Blockchain NG

Using cryptography to improve usability of the blockchain

EPFL C4DT Center for Digital Trust

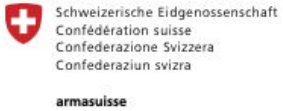
Overview

- **Introduction**
  - Who is C4DT
  - DEDIS and Blockchains
  - OmniLedger
- Use-case presentation
  - Secret key recovery
  - Auditing blockchains
- Hands-on training

EPFL C4DT Center for Digital Trust

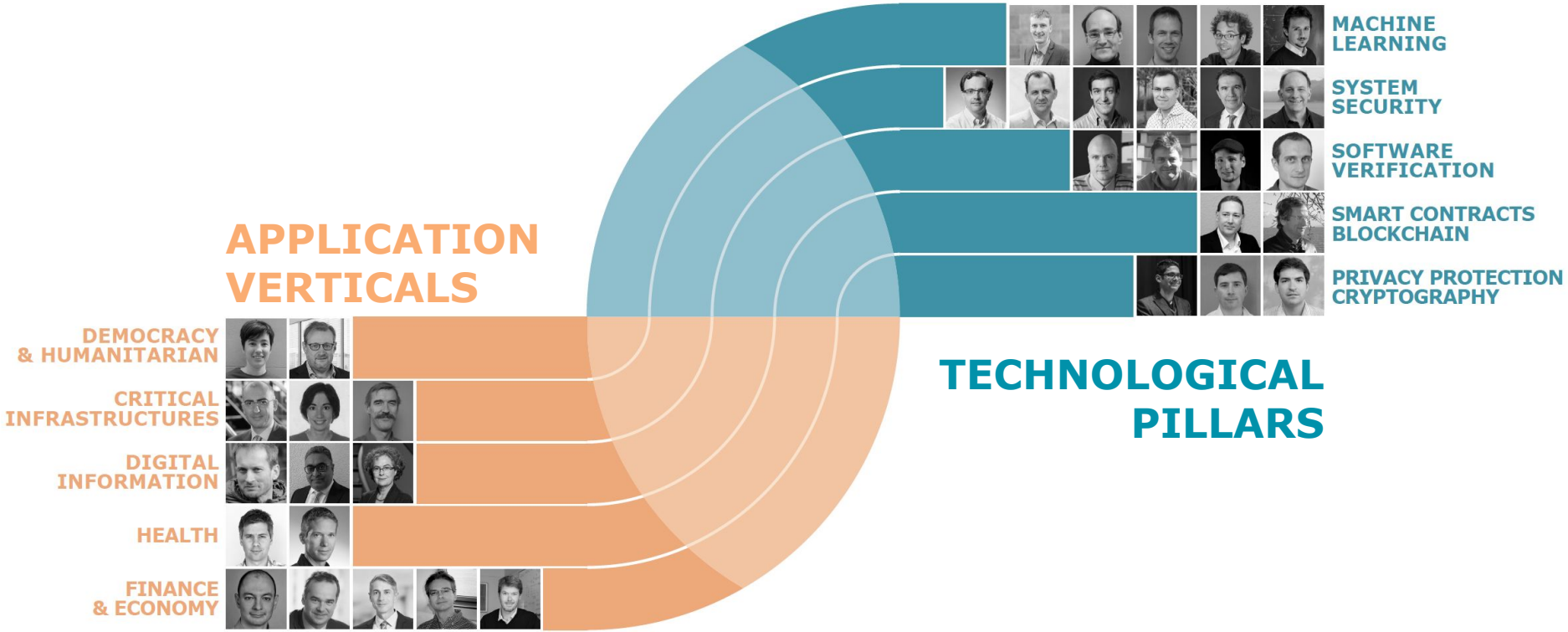
EPFL C4DT Center for Digital Trust

Partners 2019



EPFL C4DT Center for Digital Trust

More than 30 laboratories involved



EPFL C4DT Center for Digital Trust

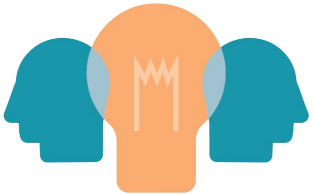
C4DT structure - 4 domains

FACTORY

Software

Sandbox

Support

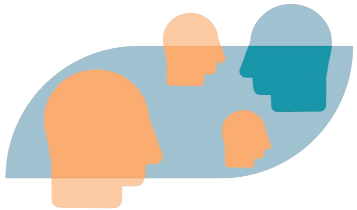


ACADEMY

Interface

Education

Experts



EMBASSY

Community

Events

Workgroups

AGENCY

Projects

Interface

Coordination

EPFL C4DT Center for Digital Trust

FACTORY - Overview

DEDICATED TEAM OF DEVELOPERS

- EPFL Labs - research
- Factory - refinement
- Partners - integration

DEMONSTRA-TORS

- Easy Access to Components
- Training on chosen technology

SOFTWARE REPOSITORY

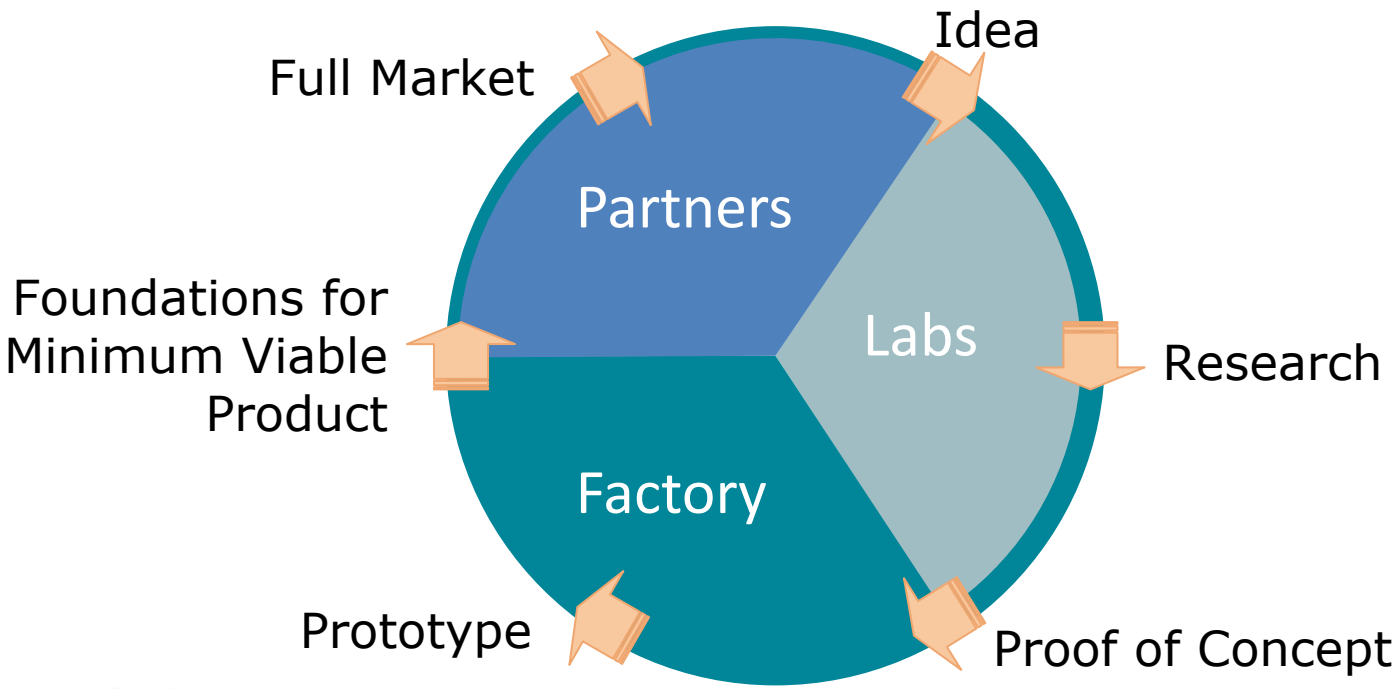
- Privacy Protection
- Decentralized Systems
- Software Verification
- Machine Learning

DEVELOPMENT SUPPORT

- Best practices
- Regular meetings
- Training
- List of requirements

EPFL C4DT Center for Digital Trust

FACTORY - Software Lifecycle



Trainings

Factory hands-on training

- Short - half a day
- On one library from Factory
- Tech-transfer
- Proof-of-concept searcher

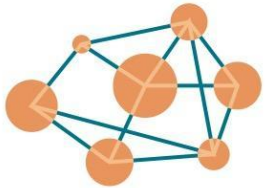
Academy training

- One-week courses
- Modular approach: full or module
- Flagship course: Foundations of ICT for Decision Makers
  - Fundamentals of ICT
  - Data protection and privacy
  - Cybersecurity and Digital Trust
  - Towards artificial intelligence
- Coming soon:
  - Advanced courses (building on foundation course modules)
  - Senior Executive trainings

EPFL C4DT Center for Digital Trust

DEDIS and Blockchains

Prof. Bryan Ford works on scalable, decentralized, self-organizing systems. Publications in top-tier conferences on cryptography and security

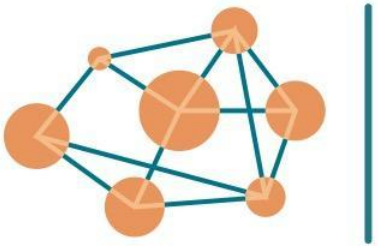


Blockchains are part of these systems

Other systems include evoting, eID, cryptography

EPFL C4DT Center for Digital Trust

OmniLedger



OMNILEDGER

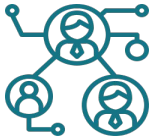
Use next generation blockchains to build trust between partners

OmniLedger: Fast by using latest research in scalable blockchain technology

Calypso: Data hiding with advanced access control mechanisms

Proof of Personhood: Improve trust through highly decentralized infrastructure

Versatility by running code from other blockchains



Tested and integrated in various prototypes with industrial partners

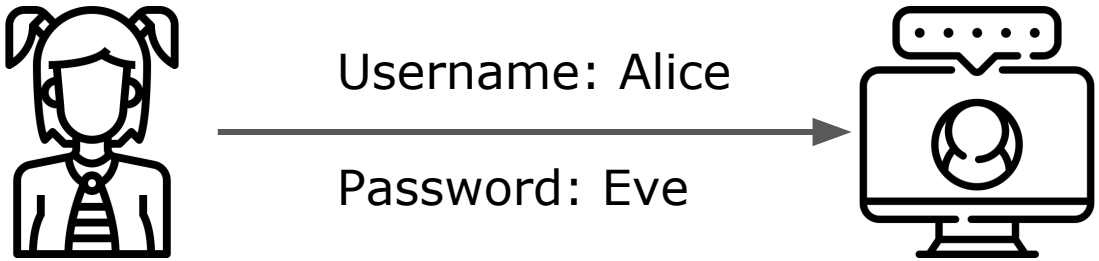
EPFL C4DT Center for Digital Trust

Overview

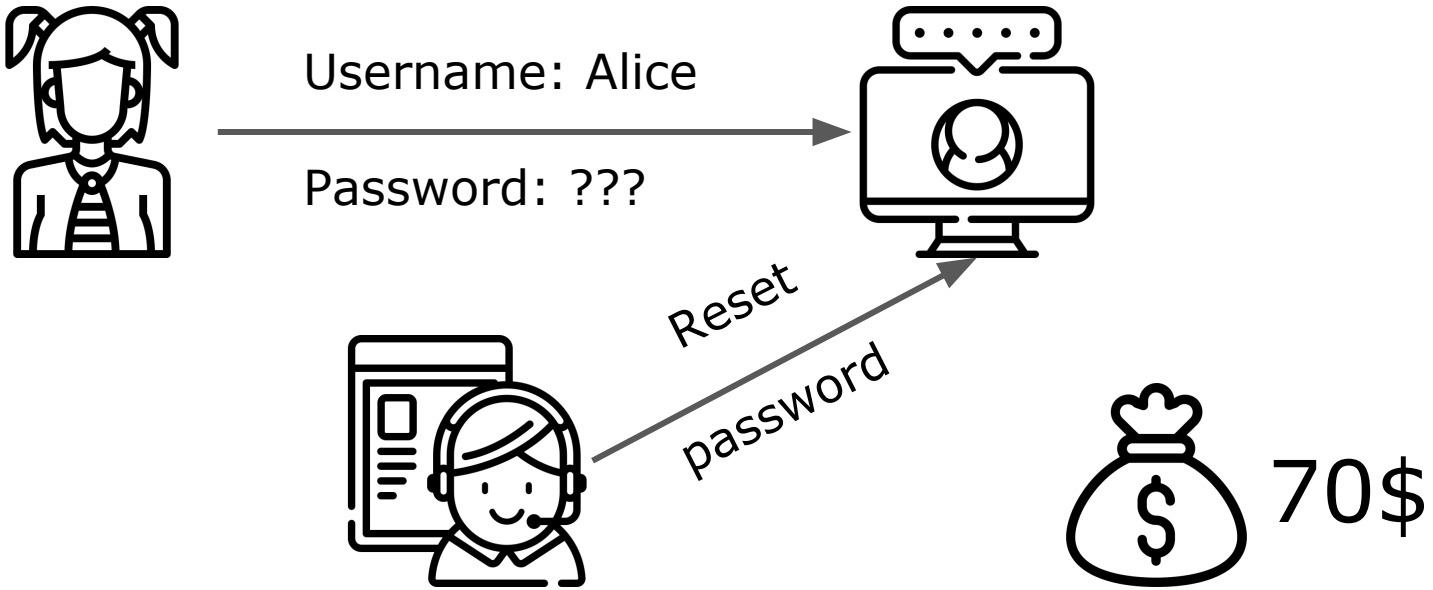
- Introduction
  - Who is C4DT
  - DEDIS and Blockchains
  - OmniLedger
- **Use-case presentation**
  - Secret key recovery
  - Auditing blockchains
- Hands-on training

EPFL C4DT Center for Digital Trust

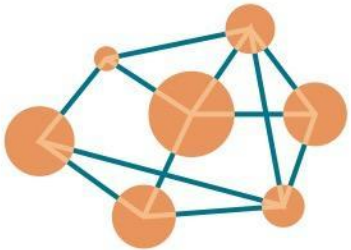
Secret Key Recovery - Password



Secret Key Recovery - Password



Secret Key Recovery - Blockchain



Blockchains process transactions

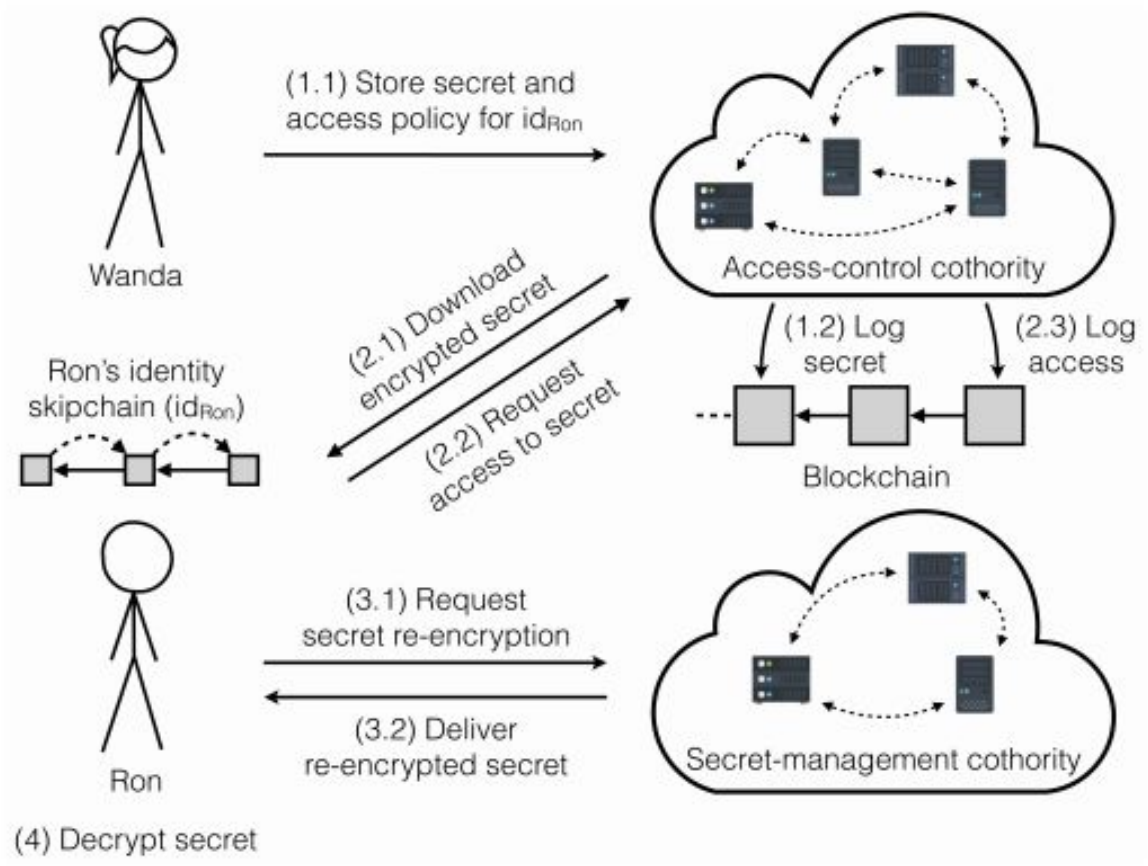
Transactions are protected by a secret key

No central administration

EPFL C4DT Center for Digital Trust

Calypso

[2018/209 - Verifiable Management of Private Data under Byzantine Failures]



EPFL C4DT Center for Digital Trust

Use Cases

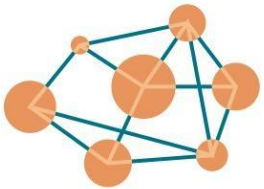
During the hands-on exercises, we'll look into the following use-cases:

1. Password manager using Calypso
2. Replacing secret keys with delegation
3. Auditing encrypted certificates

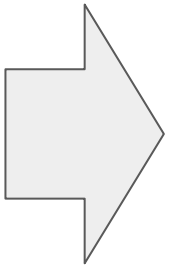
EPFL C4DT Center for Digital Trust

1 - ‘Password’ Manager

Store key encrypted on blockchain



Only the block-chain can decrypt the key



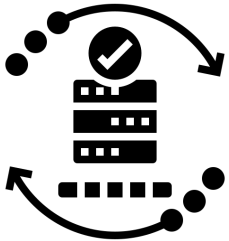
Delegate access to the key

Decryption can be audited

2 - Delegation of Access

Replace the key with a *Delegation*

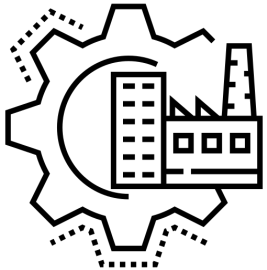
Full audit of updates and usage



Access can be updated over time

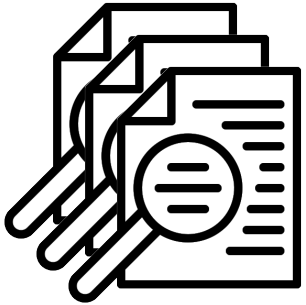
EPFL C4DT Center for Digital Trust

3 - Auditing Encrypted Certificates

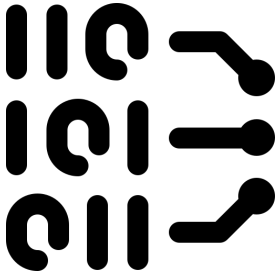


Given product info from Pharma

Attach delegation for audits



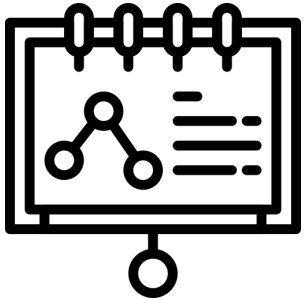
Different auditors for different batches



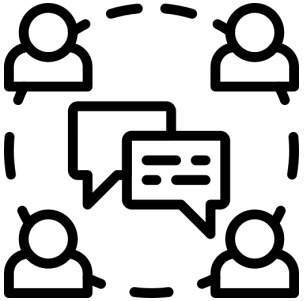
Multi-signatures
Time-based
Location-based

EPFL C4DT Center for Digital Trust

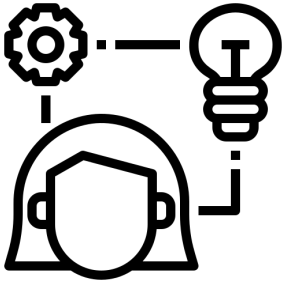
Hands-on training



Explain how it works behind the scenes



Discuss how to integrate in existing systems

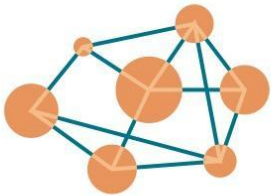


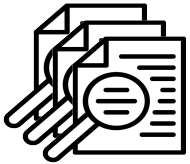
Hands-on exercise on topic

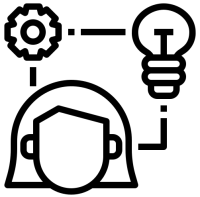
EPFL C4DT Center for Digital Trust

Overview

- Introduction
  - Who is C4DT
  - DEDIS and Blockchains
  - OmniLedger
- Use-case presentation
  - Secret key recovery
  - Auditing blockchains
- Hands-on training







EPFL C4DT Center for Digital Trust