EPFL

C4DT Center for Digital Trust

Decentralized Finance: for the few, the many, or everyone?

Prof. Bryan Ford
Decentralized and Distributed Systems (DEDIS)
Swiss Federal Institute of Technology (EPFL)

Conference on Crypto-Assets - November 5, 2021

Outline

- DeFi now: exciting but niche
- CBDCs: digital money for all?
- Digital assets in civil society
- Digital humanitarian aid

Outline

- **DeFi now: exciting but niche**
- CBDCs: digital money for all?
- Digital assets in civil society
- Digital humanitarian aid

The Promise of DeFi

Permissionless “trustless” assets, payments, exchanges, markets…

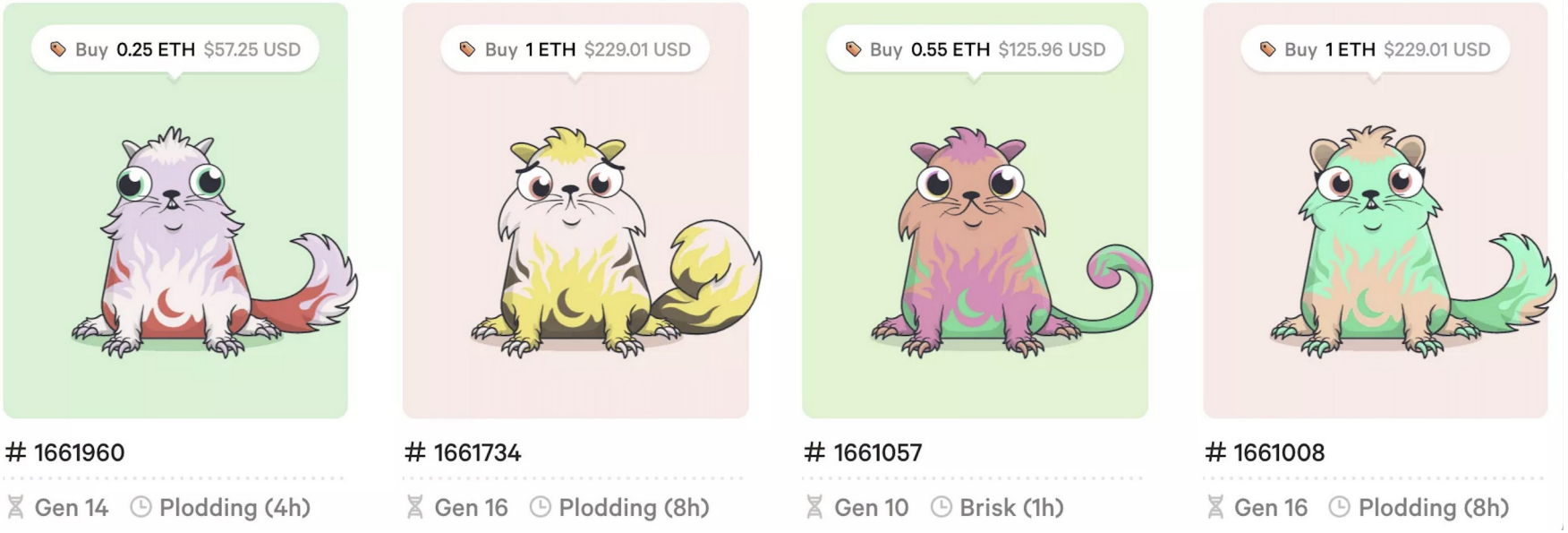
Today’s Main Audience

Geeks

Investors

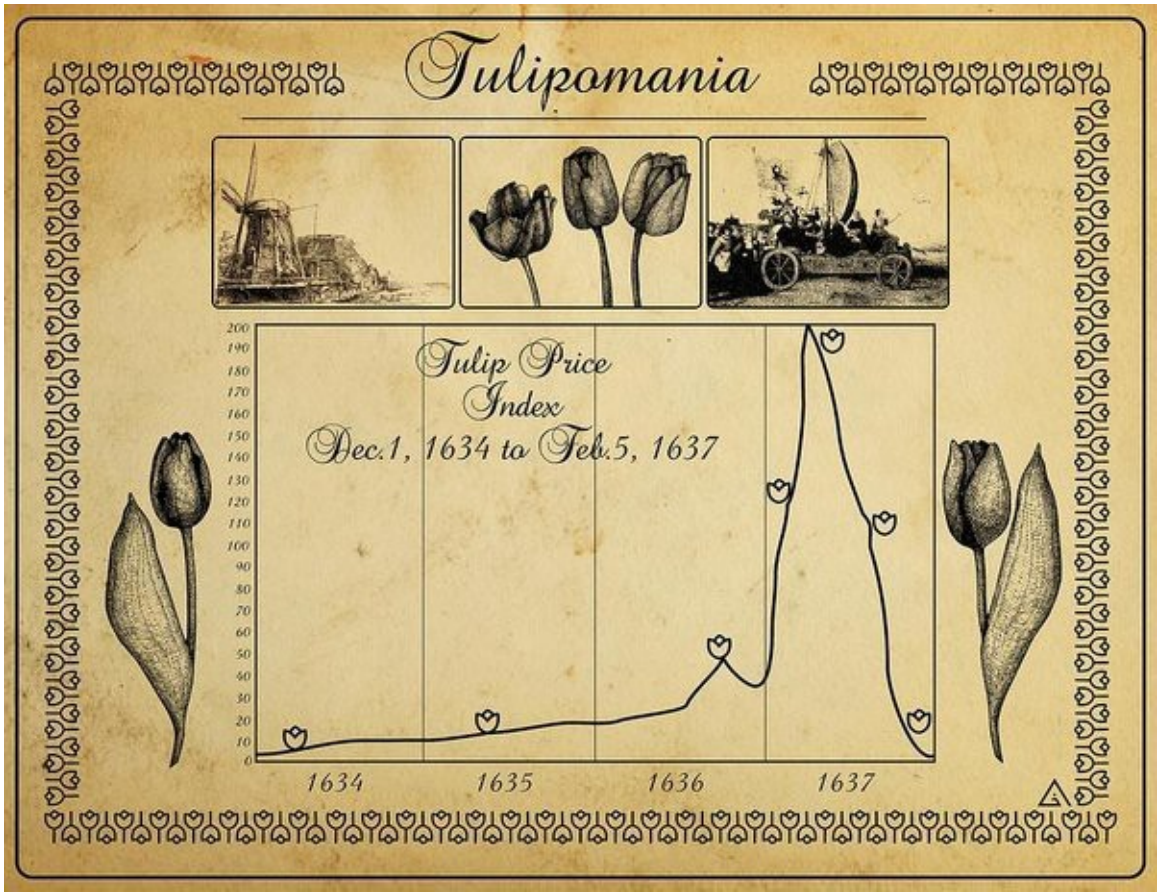
Today’s Digital “Assets”

Cryptocurrencies, tokens, NFTs…



Are these for “everyone”?

We know where mass speculation on intrinsically useless collectibles leads



Outline

- DeFi now: exciting but niche
- **CBDCs: digital money for all?**
- Digital assets in civil society
- Digital humanitarian aid

Everyone needs money

Measure, store, and exchange value

Ordinary commerce, scale → stability

The Role of Central Banks

Now issue & manage paper currency;
can issue & manage digital currency

Some Issues with CBDC

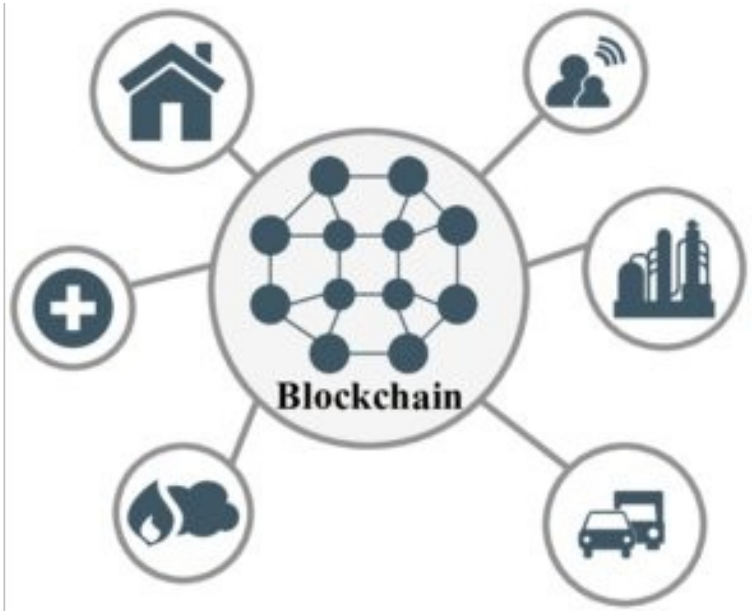
Will it work? Scale? Be secure?

Will public accept it? Should they?

Centralized CBDCs?

Could run on public or private clouds

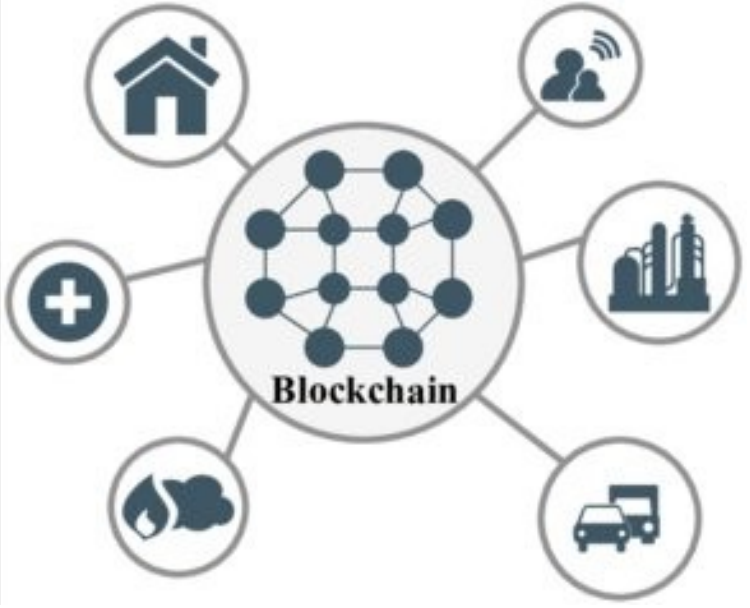
- Simple, efficient, easy to scale
- Single points of failure, compromise



Decentralized CBDCs?

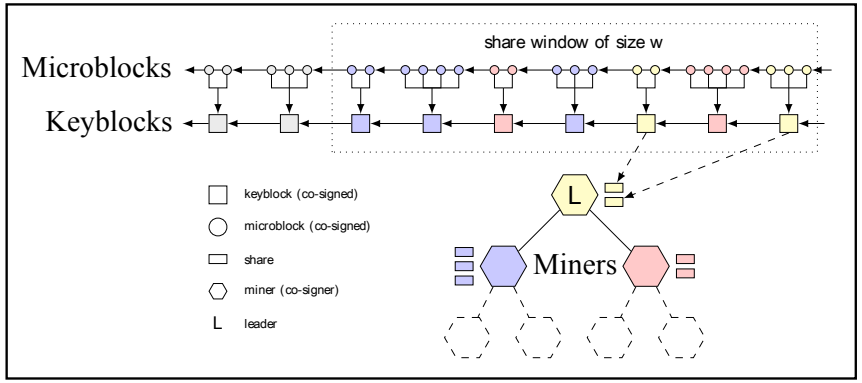
Could use public, private blockchain

- More redundancy, harder to scale
- Greater resilience to compromise

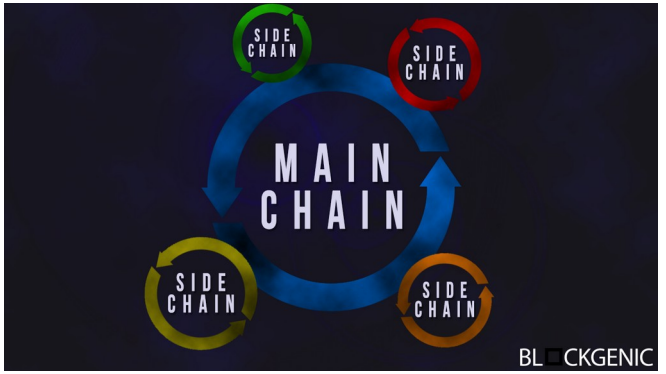


Decentralized *can* scale

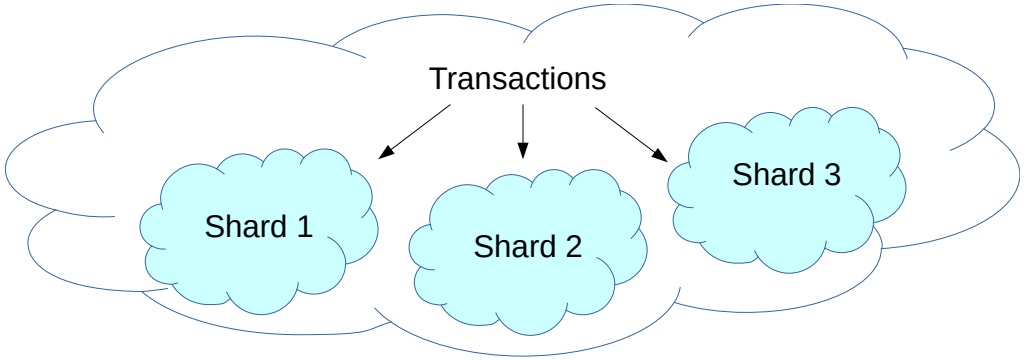
Scalable BFT



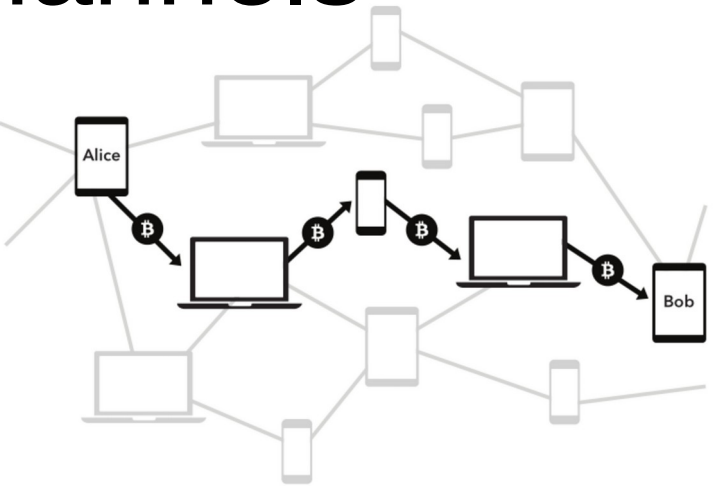
Sidechains



Sharding



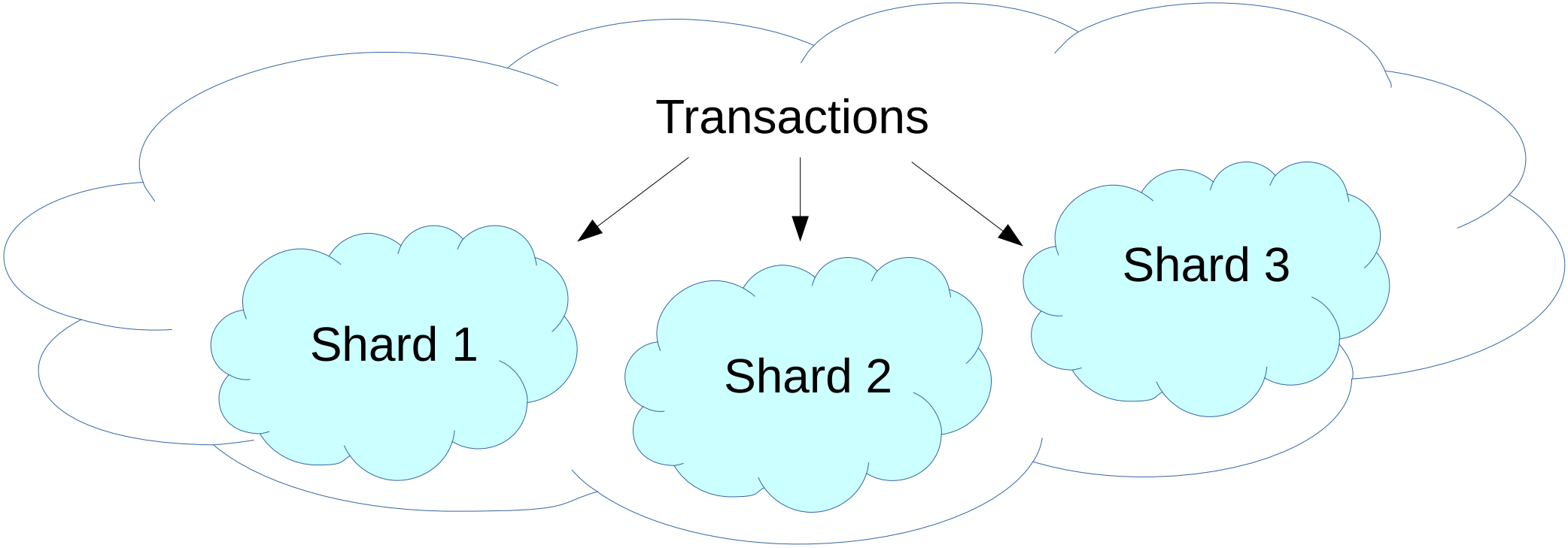
Channels



Scaling by Sharding

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

- Break large collective into smaller random subgroups
- Builds on scalable bias-resistant randomness protocol
- Commit transactions cross-shard w/ 2-phase protocol



The Privacy Challenge

Will CBDCs be, or be *perceived as*, a **digital payment panopticon**?

Privacy requirements

Must be (and can be) addressed:

- Identity privacy: who paid?
- Transaction privacy: how much?
- User accountability: AML, CFT
- Government accountability: financial inclusion, due process

Privacy *with* Accountability

User

Government

Accountability
User to Government:
protection against
money laundering,
financing terrorism,
tax evasion

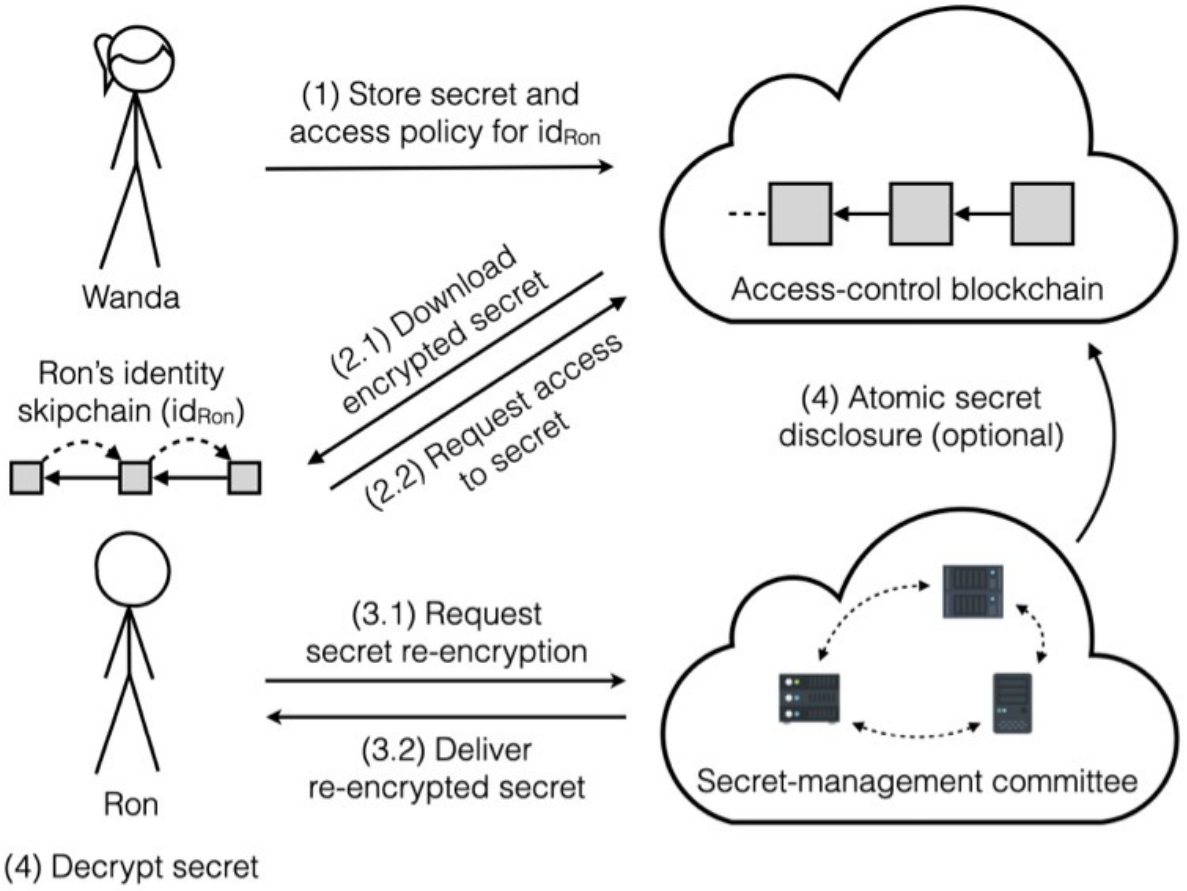
Accountability
Government to User:
protection against
unreasonable search/seizure,
financial exclusion,
denial of rights

One useful technology

Decentralized “on-chain” secret data

CALYPSO: Private Data Management for Decentralized Ledgers

[VLDB ‘21]



Privacy solution sketch

Travel Rule: TXs must carry identities

- But could be encrypted to trustees, governed by public smart contract
  - Decryptable under lawful warrant
  - Privacy-preserving blacklist checks
- Denied? Users *must* have usable, transparent recourse process

Outline

- DeFi now: exciting but niche
- CBDCs: digital money for all?
- **Digital assets in civil society**
- Digital humanitarian aid

Democratized DeFi

Healthy democracies depend on:

- **Government:** representative
- **Business:** investment/profit-driven
- **Civil society:** non-profit sector

On what basis do people *participate* and wield *influence* in each sector?

Basis of Influence

Wealth-centric

- One dollar, one vote

[Kera]

Person-centric

- One person, one vote

[Verity Weekly]

Basis of Influence

Wealth-centric

- One dollar, one vote

Business, investment

Person-centric

- One person, one vote

Government, civil society

Basis of 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 voting
- Elected parliaments
- Membership clubs
- Committees
- Town hall meetings
- Direct democracy
- Liquid democracy

Digitalization of Influence

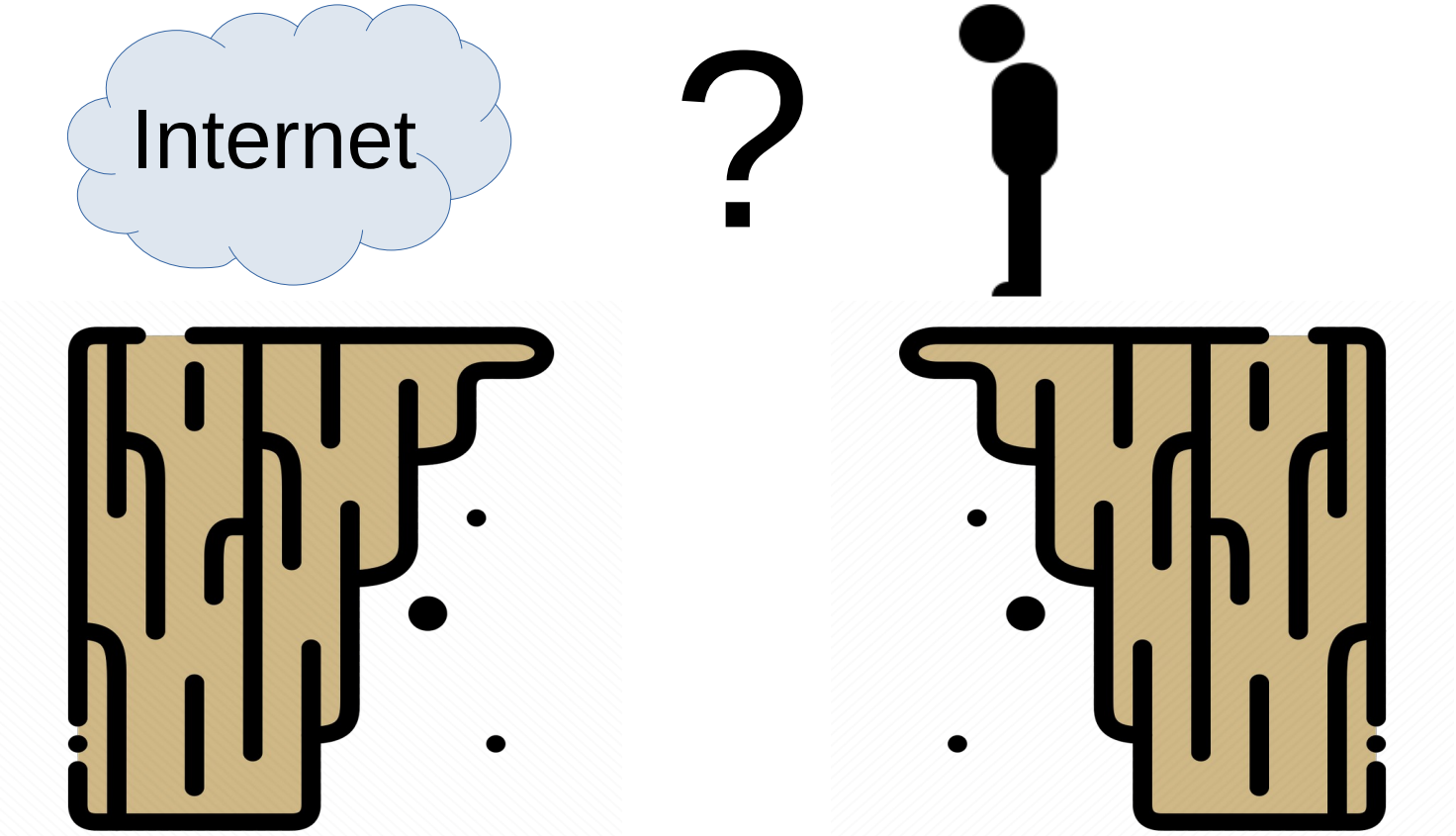
As self-governance shifts online…

- **Wealth-centric:** many solutions
- **Person-centric:** more elusive

[Infinity Economics]

A Fundamental Problem

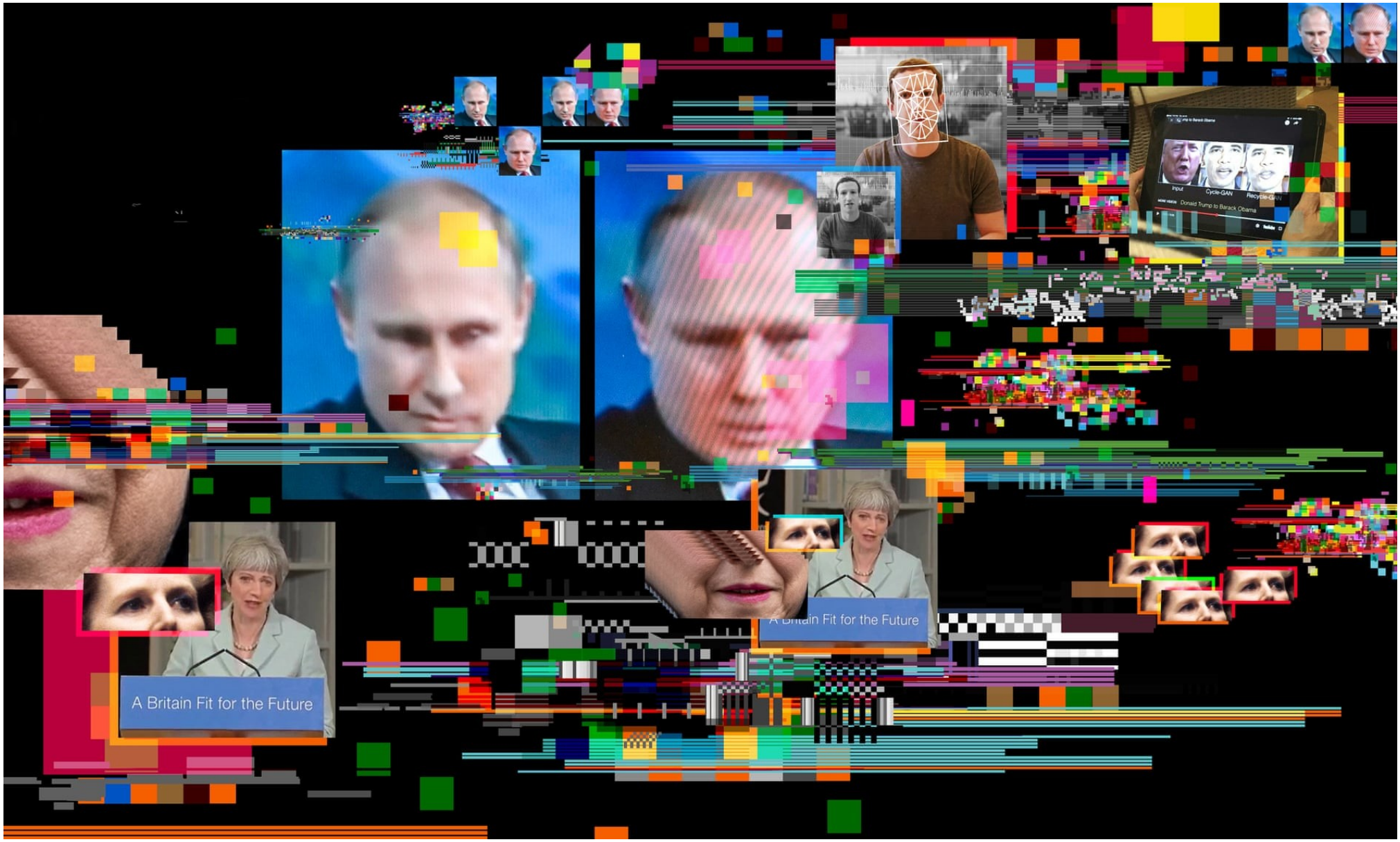
Today's Internet doesn't know what a "person" is



Online “people” are profiles

[Pixabay, The Moscow Times]

Profiles are Often Fake



[Ian Sample, The Guardian]

Profiles are Often Fake

Cheap, discardable, automated

Upside:
inclusion, privacy

Downside:
are “people” really *people*?

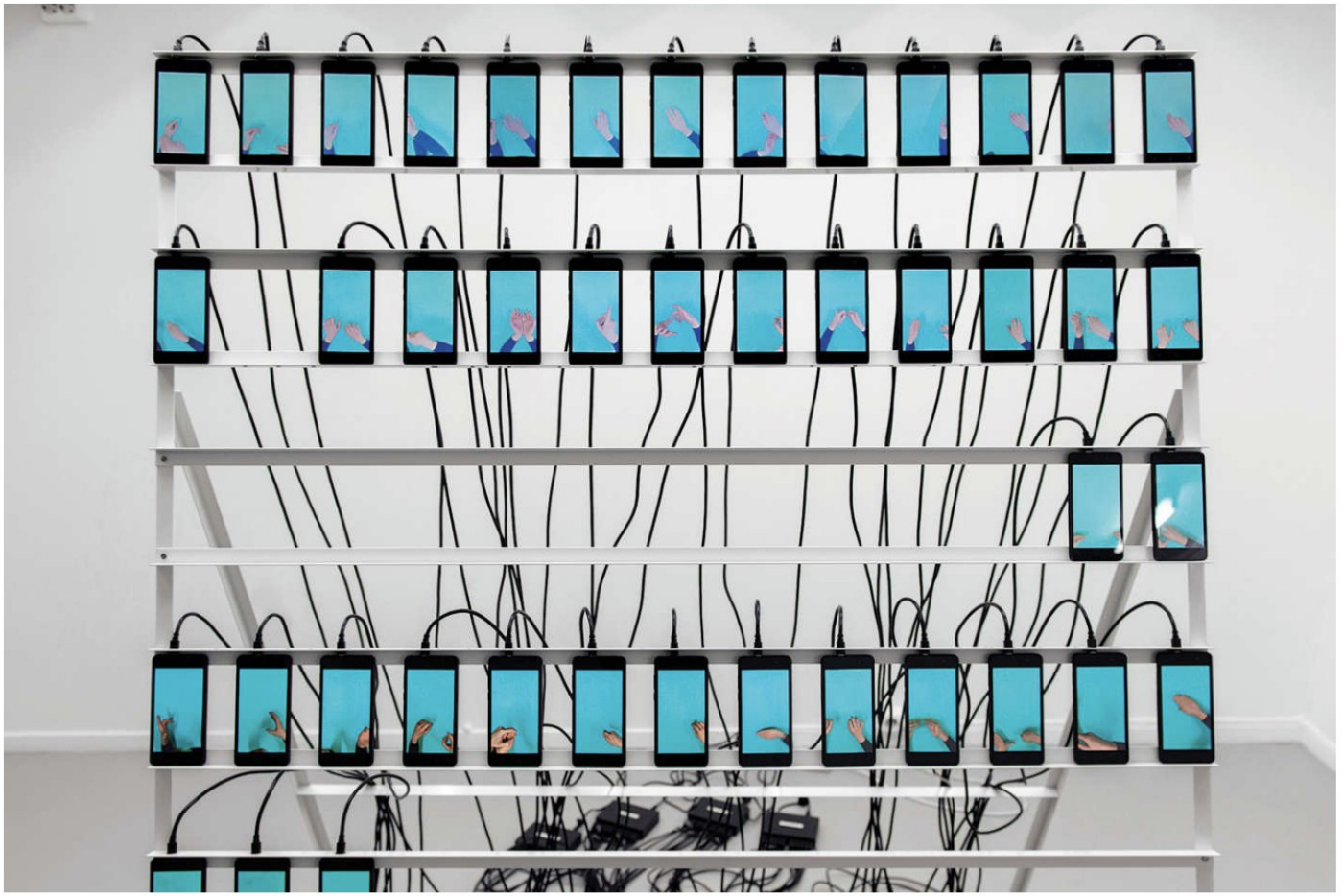
Profiles are Often Fake

[Ren LaForme, Poynter]

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]

Is a Foundation Missing?

[All About Healthy Choices]

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/

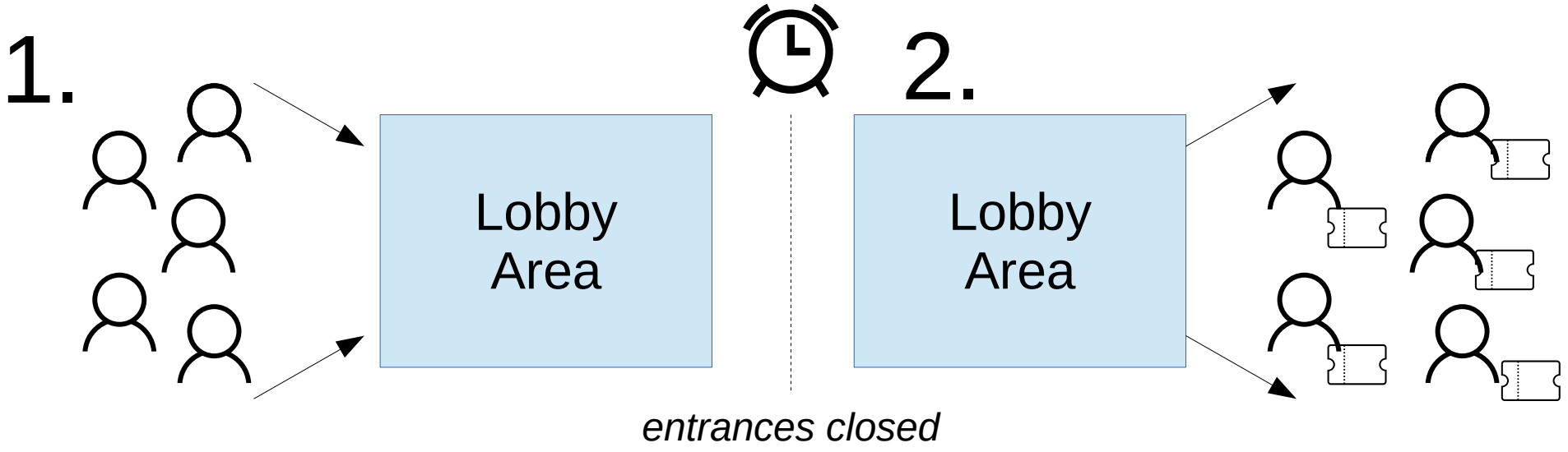
Identity and Personhood in Digital Democracy: Evaluating Inclusion, Equality, Security, and Privacy in Pseudonym Parties and Other Proofs of Personhood

Bryan Ford
Swiss Federal Institute of Technology in Lausanne (EPFL)

November 4, 2020

Pseudonym Parties

- Gather in **lobby** area by a deadline
- After deadline, no one else gets in
- Attendees get 1 token while leaving



An Explosion of Interest

Many other recent approaches and projects

- 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]

Digital Civil Society

Civil society is moving online too

- Needs permissionless participation, similar to public blockchains
- But requires “one person one vote” influence, stake, reward foundation
- Are proof-of-personhood tokens a core digital asset for civil society?

Outline

- DeFi now: exciting but niche
- CBDCs: digital money for all?
- Digital assets in civil society
- **Digital humanitarian aid**

Important Trends in Aid

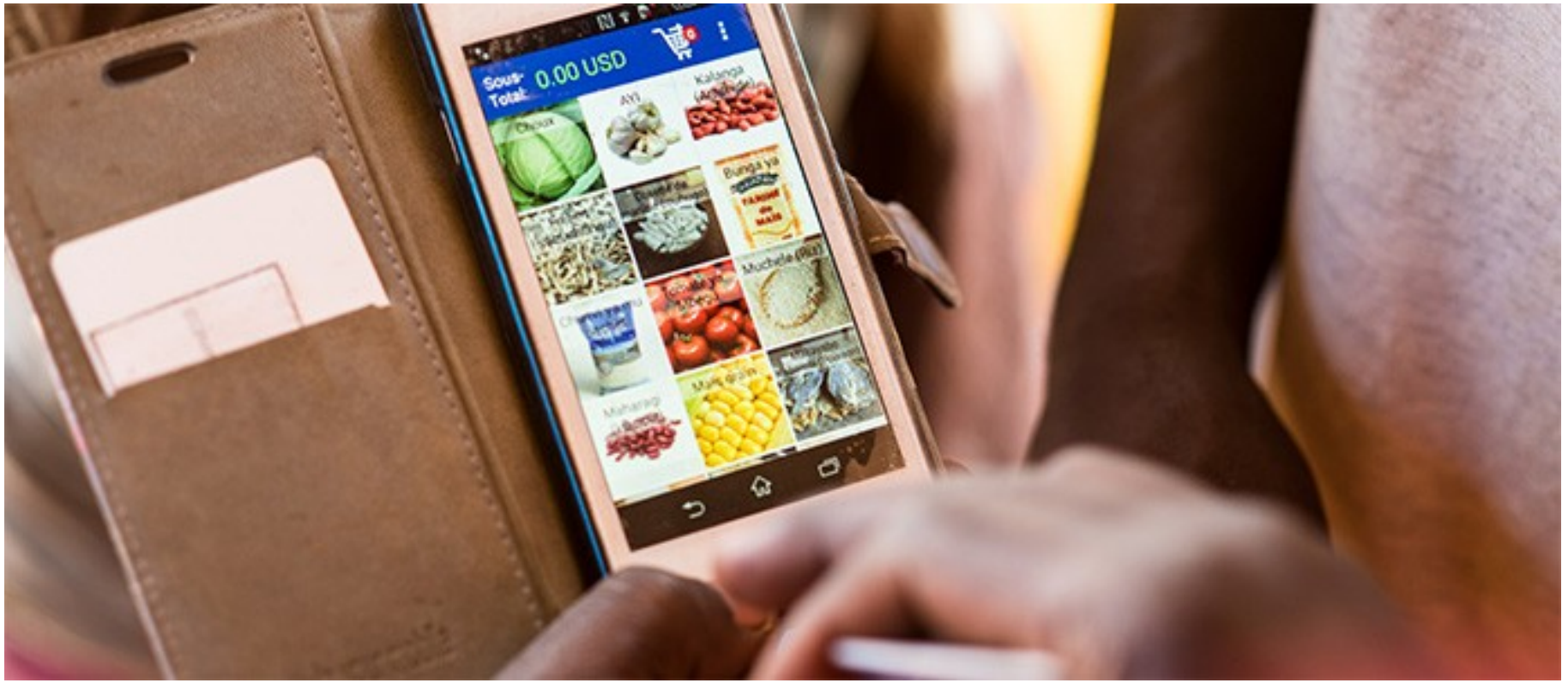
Increasing use of *cash transfer* aid

- Give beneficiaries flexibility, choice

Important Trends in Aid

Digital distribution & management

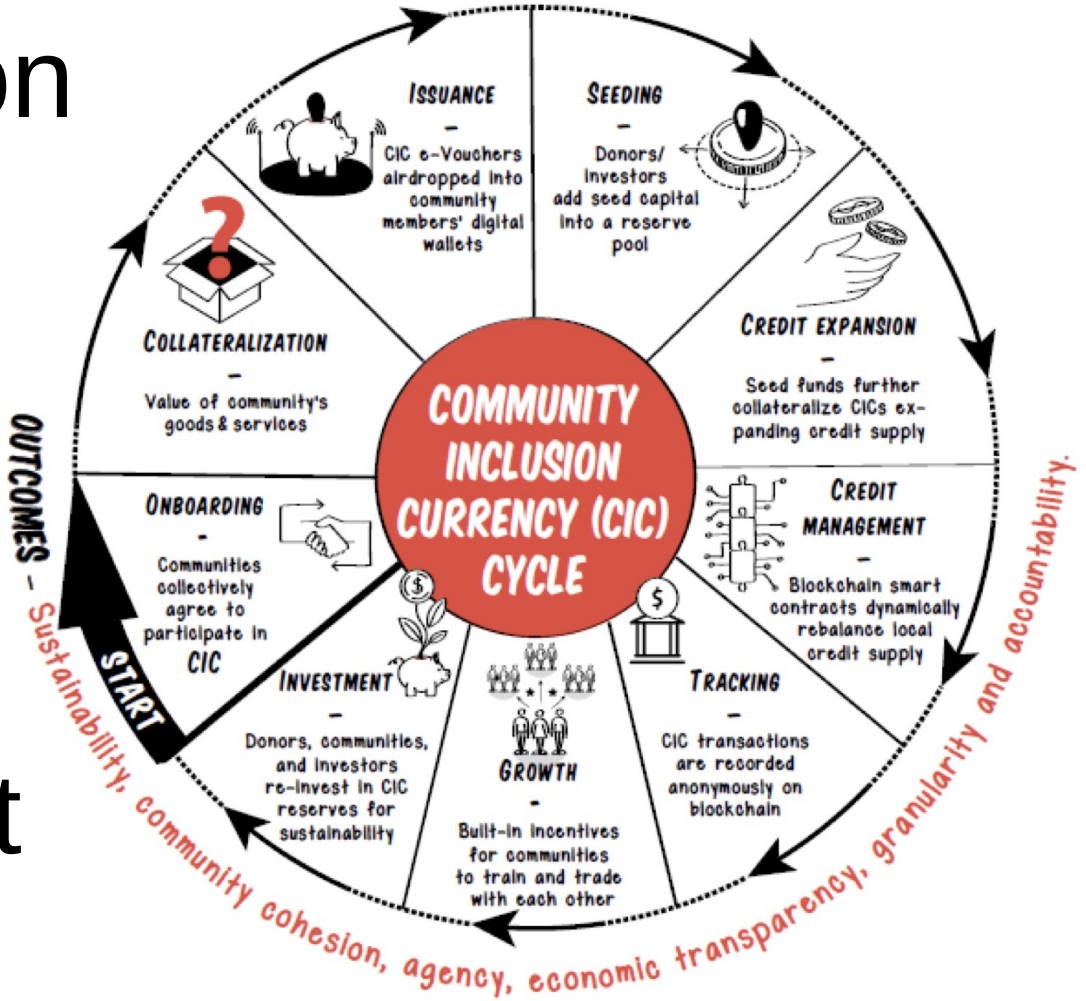
- Cost, convenience, worker safety



Important Trends in Aid

Community inclusion currencies

- Local circulation
  →
- Repeated benefits
  →
- Multiplier effect



The Identity/KYC Problem

Financial services require KYC

- For AML/CTF under FATF standard

Humanitarian agencies (e.g., ICRC) mandated to help *all in need* neutrally

- Many potential beneficiaries unable or unwilling to undergo KYC checks

One side's freedom fighter is…

New DEDIS Research

PAIDIT: Private Anonymous Identity for Digital Transfers

- EPFL-ICRC collaboration under Humanitarian Action Challenges
- Create inclusive, privacy-preserving wallet & verification technology for risk-based due diligence (RBDD)

Build on proof of personhood concept

Conclusion

Can we make digital assets relevant, safe, and inclusive for *everyone*?

- CBDCs with accountable privacy
- Proof of personhood for civil society
- Inclusive humanitarian cash aid