Aalto University
School of Electrical
Engineering

Value Network Design for Internet Blockchains aka Distributed Ledger Technologies Course E7830 Aalto University

Pekka Nikander
Feb 13th, 2018

Presentation outline

- Introduction
- Distributed Ledger Technologies, aka Blockchains
- DLT design choices
- Open Business Platforms
- SOFIE project pilots
- Applying DLT to business cases

Why blockchains?

"Blockchain *distributed consensus model* is the most important invention since the Internet itself", Marc Andreessen

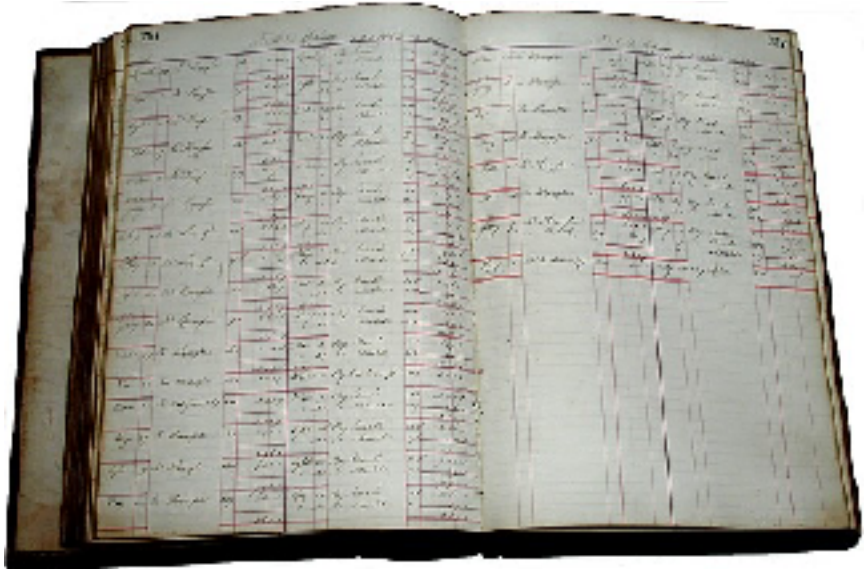
Introduction

- Research problems:
  - Is it possible to create commons-like *open business platforms* that have no owner but are jointly maintained?
- Hypotheses:
  - DLTs (aka blockchains) allow open business platforms
  - Enable business transactions across heterogeneous systems
- Two projects:
  - EU H2020 project SOFIE
  - Aalto Observatory on Digital valuation systems

Distributed Ledger Technologies aka Blockchains

- Decentralised open ledger
  - Undeniable transactions
  - Full ordering
- Accumulation of history
- Main design choices
  - Identity management — anonymous or not
  - Consistency and consensus models
  - Incentive model(s)

Open ledger



Open ledger

- Open
- Decentralised
- Undeniable
- Consistent
- Event
- Sequence

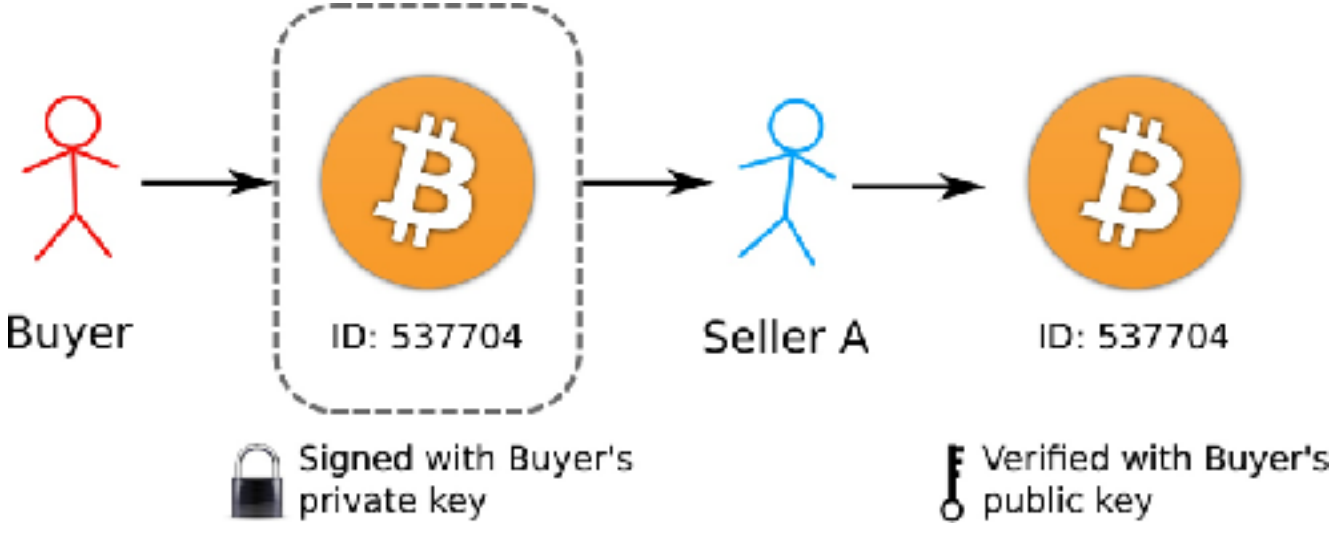
Open ledger

If it is in the ledger
I can believe in it

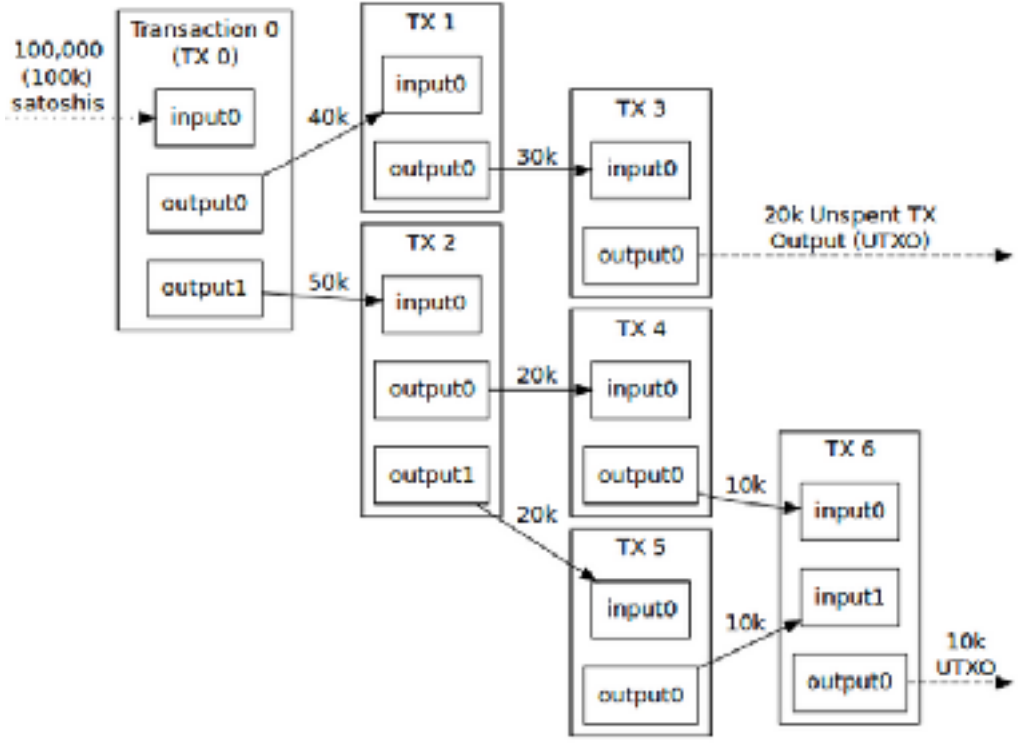
Доверяй, но проверяй
Trust, but verify

Undeniable ordered transactions

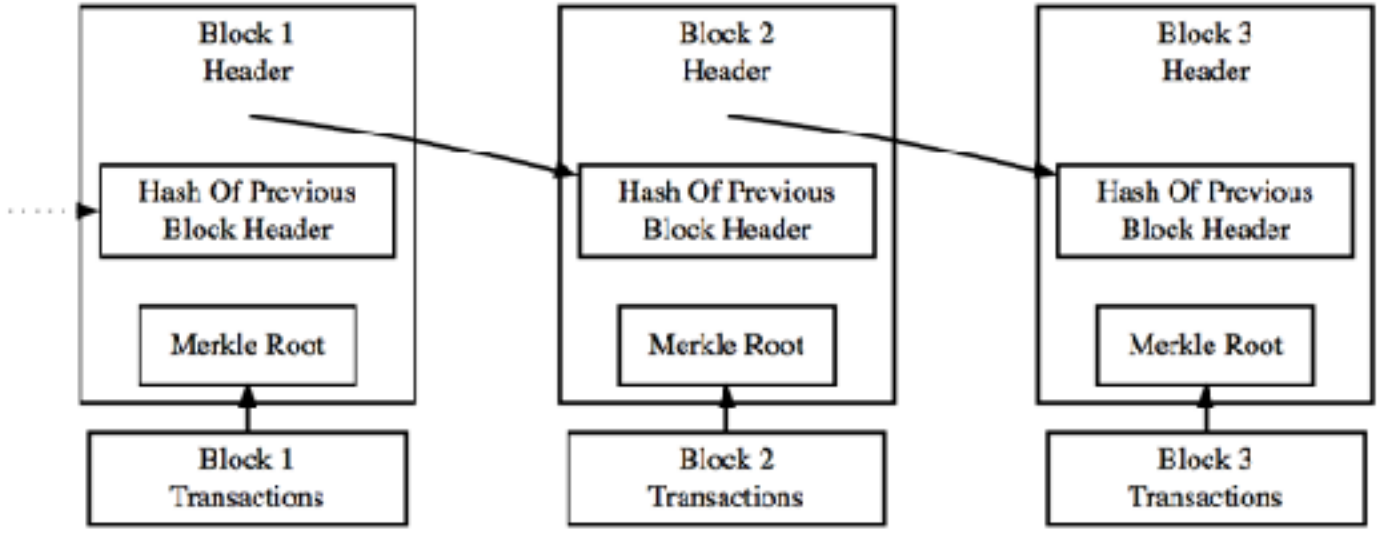
Undeniable …


Buyer
ID: 537704
Seller A
ID: 537704
Signed with Buyer's private key
Verified with Buyer's public key

… transactions …



… ordered with blocks



Simplified Bitcoin Block Chain

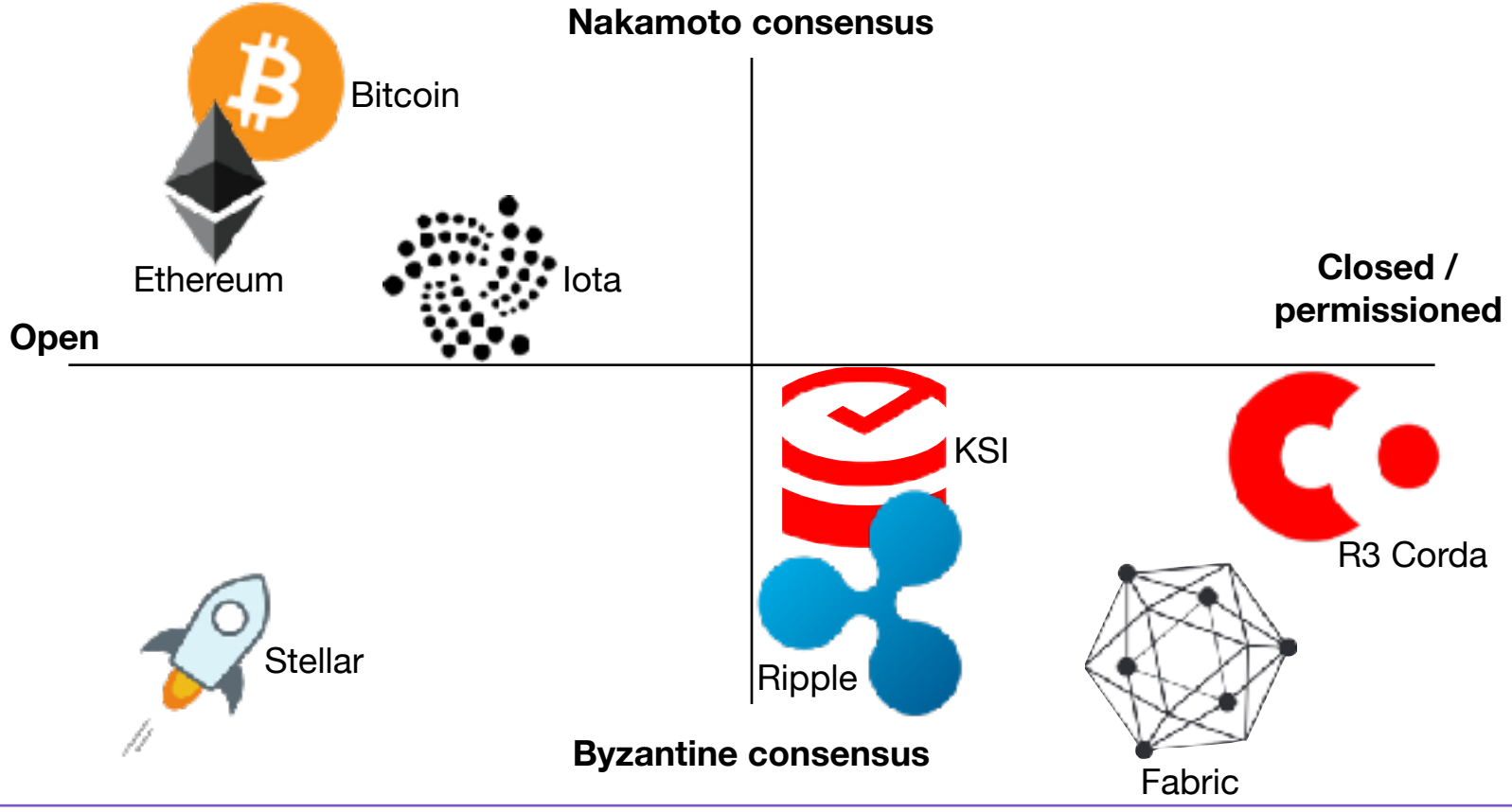
[Merkle tree allows one to check that a transaction is in the block in O(log(N))]

Accumulation of events

- **Unforgeable history**
  Spread to the network
- **Majority consensus**
  Spreading to the network
- **Forming consensus**
- **Proposed events**

The more the merrier!

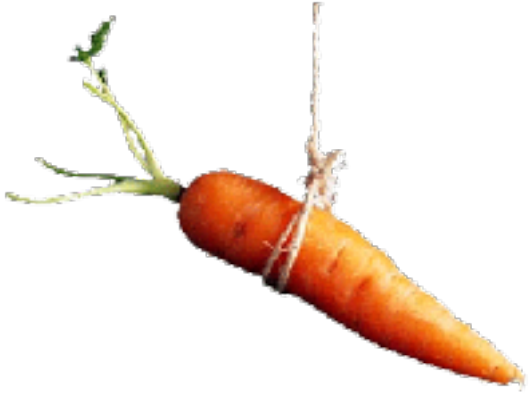
Different kinds of blockchains



Presentation outline

- Introduction
- Distributed Ledger Technologies, aka Blockchains
- DLT design choices
- Open Business Platforms
- SOFIE project pilots
- Applying DLT to business cases

Design choices



Identity

Consensus and Consistency

Incentives

Identity: Joining and mining

- Who can join?
  - Propose valid transactions
- Who can mine?
  - Define transaction order

Identity: Fundamentals

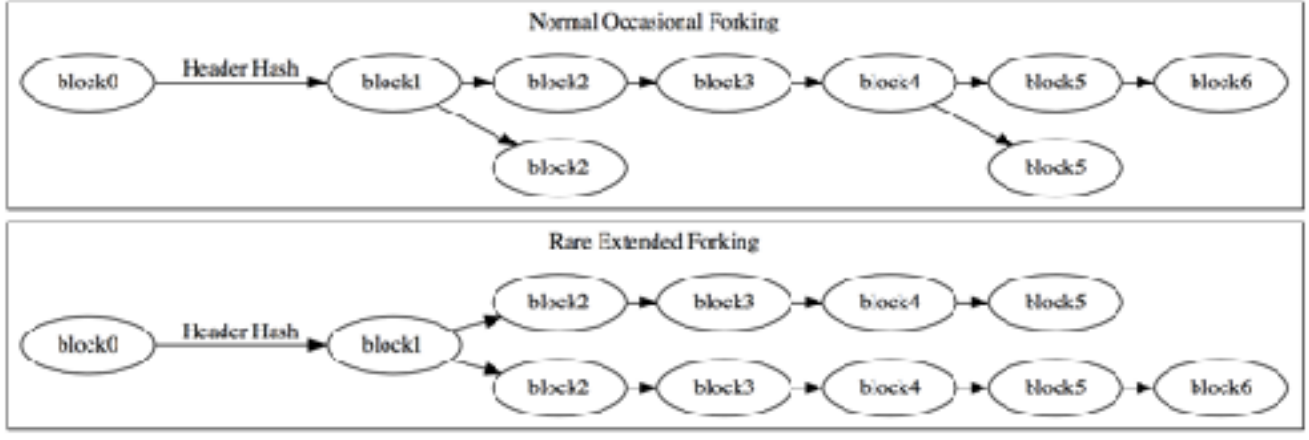
- May an identity have *negative* value?
  - You need the real world
    - or entry barrier as high as highest negative value
- Is *collusion* (Sybil attack) a threat?
  - You are likely to need the real world
- Can one benefit from *affecting the order*?
  - You may need the real wold for mining

Consistency

- Is full order / consistency really a must?
  - How fast do you need full consistency?
    - E.g. bitcoin reaches full consistency only in about an hour

- Can you remodel you problem to partial order / eventual consistency?
  - or can you do without the block chain?

Consensus

- **Usually meaning: No block chain forks …**
- 

- **… but requires rethinking with partial order or weak consistency**

Incentives

- Verification requires work
  - Check transaction chains, signatures, identities, …
- Remember the added value?
  - “If it is in the ledger, I can believe in it”

- How to make sure there is the ledger?
  - Who have the incentive to contribute it?
- How to make sure everything in the ledger has been verified?
  - How to punish the lazy bookkeeper?

Some incentive models

- Get paid through block mining (bitcoin)
  - Mining creates new “money”
- Get explicitly paid in the transactions
  - Value explicitly transferred to the miners
- Only way to propose transactions
  - Each transaction verifies some others randomly
  - Likely to work only with partial oder

Presentation outline

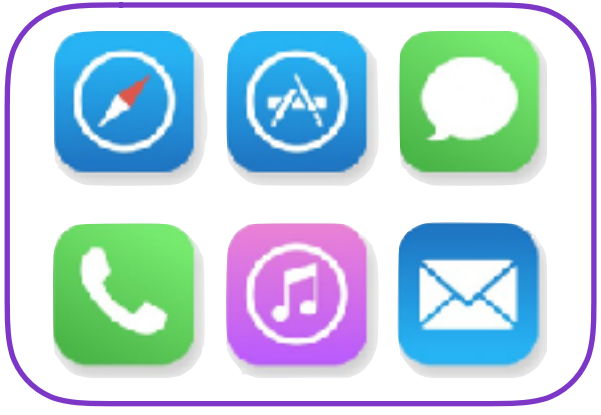
- Introduction
- Distributed Ledger Technologies, aka Blockchains
- DLT design choices
- Open Business Platforms
- SOFIE project pilots
- Applying DLT to business cases

Open business platforms

- Examples of closed digital business platforms
  - Apple and Google
  - AirBnB
- Structure of digital business platforms
- Open business platforms

Apple and Google

Developers



Users

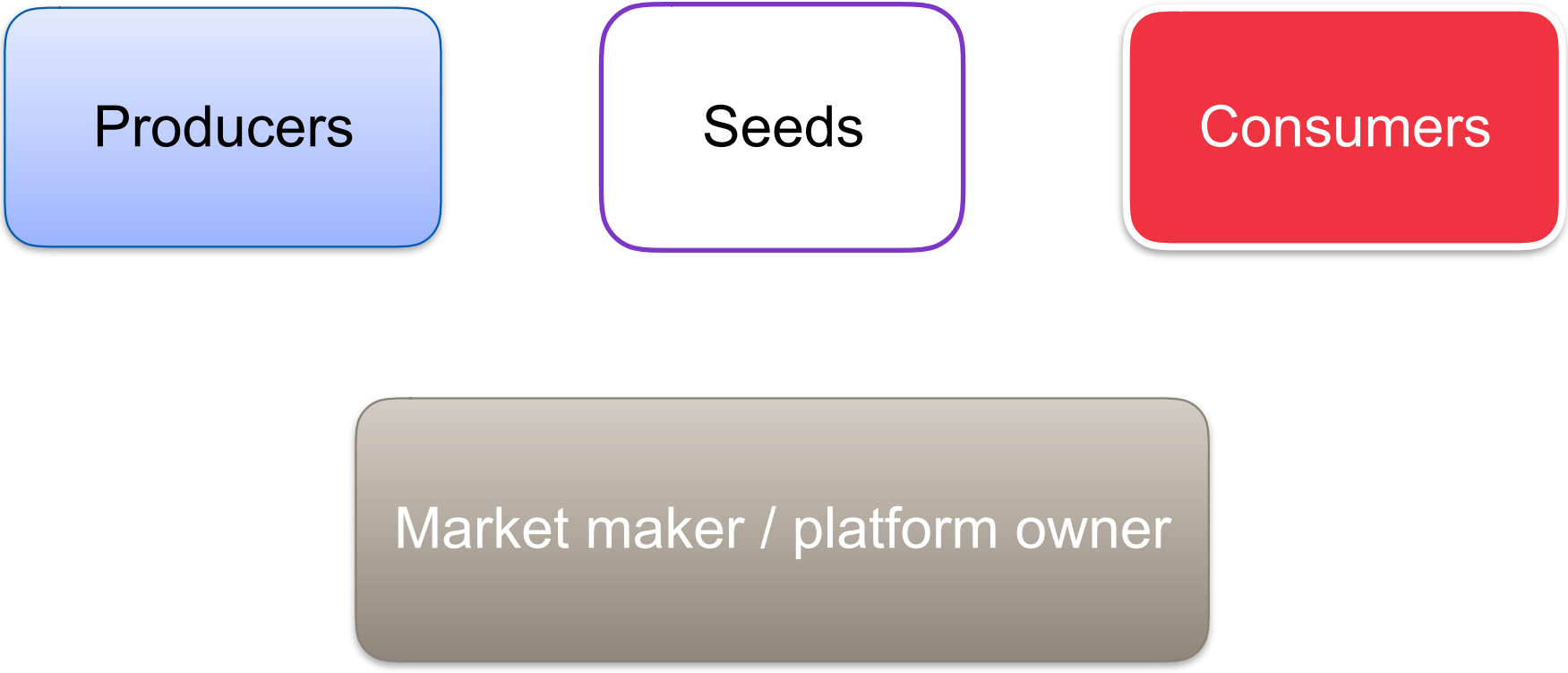
AirBnB

Hosts

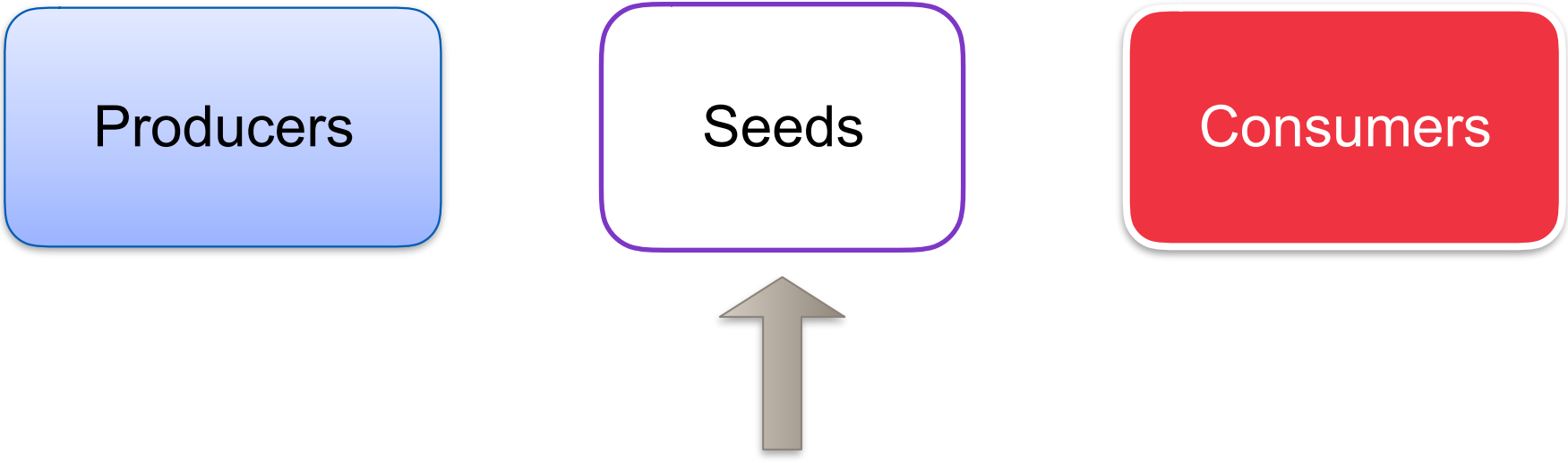
Travellers

airbnb

Platform structure

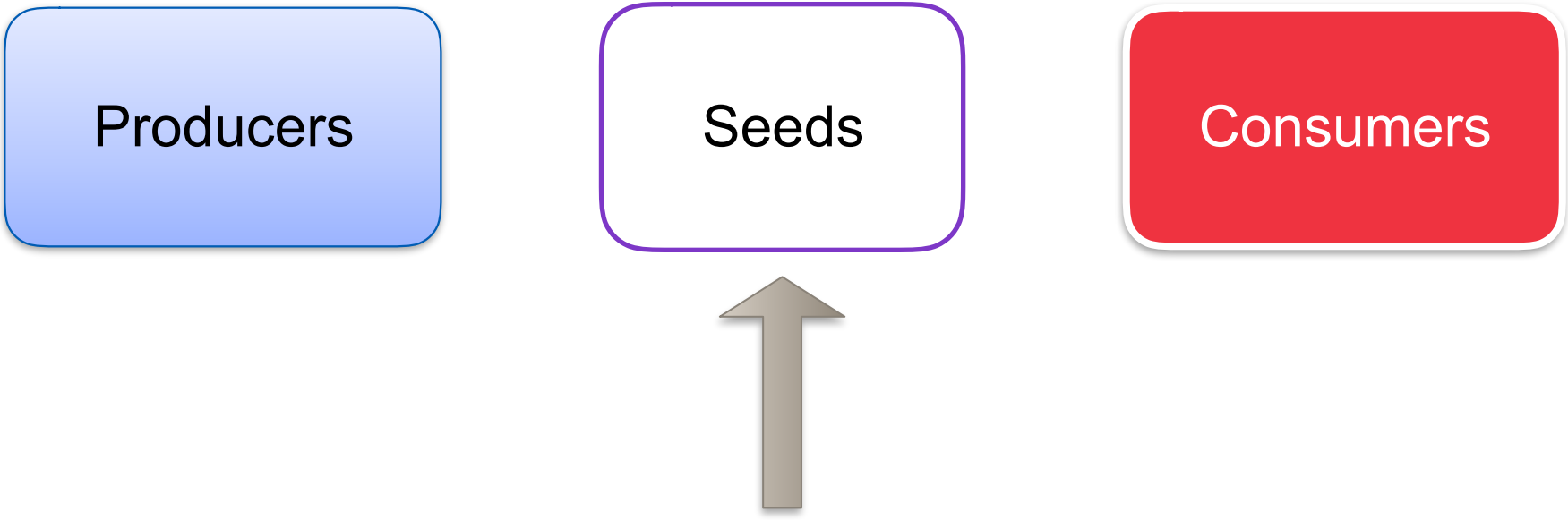


Seeds



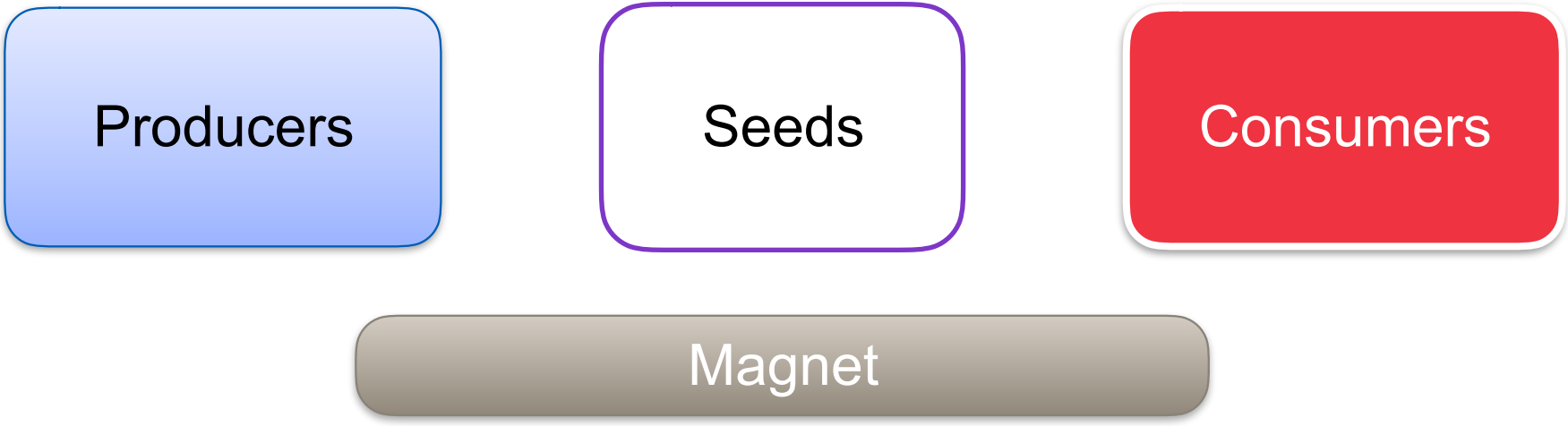
Minimum information/content required to start an interaction

Seeds



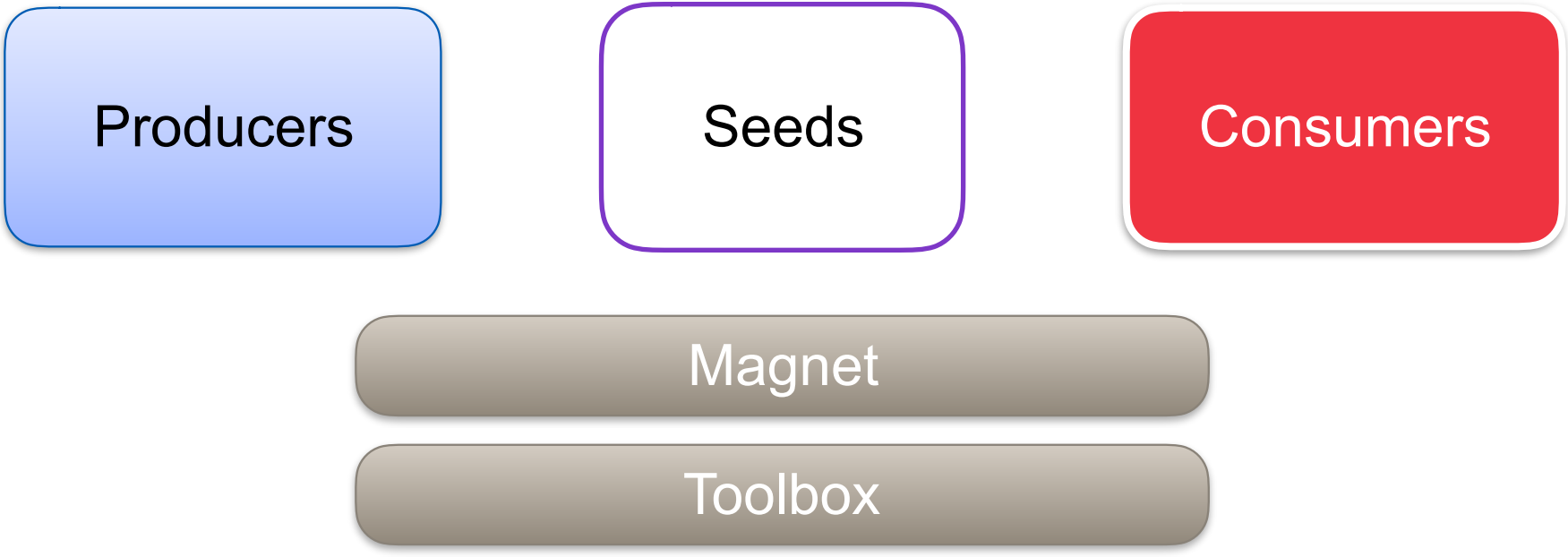
Focus on the primary interaction

Seeds: The magnet

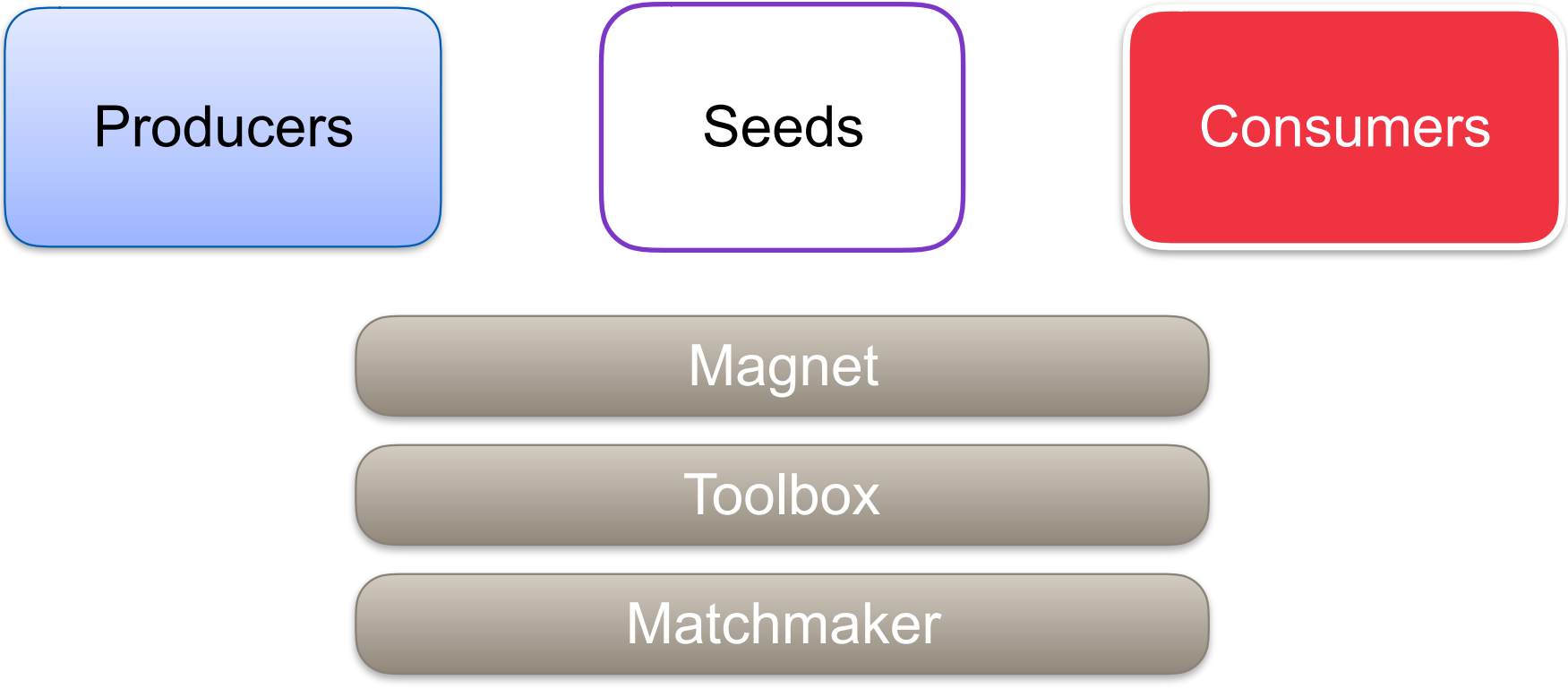


What brings produces and consumers on board?

Toolbox: Means to interact



Use data to create matches



Conditions for repeatable interactions

Matchmaking
Curation / reputation
Trust

Open business platforms

- Examples of closed digital business platforms
  - Apple and Google
  - AirBnB
- Structure of digital business platforms
- **Open business platforms**

Open platform structure

Producers

Seeds

Consumers

Decentralised platform
No owner
A commons

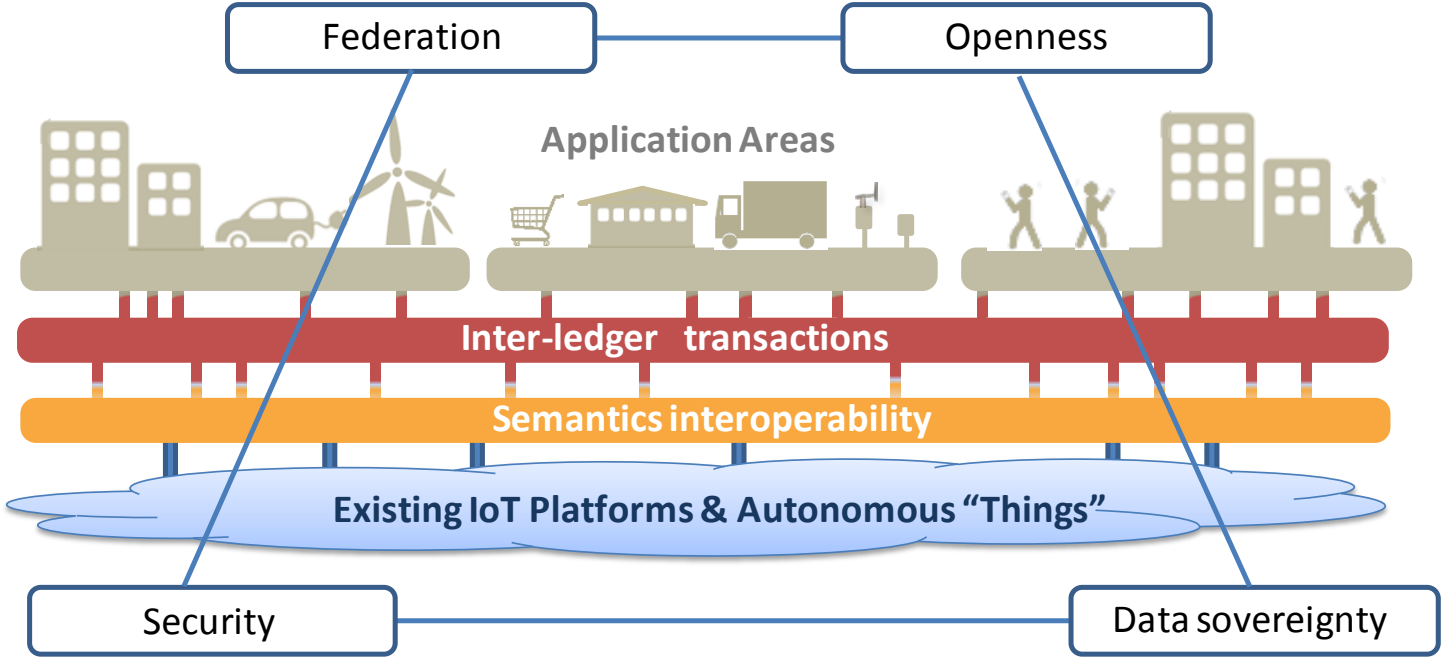
Presentation outline

- Introduction
- Distributed Ledger Technologies, aka Blockchains
- DLT design choices
- Open Business Platforms
- SOFIE project pilots
- Applying DLT to business cases

SOFIE: Introduction and goals

- **EU H2020 IoT-03 R&I project**
- **3 years 2018–2020**
- **Key idea: Secure Open Federation, using DLTs**
- **Stated concrete objectives:**
  - **Define an IoT federation *architecture* and develop a corresponding *framework***
  - ***Deploy and evaluate* the federation framework *in field trials***
  - **Evaluate the *commercial viability***
  - **Establish the IoT federation approach as *a major enabler***

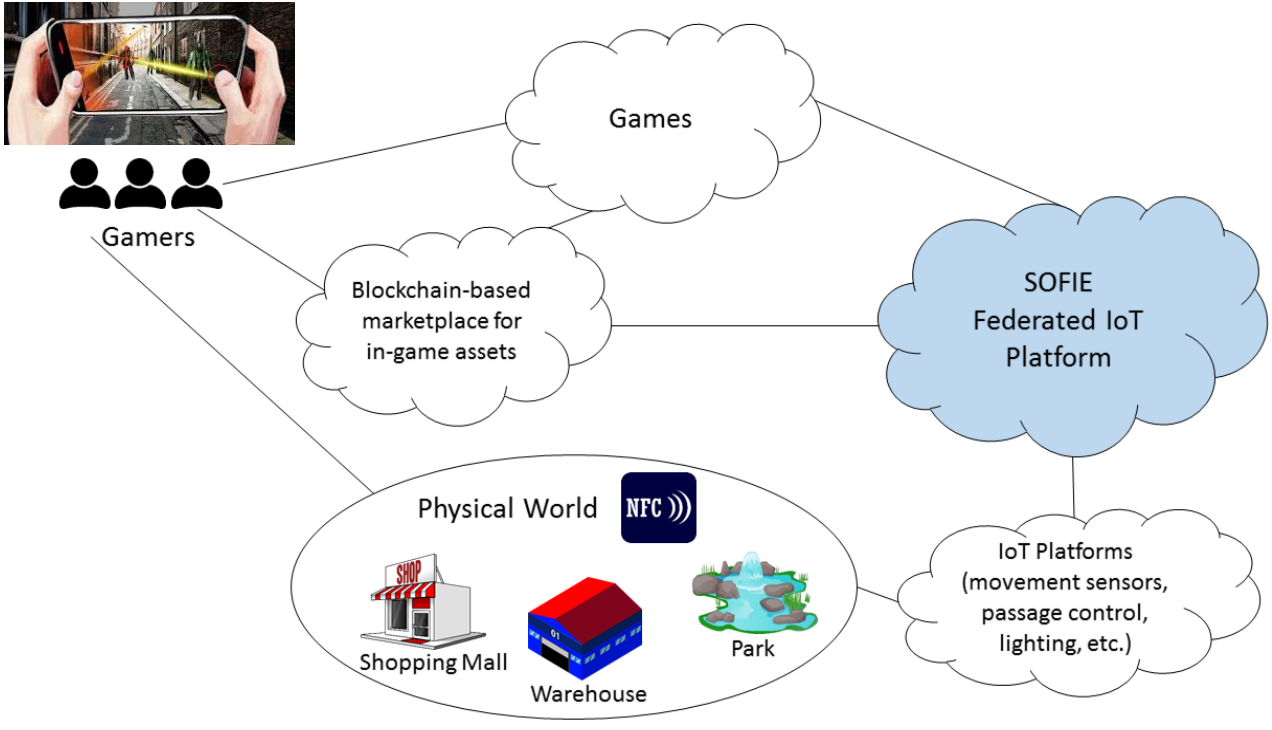
SOFIE core concept



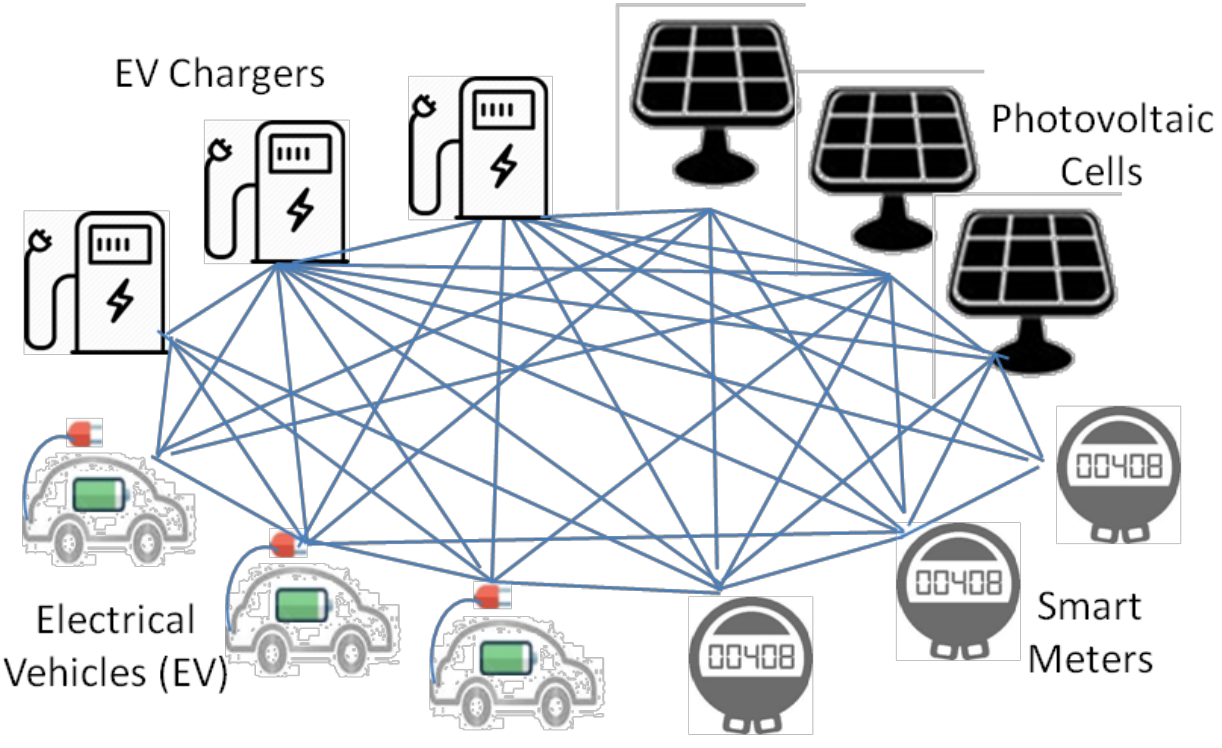
SOFIE field trials

- Mixed reality gaming
  - Rovio; AUEB for deployment
- Energy
  - Guardtime, Italian partners
- Food chain
  - Synelixis, Optimum

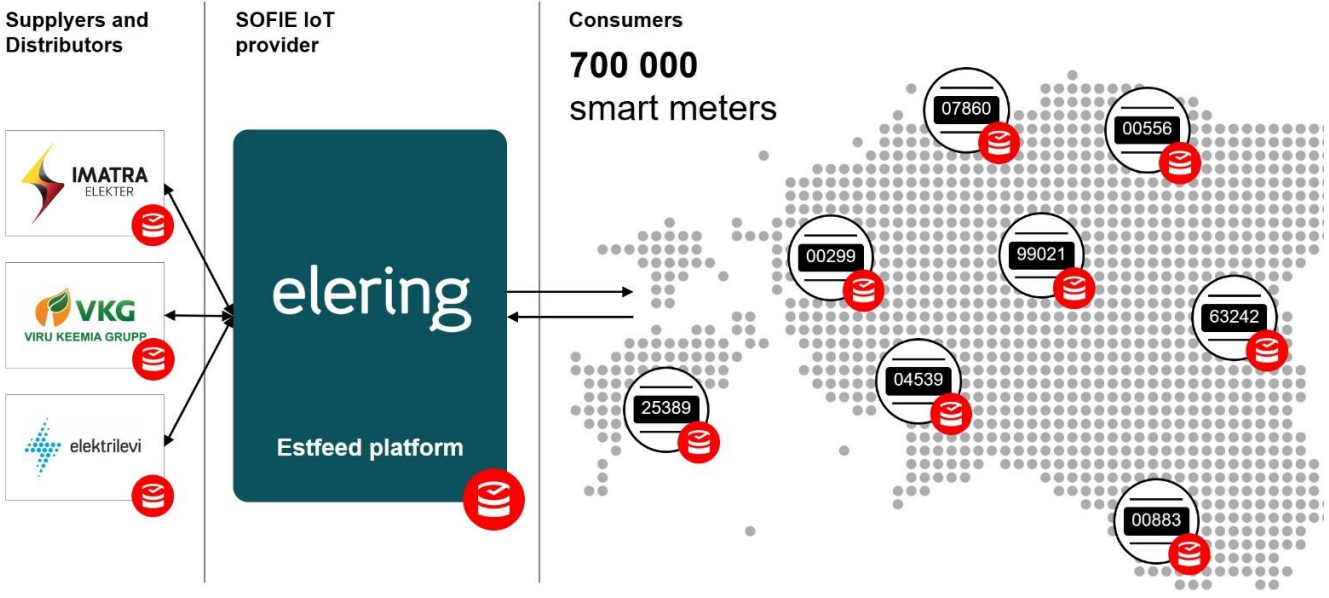
Mixed reality gaming



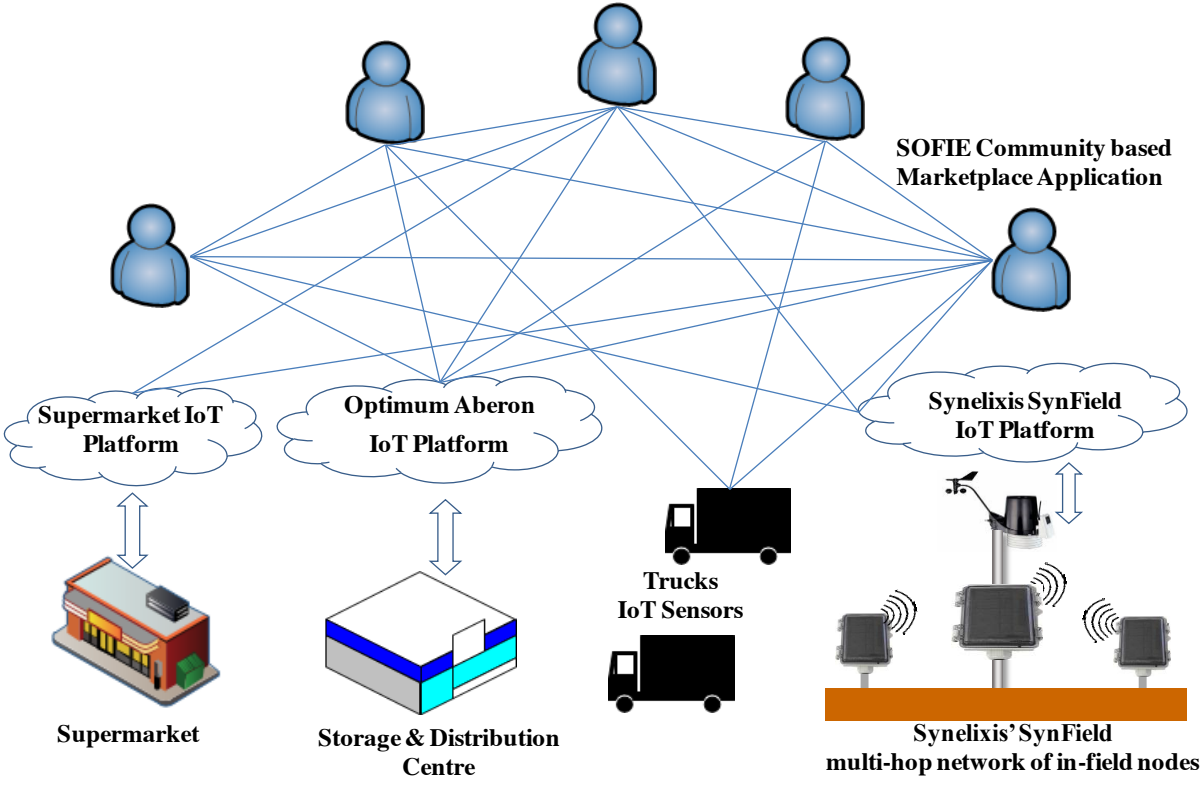
Energy: Terni



Energy: Estonia



Food chain: From field to fork



Presentation outline

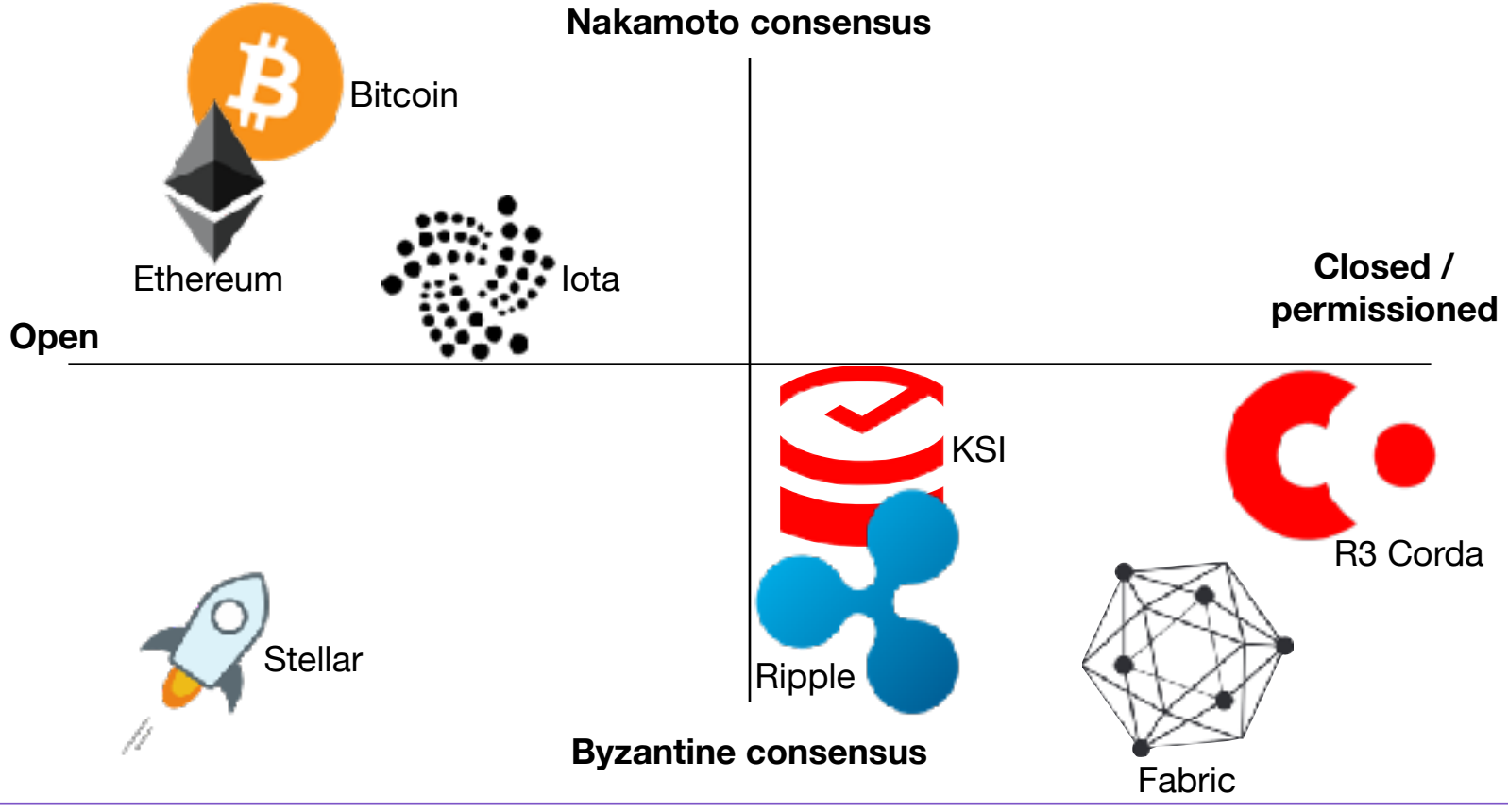
- Introduction
- Distributed Ledger Technologies, aka Blockchains
- DLT design choices
- Open Business Platforms
- SOFIE project pilots
- Applying DLT to business cases

DLTs are not silver bullets

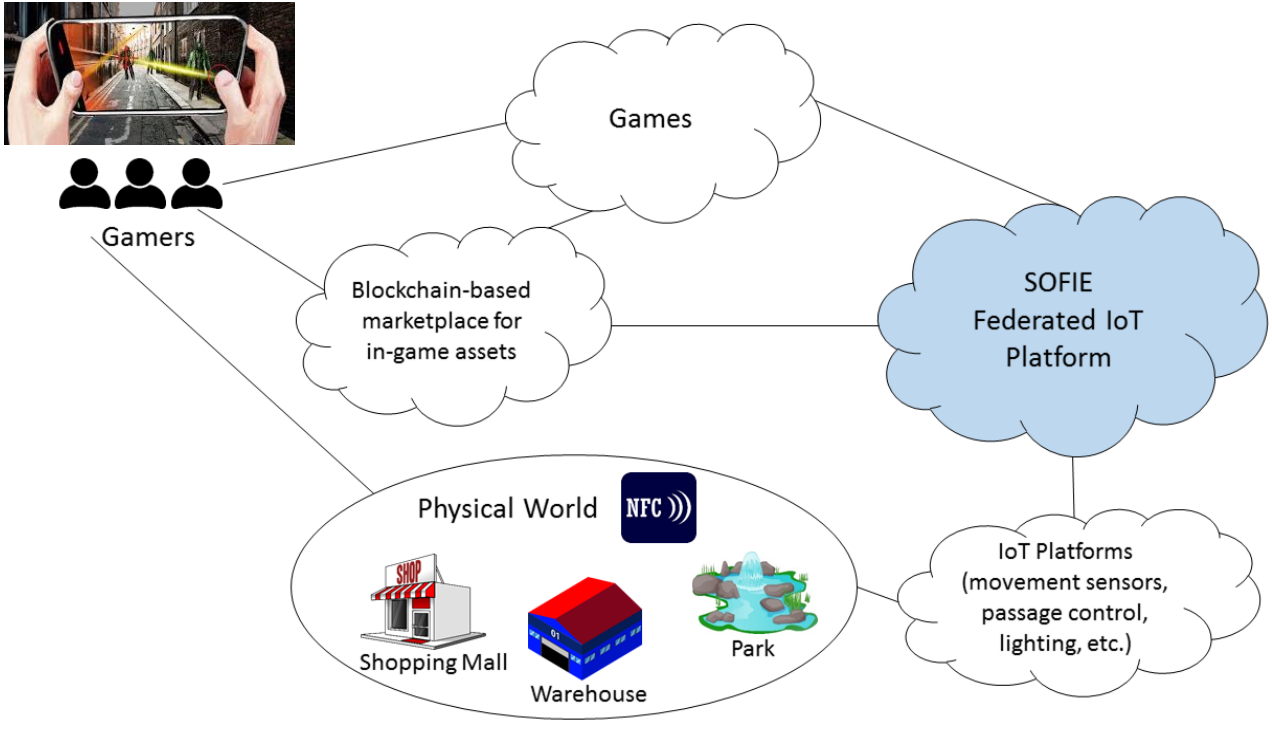
These four conditions must apply for a DLT to be useful:

1. **Shared database between multiple parties**
2. **Absence of trust ("trustless")**
3. **Need explicit consensus**
   - ***Conflicting* transactions must be resolved**
4. **Desirability of no intermediation**
   - **E.g. issues with trust or cost structure**

DLTs are different



Example: Mixed reality gaming



Example: Mixed reality gaming

1. Shared database between multiple parties
   - Gamers, gaming company, building owners, …
2. Absence of trust (“trustless”)
   - Multiple gaming companies?
3. Need explicit consensus
   - Who owns the in game asset, right now?
4. Desirability of no intermediation
   - A super-gaming company instead?
- Or would an unforgeable audit trail be enough?

Example: Mixed reality gaming

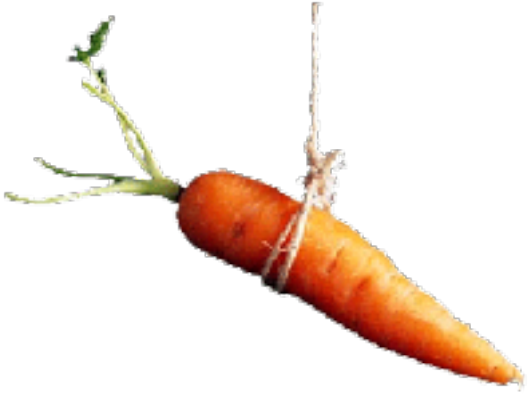
Producers

Seeds

Consumers

Decentralised platform
No owner
A commons

Example: Mixed reality gaming



Identity

Consensus and Consistency

Incentives

Summary


I THINK WE SHOULD BUILD A BLOCKCHAIN
UH OH
DOES HE UNDERSTAND WHAT HE SAID OR IS IT SOMETHING HE SAW IN A TRADE MAGAZINE AD?
WHAT COLOR DO YOU WANT THAT BLOCKCHAIN?
I THINK MAUVE HAS THE MOST RAM