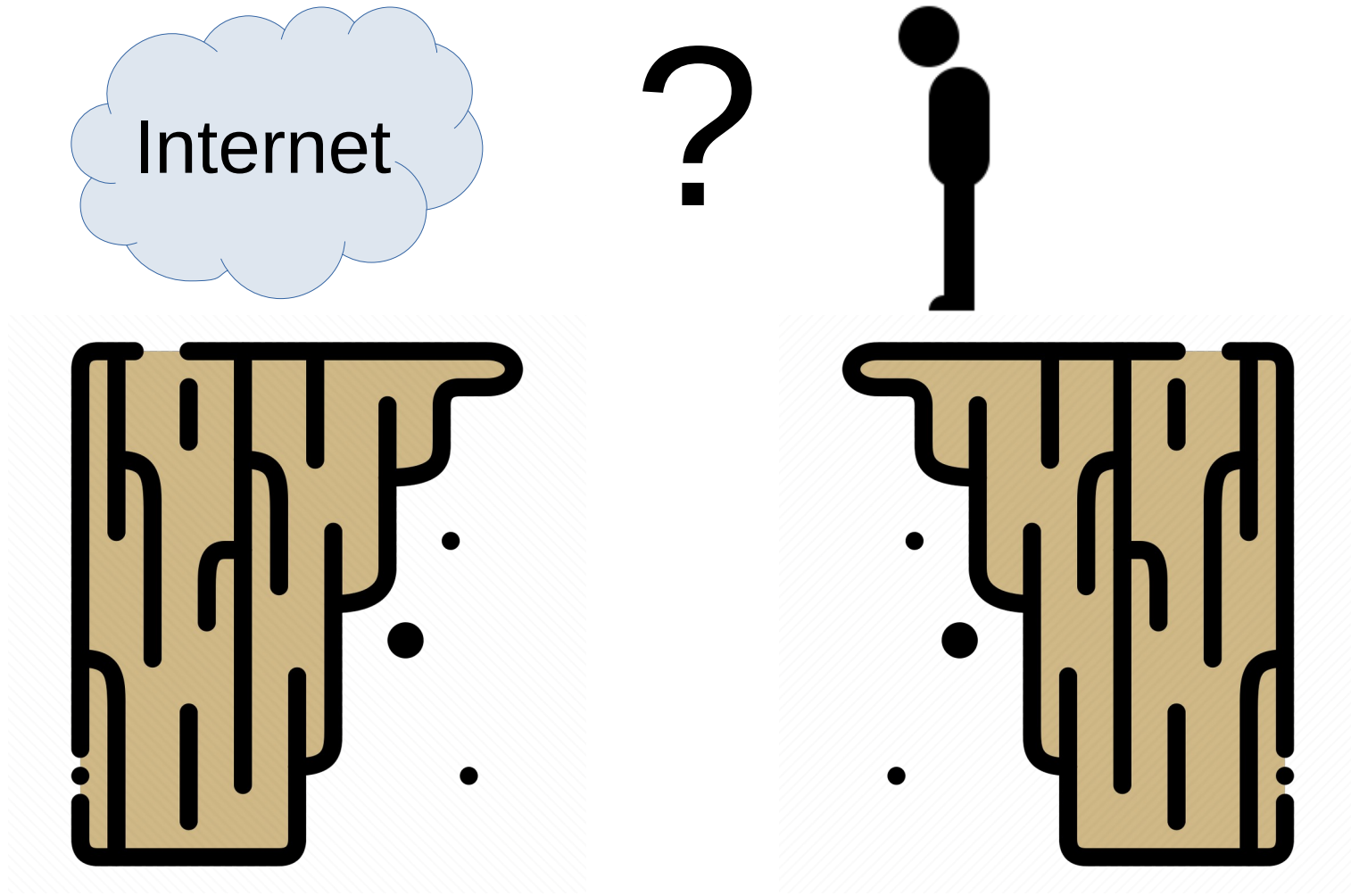
- One person, one vote



[Verity Weekly]

# The Fundamental Problem

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

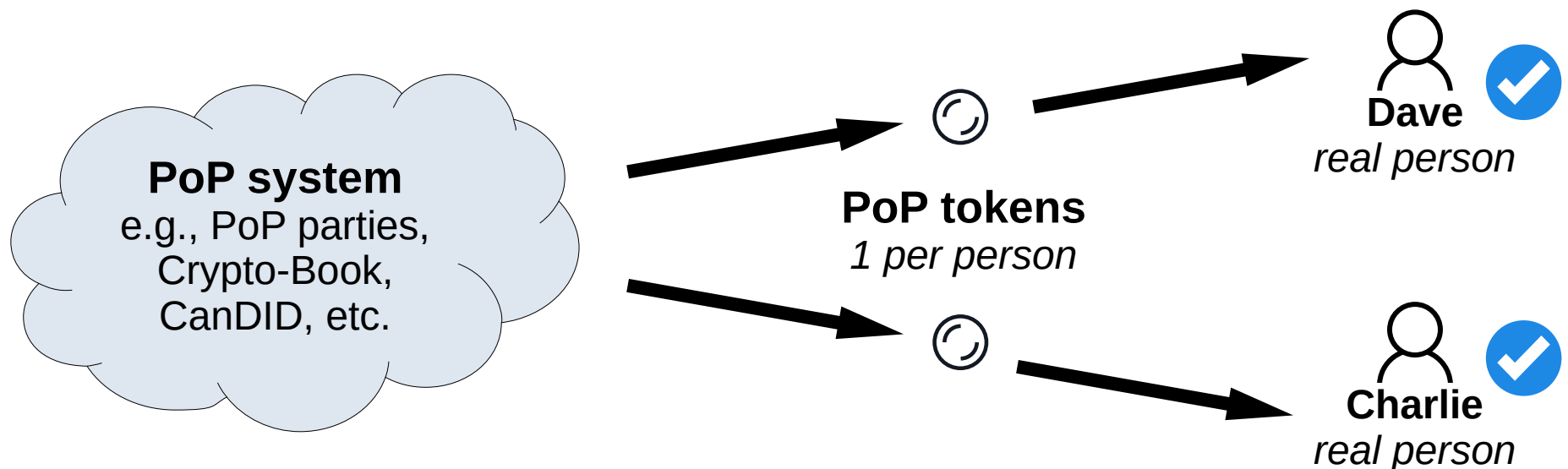


# Proof of Personhood (PoP)



Any method of assigning tokens “**1 per person**”

- “Identity and Personhood in Digital Democracy”
- Ideally: **inclusive, equal, secure, and private**



# There are many approaches to PoP ... *all with appeals & tradeoffs*

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

# Privacy in Proof-of-Personhood

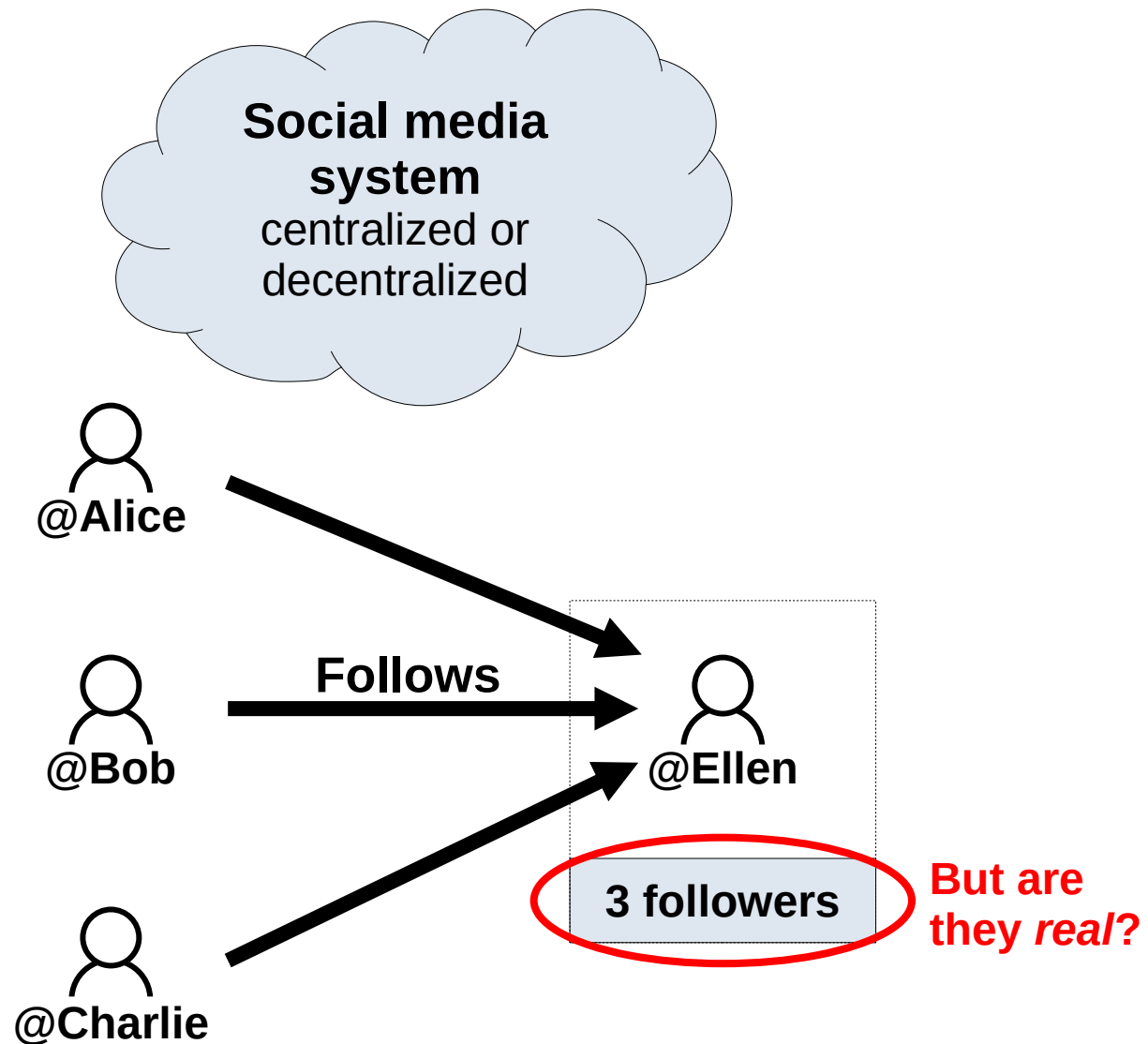
Privacy is important in at least two different ways:

- Privacy in how PoP tokens **are created**
  - What info must you disclose, to whom, to convince everyone your PoP token represents a real person?
- Privacy in how PoP tokens **are used** This talk's focus
  - What info must you disclose (or leak) each time you “show” your PoP token for some purpose?

If you don't care about privacy, then maybe just reveal your SS#/AVS#/equivalent to everyone



# Example application: social media

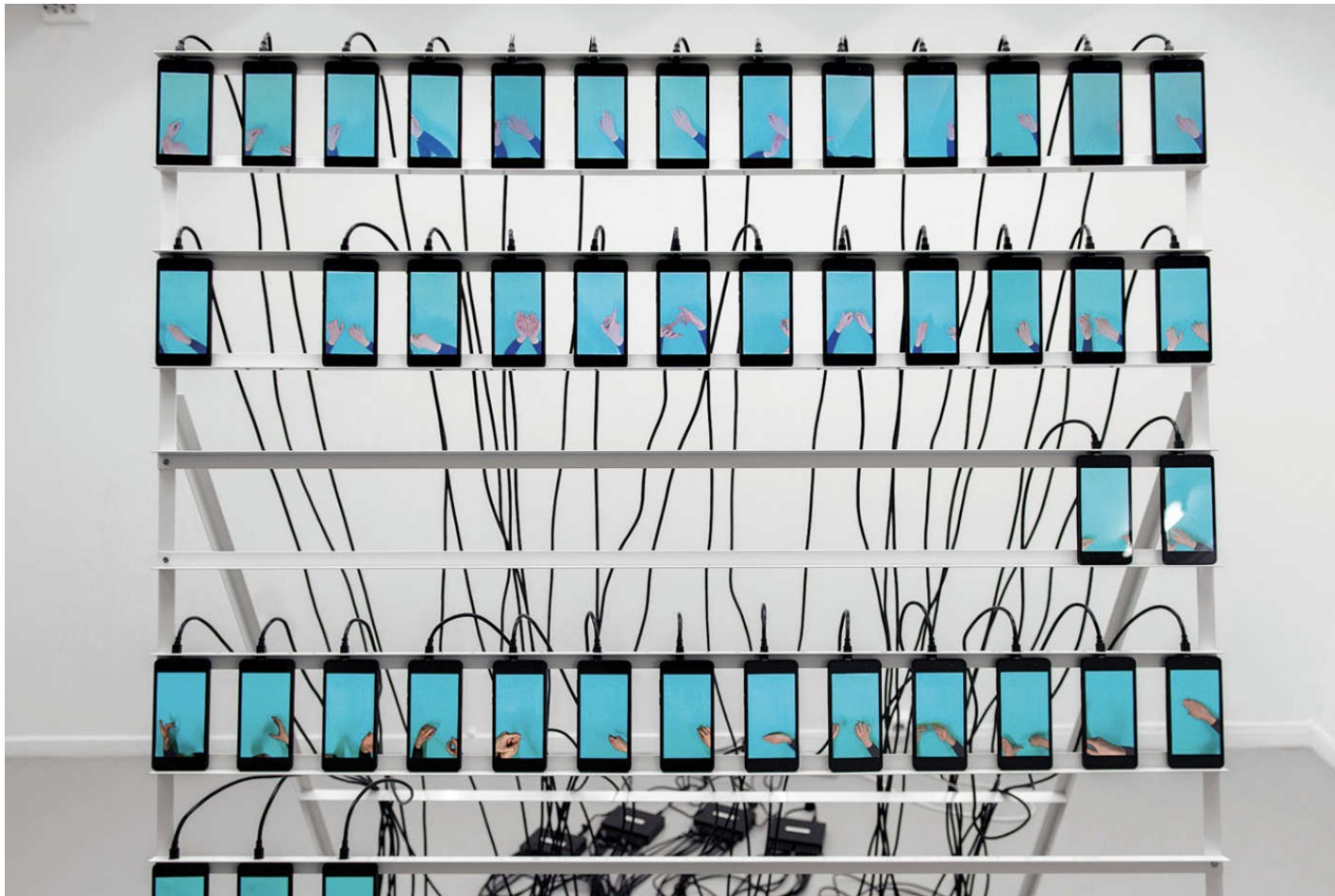




LIFE IN PIXELS | DEC. 26, 2018

## How Much of the Internet Is Fake? Turns Out, a Lot of It, Actually.

By Max Read [@max\\_read](#)



[Ayatgali Tuleubek, Intelligencer]

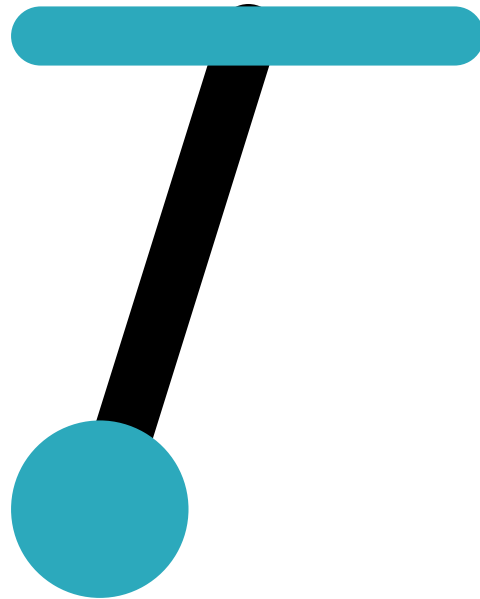
# Privacy versus accountability online

“Privacy is good!”

“Anonymity is a human right!”

“Pseudonyms can protect free speech!”

“Everyone plays several roles in life!”



# Privacy versus accountability online

“Privacy is good!”

“Anonymity is a human right!”

“Pseudonyms can protect free speech!”

“Everyone plays several roles in life!”



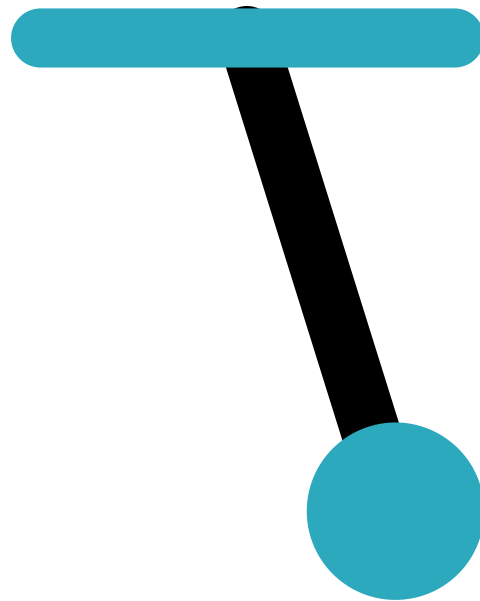
“What are you hiding?”

“Anonymity protects abusive behavior!”

“We need online accountability!”




“Real names!”

“Blue verified accounts!”



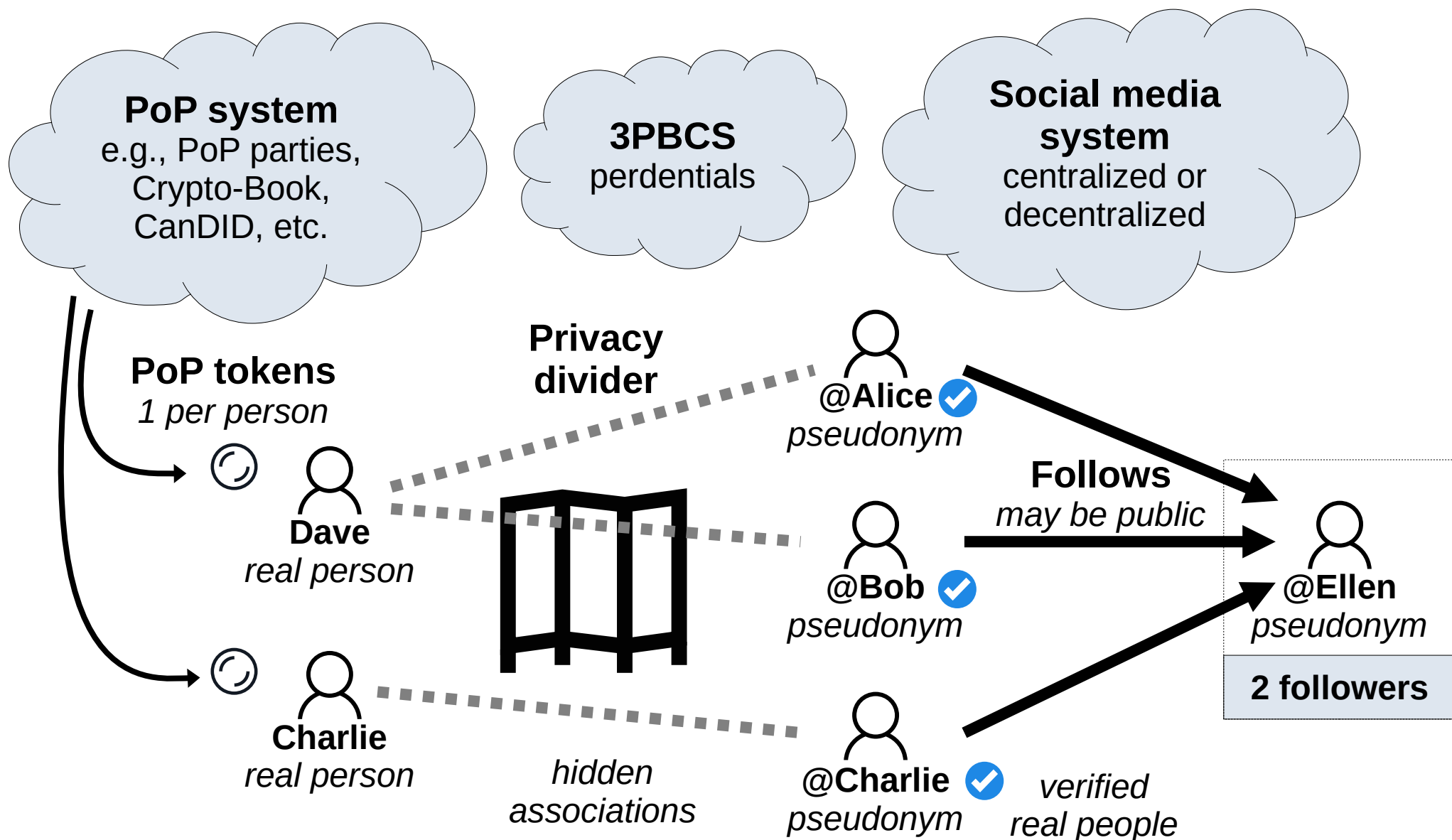
# 3PBCS: a privacy-preserving personhood-based credential system

3PBCS creates **perdentials**: credentials usable to

- Reveal & prove **properties** about the bearer
  - e.g., age > 18, have Ph.D. from U, usual SSI stuff
- Create **pseudonyms** with “real person” status 
  - *Sybil*s allowed! professional, personal, hobby...  
- Allow **counts/quotas** with 1-per-person weight
  - Followers, likes, etc. count only *unique real people*

Builds on *any* PoP scheme + Coconut credentials

# Perdentials: an illustrative scenario



# Social media with 3PBCS

Everyone including @Ellen can see and know:

- “@Alice follows @Ellen”
- “@Bob follows @Ellen”
- “@Charlie follows @Ellen”
- “Ellen has 2 (real-person) followers”

But *no one* learns which 2 accounts are pseudonyms of the *same* real person

- Not even the social media platform

# Limitations, challenges, future

Initial mechanism has unscalable elements

- PoP credential → Coconut credential proof currently linear in anonymity set size (fixable)
- Difficult: preserving privacy under dynamics
  - E.g., if adversary sees “everything” both before & after Alice follows Ellen
- Performance, scalability, generality, ...



# Conclusion



Decentralized technologies can't solve world's hard problems if they can't represent everyone

- Achieving that will require *some* form of PoP
- Both *creation & use* of PoP tokens need privacy

**3PBCS** creates pseudonym-friendly **perdentials**

- Prove “real person” status, allow  $>1$  per person
- Metrics (e.g., “followers) count *unique people*

Privacy can work *with*, not *against*, accountability!