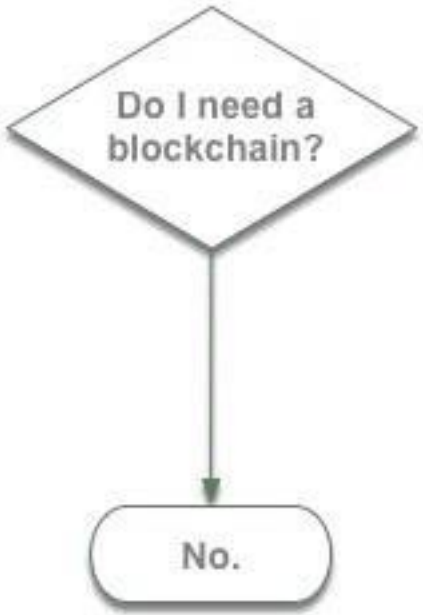
Shall I use blockchain?

Analyzing the suitability of blockchain for a business scenario

Prof. Marco Comuzzi
Department of Industrial Engineering
Ulsan National Institute of Science and Technology (UNIST)
mcomuzzi@unist.ac.kr

Thank you, see you next week



Marco Comuzzi mcomuzzi@unistac.kr

What's the plan for this lecture?

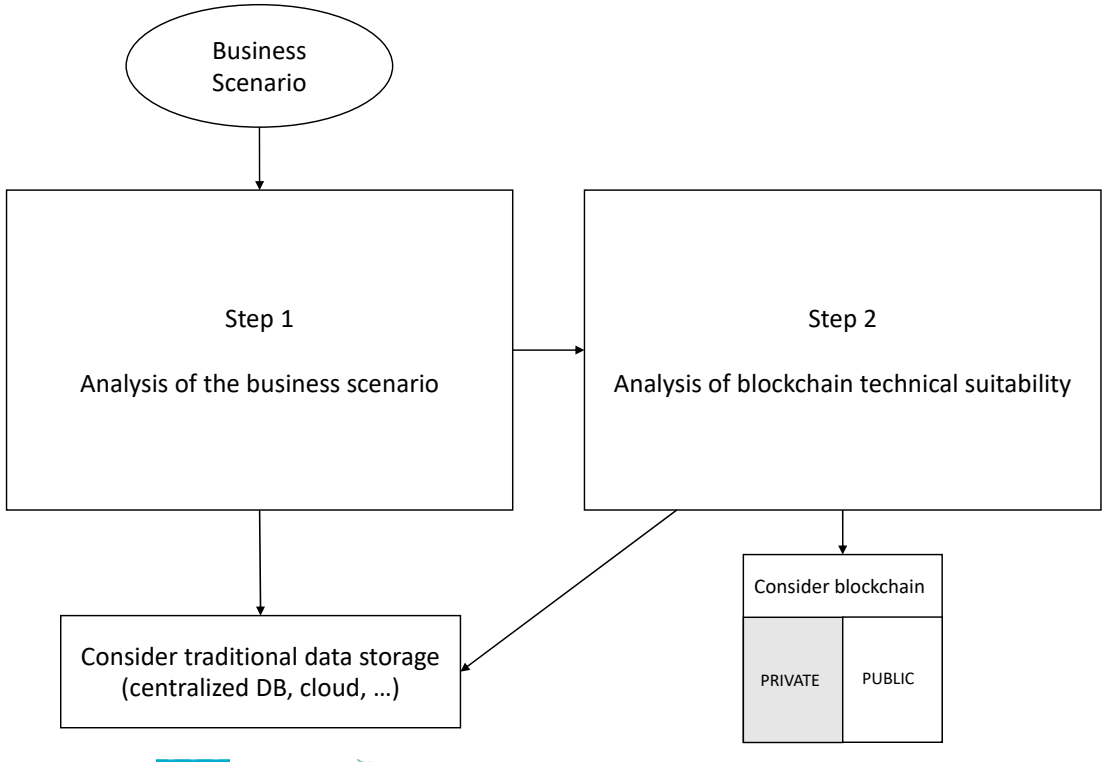
Marco Comuzzi mcomuzzi@unistac.kr

1.
Decision Problem

Decision problem

Given a business scenario, is blockchain a good solution to manage information, assets etc. within this scenario?

If yes, what type of blockchain, public or private?



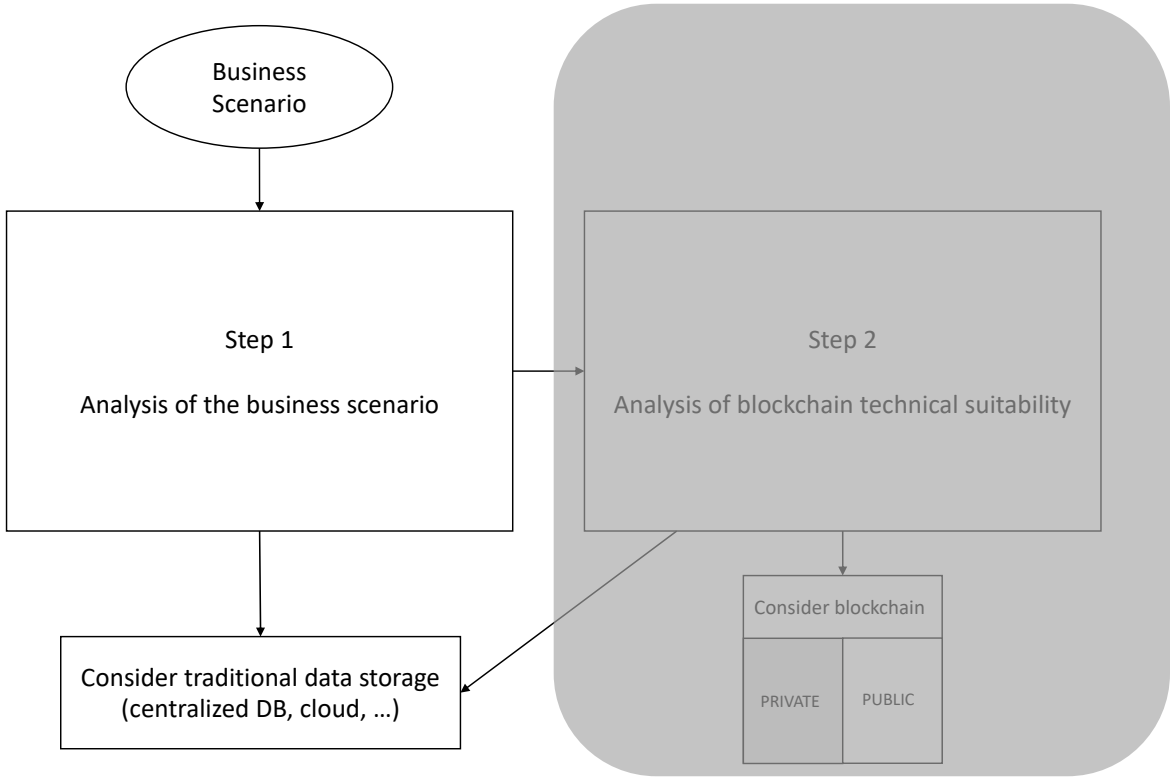
2.
Step 1:
Scenario Suitability

Step 1 in the decision process

We look first at specific characteristics of the business scenario

The outcome of Step 1 can be:

Proceed to Step 2
Consider traditional storage



Characteristics of a business scenario for blockchain

Is the scenario multi-party?

Is a trusted authority lacking?

Is operation centralized?

Is data immutability beneficial?

Marco Comuzzi mcomuzzi@unistac.kr

Multi-party

A business scenario is multi-party if it cannot exist without the presence of two or more collaborating business actors

Business scenario that include only one party are becoming rare

Still, in many scenario one party has often “full control” (e.g. automotive)

Blockchain makes sense in multi-party scenario
(the more ”equal” the parties, the better)

Marco Comuzzi mcomuzzi@unistac.kr

Typical multi-party scenarios

Business scenario type	Actors involved
Global supply chain management	Clients, suppliers, logistic service providers, transportation companies, port and custom authorities, insurers, banks and credit providers.
Healthcare	Patients, private clinics, public hospitals, government agencies, private insurers.
Credit card operations	Credit card issuers, client banks, merchant banks, high street merchants, insurers.

Trusted authority

Blockchain makes sense in scenarios where a trusted central authority/intermediary can neither be identified, nor designated

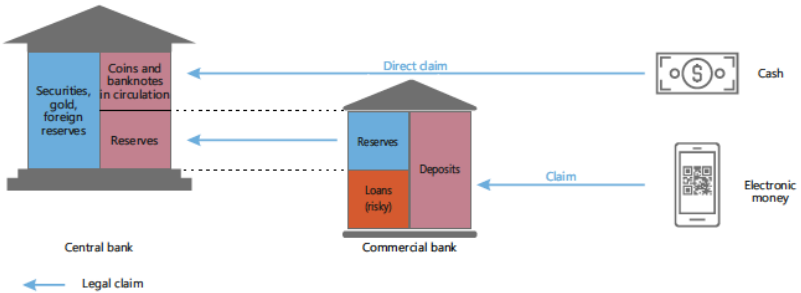
Marco Comuzzi mcomuzzi@unistac.kr

Trusted authority scenarios: examples

National banking systems

Every bank has an account at the central bank

The central bank records every transactions among banks (i.e., the "golden ledger")



Gambling

The state of Nevada monitors the cash flow and the employees of every casino in Las Vegas, issuing/revoking licenses.

Marco Comuzzi mcomuzzi@unistac.kr

When is a trusted authority lacking?

International business

Many businesses are regulated only nationally (banks, real estate, etc.)

New business scenarios

New industries are born without trusted authorities. These may be created later, when an industry grows. E.g. regulation of cryptocurrency and NFT markets

Closed business scenarios

Where new participants cannot be easily admitted or created

E.g., National nuclear programs (several agencies controlling only part of the program, like nuclear energy production, nuclear waste disposal, atomic military program, nuclear R&D)

Marco Comuzzi mcomuzzi@unistac.kr

Centralized operation

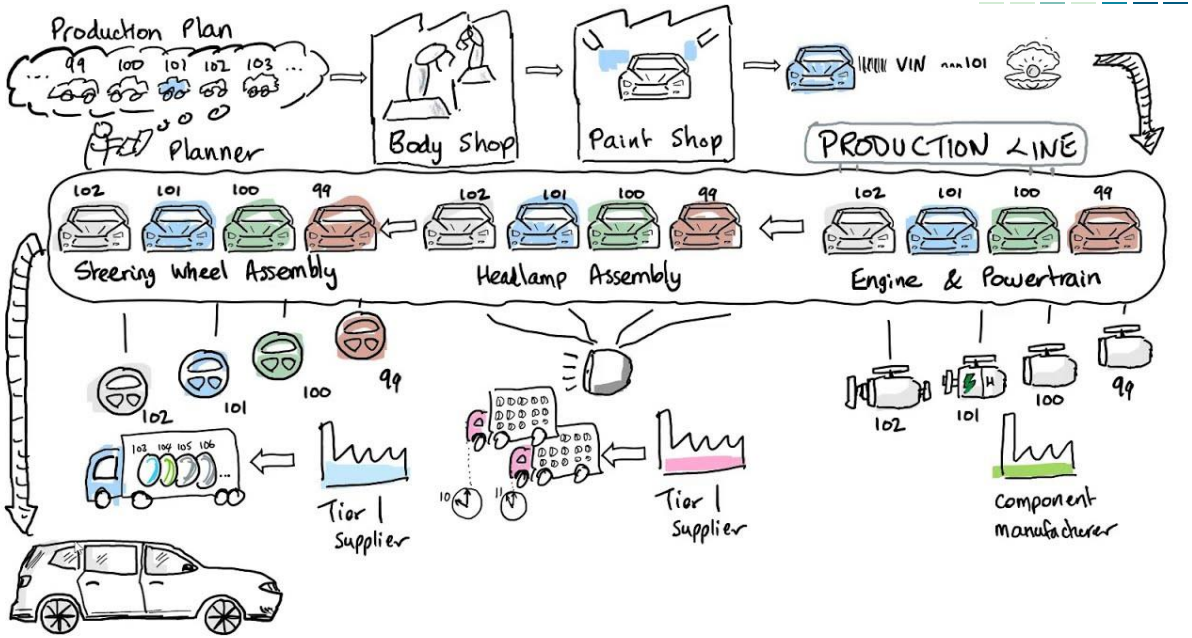
Blockchain makes sense in business scenario where operation is not centralized

Centralized operation
Even if a scenario is multi-party, the execution of the business can still be controlled by one of the parties

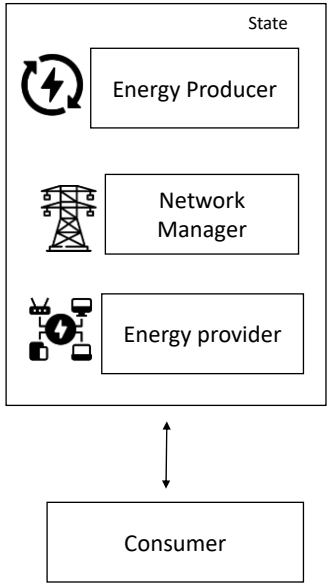
Marco Comuzzi mcomuzzi@unistac.kr

Centralized operation: automotive

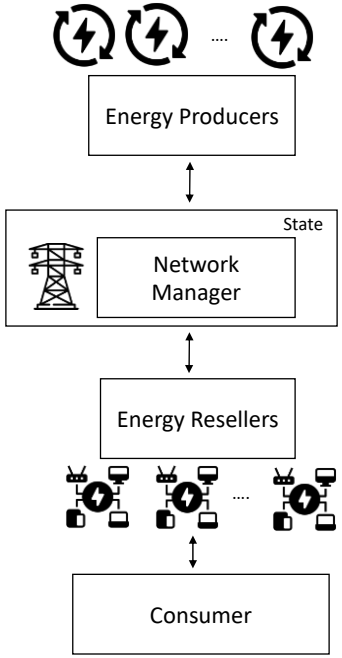
The industry depends heavily on the market position and plans of the vehicle manufacturer



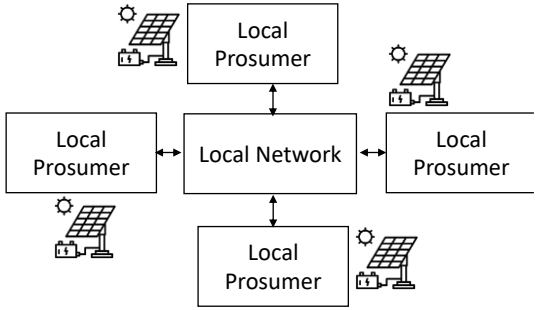
(De-)Centralized operation: Energy Markets



a) Centralized energy production and distribution



b) Deregulated energy market



c) Microgrid

(Data) Immutability

Blockchain entails by design the immutability of the data stored in it

Immutability is not always desirable!

Marco Comuzzi mcomuzzi@unistac.kr

Immutability? No, thank you

"the right to be forgotten" of customers

EU GDPR, California CPPA

Expunging of criminal records

Art. 17 GDPR

Right to erasure ('right to be forgotten')

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

   (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

   (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

   (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

   (d) the personal data have been unlawfully processed;

   (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

   (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

Marco Comuzzi mcomuzzi@unistac.kr

Immutability

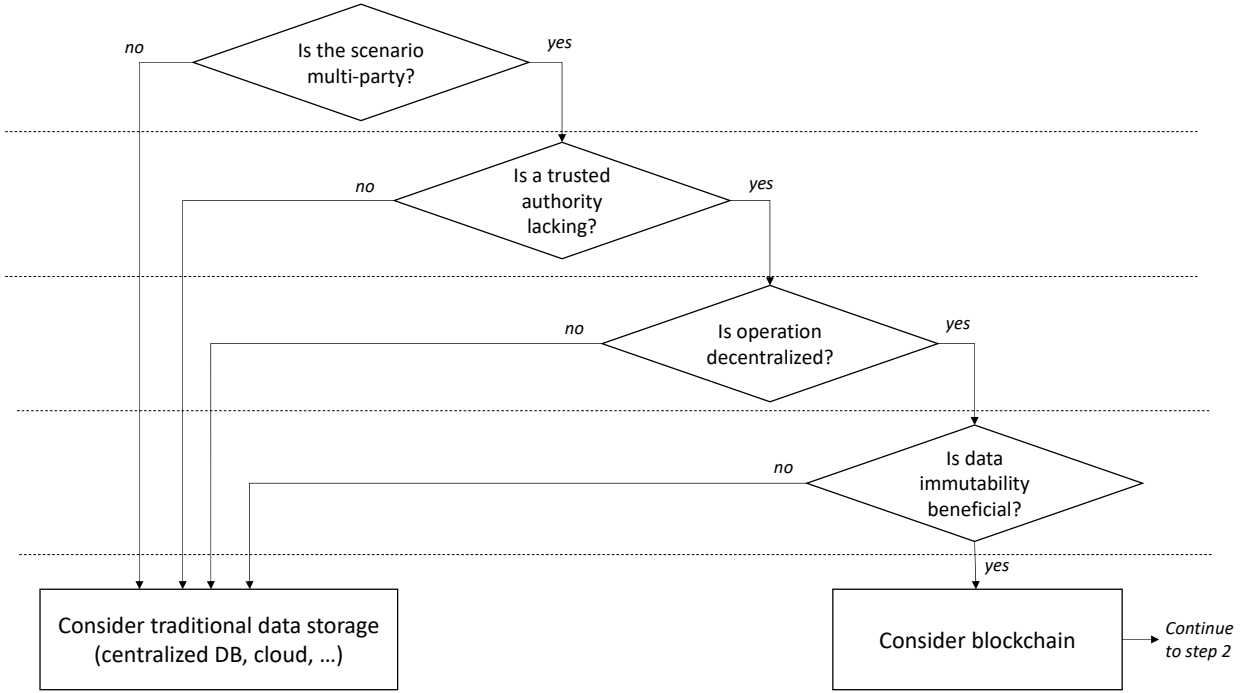
Immutability of data can be “managed” carefully on a blockchain

Ex.
“Need-to-know” ledgers (see Corda or HLF)

Smart contracts to control data access

Marco Comuzzi mcomuzzi@unistac.kr

Summing up…

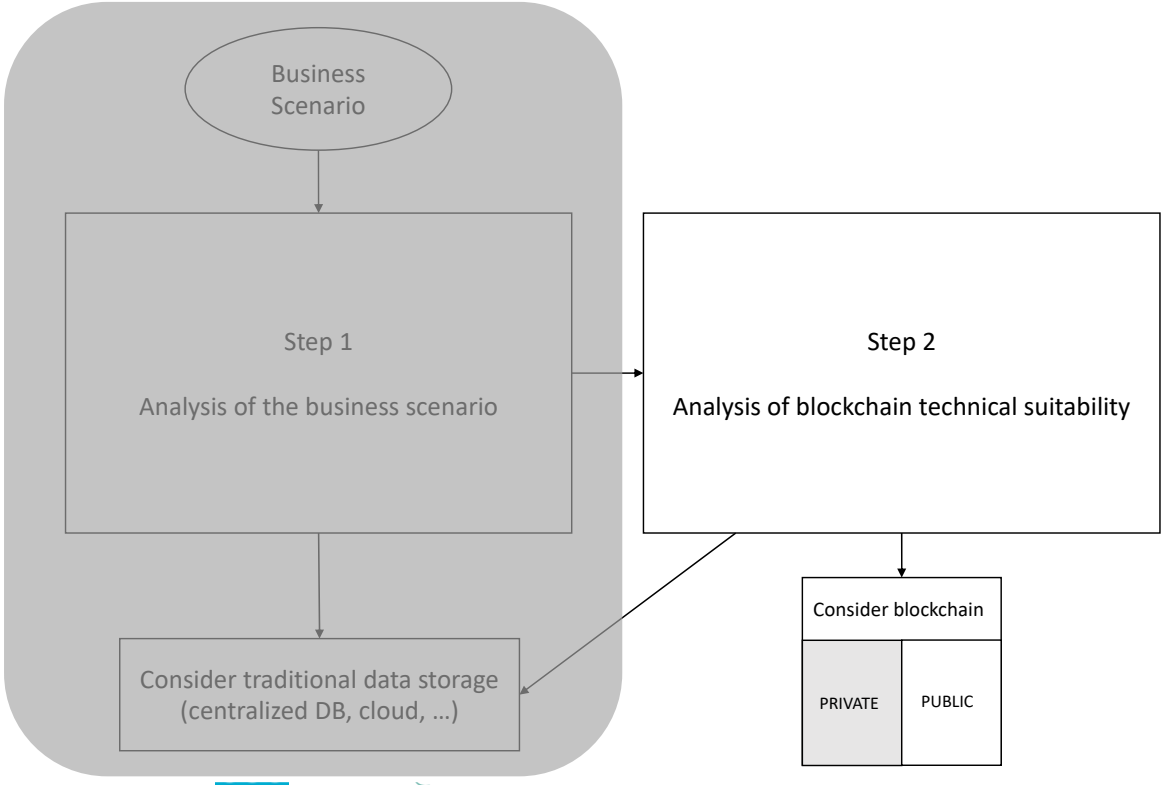

Is the scenario multi-party?
no
yes
Is a trusted authority lacking?
no
yes
Is operation decentralized?
no
yes
Is data immutability beneficial?
no
yes
Consider traditional data storage (centralized DB, cloud, …)
Consider blockchain
Continue to step 2

3.
Step 2:
Technical Suitability

Step 2 in the decision process

We look now at more technical characteristics of the IT solution that will be implemented in a business scenario

We may still revert to non-blockchain technology if necessary



Aspects to be considered in Step 2

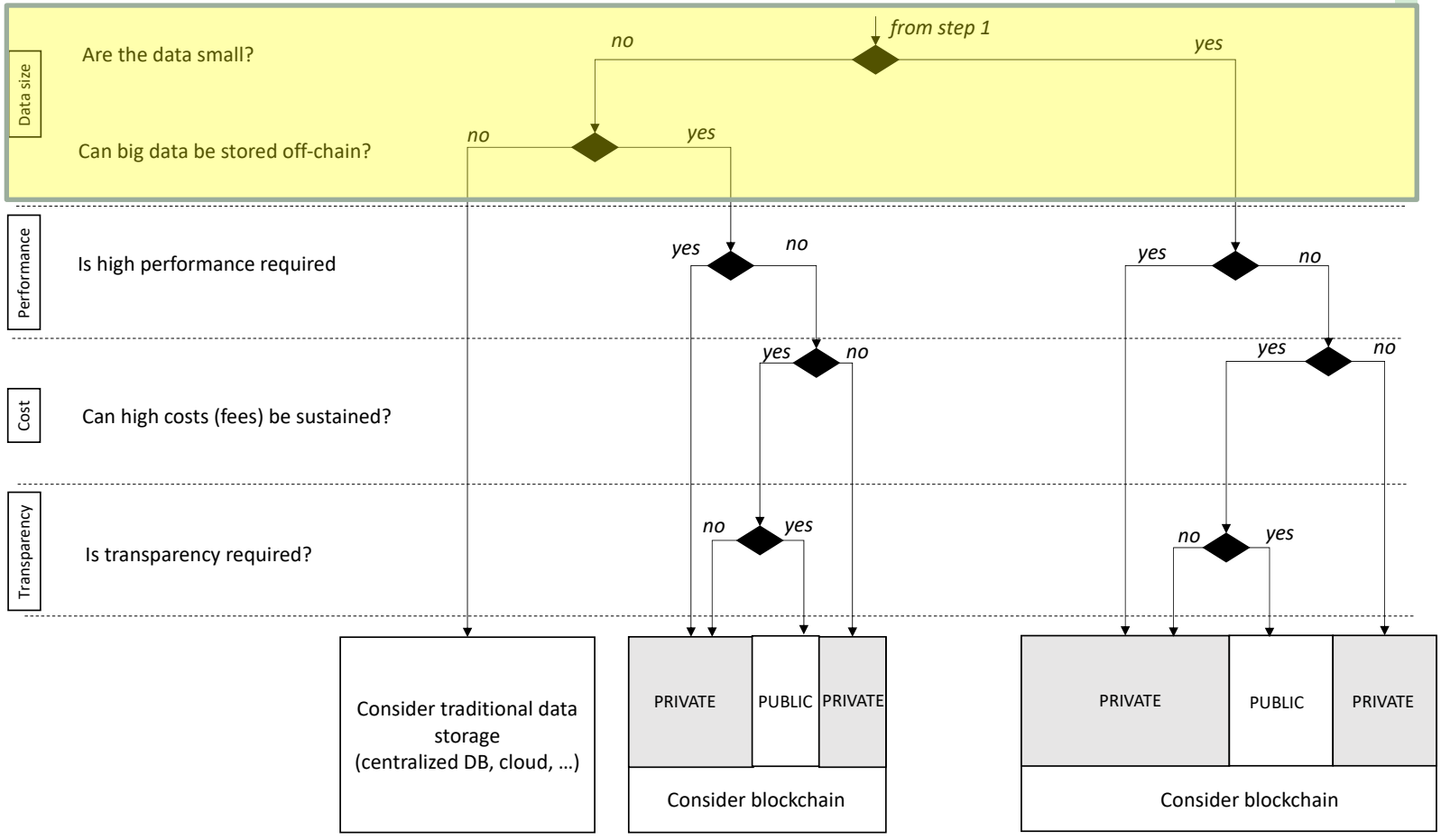
Size of the data

Level of performance required

Costs

Data transparency

Marco Comuzzi mcomuzzi@unistac.kr


Data size
Are the data small?
from step 1
no
yes
Can big data be stored off-chain?
no
yes
Performance
Is high performance required
yes
no
yes
no
yes
no
Cost
Can high costs (fees) be sustained?
yes
no
yes
no
Transparency
Is transparency required?
no
yes
no
yes
Consider traditional data storage (centralized DB, cloud, …)
PRIVATE
PUBLIC
PRIVATE
Consider blockchain
PRIVATE
PUBLIC
PRIVATE
Consider blockchain

Data in blockchain are small

Transactions in Bitcoin and Ethereum are a few KBs at most

Blockchain can usually handle “small” data (in absolute terms!)

Cryptocurrency, token transfers
Moves in a game of chess
Readings of IoT sensors

Data can easily become (very) big

1000s of IoT sensors sending readings every 0.5s

(Supply chain) store scanned/electronic versions of every document generated

Healthcare data: scanned/electronic copies of multimedia output of diagnostic exams

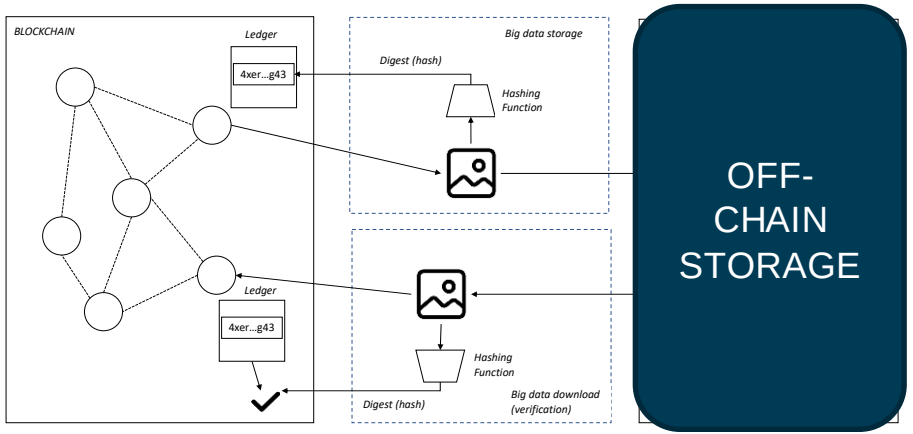
How to handle big data with blockchain

Create a hash (digest) of the big data stored on-chain

Leave the big data off-chain (possibly encrypted)

Verify the digest every time that the data are downloaded for use (public key to decrypt stored on-chain with digest or obtained on-demand)

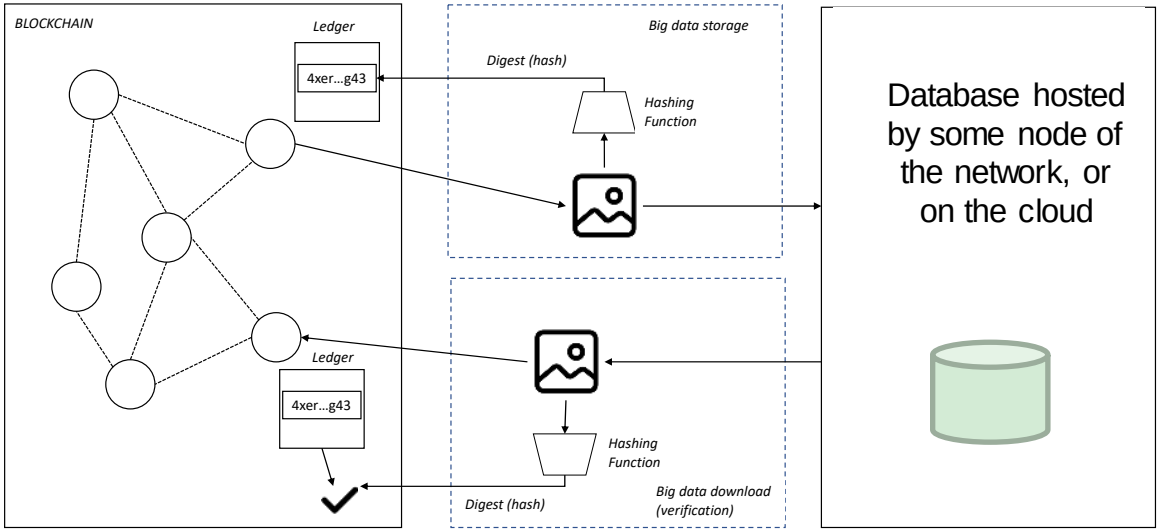
Guarantees data integrity (= are we using the correct data?),
but not availability (= will the correct data be always available?)



Marco Comuzzi mcomuzzi@unistac.kr

Leave big-data off-chain: solution 1

OK, but the database host becomes an intermediary who must be trusted



Marco Comuzzi mcomuzzi@unistac.kr

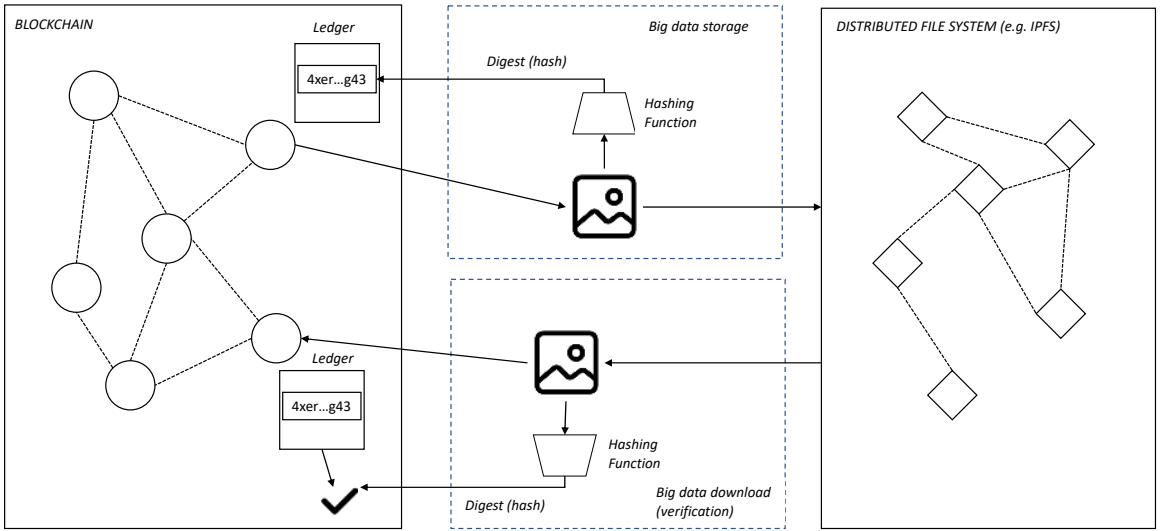
Leave big-data off-chain: solution 2

InterPlanetary File System: A P2P (distributed) file system

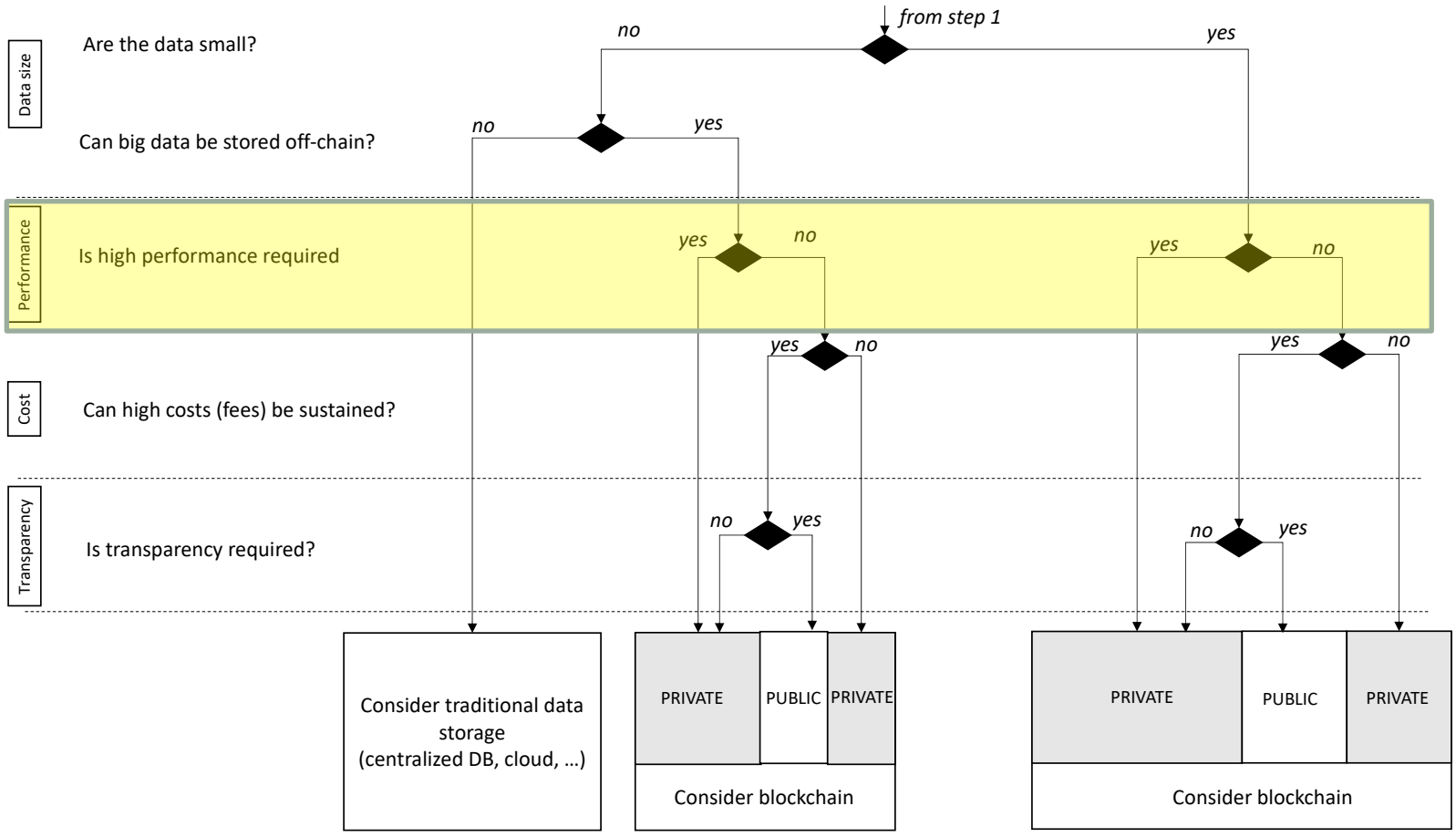
Files are sharded and stored across a number of different nodes (similar to “torrents”)

Can also be installed on a network of private nodes

Commonly used by Ethereum Dapps



Marco Comuzzi mcomuzzi@unistac.kr


Data size
Are the data small?
from step 1
no
yes
Can big data be stored off-chain?
no
yes
Performance
Is high performance required
yes
no
yes
no
Cost
Can high costs (fees) be sustained?
yes
no
yes
no
Transparency
Is transparency required?
no
yes
no
yes
Consider traditional data storage (centralized DB, cloud, …)
PRIVATE
PUBLIC
PRIVATE
Consider blockchain
PRIVATE
PUBLIC
PRIVATE
Consider blockchain

Performance of a blockchain

Response time

The time it takes to a system to process a transaction

E.g., time to include a transaction in a block, time required to reach consensus on chain of blocks (PoW, PoS)

Throughput

The number of transactions that a systems can process in a fixed amount of time.

Blockchain: low performance

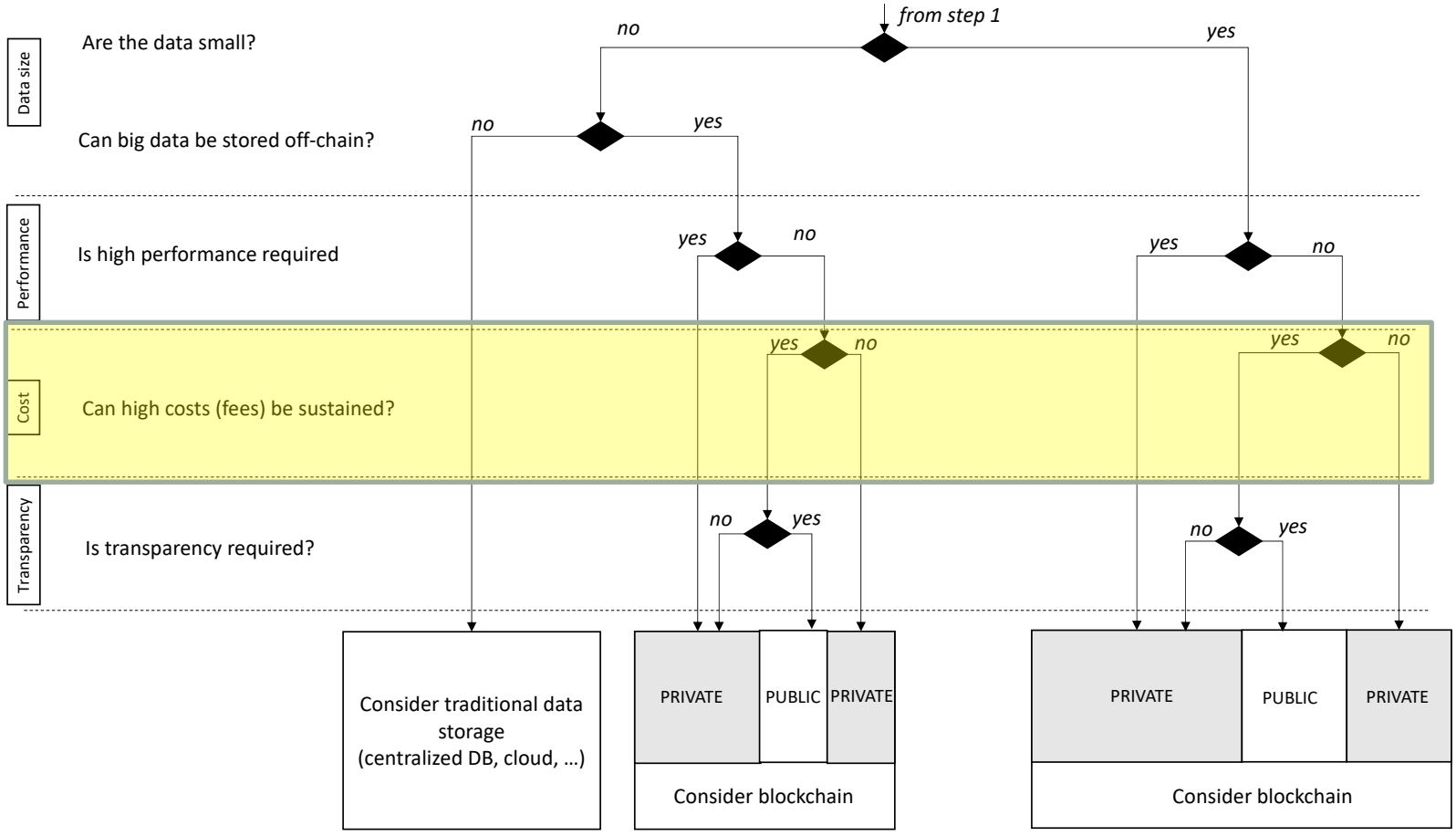
Public blockchain

Even considering only the time to include a transaction in a block (a few transaction per second)

Private blockchain

Better than public blockchain, but still consensus and digital signatures decrease the performance (w.r.t. non-blockchain systems)

Marco Comuzzi mcomuzzi@unistac.kr


Data size
Are the data small?
from step 1
no
yes
Can big data be stored off-chain?
no
yes
Performance
Is high performance required
yes
no
yes
no
Cost
Can high costs (fees) be sustained?
yes
no
yes
no
Transparency
Is transparency required?
no
yes
no
yes
Consider traditional data storage (centralized DB, cloud, …)
PRIVATE
PUBLIC
PRIVATE
Consider blockchain
PRIVATE
PUBLIC
PRIVATE
Consider blockchain

Cost of an information processing system

Infrastructure cost

Cost of setting up, operating, and maintaining a system

Transaction costs

Cost associated with a specific interaction with the system (transaction)

Marco Comuzzi mcomuzzi@unistac.kr

Cost of a blockchain

	Infrastructure costs	Transaction costs
Public blockchain	Usually none (the system exists, the protocol incentives ensure its survival)	Transaction fees (may be high and volatile)
Private blockchain	Blockchain setup, operation and maintenance. (can be high, but always comparable to the costs of similar non-blockchain solutions)	Usually none

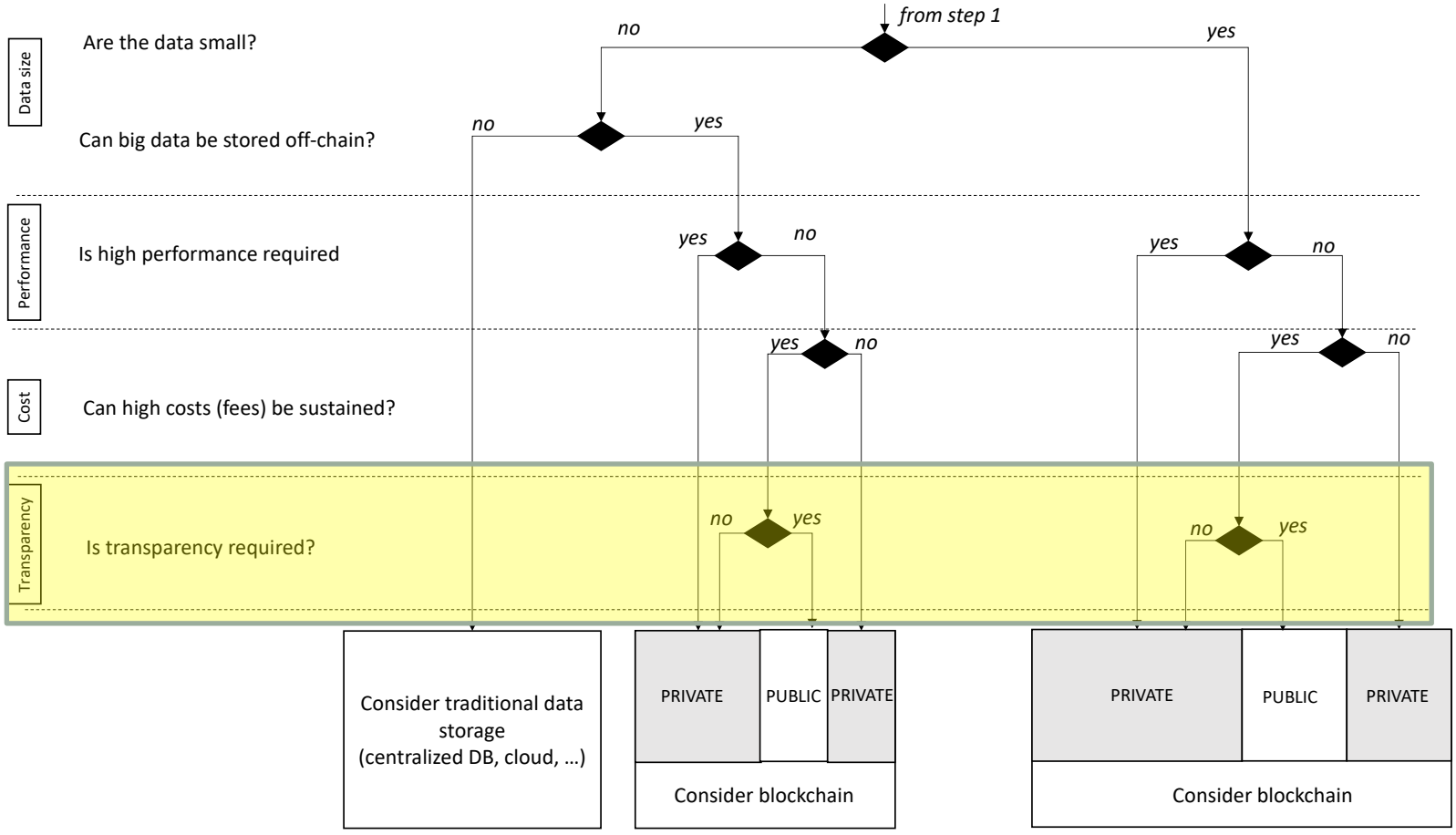
Transaction costs in public blockchain

Can be high, but sustainable (compared to the value of the assets/information exchanged)…

…for instance if the assets exchanged are very valuable (diamonds in Everledger)

Remember the guest lecture? Engineer a solution to reduce the number of transactions sent to the public blockchain.

Marco Comuzzi mcomuzzi@unistac.kr

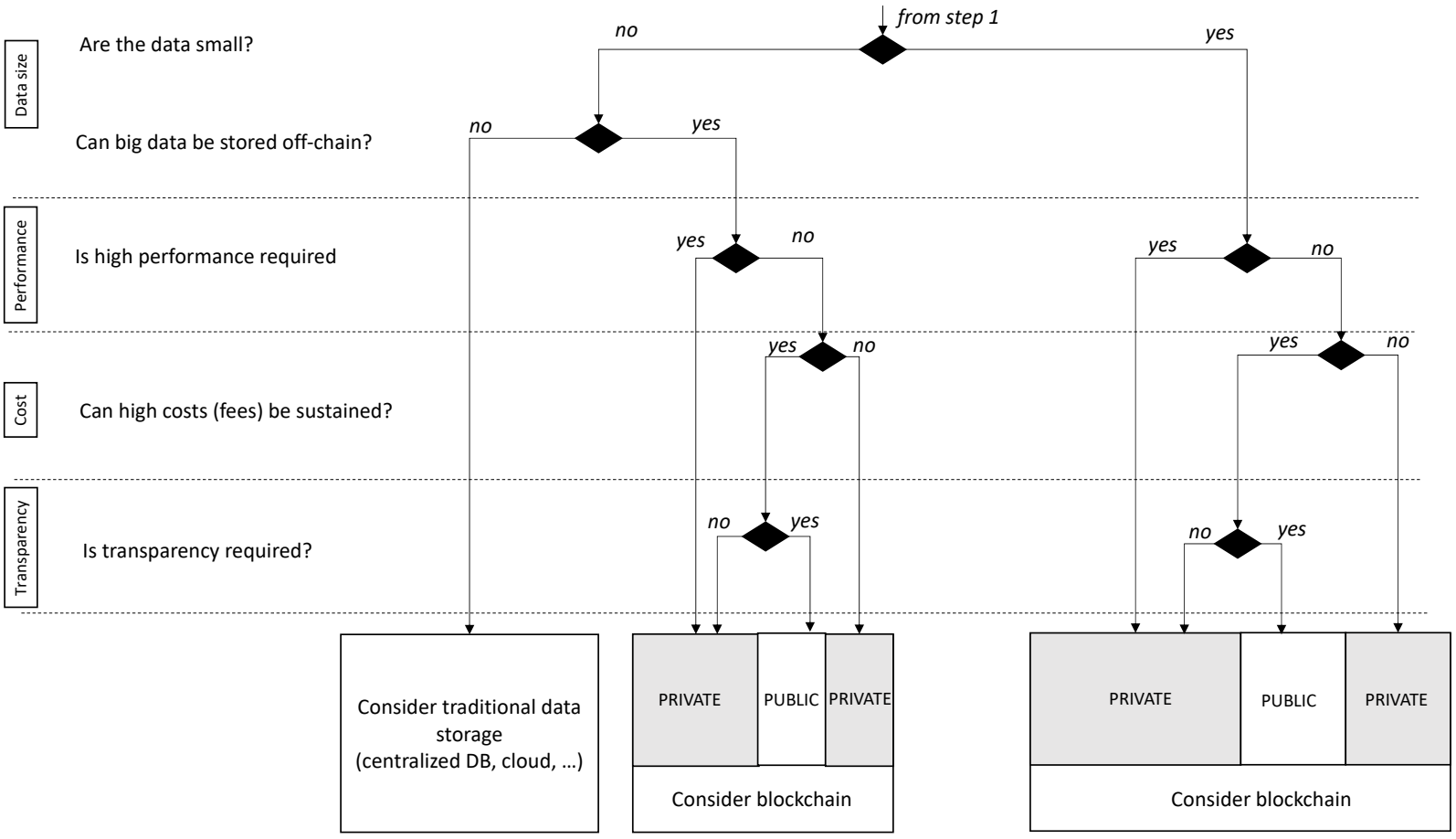

Data size
Are the data small?
from step 1
no
yes
Can big data be stored off-chain?
no
yes
Performance
Is high performance required
yes
no
yes
no
yes
no
yes
no
Cost
Can high costs (fees) be sustained?
Transparency
Is transparency required?
no
yes
no
yes
Consider traditional data storage (centralized DB, cloud, …)
PRIVATE
PUBLIC
PRIVATE
Consider blockchain
PRIVATE
PUBLIC
PRIVATE
Consider blockchain

Transparency in blockchain

Public blockchain is generally highly transparent (every node access all the data)

Private blockchain transparency can be limited using ad-hoc solutions (see Corda, channels and PDCs in HLF)

Marco Comuzzi mcomuzzi@unistac.kr


Data size
Are the data small?
from step 1
no
yes
Can big data be stored off-chain?
no
yes
Performance
Is high performance required
yes
no
yes
no
yes
no
Cost
Can high costs (fees) be sustained?
yes
no
yes
no
Transparency
Is transparency required?
no
yes
no
yes
Consider traditional data storage (centralized DB, cloud, …)
PRIVATE
PUBLIC
PRIVATE
Consider blockchain
PRIVATE
PUBLIC
PRIVATE
Consider blockchain

4.
Case Studies

Three classes of business scenarios

1. Disposal of hazardous industrial waste
2. Management of electronic health records
3. Self-sovereign identity management

Marco Comuzzi mcomuzzi@unistac.kr

Disposal of industrial waste: Scenario

Disposing of (hazardous) industrial waste should follow precise procedures

It costs a lot, (cheaper) unlawful opportunities may exist…

If unmanaged, can be source of public concern

Marco Comuzzi mcomuzzi@unistac.kr

Disposal of Industrial Waste: Step 1

Multi-party

Waste producers, treatment services, government agencies, local env. associations

No Trusted authority

Enforcement of regulations by many agents: police, local administration, specialized monitor agencies

Decentralized operation

No one controls the entire process

Data immutability

Welcome. It is a monitoring (track and tracing) scenario

Marco Comuzzi mcomuzzi@unistac.kr

Step 2

Small or big data?

Small data on-chain: id and location of drums/packages/treatments/human resources

Big data can be stored off-chain: scanned copies of packaging, loading, transportation documents

High performance required?

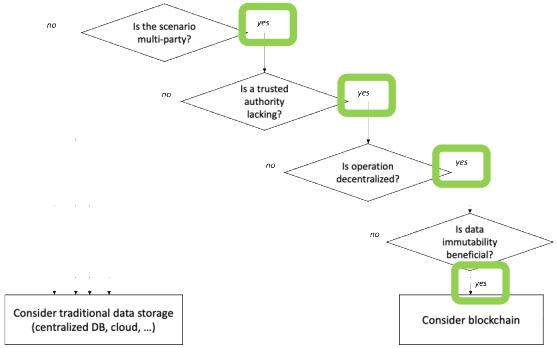
No (long-lived processes)

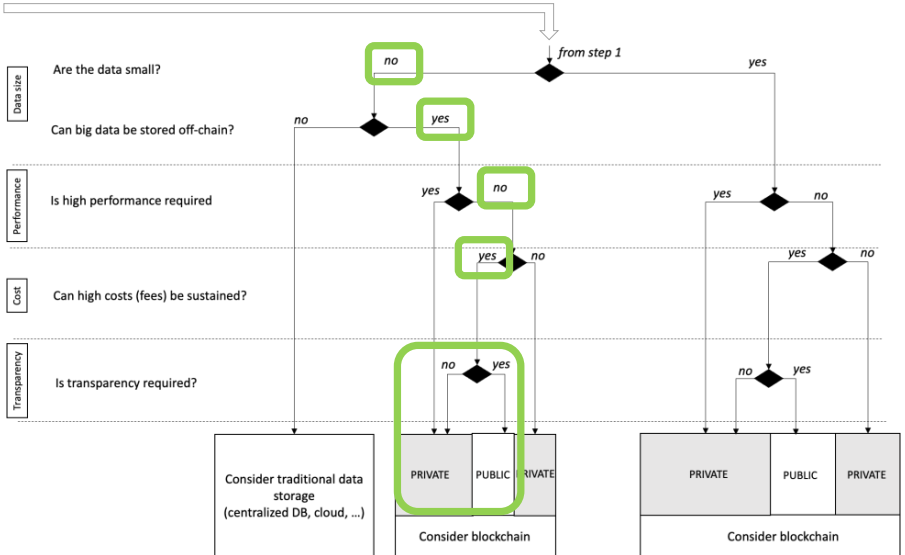
Costs and transparency

Highly valuable/risky materials (e.g.: maximum transparency required, TBC TBC)

Marco Comuzzi mcomuzzi@unistac.kr

Disposal of industrial waste: summary





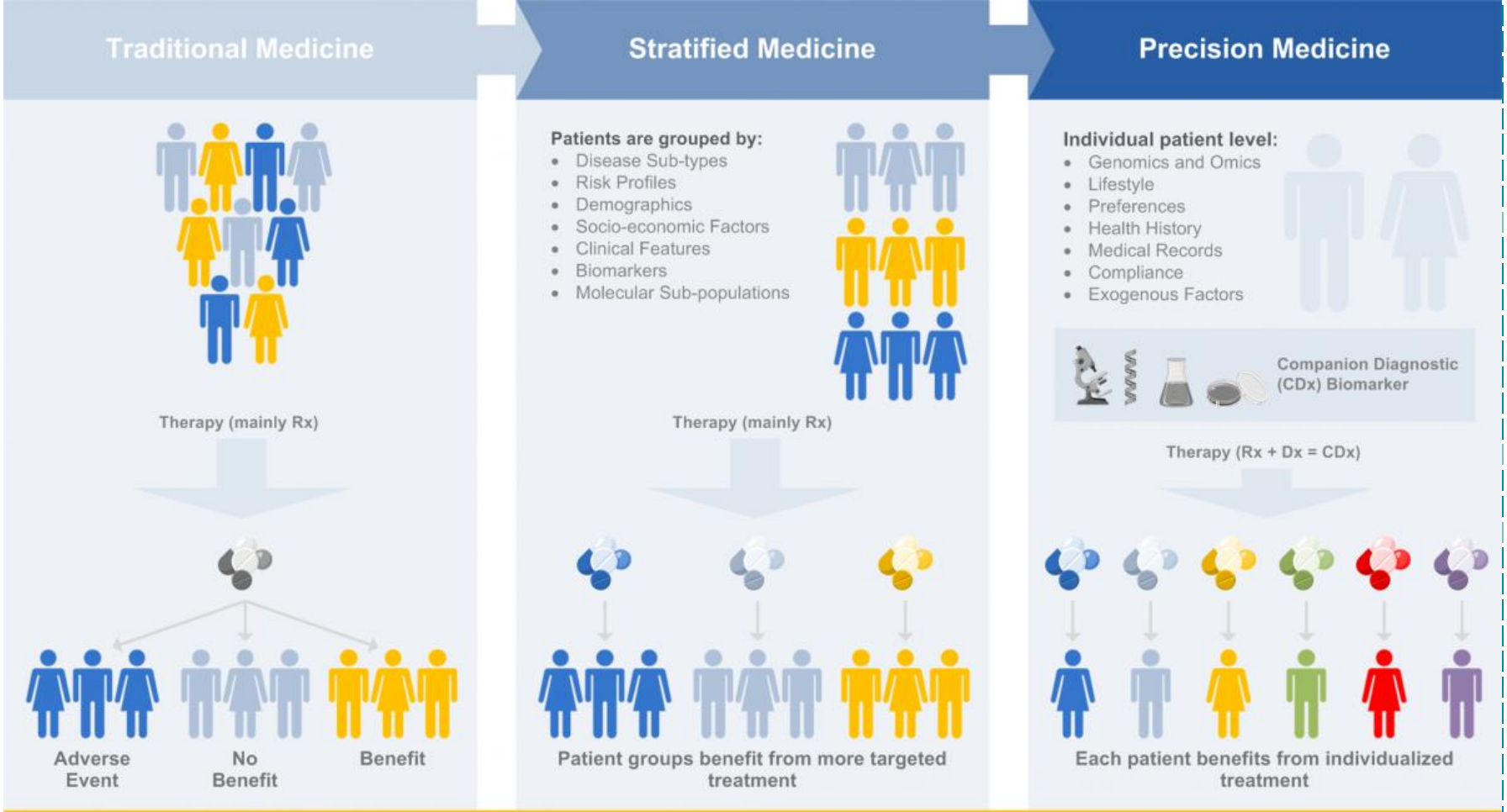
Management of electronic health record: Scenario

Precision medicine

Achieve personalized diagnosis and treatment based on full medical history of individuals

AI/machine learning to learn models that can predict (long term) diseases and conditions

Marco Comuzzi mcomuzzi@unistac.kr



Precision medicine research enables development and delivery of the right patient intervention

Precision medicine from a patient perspective

Electronic Health Records (EHR)

Diagnosis and treatment scattered at different healthcare providers

Hard to merge into a single complete patient history

Owned by healthcare providers

Personal Health Records (PHR)

A single repository where healthcare providers can add data whenever needed

Enable patients to reproduce their full medical history

Owned by the patients

Marco Comuzzi mcomuzzi@unistac.kr

Blockchain for PHR? Step 1

Multi-party

Multiple healthcare providers, possibly in different countries (hospitals, GPs, private clinics, …)

No Trusted authority

Some efforts to standardize and regulate HRs at national level (but it's hard); can also be "international"

Decentralized operation

Every healthcare provider provides diagnosis and treatment independently; they may even "compete" for patients

Data immutability

Welcome, as the only way to build a reliable record of entire patient medical history

Marco Comuzzi mcomuzzi@unistac.kr

Blockchain for PHR? Step 2

Small or big data?

Data are big (X-ray images, CTR scans, exam reports), and very sensitive (cannot be store off-chain)

High performance required?

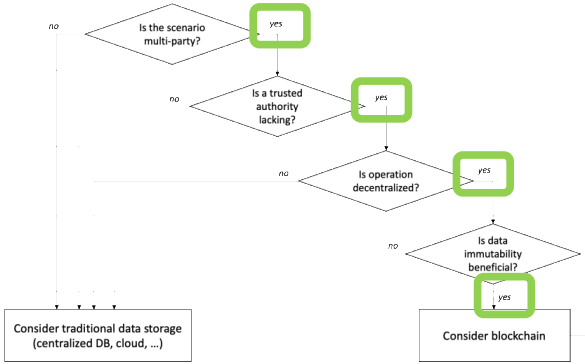
Possibly, depending on adoption

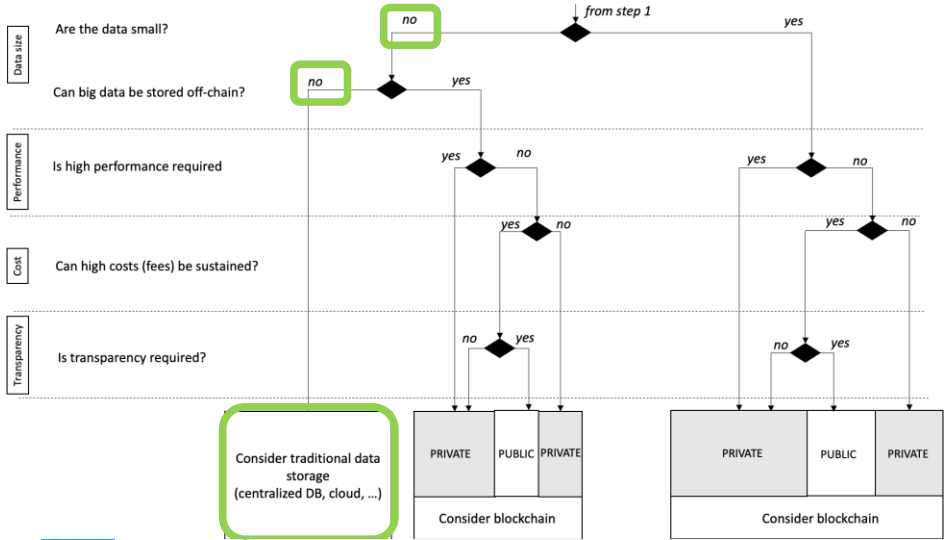
Costs and transparency

Highly sensitive data, should not be available to anybody

Marco Comuzzi mcomuzzi@unistac.kr

Electronic Health Records: summary





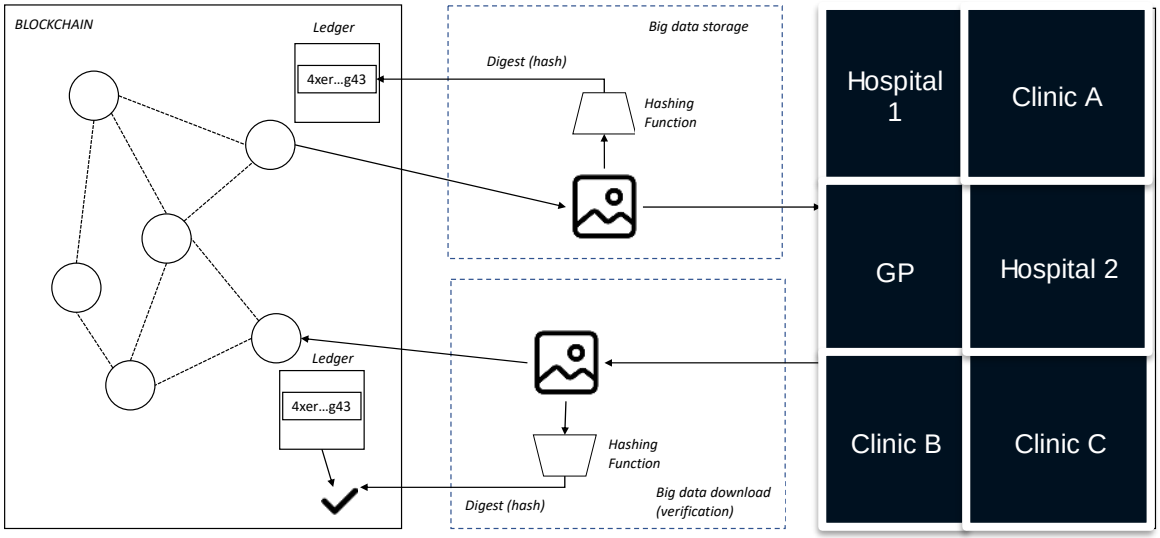
Still, a lot of blockchain startups in the healthcare …

Medical data reside with the providers, public blockchain to create a reliable, immutable record of access to medical records

Monitor whether providers "sell" patient data

Reward patient for providing their data for medical research

…



Marco Comuzzi mcomuzzi@unistac.kr

Self-sovereign v. traditional identity management

Traditional IDM

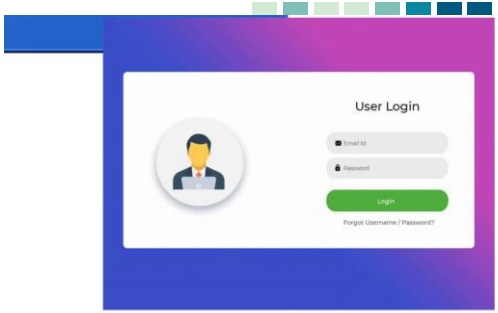
Users maintain different auth. tokens with each service provider (username, passwords, 2F-auth)

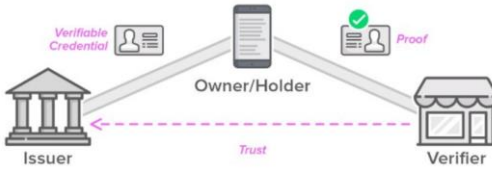
Cumbersome for users, unsafe, not private

Self-Sovereign IDM

User collects and owns identity tokens certified by different issuers (gov., banks, …)

Service providers decide which token they require from users to authenticated them





Marco Comuzzi mcomuzzi@unistac.kr

Self-sovereign identity?

We do not get identity tokens from each country that we want to visit

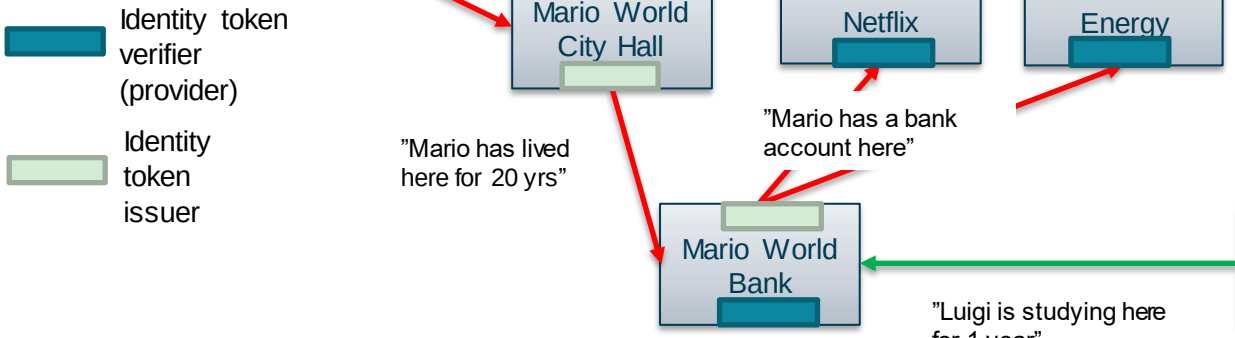
Countries accept a passport (+visa in some cases) as a proof of identity

Problem: passports and visas issued by centralized authorities!

Marco Comuzzi mcomuzzi@unistac.kr

Mario has lived in Mario World for 20 years, wants to open a new bank account, Netflix account and change energy provider

Luigi comes from overseas to study at Mario World University, has no record in the city hall, but needs a bank account in Mario World



Marco Comuzzi mcomuzzi@unistac.kr

Blockchain for SS-IDM? Step 1

Multi-party

Several service providers and several issuers of identity tokens

No Trusted authority

SS-IDM is based on the idea that identity is not verifiable using credentials issued by a central authority

Decentralized operation

Every service provider acts independently

Data immutability

Identity tokens may have a validity and be renewed, but nobody should be able to modify them

Marco Comuzzi mcomuzzi@unistac.kr

Blockchain for SS-IDM? Step 2

Big or small data

Data are small (citizen registry data, id of accounts), no need for storing big data

High Performance required?

No, identity tokens are not collected or used very often.

Cost and transparency

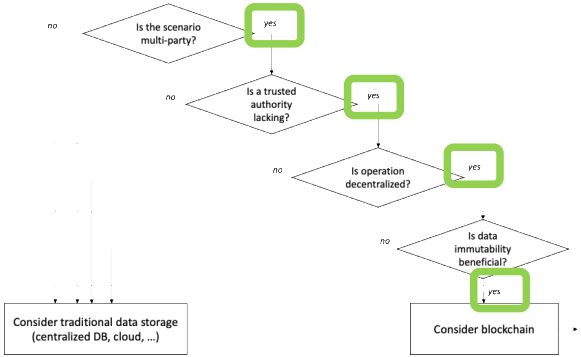
Identity management should be “universal”, so a public blockchain is recommended.

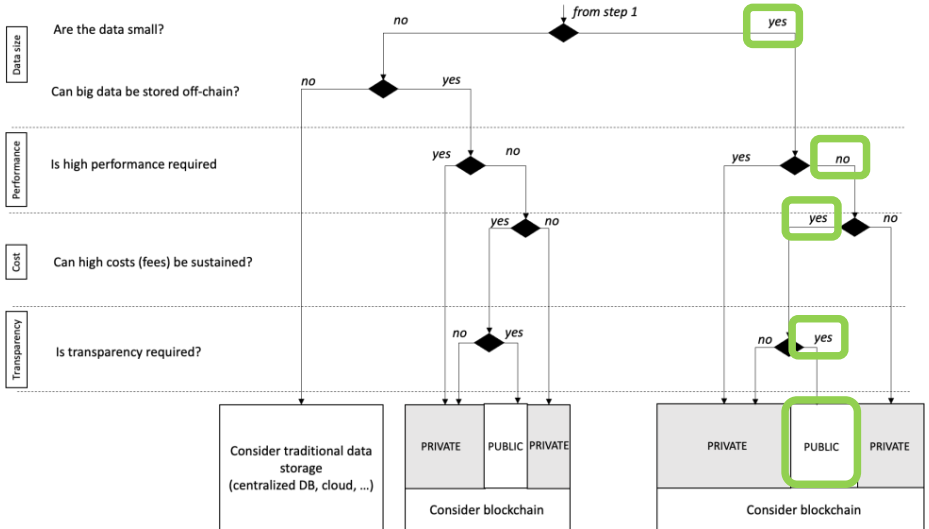
Service providers and users may bear the cost of using the public blockchain.

(Concrete implementations in local contexts are still using private blockchain implementations)

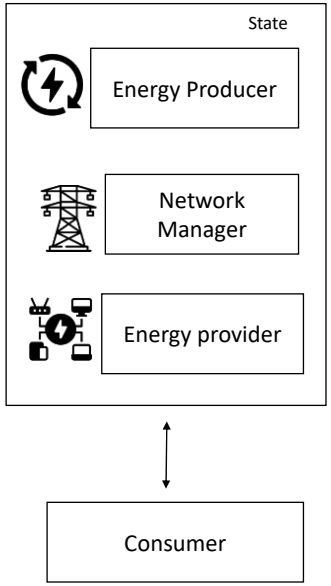
Marco Comuzzi mcomuzzi@unistac.kr

Self-sovereign identity: summary

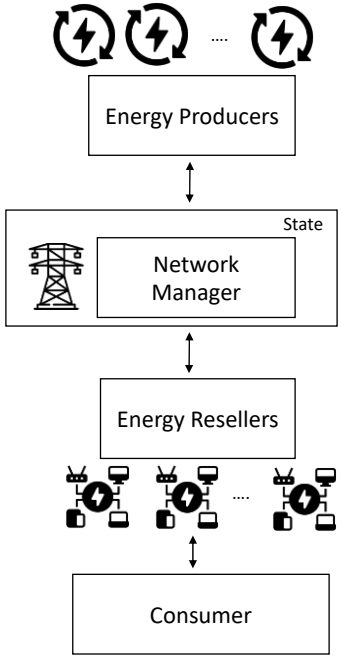




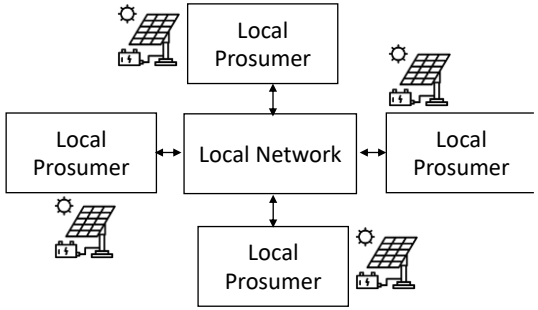
(De-)Centralized operation: Energy Markets



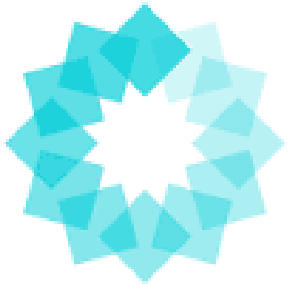
a) Centralized energy production and distribution



b) Deregulated energy market



c) Microgrid



Power Ledger

Energy industry (electricity)

Most energy companies claim to be "customer-focused", but in reality…

… they are big companies with full control over where and when they build generating capacity and prices

Customers are pushed into categories, with little service customisation

They require strong regulation

Distributed (clean) Energy Revolution

Energy produced locally in smaller amounts, shifting power to the edges of the network

Local energy is usually more “clean”

Solar photovoltaic systems

Wind farms

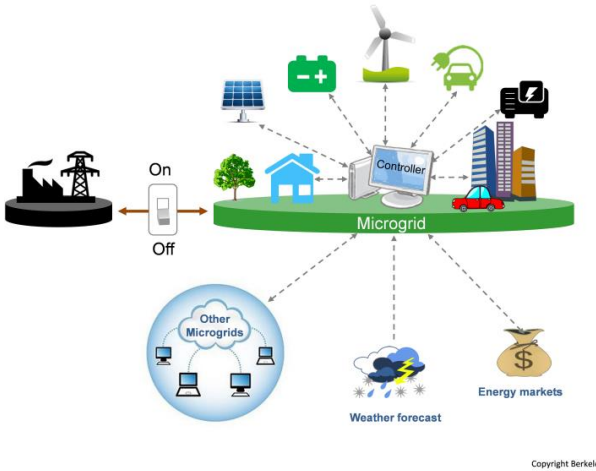
…

Microgrids

…

uzzi@unistac.kr

Microgrids



A localised system of energy sources and loads that can operate both connected to the traditional "macrogrid" or in isolation

Use renewable resources when available

Connect to macrogrid when needed

Offload excess production (marketplace)

Re-defining energy distribution

CENTRALISED ENERGY PROVIDER

- Few centralised energy providers with full control over distribution and prices
- One-directional network

DISTRIBUTED ENERGY MANAGEMENT

- Millions of active prosumers

Possibly organised in self-sustaining microgrids

- Bi-directional energy flows traded on a "trustful" distributed platform

What is Powerledger?

A distributed trading platform for users to realise DE investments by monetizing excessive energy

A sort of AirBnb for clean energy sharing

Blockchain technology provides the “agreement machine” for users to trade without the need for a central 3rd-party

Why blockchain for distributed energy management (trading)?

Need for a completely distributed system

No central intermediary allowed

Combine exchange of one fungible asset (energy) for another fungible asset (currency) without intermediaries

Powerledger applications

Xgrid

P2P energy transacting through the traditional distribution network

Mgrid

P2P energy transacting in microgrids

C6

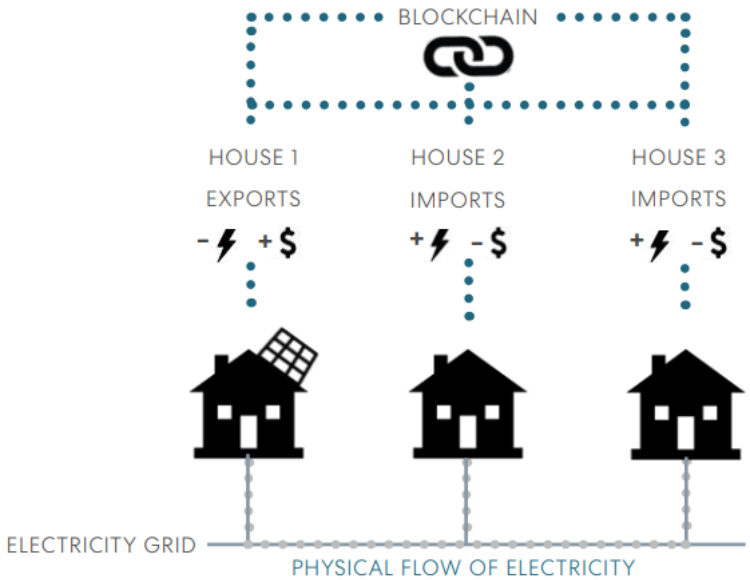
Digital clean energy certifications

Power Ledger Platform: xGrid

P2P electricity trading through the regulated network

Producers export excessive clean capacity

Consumers import clean energy through the main network



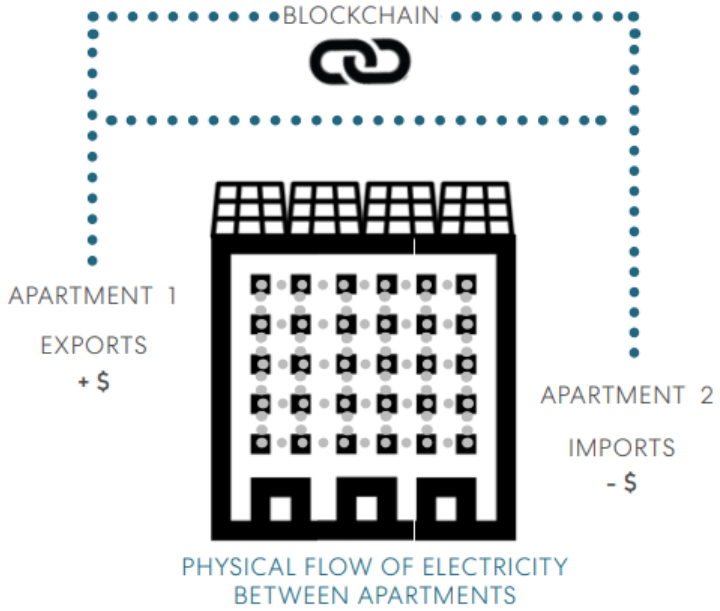
Power Ledger Platform: mGrid

- Microgrids

Self-reliant energy systems

E.g. Gated communities

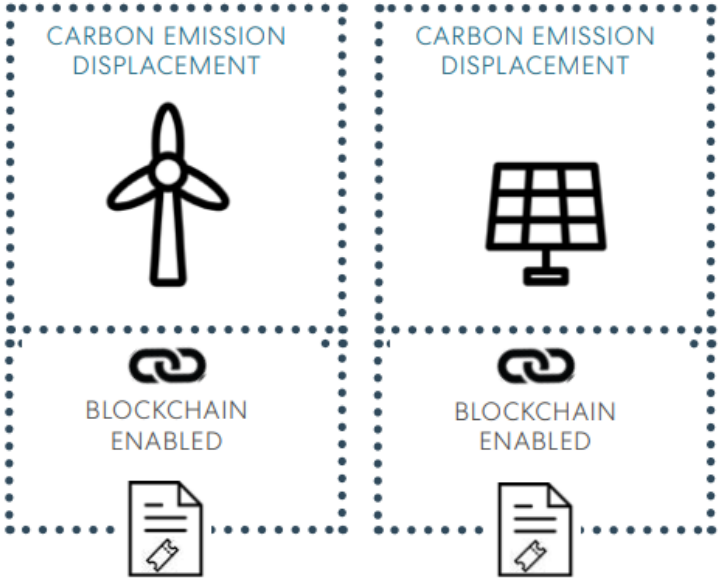
P2P electricity trading behind the regulated network



Power Ledger Platform: C6

Carbon offsets credits and certificates

Create immutable digital records of clean energy generation



Power Ledger deploys first blockchain-based P2P energy trading system in Chicago

Mike Butcher @mikebutcher / 6 months ago

STARTUP NEWS & ANALYSIS

"No small fry": Power Ledger locks in trial partnership with second-largest Japanese energy retailer KEPCO

DOMINIC POWELL / Thursday, April 26, 2018

Power Ledger co-founder and managing director David Martin. Source: Supplied.

Australian blockchain company Power Ledger has landed
its peer-to-peer energy trading with Japan's second-large
Electric Power Co (KEPCO), in another win for one of Aus
blockchain companies.

BLOCKCHAIN NEWS AUGUST 28, 2018 11:53 CET

Aussie Blockchain Powers P2P Solar Power Trading in Upscale Bangkok Community

THANKS!

https://sites.google.com/site/marcocomuzziphd

http://iel.unist.ac.kr/

You can find me at:

@dr_bsad

mcomuzzi@unist.ac.kr