Blockchain, Distributed Trust and Privacy

Dr. Zeki Erkin

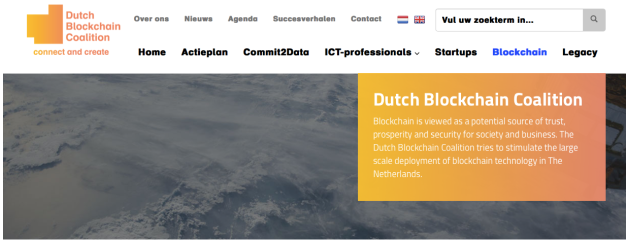
Assistant Professor
Cyber Security Group / Blockchain Lab
Dep. Intelligent Systems
Delft University of Technology

Assist. Prof. dr. Zekeriya Erkin

- Cyber Security Group/ TU Delft
- Digital Security Group/ RUN

- **Research Interest**
  - Secure Information Sharing
  - Processing Sensitive Data
  - De-centralized Systems

- **Teaching**
  - Security and Cryptography (MSc)
  - Privacy Enhancing Technologies (MSc)
  - Blockchain Engineering (MSc)



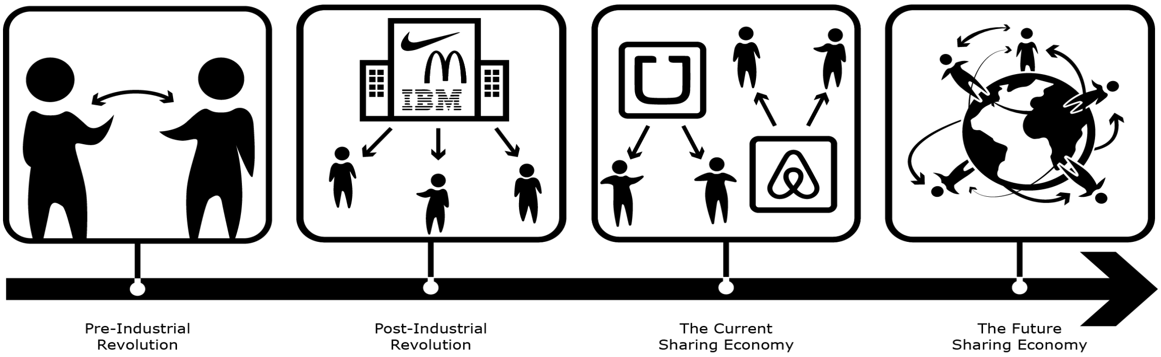
Dutch Blockchain Coalition

Blockchain is viewed as a potential source of trust, prosperity and security for society and business. The Dutch Blockchain Coalition tries to stimulate the large scale deployment of blockchain technology in The Netherlands.

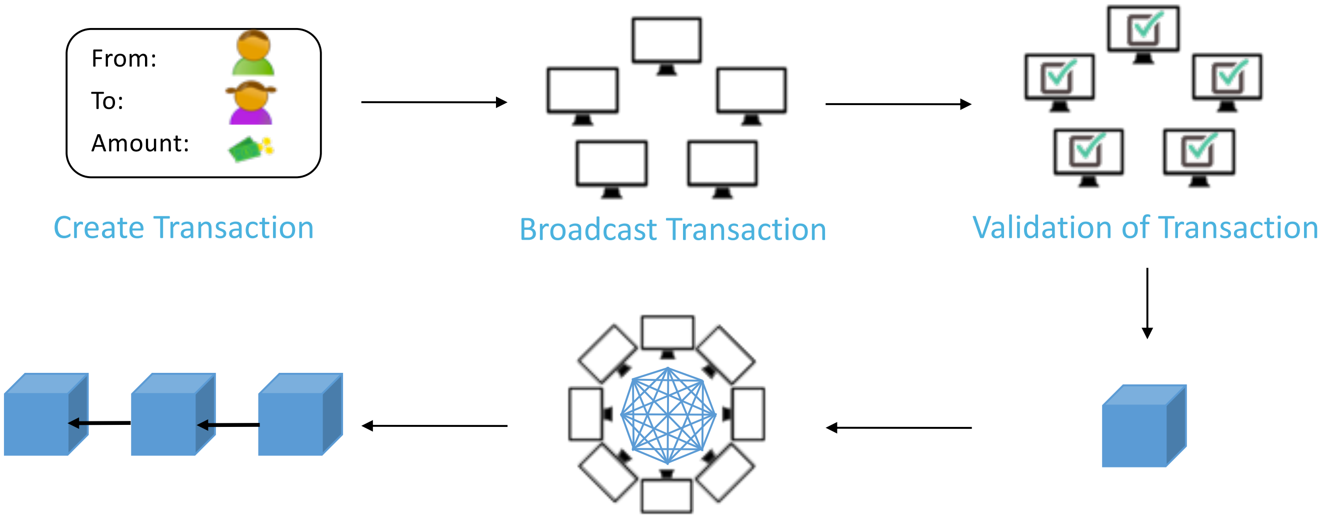
BLOCKCHAIN LAB

Delft University of Technology, The Netherlands
Established 29 August 2007

Evolution of Trust


Pre-Industrial Revolution
Post-Industrial Revolution
The Current Sharing Economy
The Future Sharing Economy

Blockchain Technology



From:
To:
Amount:

Create Transaction

Broadcast Transaction

Validation of Transaction

Immutable Block

Distribute Block

Block Creation

But whose block to add?

- Everyone in the network sees the transactions
- And can create a block
- Which block to add to the chain?

- Depends on the blockchain
  - Permissionless
  - Permissioned

Permissionless Blockchain

- ANYONE can join! (Bitcoin)

- A lottery system is needed to select the round leader
  - to add his/her block

- How?
  - Proof-of-Work (51% rule)
  - Proof-of-Stake
  - Proof-of-Activity
  - Proof-of-Luck

Blockchain, Where to use?

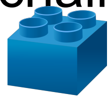
- Multiple actors with trust issue
  - **Finance**: cryptocurrency, credit cards, currency exchange,…
  - **Government**: auditing, voting, registration.
  - **Logistics**: supply chain, tracking, shipment,…
  - **Healthcare**: tests, validation, sharing information, …
  - **IoT:** authentication, revocation,…
  - **Smart Grids:** load balancing, statistics, self-sufficient micro-grids

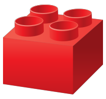
What to do with blockchain

- **Documents** (sharing)
  - medical records, manifests, certificates, governmental documents, declarations…
- **Identities**
  - universal identity, sovereign identities, passports, credit cards,…
- **Values**
  - cryptocurrencies, tokens, loyalty points, green points, …
- **Smart Contracts**
  - business logic

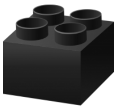
What are we waiting for?

- The tools we have now:
  - Public Blockchain:
    - Bitcoin
    - Ethereum



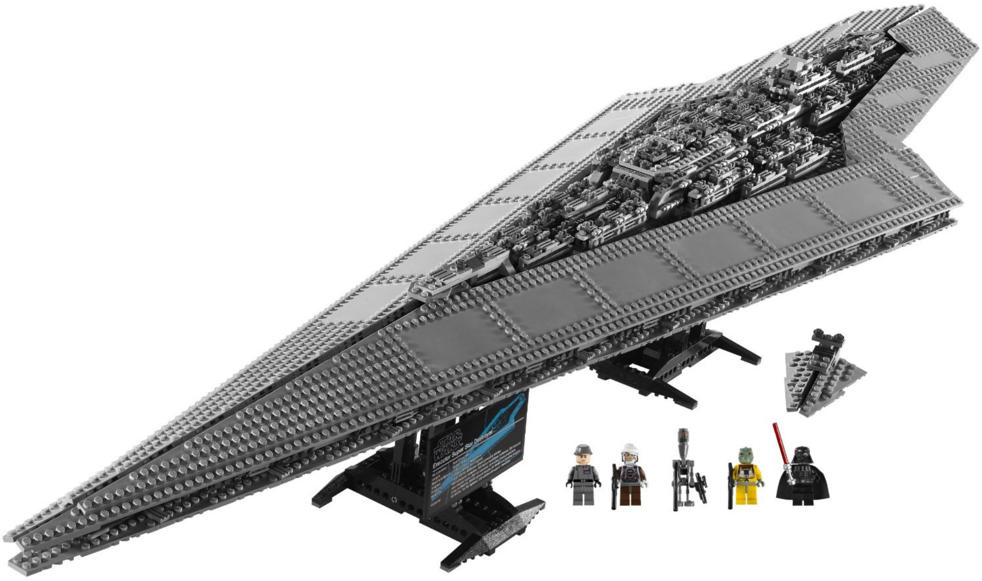


  - Private (consortium) Blockchain:
    - Hyperledger-fabric
    - Tendermint



What are we waiting for?

- The things we want to build:



What’s wrong?

- Dilemmas in blockchain:
  - Throughput vs. Scalability
  - Privacy vs. Reliability
  - Lightweight vs. Reliability
  - Flexibility vs. Security

Don’t be frustrated!

Will blockchain be the next “Internet”?

The real questions is

Will your application be the next e-mail, Yahoo, Google, Facebook…?

Domains in Cyber Security Group

- Logistics: BlockLab and TKI Project
- Smart Grids: CGI+PowerWeb
- Medicine (EU project proposals)

Application Driven Research

- Finance
    - DegReg: Double-Financing of invoices
    - KYC (Real estate, MoJ, NN)

- Logistics
    - **PassPort: Container Tracking System**
    - **Trade SCM System**
    - **DeCouples: SCM System**
    - **Container Management System**

- Smart Grids
    - Load Balancing with EV (TBM)
    - Load Balancing with EV using Game Theory (3ME)
    - DoxChain: Emission Trade Market (BE)
    - ExChain: Energy Trade Market (BE)

Research

- Efficient and Scalable Consensus Algorithms
- Leadership Selection

- Key management for large networks (IoT)
- Retrieving external data: Oracles
- Privacy, anonymity, traceability

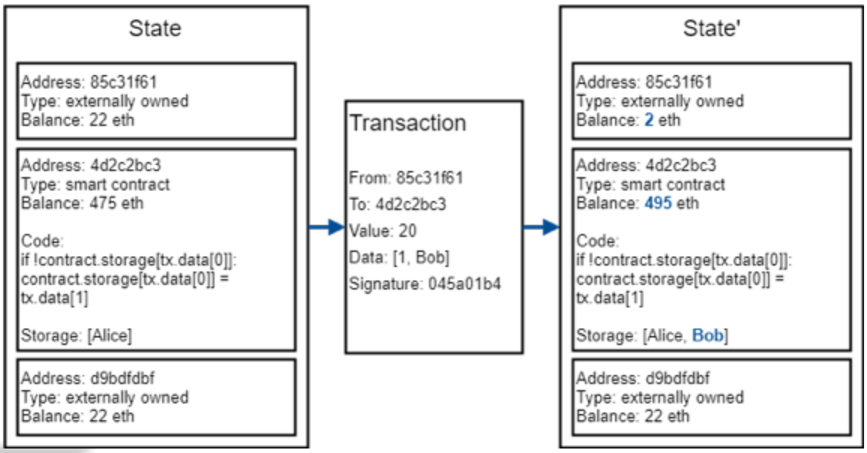
- Adversarial Machine Learning

Oracles

Smart Contracts

Storage Contract

```
function store(key, value) {
    if not contract.storage[key] {
        contract.storage[key] = value
    }
}
```



State

Address: 85c31f61
Type: externally owned
Balance: 22 eth

Address: 4d2c2bc3
Type: smart contract
Balance: 475 eth

Code:
if !contract.storage[tx.data[0]]:
contract.storage[tx.data[0]] =
tx.data[1]

Storage: [Alice]

Address: d9bdfdbf
Type: externally owned
Balance: 22 eth

Transaction

From: 85c31f61
To: 4d2c2bc3
Value: 20
Data: [1, Bob]
Signature: 045a01b4

State'

Address: 85c31f61
Type: externally owned
Balance: 2 eth

Address: 4d2c2bc3
Type: smart contract
Balance: 495 eth

Code:
if !contract.storage[tx.data[0]]:
contract.storage[tx.data[0]] =
tx.data[1]

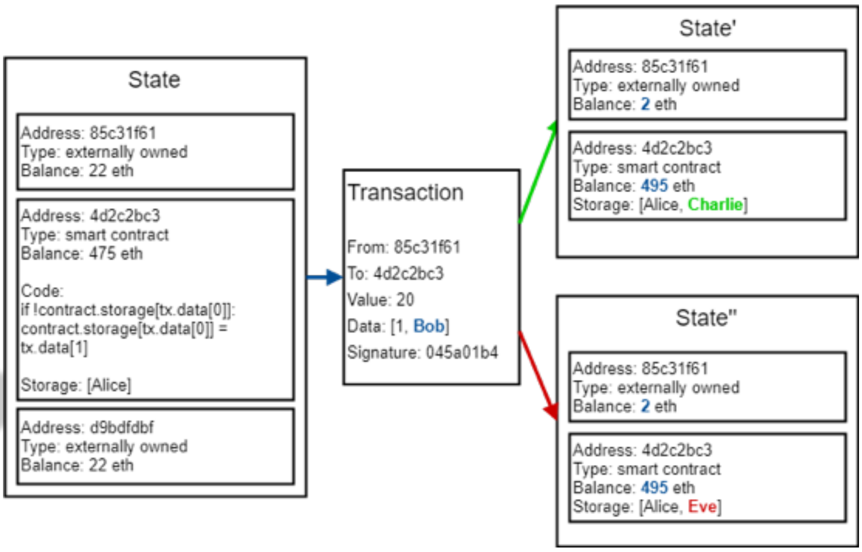
Storage: [Alice, Bob]

Address: d9bdfdbf
Type: externally owned
Balance: 22 eth

Smart contracts + non-deterministic data

Smarter Storage Contract

```
function store(key, value) {
    if not contract.storage[key] {
        val = api.get(storage.com/?v=value)
        contract.storage[key] = val
    }
}
```



State

Address: 85c31f61
Type: externally owned
Balance: 22 eth

Address: 4d2c2bc3
Type: smart contract
Balance: 475 eth

Code:
if !contract.storage[tx.data[0]]:
contract.storage[tx.data[0]] =
tx.data[1]

Storage: [Alice]

Address: d9bdfdbf
Type: externally owned
Balance: 22 eth

Transaction

From: 85c31f61
To: 4d2c2bc3
Value: 20
Data: [1, Bob]
Signature: 045a01b4

State'

Address: 85c31f61
Type: externally owned
Balance: 2 eth

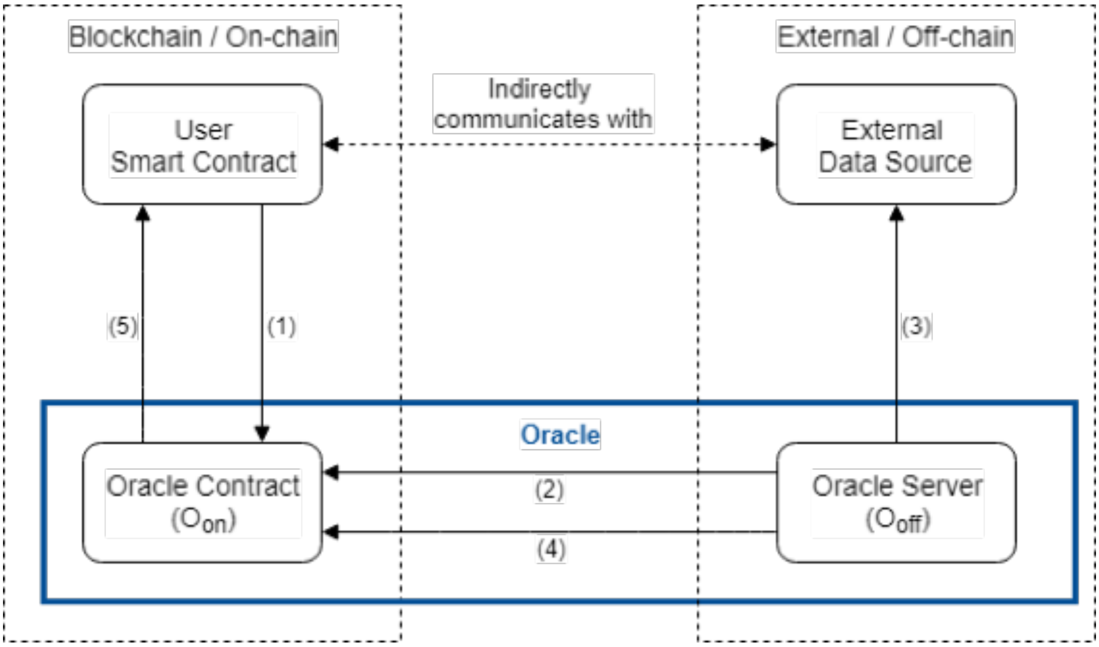
Address: 4d2c2bc3
Type: smart contract
Balance: 495 eth
Storage: [Alice, Charlie]

State''

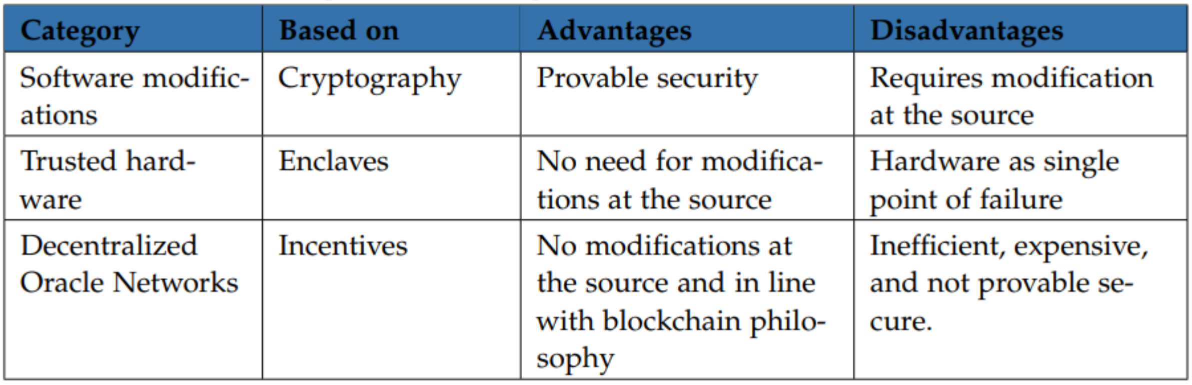
Address: 85c31f61
Type: externally owned
Balance: 2 eth

Address: 4d2c2bc3
Type: smart contract
Balance: 495 eth
Storage: [Alice, Eve]

Data Retrieval



Existing Solutions



Category	Based on	Advantages	Disadvantages
Software modifications	Cryptography	Provable security	Requires modification at the source
Trusted hardware	Enclaves	No need for modifications at the source	Hardware as single point of failure
Decentralized Oracle Networks	Incentives	No modifications at the source and in line with blockchain philosophy	Inefficient, expensive, and not provable secure.

Current research on Muscle=ChainBridge+Multi-Key Homomorphic Signatures

Trade and Decouples

- **Humanitarian Aid**

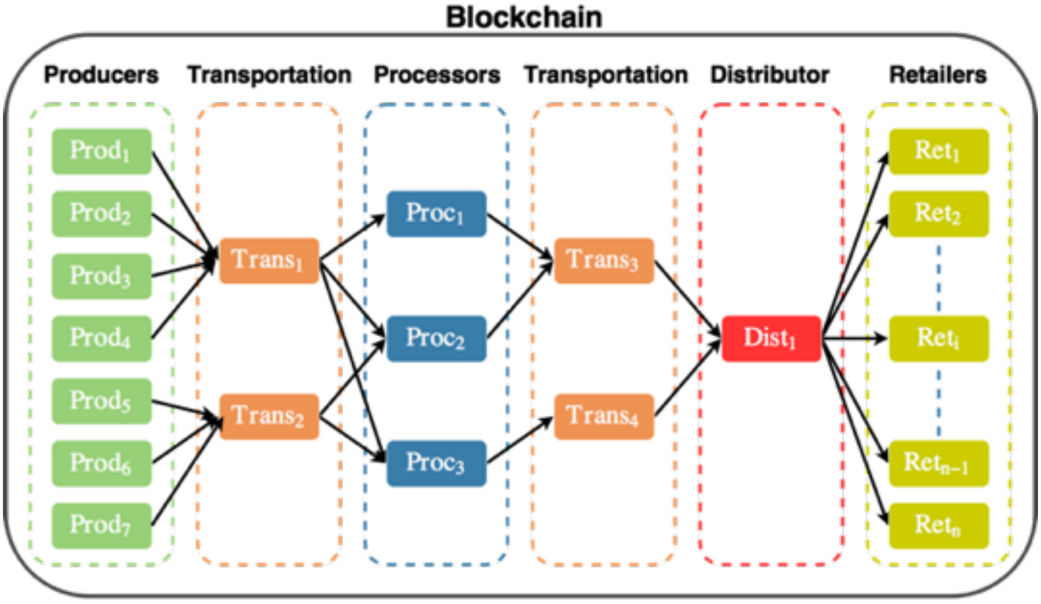
ACTION AGAINST HUNGER

WFP World Food Programme

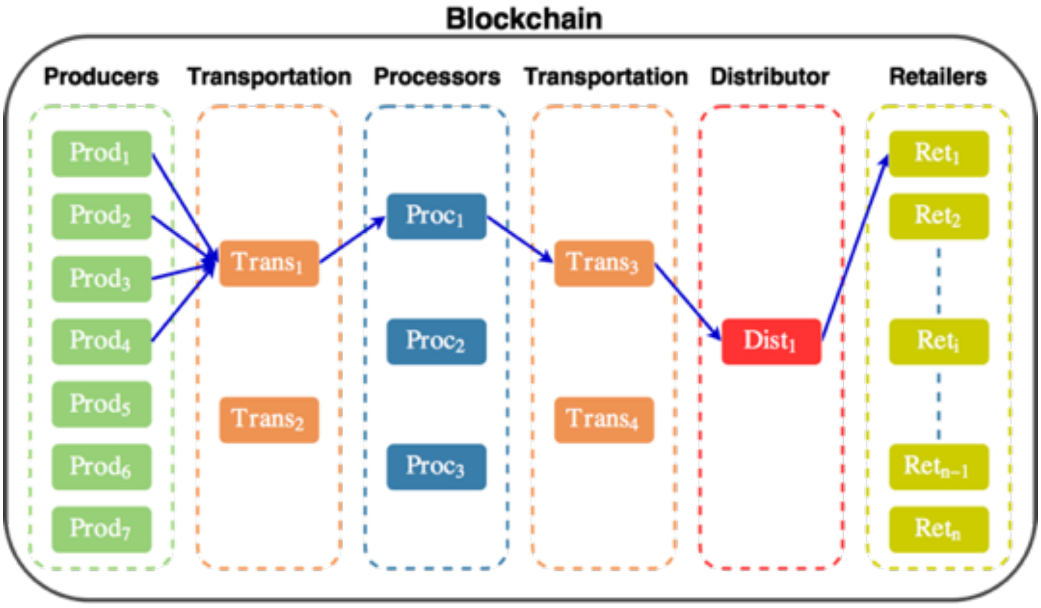
unicef

Oxfam International

Trade



Trade



M. El Maouchi, O. Ersoy and Z. Erkin. TRADE: A Transparent, Decentralized Traceability System for the Supply Chain, accepted, ERCIM Workshop on Blockchain Engineering: Challenges and Opportunities for Computer Science Research, May 2018, Amsterdam, The Netherlands.

Research

- Data collection/sharing
    - Data in/out with sensors
    - Oracles

- Privacy, traceability, transparency; anonymity, unlinkability

- Cryptographic constructions (efficiency)
    - Signatures
    - ZKPs
    - Commitments
    - Practical and secure key management

Thank you!

z.erkin@tudelft.nl