Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

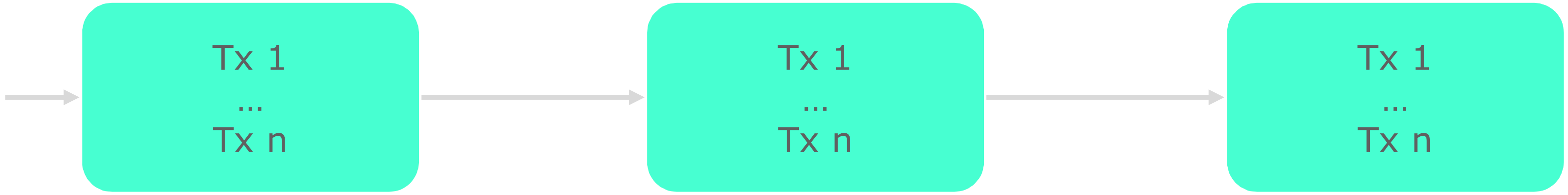
FH Zentralschweiz

Blockchain Technology:
Introduction and use in the context of electronic Identity Solutions

18. MAGGLINGER RECHTSINFORMATIKSEMINAR

Dr. Mathias Bucher
Lecturer HSLU, Founder & CEO Diamond Digital AG

Blockchain: Secure, resilient state transition machine



Current state

The result of all previous transactions

Status update

All new transactions

- collected during blocktime
- Validated by consensus of all network nodes

Result

"Chain of Blocks"

➔ Blockchain

© Mathias Bucher

Characteristics of a Blockchain state transition machine

- Functionality F (can be arbitrary code):
  Operation o transforms a state s to new state s' and may generate a response r

$$(s', r) \leftarrow F(s, o)$$

- Validation condition (only valid transactions are executed):
  Operation needs to be valid, in current state, according to a predicate P()

$$P(s,o) = \text{TRUE}$$

- Append-only log: Every operation o appends a "block" of valid transactions (tx) to the log

- Log content is verifiable from the most recent element

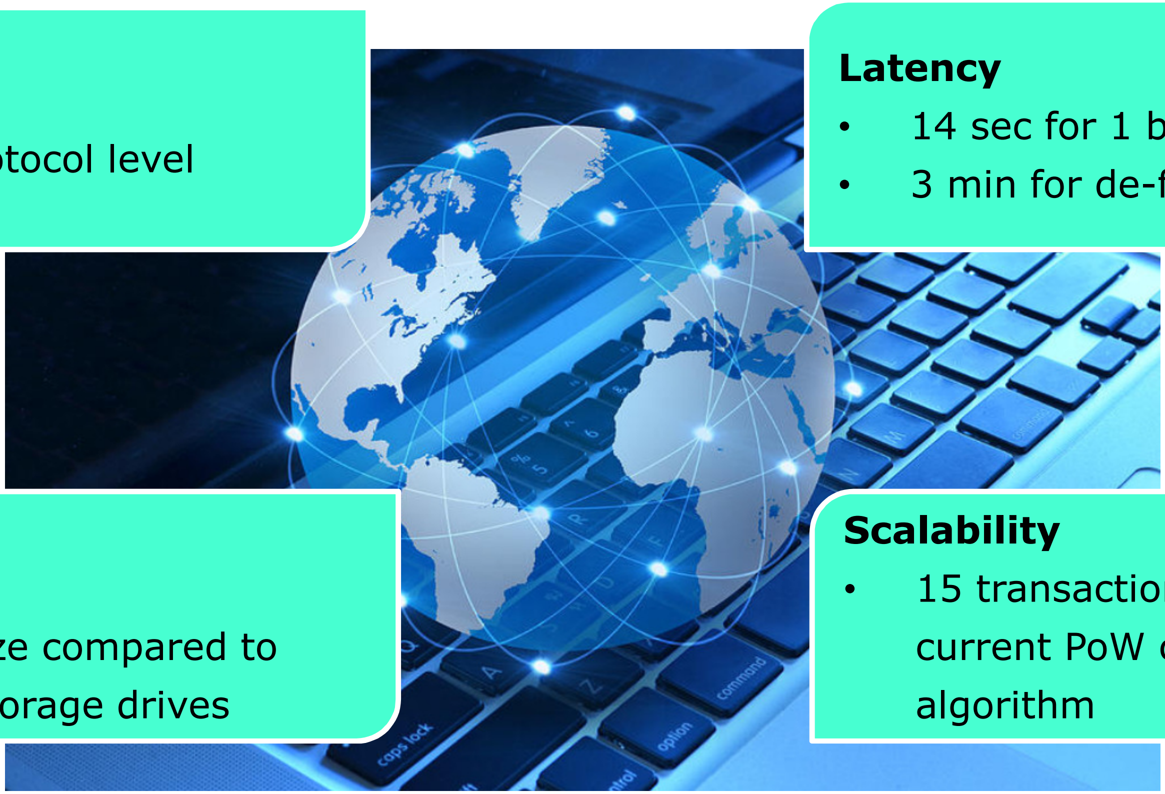
- Log entries form a hash chain:

$$h[t] \leftarrow \text{Hash}(\ [tx\ 1\ ,\ tx\ 2\ ,\ \ldots\ ]\ ||\ h\ [t-1]\ ||\ t)\ .$$

Blockchain – World Computer???

"Computer" Analogy is misleading – creates wrong expectations

Blockchain – World Computer???



Privacy

- Low at protocol level

Latency

- 14 sec for 1 block,
- 3 min for de-facto finality

Storage

- Expensive
- Limited size compared to modern storage drives

Scalability

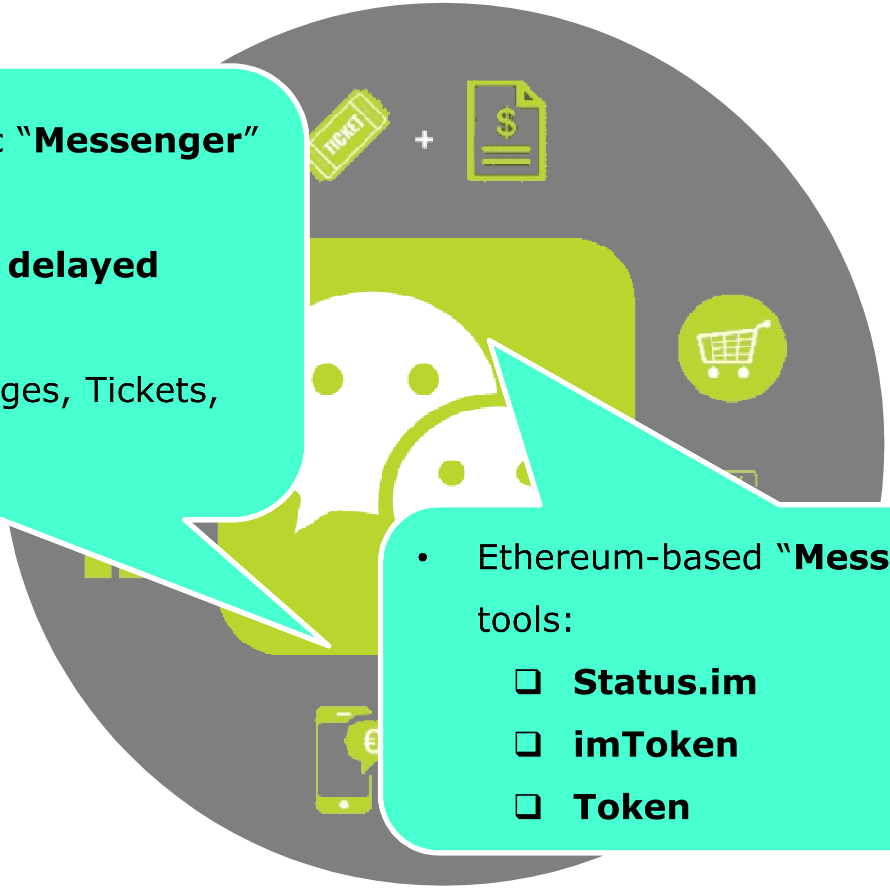
- 15 transaction / sec with current PoW consensus algorithm

Analogy: Blockchain V1.0 (Bitcoin)

Specialized Tool
(Bitcoin Protocol)

Built to do **one thing** very good
(Bitcoin token transactions)

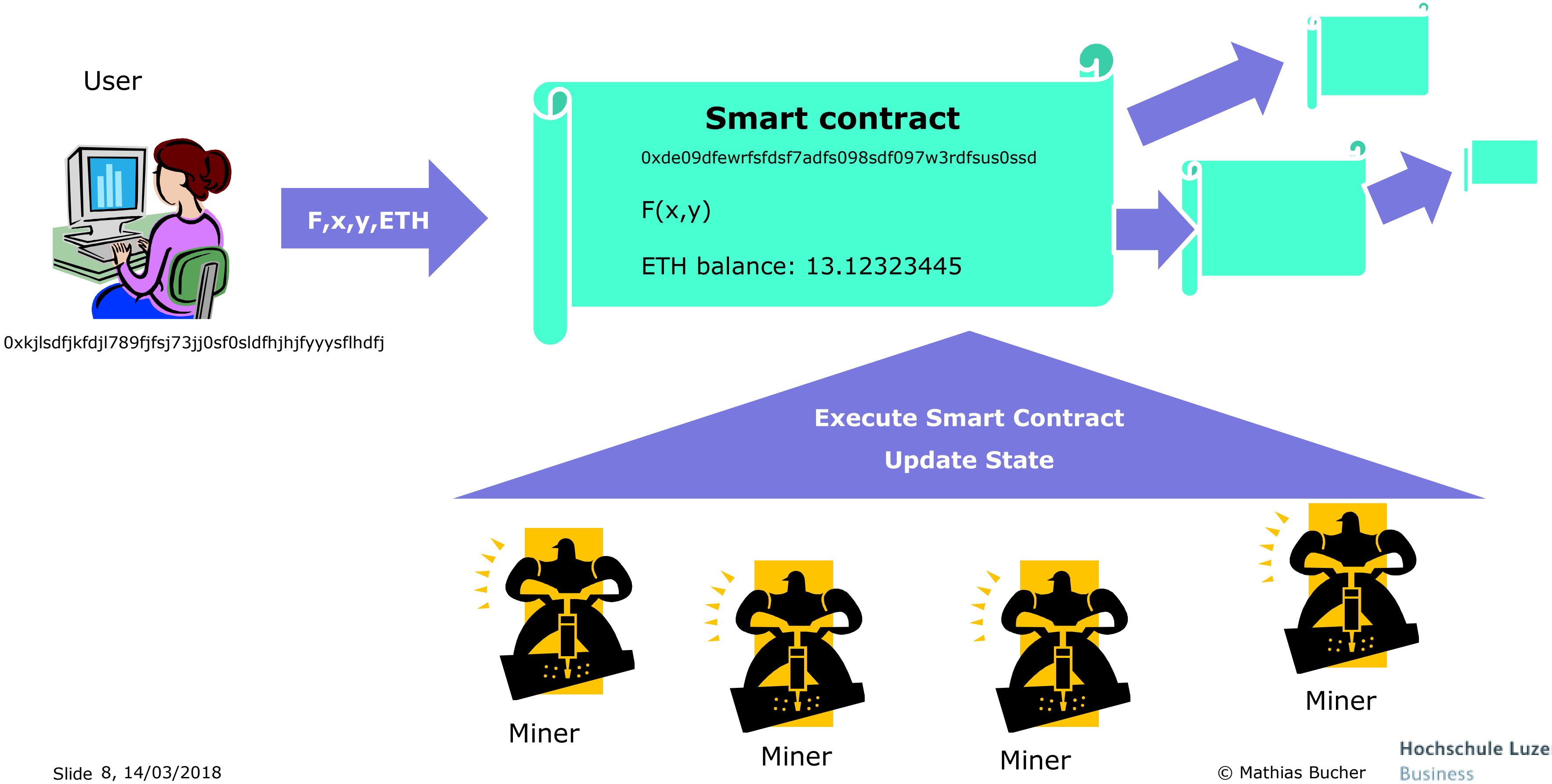
Analogy: Blockchain V2.0 (Ethereum)



- **Consumer**-centric “**Messenger**” (think **WeChat**)
- User input creates **delayed response**
- **Multi-tool**: Messages, Tickets, Voting, Shopping

- Ethereum-based “**Messenger & Wallet**” tools:
  - ❑ **Status.im**
  - ❑ **imToken**
  - ❑ **Token**

Blockchain 2.0: Ethereum state transition machine



User

0xkjlsdfjkfdjl789fjfsj73jj0sf0sldfhjhjfyyysflhdfj

F,x,y,ETH

Smart contract

0xde09dfewrfsfdsf7adfs098sdf097w3rdfsus0ssd

F(x,y)

ETH balance: 13.12323445

Execute Smart Contract

Update State

Miner

Miner

Miner

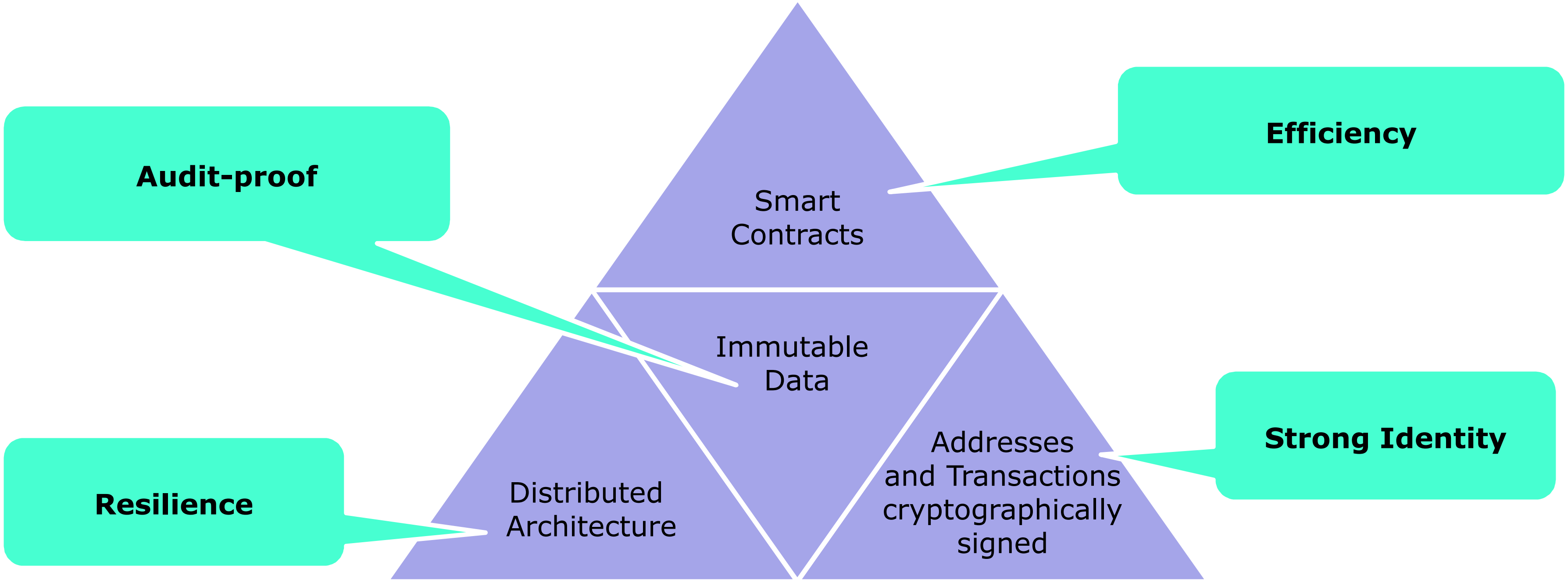
Miner

© Mathias Bucher

Blockchain 2.0: Ethereum state transition machine

- Ethereum is a blockchain architecture with an associated state database, capable of storing programs and their state.
- Programs on Ethereum are called “Smart Contracts”
  - can be deployed by any Ethereum user
  - has a function-based interface
  - Once deployed, the smart contract can be referenced by its address (cryptographic identifier)
- A user can call a smart contract function
  - by sending a transaction with this address as the destination
  - with the data payload of the transaction containing the function signature and input parameters
- If a Smart Contract function is called, the “miners” (consensus validators) of the network execute the program in a trust-minimized way and update its state
- A smart contract can hold and send the native value token Ether, and can furthermore call functions of other smart contracts.

Advantages of the Blockchain



Audit-proof

Efficiency

Smart Contracts

Immutable Data

Distributed Architecture

Addresses and Transactions cryptographically signed

Strong Identity

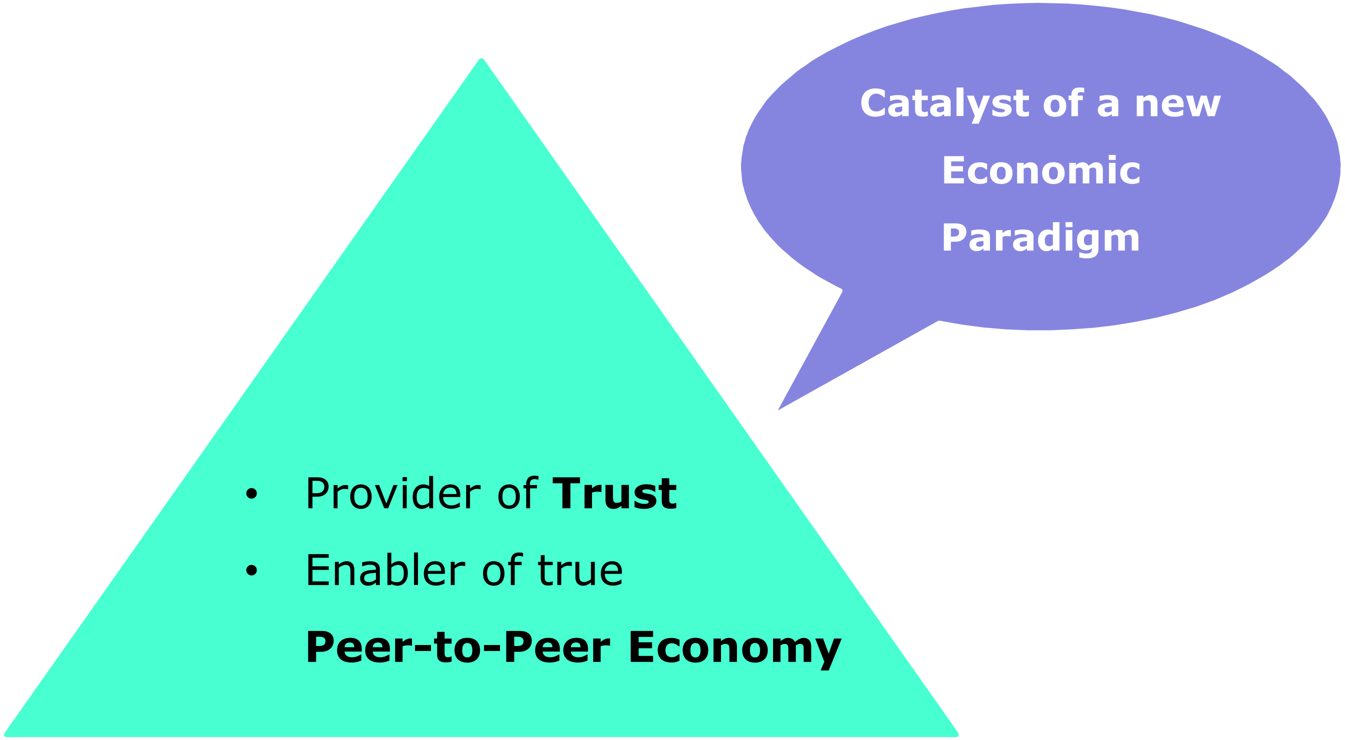
Resilience

© Mathias Bucher

Blockchain: Coordinating the Participants of a Global P2P Economy

© Mathias Bucher

Blockchain: GLOBAL Source of Truth



Catalyst of a new Economic Paradigm

- Provider of **Trust**
- Enabler of true **Peer-to-Peer Economy**

© Mathias Bucher

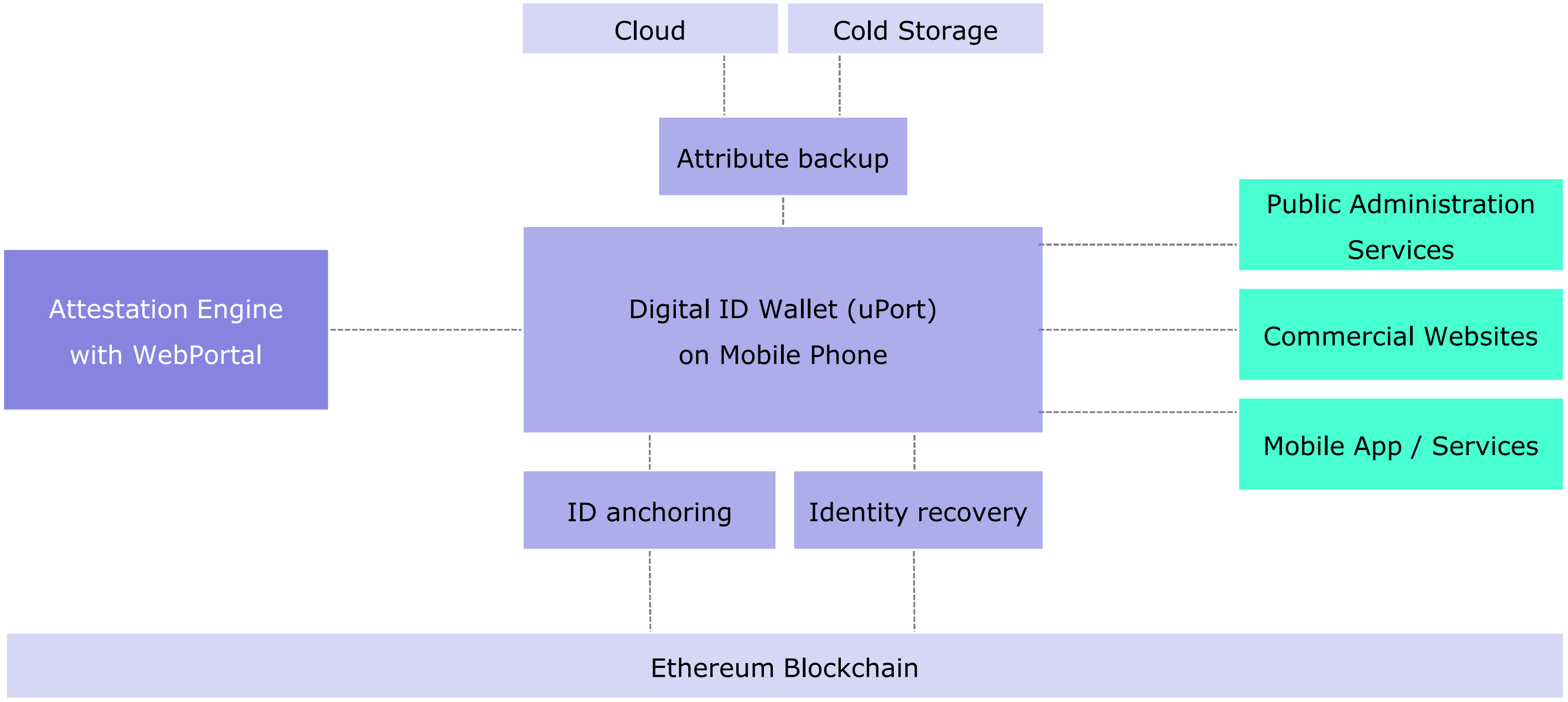
Use of Blockchain for digital IDs

Goals in our Project with City of Zug:

- Data self-sovereignty for user
- «Intelligent» use of Blockchain
- Real-world usability
  - Easy user interface
  - Use of existing credential standards
  - Use of existing hardware
  - Attestation of data by authorities

© Mathias Bucher

Blockchain-based eID Solution



© Mathias Bucher