



Digital Architecture for Trust in the 21st Century

Prof. Bryan Ford

Decentralized and Distributed Systems (DEDIS)

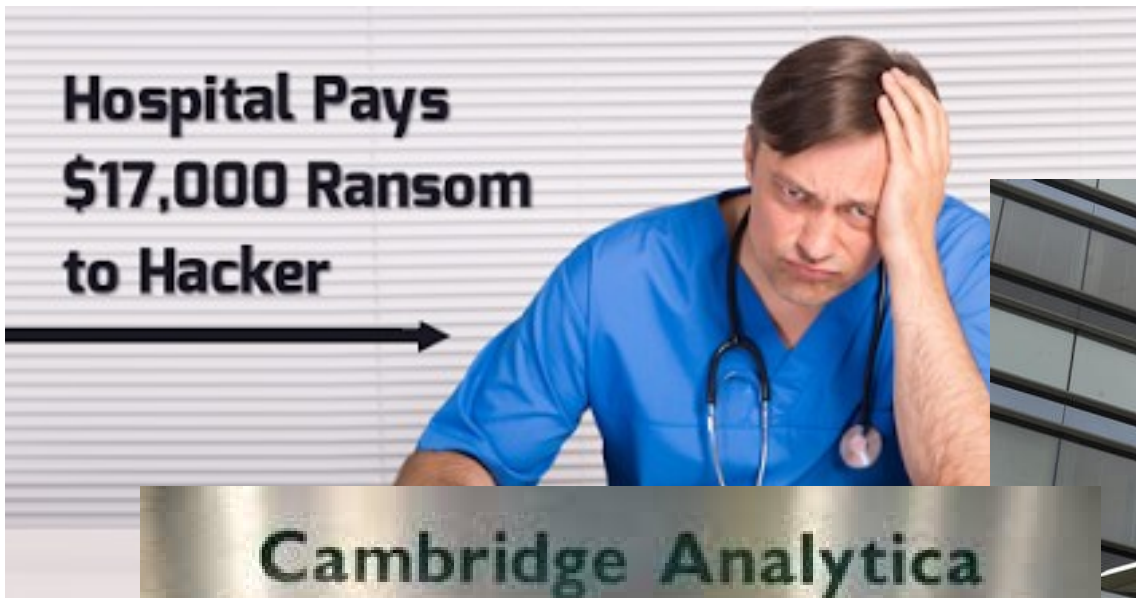
School of Information and Communications (IC)

dedis@epfl.ch – dedis.epfl.ch

House of Switzerland – Davos – January 22, 2020

Why should we trust technology...

...when it so routinely **violates** our trust?



Critical hacks

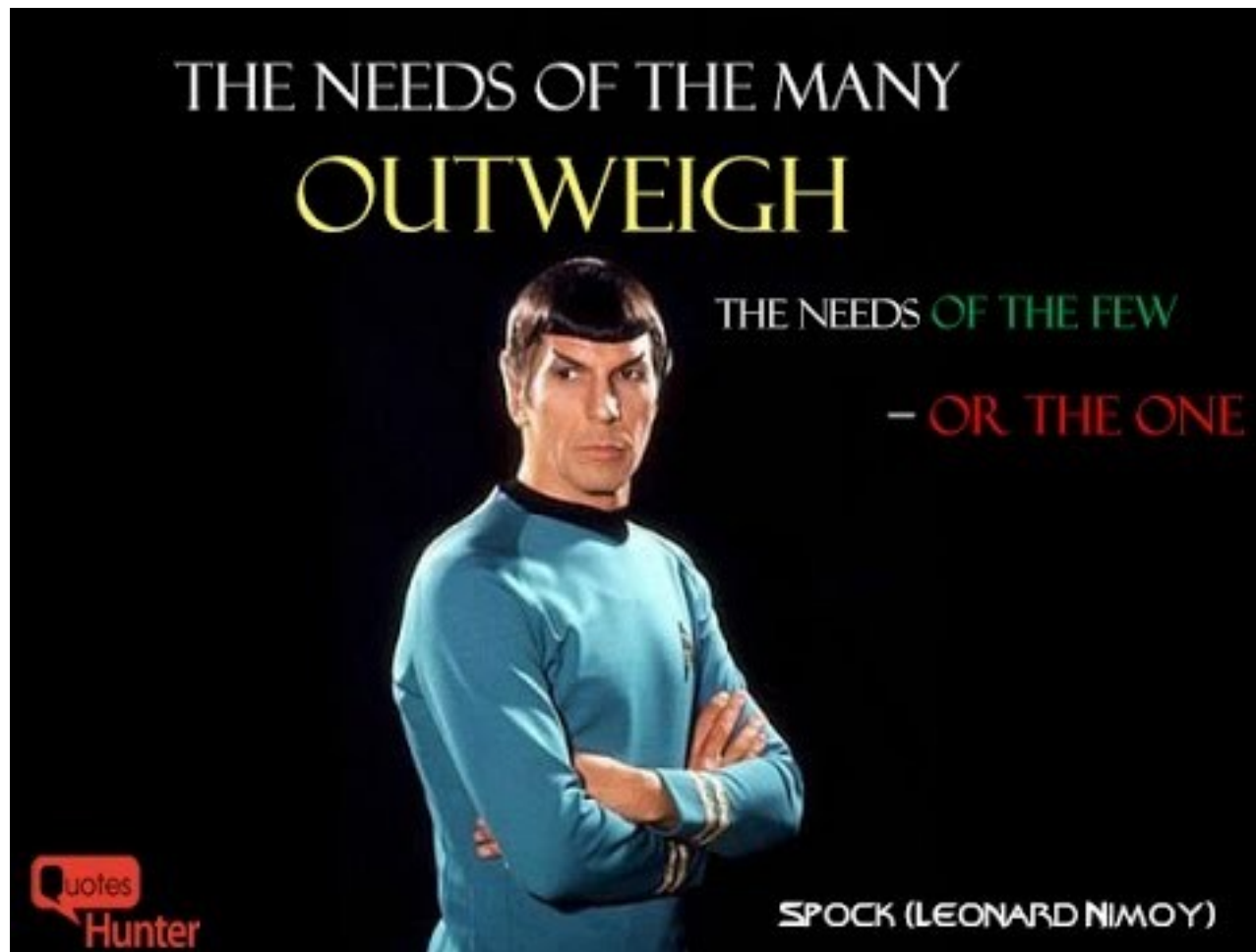


*Privacy breaches
Misuse of data*

Who is technology accountable to?

Like an organization: it depends on **architecture**.

- Does tech serve the **one**, the **few**, or the **many**?



When we get the answer wrong...



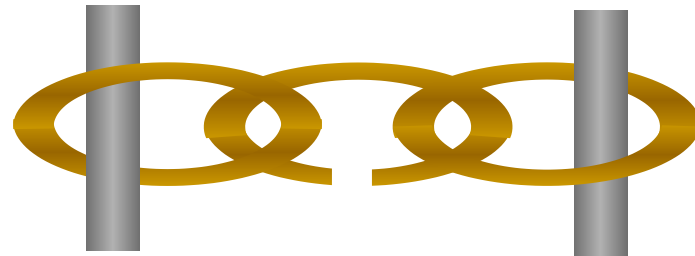
Have we created a tech monster?



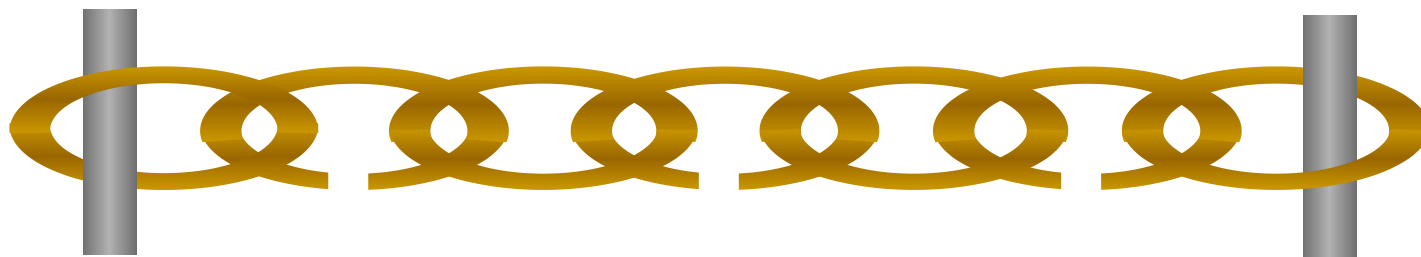
Whom do you serve?

Today's Weakest-Link Security

Any **one** developer, server, administrator can completely compromise security and privacy



More data, connectivity → weaker security



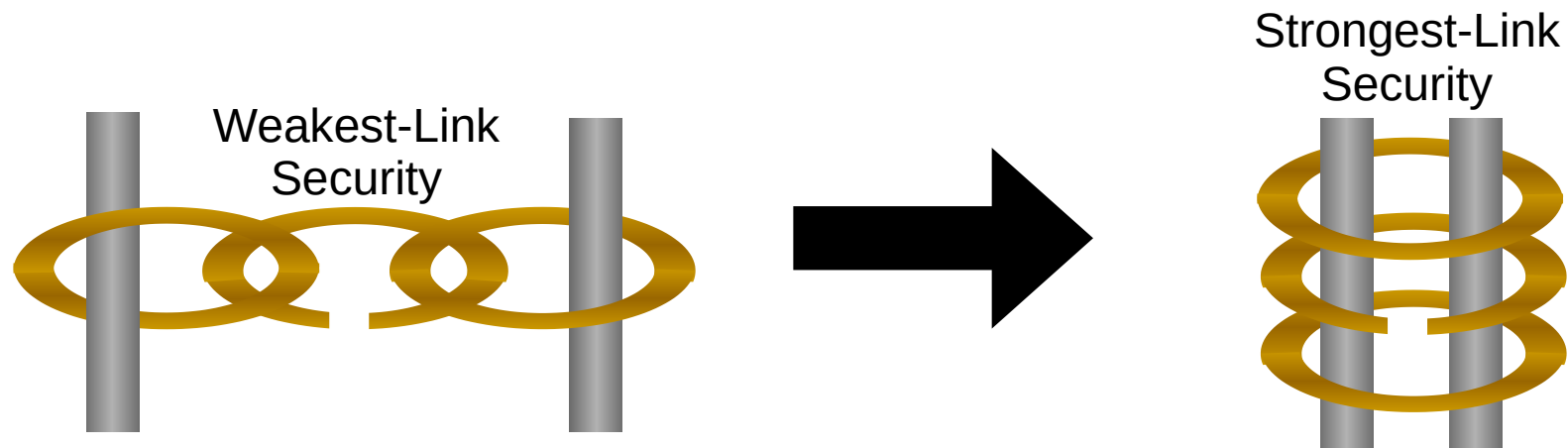
The DEDIS lab at EPFL: Mission

Build advanced **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


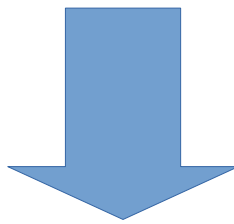
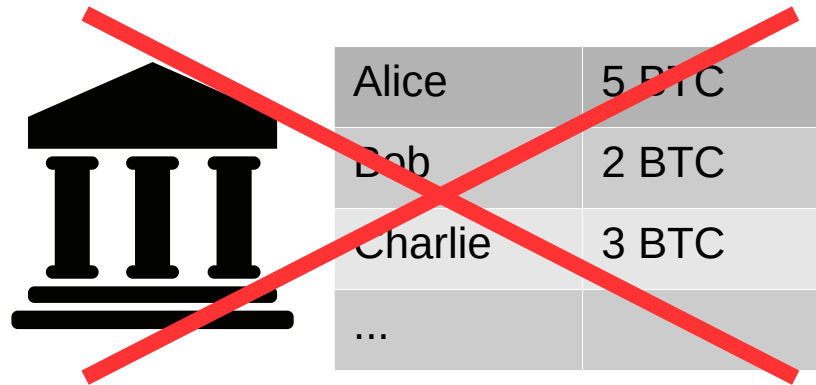
Systems that **distribute trust** widely with **strongest-link security**

<https://dedis.epfl.ch>




The Promise of Distributed Trust

Why blockchains, distributed ledgers are exciting




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

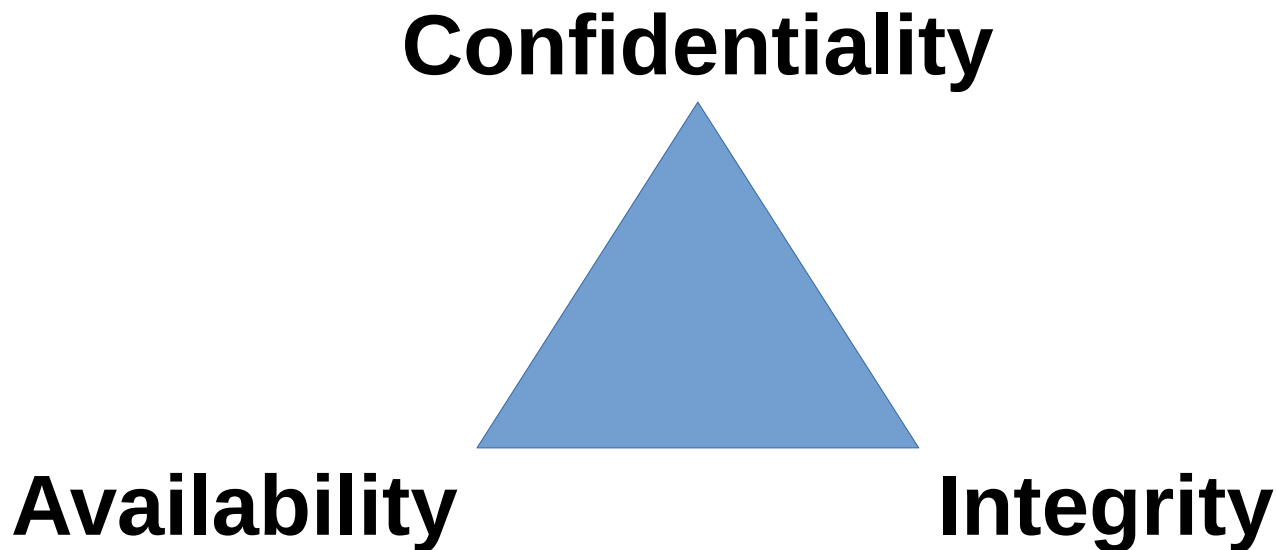
Alice	5 BTC
Bob	2 BTC
Charlie	3 BTC
...	

Yes this can work, but...



The C-I-A (or A-I-C) Principle

Information security requires *three properties*:



Blockchains **strengthen** Integrity and Availability, but replicating data **weakens** confidentiality!

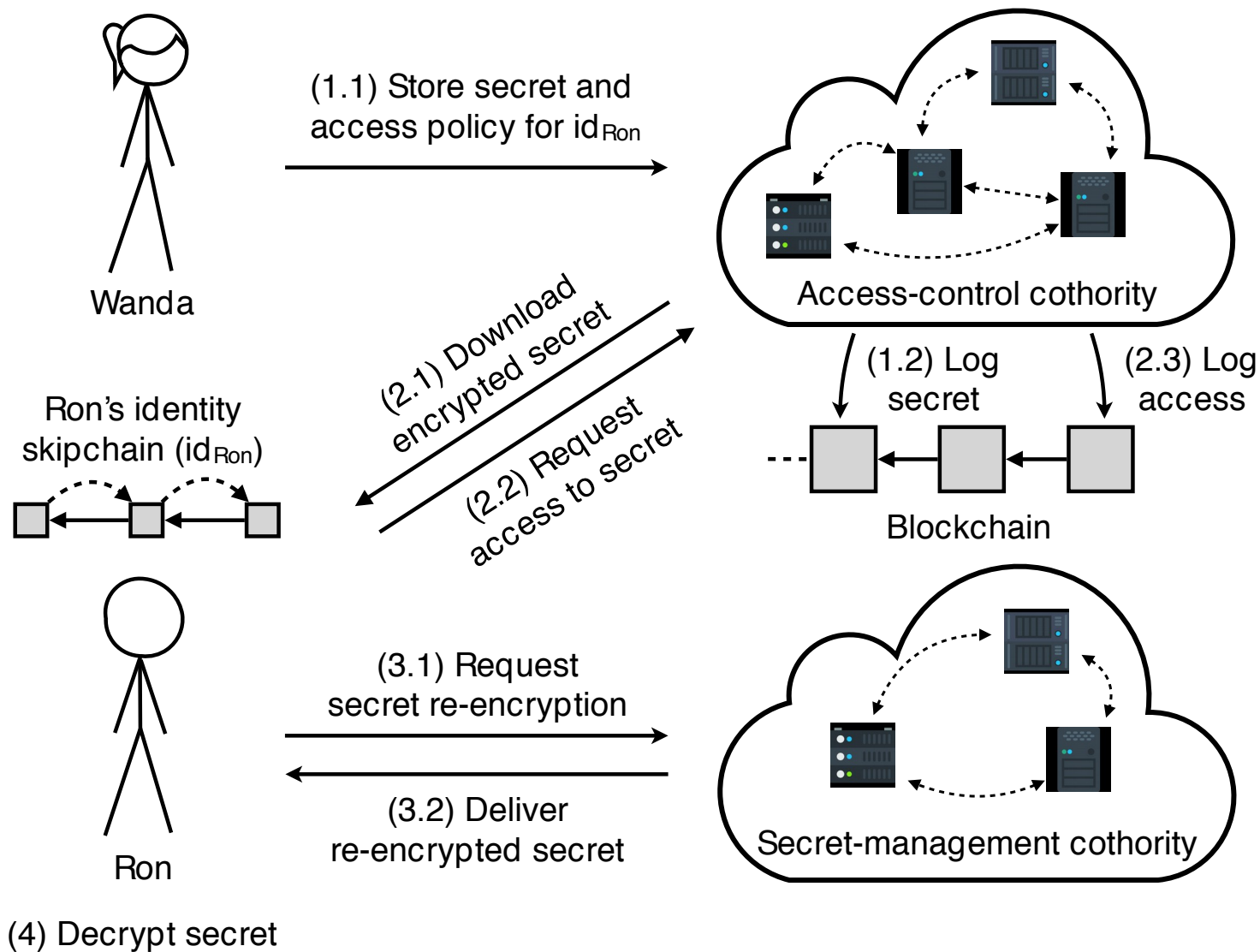
A Blockchain is a 2-legged Tripod

Strong integrity and availability, but weak privacy



Towards Three-Legged InfoSec

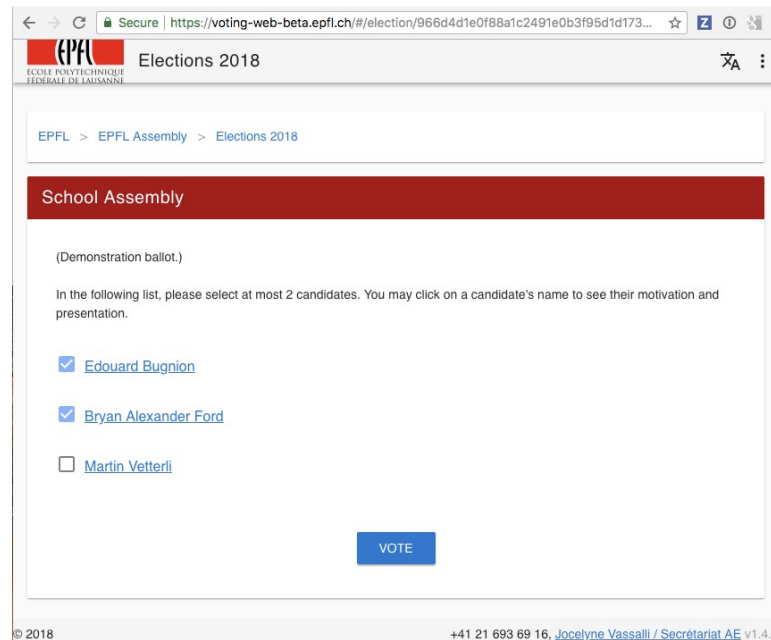
Calypso: architecture for distributed-trust **privacy**



Application: Electronic Voting

Serving ~10,000 eligible voters at EPFL each year

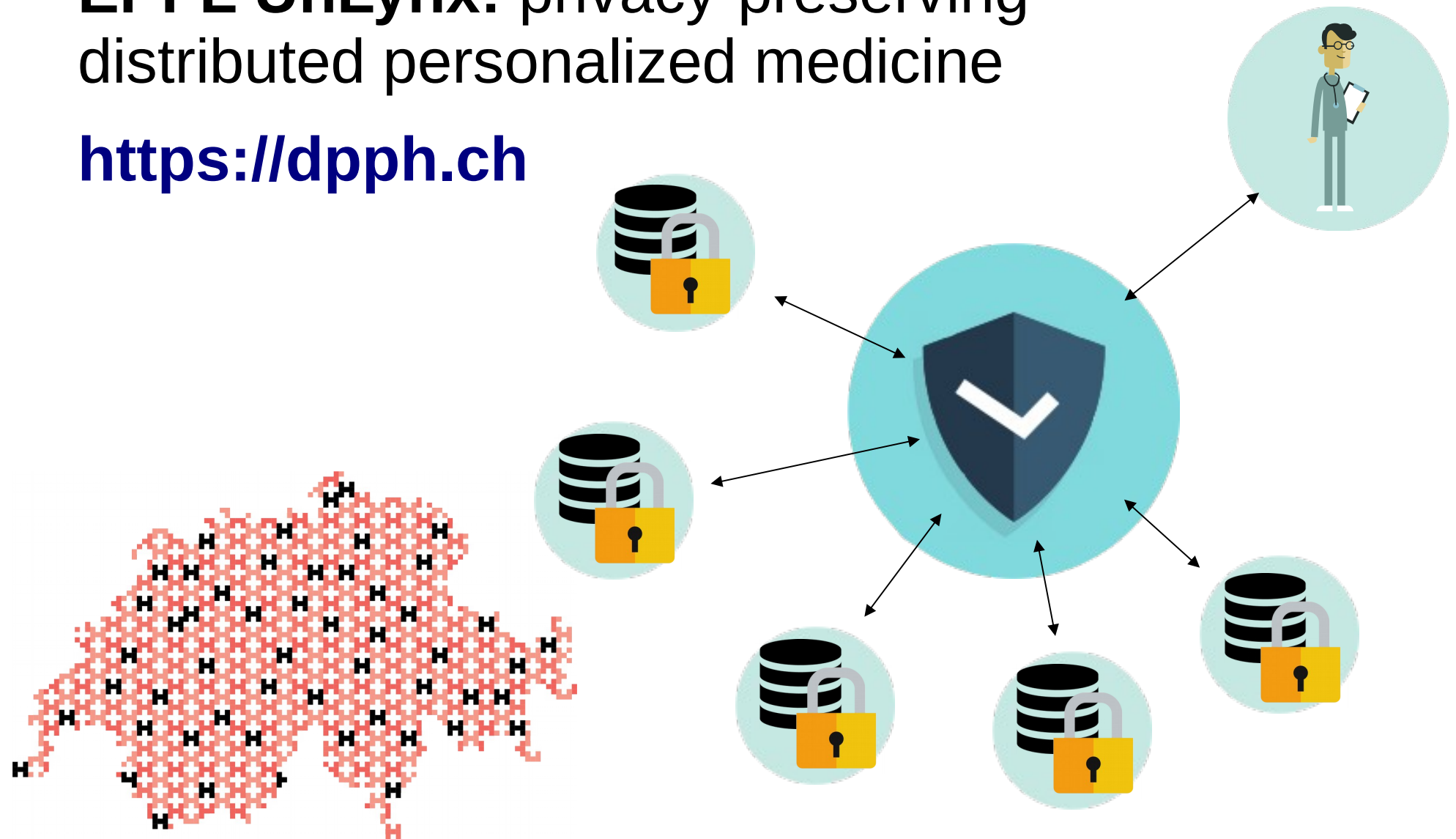
- <https://blog.dedis.ch/post/evoting/>



Application: Medical Data Sharing

EPFL UnLynx: privacy-preserving distributed personalized medicine

<https://dpph.ch>



EPFL Blockchain Industry Impact



Supporting partners

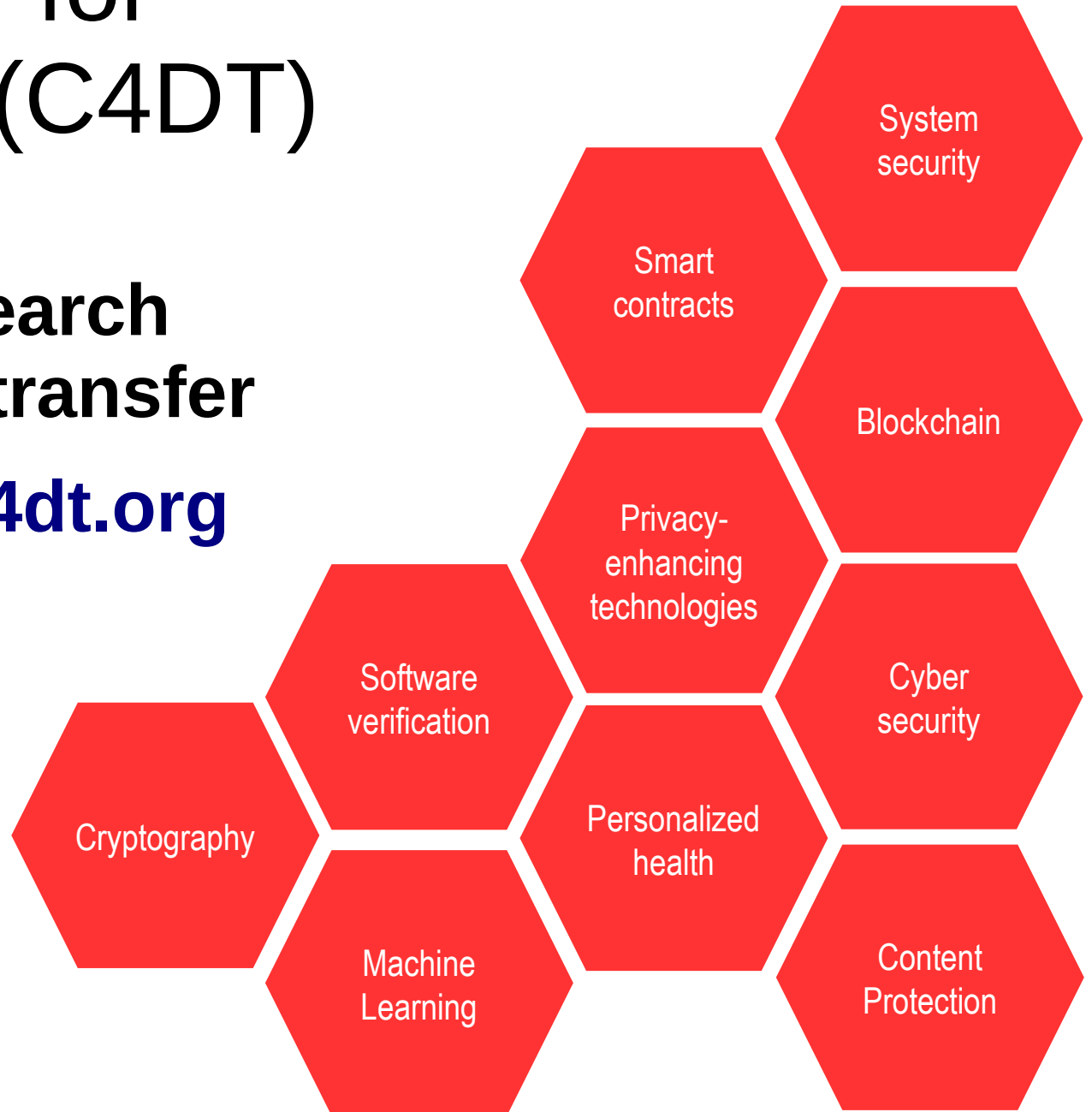


Companies adopting DEDIS research

EPFL Center for Digital Trust (C4DT)

Coordinating **research**
and **technology transfer**

- <https://www.c4dt.org>



Who do today's blockchains serve?

Permissioned:
only members of an
exclusive “club”



Permissionless:
in principle, *anyone*
in practice, a few
miners, developers,
investors



Distributed Trust: the Real Goal

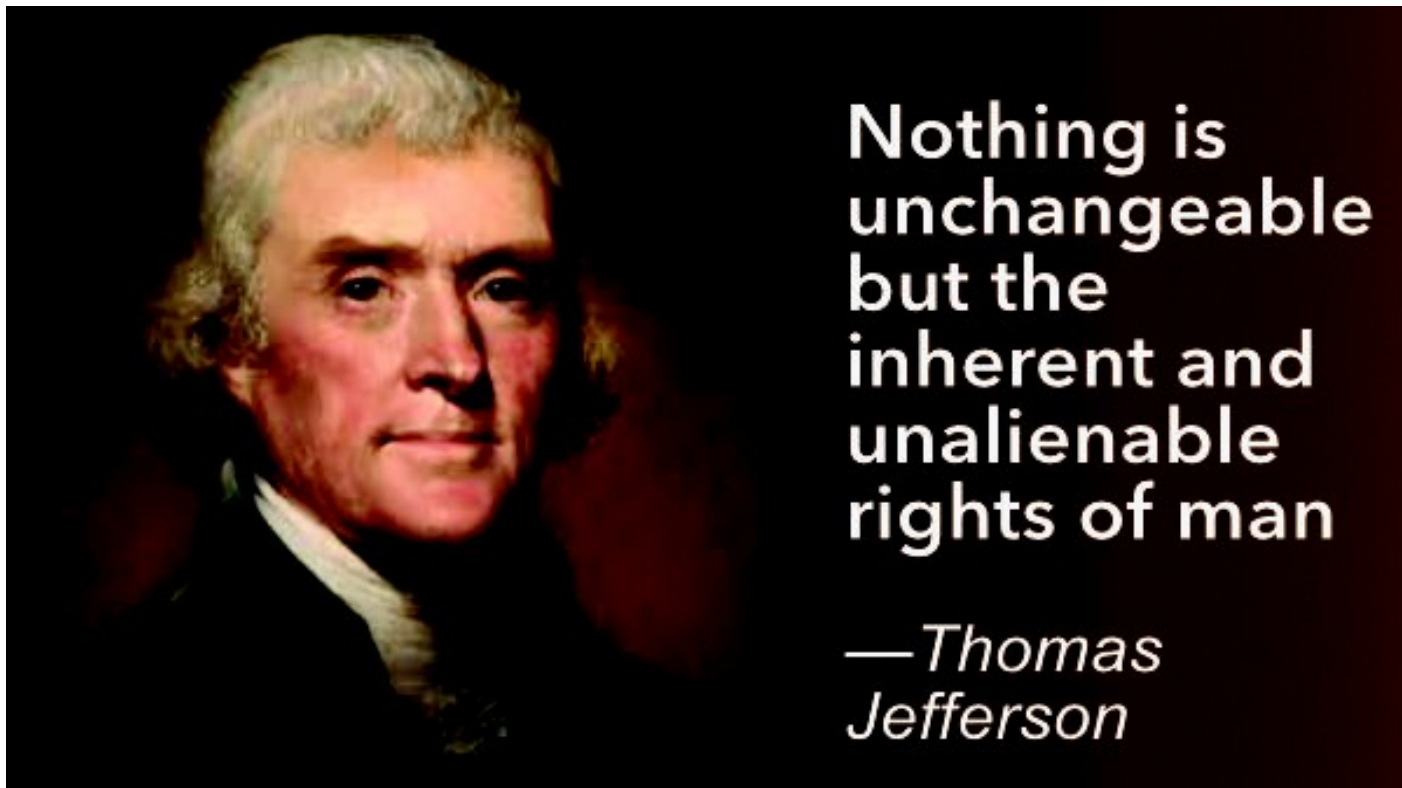
For technology to be **trusted by everyone**,
it must **serve** and be **accountable to everyone**.



Can technology serve **everyone**?

Can decentralized systems give **all real people**

- **Inclusion:** secure voice, vote, economic stake
- **Protection:** secure from hacking, digital fakery



Who is a (Real) Person Online?

Today's digital technology has no *secure* way to distinguish between **real** and **fake**

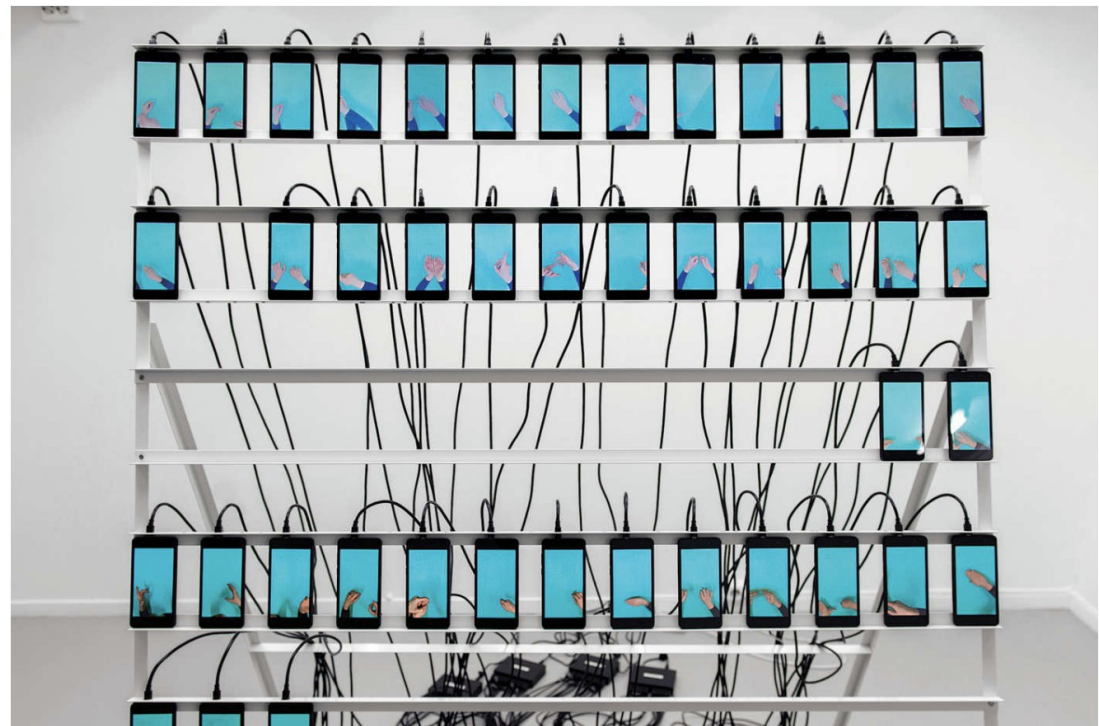
- People
- Reviews
- News



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](#)



AI can't solve this problem

Because better AI will keep making better fakes



Deepfakes are coming. We're not ready.



e-Identity can't solve this problem

All digital identities can be lost, stolen, or bought

- Even with trusted hardware, biometrics, etc.



Back to (non-digital) Reality

Can we anchor *digital trust* in the *physical world*?



Trust in Digital Governance

Can we create real trust in **digital governance**?



Trust in Digital Economy

Can we enable sustainable digital economics?



Architecting Inclusive Digital Trust

Technology can and must serve **all real people**.

We have most of the technology **pieces**, but they must fit into the right **architecture**.

<http://dedis.epfl.ch>

<https://www.c4dt.org>

<https://www.epfl.ch/>

