



# **Blockchain, Privacy, and Accountability**

Prof. Bryan Ford

Decentralized and Distributed Systems (DEDIS)

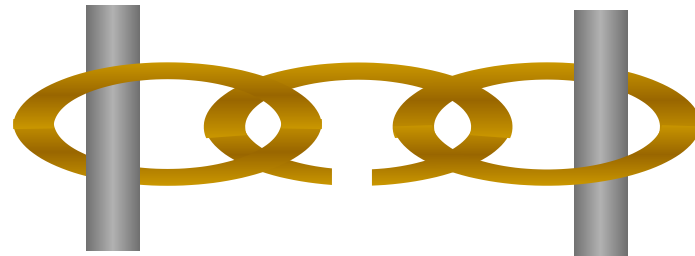
School of Information and Communications (IC)

[dedis@epfl.ch](mailto:dedis@epfl.ch) – [dedis.epfl.ch](http://dedis.epfl.ch)

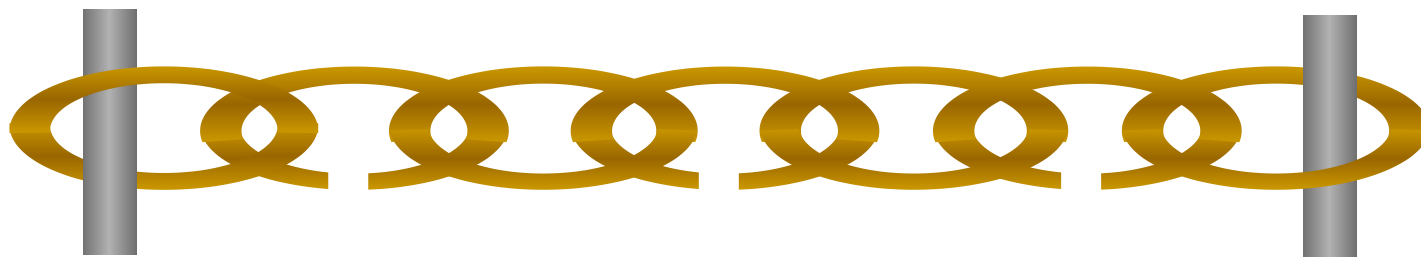
Caspian Week – Davos – January 23, 2020

# Today's Weakest-Link Security

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



More data, connectivity → weaker security



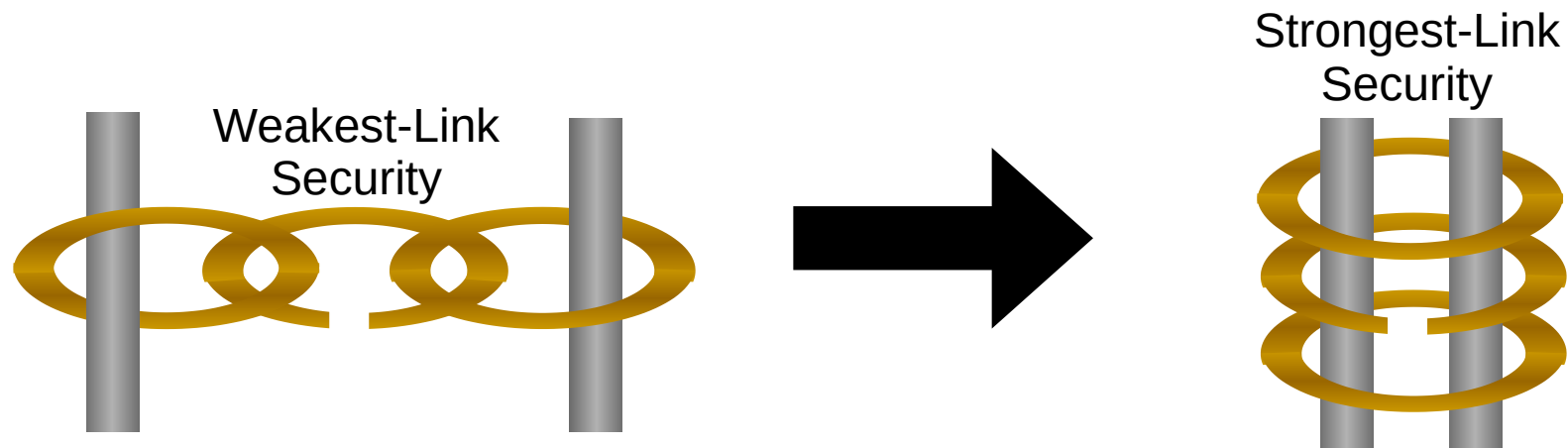
# The DEDIS lab at EPFL: Mission

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


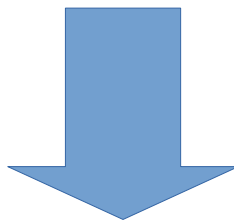
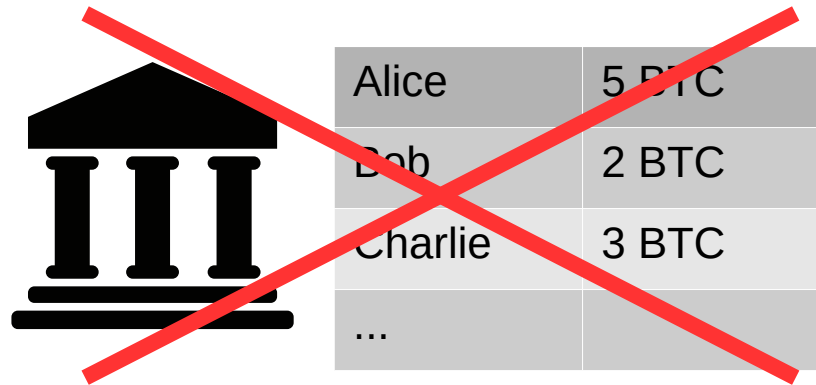
Systems that **distribute trust** widely with **strongest-link security**

<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**

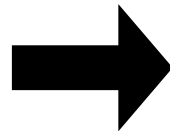
Alice	5 BTC
Bob	2 BTC
Charlie	3 BTC
...	

# Turning Around the Security Game

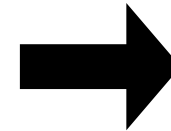
Design IT systems so that making them bigger makes their security *increase* instead of *decrease*



Weakest-link security



Strongest-link security



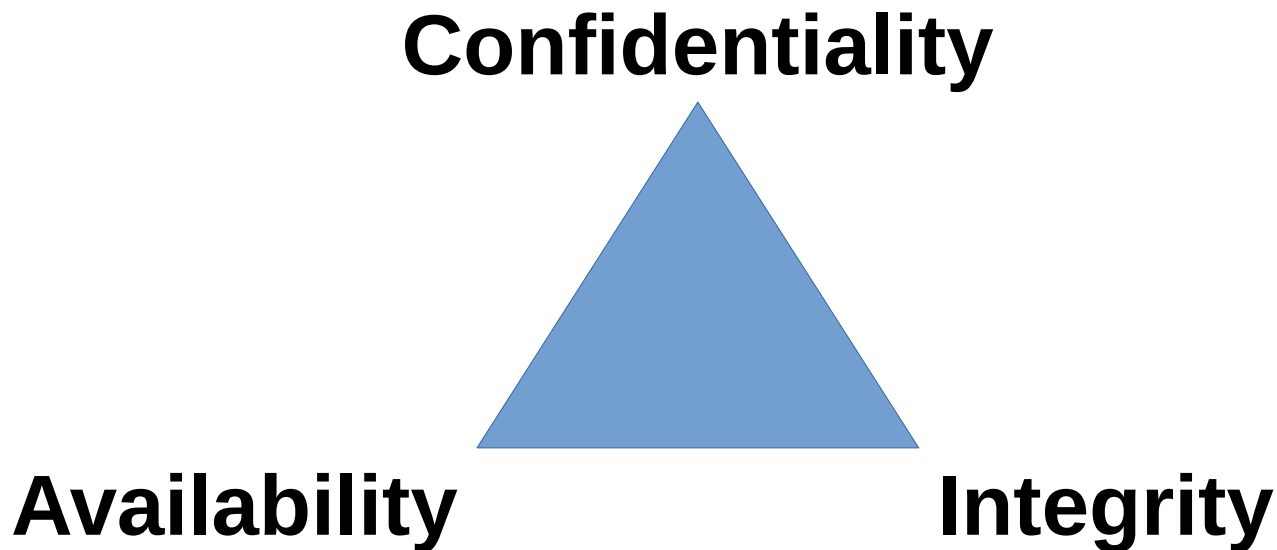
Scalable  
Strongest-link security

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

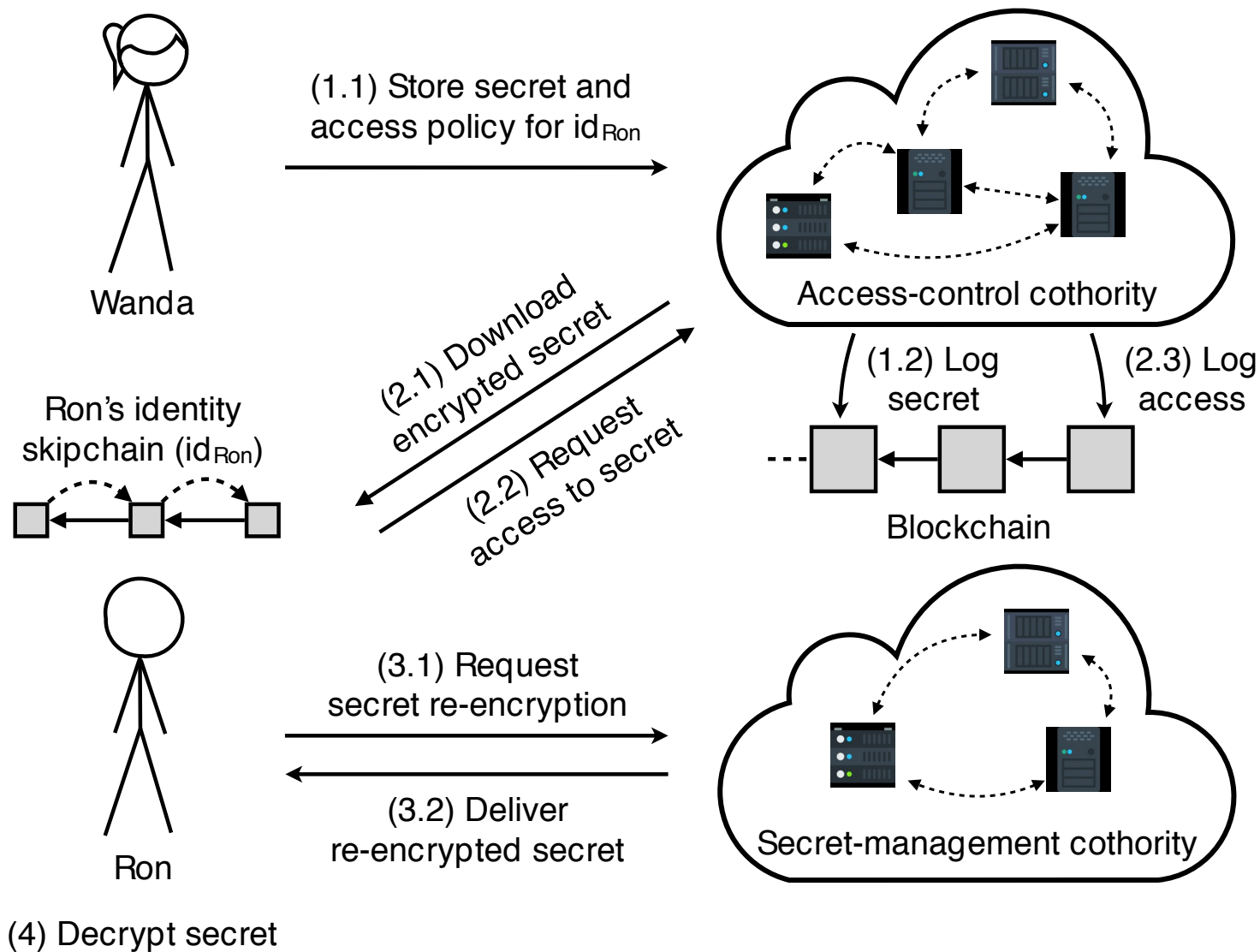
Strong integrity and availability, but weak privacy





# Towards Three-Legged InfoSec

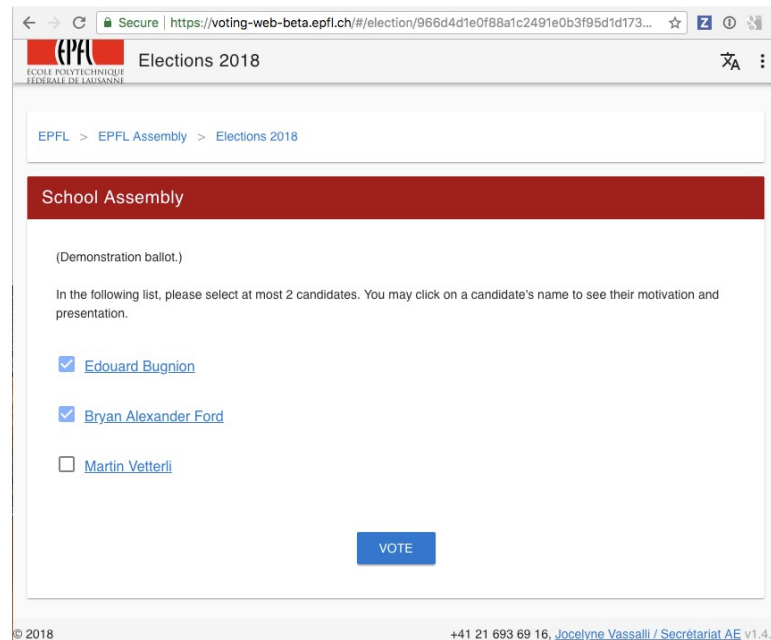
## Calypso: architecture for distributed-trust **privacy**



# Application: Electronic Voting

Serving ~10,000 eligible voters at EPFL each year

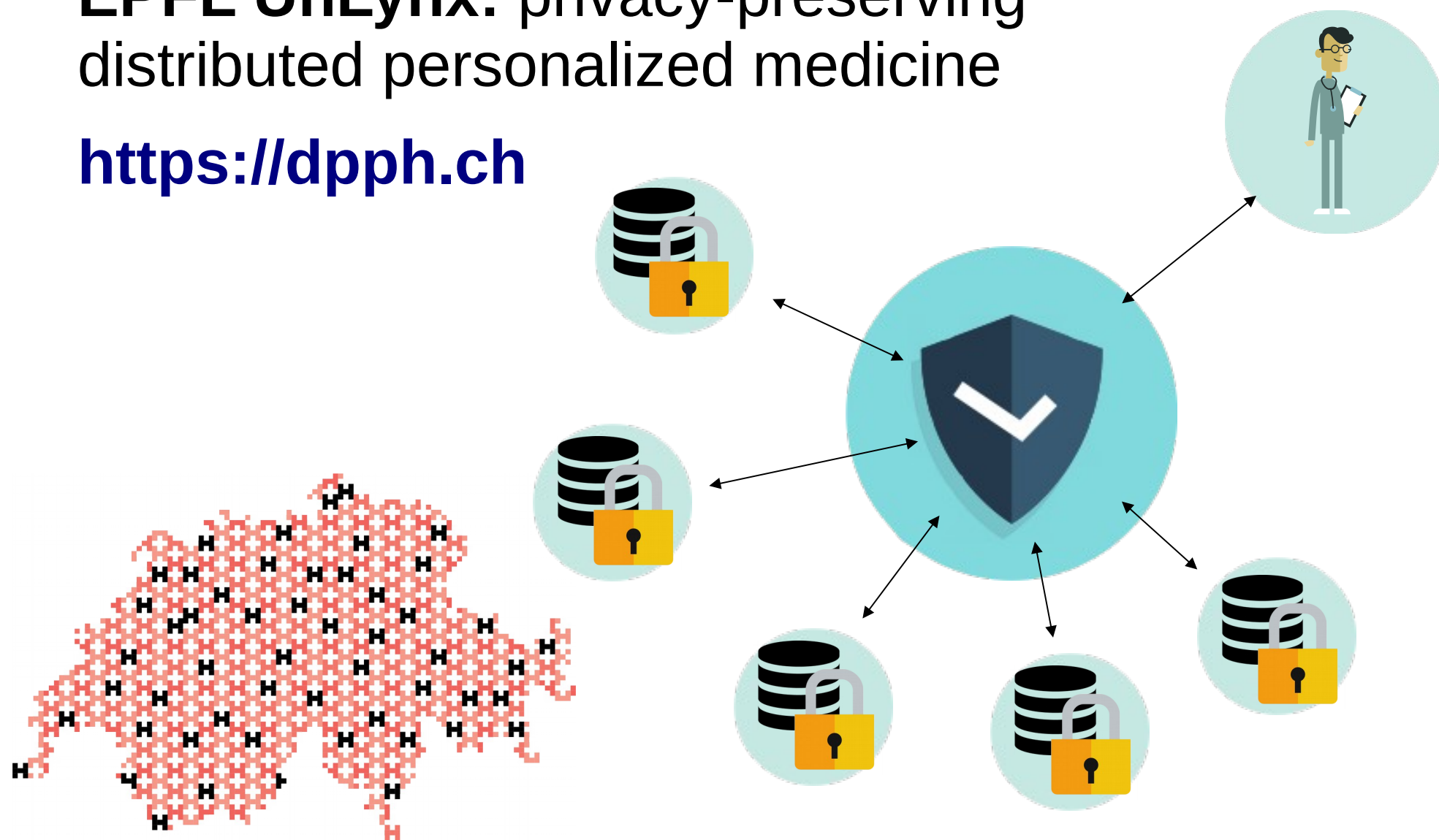
- <https://blog.dedis.ch/post/evoting/>



# Application: Medical Data Sharing

**EPFL UnLynx:** privacy-preserving distributed personalized medicine

<https://dpph.ch>



# EPFL Blockchain Industry Impact



## Supporting partners

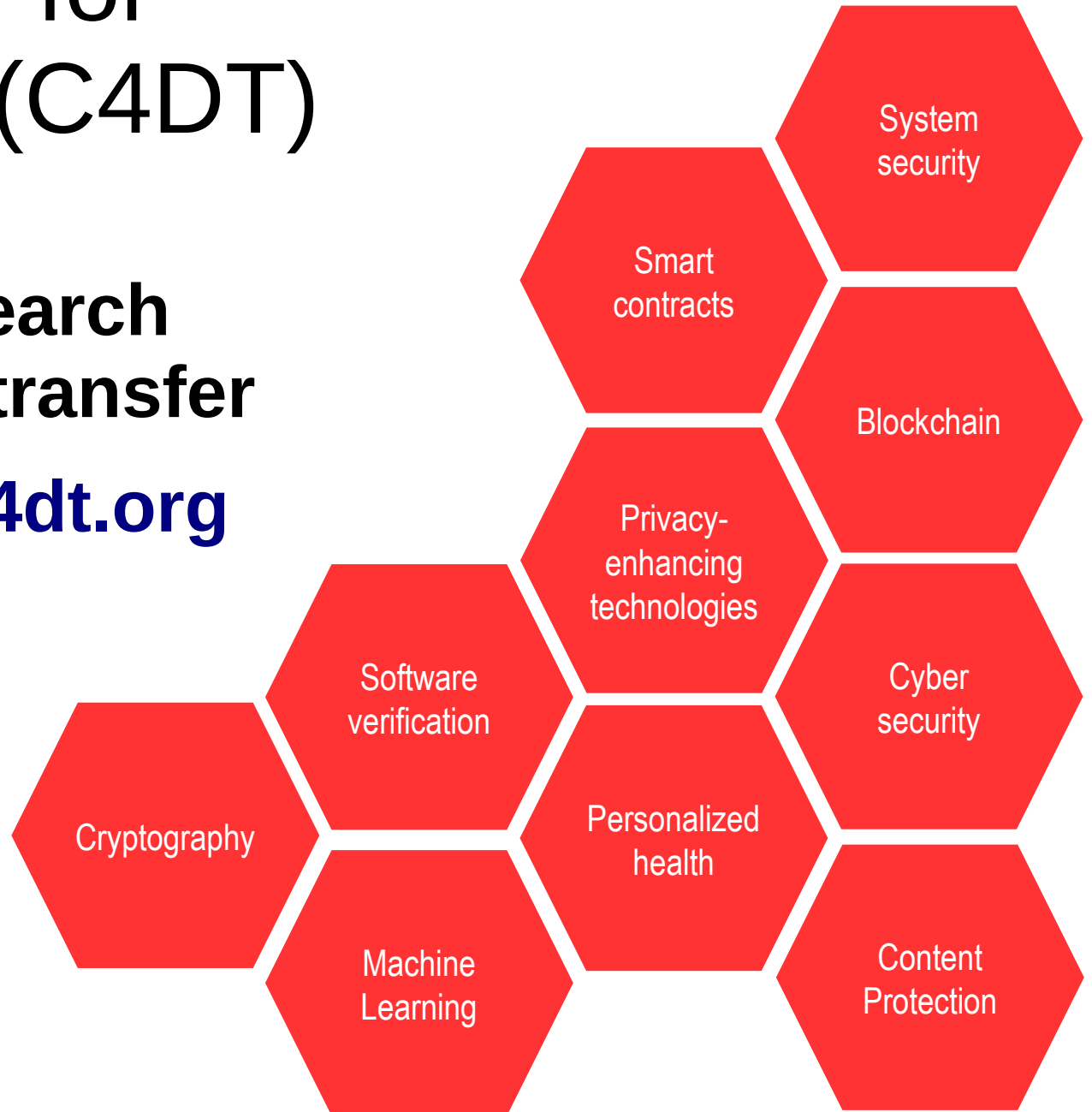


## Companies adopting DEDIS research

# EPFL Center for Digital Trust (C4DT)

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

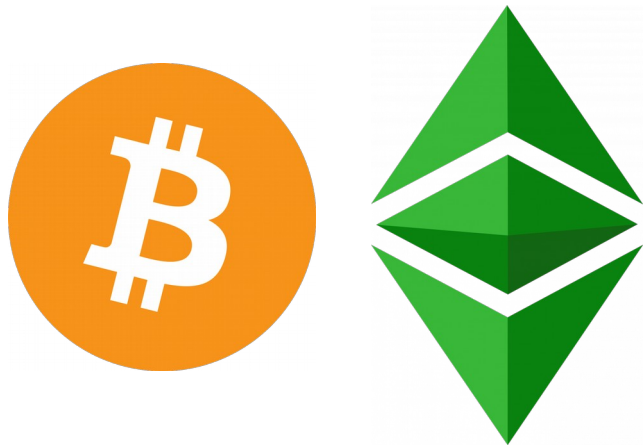
- <https://www.c4dt.org>



# Identity versus Privacy in Fintech

Today's cryptocurrencies: an "either-or" approach

- Bitcoin, Ethereum: weak **pseudonymity**
- Zcash, Monero: stronger **anonymity**



Traceable coins  
Blockchain analysis



"Untraceable" coins  
Analysis resistant

# The technical reality isn't "either-or"

There are *many* ways in principle to achieve **strong privacy** together with **accountability**

- Example: strong privacy for **low-value wallets** and small personal transactions
- Example: on-chain secret identities (Calypso) with regulator/law enforcement **access policy**
- Example: stronger cryptocurrency **governance**, community self-policing, revoking criminal funds

Cryptocurrencies work as we **design** them...

# Who governs cryptocurrencies?

**Permissioned:**  
members of an  
exclusive “club”



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





# Towards broad-based accountability

For cryptocurrencies to gain broad-based **trust**,  
must have broad-based stakeholder **community**.

Communities of  
**real people** –  
not just  
developers,  
tech companies,  
large investors



# Who is a (Real) Person Online?

## Key problem:

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



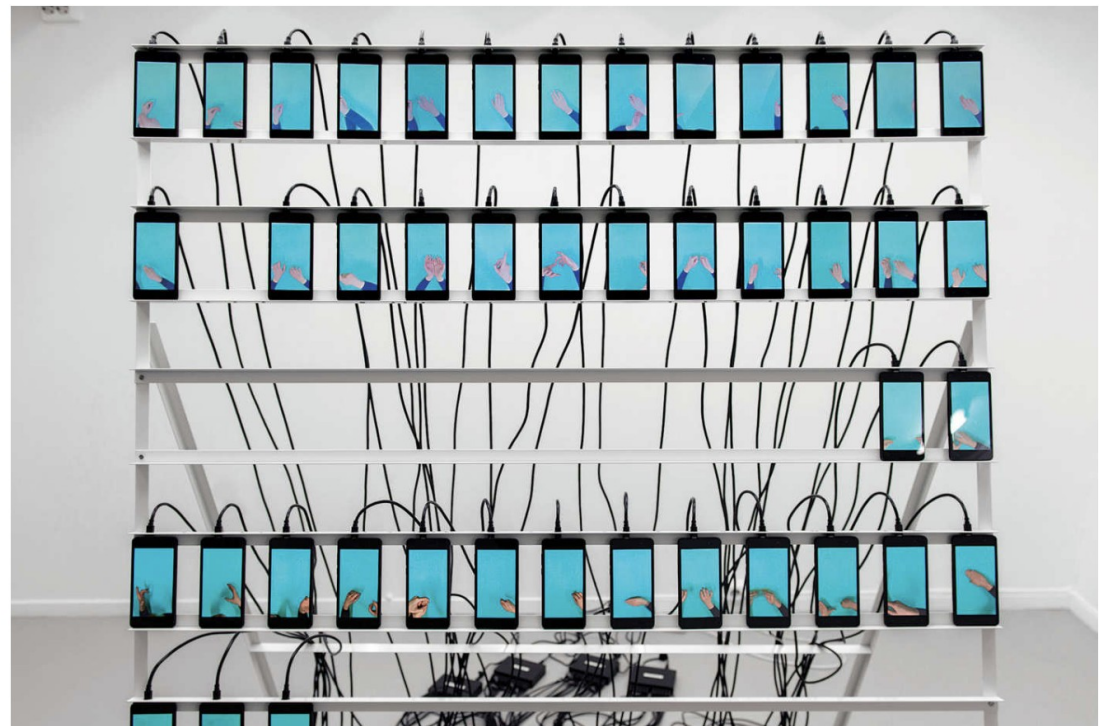
**Intelligencer**



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](#)



# ID card checking is a dead end

IDs already easy, cheap for real criminals to fake

## Prices of Stolen Passports and Fake IDs

Average Price of a Stolen Passport for Sale	<u>\$3,500</u>
Black Market Driver License – New Jersey	<u>\$2,500 to \$7,000</u>
Black Market Passport – Nepal	<u>\$6,961</u>
Black Market Passport – Peru	<u>\$1,750</u>
Black Market Passport – Sweden	<u>\$12,200</u>
Black Market Passport and Visa – Australia	<u>\$15,000</u>
Blank Stolen Passport – UK	<u>\$1,642</u>
Fake Green Card	<u>\$75 to \$300</u>

# AI can't solve this problem

Because better AI keeps making better fakes



# Deepfakes are coming. We're not ready.



# Back to (non-digital) Reality

**Digital trust** must have a **physical-world anchor**

- Privacy-preserving online+offline communities



# Privacy, Identity, and Accountability

There is huge design space for blockchain privacy

Cryptocurrencies *could* have **strong privacy** with **accountability**

Sustainable AML/CTF requires accountability to **real communities** of **real people** in the **real world**



<http://dedis.epfl.ch> – <https://www.c4dt.org>