RESEARCH DATA ALLIANCE

Blockchain Applications in Health WG @P13

State of the Art Report
4 April 2019, 9:00-10:30

Co-chairs: Edwin Morley-Fletcher, David Manset, Aggelos Kiayias

research data sharing without barriers
rd-alliance.org

AGENDA

1. **Short introduction recalling the precursor sessions and the WG's Goals and Working Plan** Ludovica Durst, Researcher & Consultant at Lynkeus
2. **Introduction to the "State of the Art Report": Blockchain and Health Data Environment** Mirko de Maldè, COO at Lynkeus and President of Blockchain Government Association Italy
3. **Open discussion and contributions to the "State of the Art Report"**
4. **Further steps** for the next Report on Regulatory and Legal Issues in view of P14

Background
Establishing a WG focusing on Blockchain in Health Data

- RDA P9 (Barcelona) and P10 (Montreal) BoF and discussion in the Health Data Interest Group (HDIG) to gain support within the RDA community for establishing the WG
- RDA P11 (Berlin) carrying on the debate on the WG objectives, with special regard to the potential of such a system and compliance with advanced data protection requirements
- **RDA P12 (Gaborone) first official meeting, WG endorsed** discussion on potential uses and challenges coming from crytpocurrencies such as “tokenomics”

Working Plan and GOALS of the WG (18 months)

- **P13 First report** on State of the Art (6 months)
- **P 14 Second report** on Regulatory and Legal Issues (12 months)
- **P 15 Final outcome**: set of Guidelines on Blockchain Applications in Health, establishing a scalable blockchain-based data sharing system in healthcare (including the two previous reports)

First Report on State of the Art

The report aims at giving a first hint in order to:

- analyse and compare usages of the blockchain in healthcare, implementations of blockchain architectures, associated legal and socio-economic impacts and perspectives,
- assess both incremental and disruptive innovation and relevant innovative business models,
- understand the connection with other technologies toward the creation of new data-driven services and market,
- assess the potential of blockchain-based self-enacting smart contracts in handling consent and data permission systems minimising transaction costs.

RESEARCH DATA ALLIANCE

Blockchain Applications in Health WG @P13

State of the Art Report

Mirko de Maldè
(Lynkeus)

research data sharing without barriers
rd-alliance.org

Topics addressed by the report

Some key health data challenges

- Data mobilisation
- Legal and regulatory challenges
- Security

Blockchain – technical features and areas of interest in the health domain

- Blockchain 101
- Areas of interest

Future perspectives and integration/interaction with other technologies

- Business perspectives
- AI and blockchain

Existing solutions

Blockchain can mean different things for different actors:

- For **hospitals** it might be a way to solve data insecurity and interoperability;
- For **doctors** it might help manage professional identity and simplify payments;
- For **pharma** and **medical device companies** distributed ledgers can assist in supply chain, inventory management and frauds detection.
- For **patients** it can provide the opportunity to control and own their data, their insights and their health

Data Access and exchange	• Improved access to data • Identity management tools • Longitudinal health record
Drugs authenticity	• Supply chain transparency • Provenance tracking • Reduce drugs counterfeiting
Clinical trials	• Improve transparency and auditing • Improve relationship management among stakeholders • Facilitate protocol and consent management and updates
Epidemiology and public health	• Improve data flow on the spread of contagious diseases
Medical IoT	• Encrypt and share securely patient generated data • Ensure privacy and security and identity of the medical device
Improved service management	• Improved control and transparency over access to health services by individuals, including visit to GPs, drugs consumption, access to Emergency rooms
Introduce reward systems of service tokenisation	• Improve engagement of individuals, encouraging healthy behaviours or facilitating access to specific services
Blockchain-based claims billing management / health insurance	Improve health insurance services providing , tamper-proof claim management and fraud reduction, reduction of administrative burdens, as well as enabling personalised services, dynamic pricing, improved access

Blockchain BrioView

THE CURRENT INITIATIVES IN THE CRYPTO HEALTH SPACE

PATIENT CENTERED

PROVIDER CENTERED

Public Blockchains

Tokenized

Behavioral Health

Addiction

Dental

Health Education

PeerAtlas, VoxelX

Pharma

elige, BLOCKMEDX

Adherence

Academic Research

Diagnostics

DeepRadiology

Protocol

simplyvital health

IoT Security

Organizational Efficiency

VERIS FOUNDATION

Claims Management

Supply Chains

Medi Trace

Credentialing

Genomics

ENCRYPGEN, zenome, DOGE, luna

Healthcare Marketplace

CITIZEN HEALTH, À, well, UNIVERSAL HEALTH COIN, CoinMD

Clinical Research

OPEN LONGEVITY, CURECOIN

Personalized Medicine

BOWHEAD, doc.ai, NWP, CORAL HEALTH

Fitness/Wellness

belttcoin, Lympo, TEAMMATE, LENUS CHAIN, Fitrova, AIDOC, GYMREWARDS

Personal Health Data Management

CoverUS, wizz, IRYO, MEDIBLOC, MEDICHAIN, Genesis, BEAT, mint health, Linnia, LUMENUS

Insurance

TIDES, LINDA HEALTHCARE, Medishares

Quality of Care

Value Based Care

MediCoin

Patient Engagement

eCuris

EHR Data

PatientDirected, KINECT, PROOF WORK

Care Coordination

CARE 4 ME, aimedis, medicohealth, ETHEAL, healthbase, EARTHMEDZ, BitMED, EHF

Telemedicine

MedCredits, Doctor Smart

Blockchain Interoperability (Cross Chain)

SOLASTER, MedChain

Non - Tokenized

GENOBank.io, BITMARK, BLOCK M.D., Clinishare, enigma, PARTICLE HEALTH, Decent

Updated 06.12.18

Blockchain

- A **shared** immutable **distributed ledger that records and stores digital assets and where** transactions are **recorded chronologically and publicly, establishing establish trust, accountability, and transparency**.
- The resulting database allows the **transfer of value** within computer networks, ensuring **trustworthy transactions without the necessity of a third party**.
- Blockchain make it **easier to keep track of information and reduce settlement times**.
- Each participating node has a full copy of the ledger, and – through consensus mechanisms – all these node eventually have a single ledger representing the **"truth" of what has happened**.
- The distributed ledger is **owned, maintained, and updated by each node**. It's a peer-to-peer system. **No central authority** manages the transaction flow.

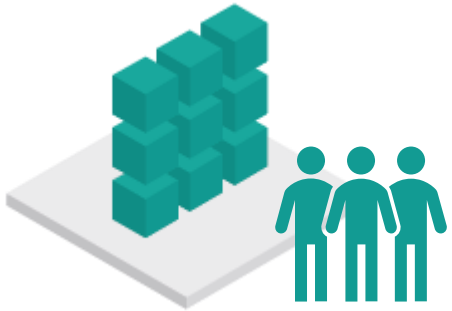
Key characteristics of a blockchain

- **a. Shared recordkeeping:** enables multiple parties to collectively create, maintain, and update a shared set of authoritative records (*the 'ledger'*).
- **b. Multi-party consensus:** enables all parties to come to agreement on a shared set of records
- **c. Independent validation:** enables each participant to independently verify the state of their transactions and integrity of the system.
- **d. Tamper resistance:** makes it hard for a single party to unilaterally change past records (i.e. transaction history) and allow each participant to detect non-consensual changes applied to records trivially (tamper evidence).

Smart contracts

- Smart contracts are computer programs that autonomously execute instructions when triggered by external events, used to automate business processes across different entities

- Two or more parties define the contract and the condition of its execution



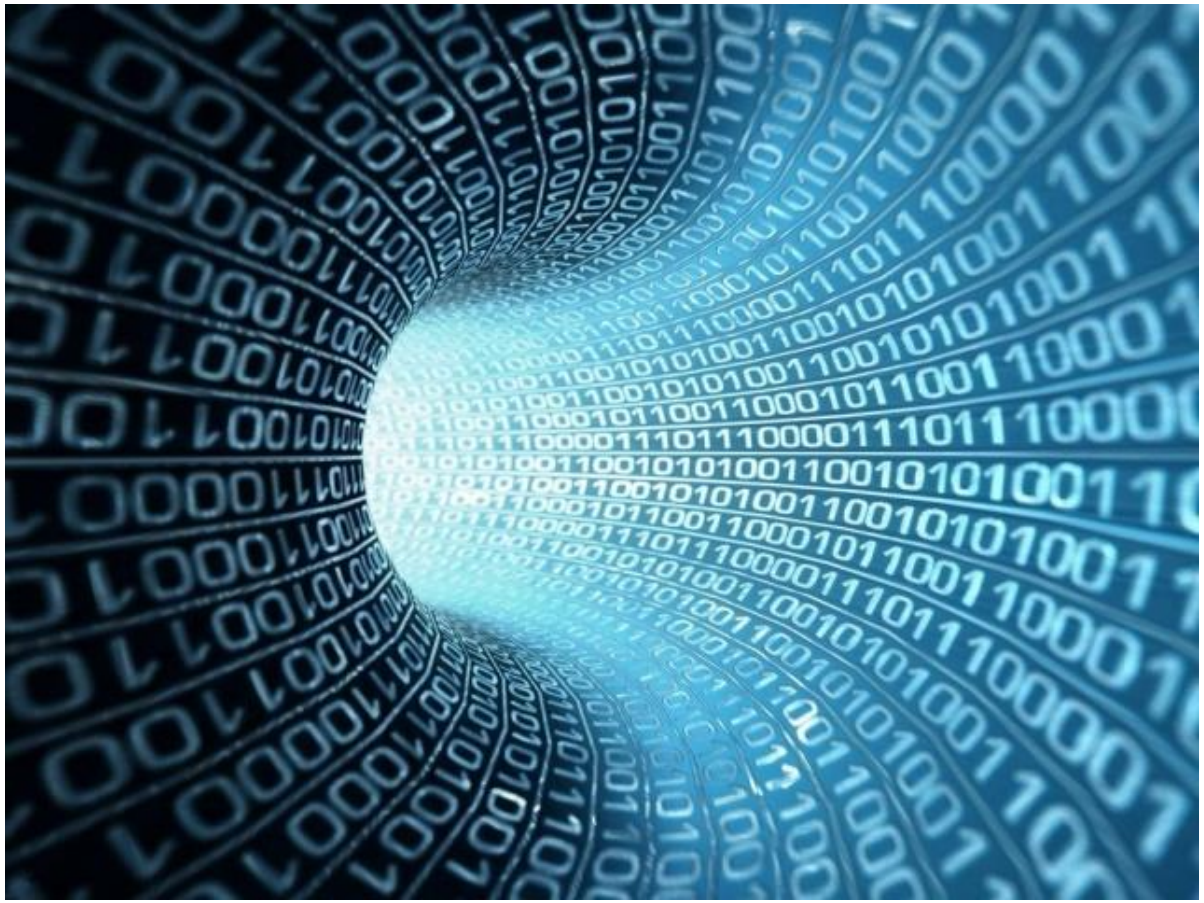
- When the defined condition are met, the smart contract is activated
- The execution is automated and autonomous (no human intervention needed)
- All nodes execute the smart contract

- The output from executed smart contracts can be audited and verified by all participants in the network

Blockchain benefits

- Ability to create trust in trustless environments;
- Security mechanisms for the transfer of value;
- Efficiency in streamlining business processes, particularly between different entities; and
- Enhanced auditability and transparency

Medicine: increasingly a data-driven science

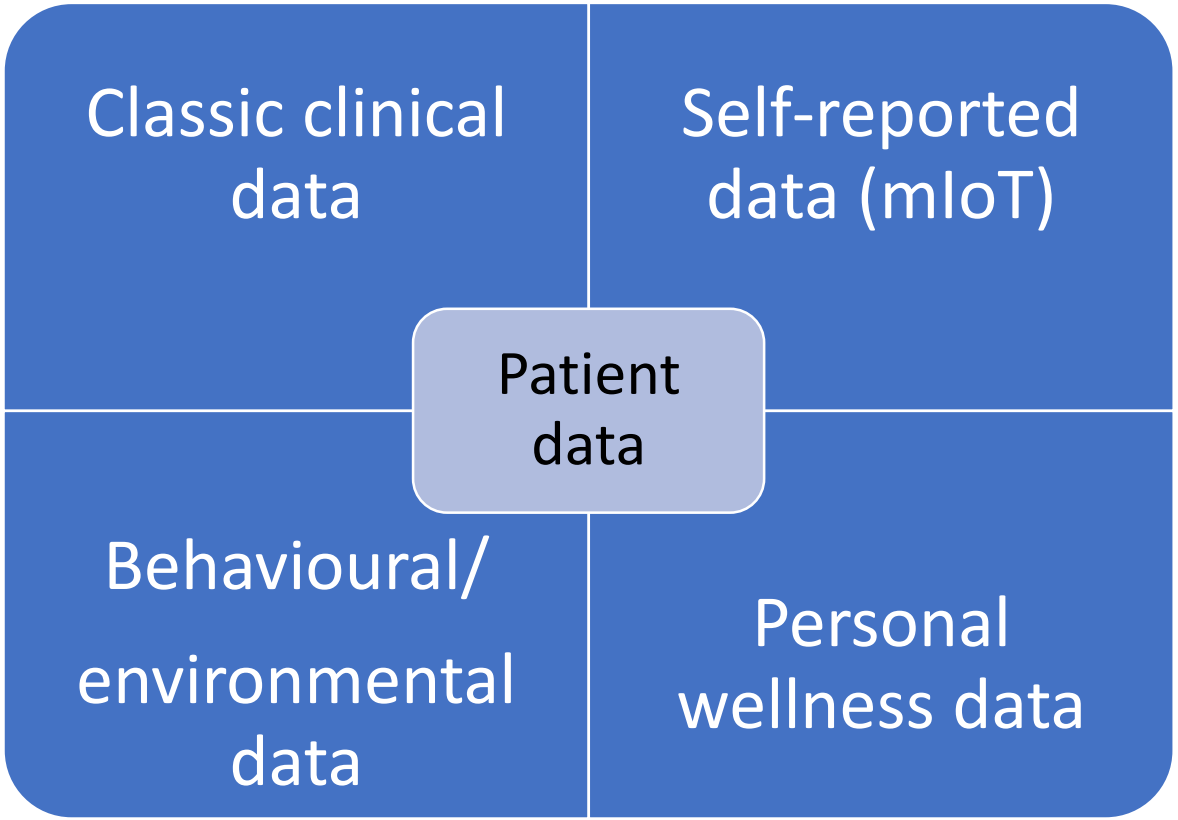


"*big-data_conew1*" (CC BY-SA 2.0) by luckey_sun

- With **its 150 exabytes of stored data worldwide per year**, Healthcare is a bright example of **"data explosion"** phenomenon
- Within 2020 – **40% of IoT technologies will be healthcare-related**
- This will be the basis of the "Internet of Medical Thing" (IoMT), or **medical Internet of Thing (mIoT)**

Health data megatrends

- Patient datasets are expanding, thanks to genomic data and patient-generated data
  - convergence of medical data about patients generated by healthcare providers with a plethora of non-medical, lifestyle related data, much of which is generated by the patient.
  - Some forecasts see a **300% growth** in healthcare data between 2017 and 2020.
- Improved patient engagement and self-management will occur as a result



Data-related pain points

- We are in a “data-rich but information-poor” paradox, as currently the available is not leveraged enough to help providers help patients.
- It is very difficult to mobilise data, both due technical shortcomings and regulatory constraints
- There are no available solutions for integrating sparse sources of data (data generated in the hospitals, patients-generated data, etc.) in a meaningful way.
- Data usage for research and commercial purpose is limited and difficult

Three key issues

ACCESS

- Access to personal health data for patient is not straightforward, not timely, and often patients are not offered with option for easily share their data with other individuals

SECURITY

- There is a growing concern regarding data security, given the increase of identity theft and data breaches

DATA VALUE

- Hospitals and other healthcare providers are not able to extract maximum value from their data, allowing processing by third party tools for getting improved diagnosis and therapies.

Data issues and Blockchain benefits

Issue	How blockchain can contribute
New ways of mobilising data	Act as a **orchestration layer** in charge for managing and authorising data exchange and access **Regulate data access** on the basis of user-defined permission/consent settings
New ways of integrating data from various sources for meaningul use	Create **distributed architecture for gathering data** from different sources (in particular patient-generated data from mIoT and mobile apps), allowing full visibility of all data available for an individual user in a **personal virtual data wallet**
New consent management and direct data access and control tools for enabling individuals engagement	Enabling individual **data self-sovereignity and patient-centric healthcare** (also through direct control of data by patients) through smart contract and dApps
Enhance data security	Through **encryption and hashing** it makes difficult to access data without authorisation Introduce new ways of **storing data in distributed architecture**, overcoming issues associated with **centralized healthcare data structures** Improving **authorisation and identification schemes** using distributed approaches (removing the need of single central entities providing authorisation to many actors)

Data issues and Blockchain benefits

Issue	How blockchain can contribute
Data provenance and integrity	Blockchain-based tools allow to always **track down** a piece of data to its original owner, also providing guarantees that **data has not been tampered with**
Track data exchange and ensure compliance with GDPR	Provide full **traceability and auditability** of data access and exchange Implement **GDPR compliance** in particular in regard to right to erasure/correction
Create new data-driven business model	Improving economic **incentive schemes** and provide individuals with additional motivations for engaging with their health **Tokenisation** and **fractional ownership**
Facilitate data usage and valorisation	Enable **data browsing** by recording on the blockchain a “proof of existence” of a given piece of data and associating to this the relevant metadata to be published in a **public metadata catalogue**

Long term expected benefits

- **Patients:** improved and more personalised treatment and engagement in the care process, improved self management, improved communication with the care providers
- **Hospitals:** improved GDPR compliance, improved communication with patients, more efficient resource consumption, improved care outcomes, improved population-level monitoring
- **Researchers & industry**: facilitated access to relevant and high-quality data for fundamental research, drugs and medical device development and testing

Current initiatives specifically on data management

- MyHealthMyData – a H2020 project
- Patientory
- Medicalchain
- Longenesis
- Healthbank
- HIT Foundation
- others….

Current initiatives specifically on data management

- **MyHealthMyData – a H2020 project**
- Patientory
- **Medicalchain**
- Longenesis
- **Healthbank**
- HIT Foundation
- others….

What role blockchain plays in MHMD?

MY HEALTH MY DATA

- Act as a orchestration layer in charge for managing and authorising data exchange and access
- Regulate data access on the basis of user-defined permission/consent settings
- Provide full traceability and auditability of data access and exchange
- Automate data “sanitisation” and data provision thanks to smart contract
- Implement GDPR compliance in particular in regard to right to erasure/correction

Blockchain records

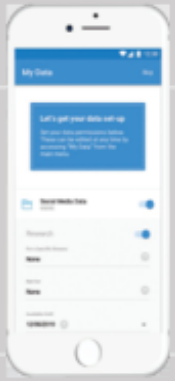
MY HEALTH MY DATA

MULTILAYER, PRIVACY PPRESERVING BACK-END

citizen

hospital

business/researcher



Signs up → Sets permissions → Monitors transaction

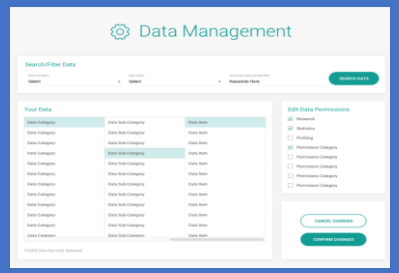
Registers institution → Registers data → Sets permissions and privacy settings

Browses data → Requests access → Download and uses data

Data source

Hospital

Data mapping
Access preferences definition



Local Driver (Local DB)

Matching

Blockchain

New transaction: “Data registered in the platform” (**hash** of the new dataset recorded in the blockchain)

Smart contract’s Function “Create study” invoked (includes study definition/data request)

Smart contract informs the network of the data request

Local drivers at hospitals match data request with their available data and control consent **(bitmap)**

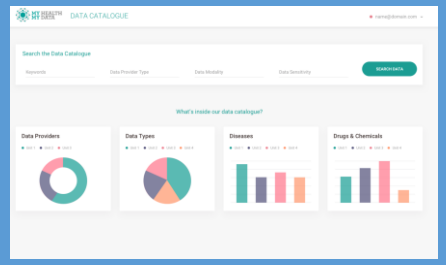
Smart contract’s Function “Study Response” invoked
(Data available at the hospital – access granted)

When enough responses are received the smart contract change the status of the study to “Ready” and provide link for off-chain data download

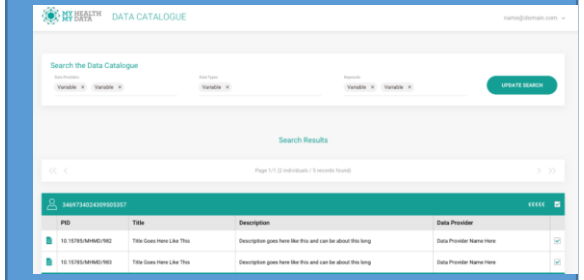
Study Definition

Data download

Researcher/ Business

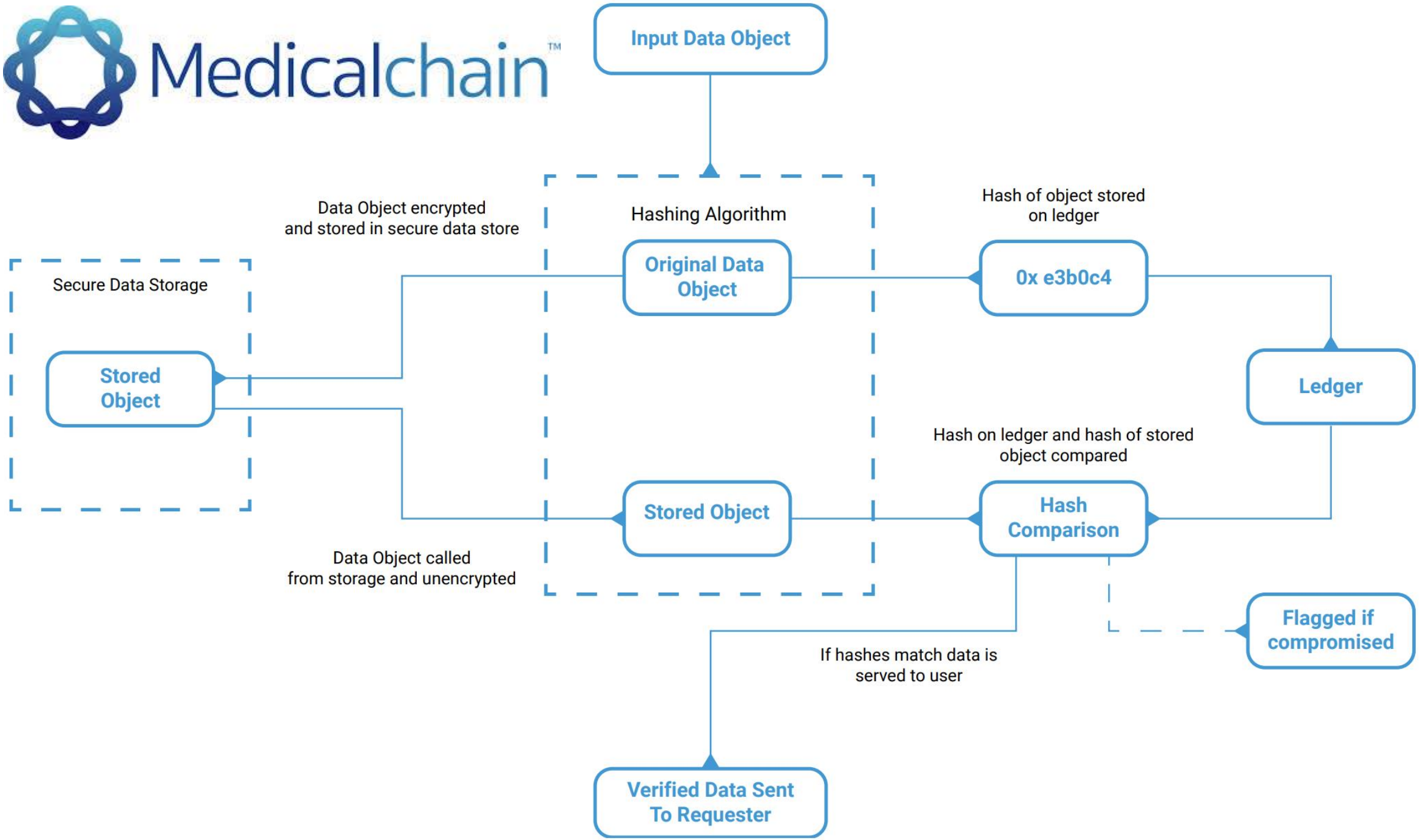


Data catalogue query and data request



MY HEALTH MY DATA

Medicalchain™



The workflow

Medicalchain™

DATA IS GENERATED

(wearable device, machine at hospital, analysis labs, etc.)

DATA IS ENCRYPTED

A persistent identifier (hash) is linked to the data and shared on the blockchain, ideally linked to a patient's "personal data wallet"

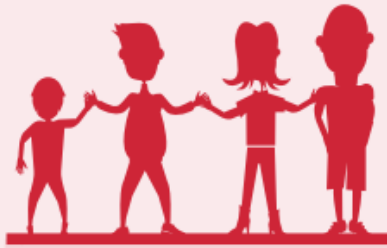
DATA IS REQUIRED BY A THIRD PARTY

The Persistent ID is used to retrieve the data

DATA IS MADE AVAILABLE AND DE-CRYPTED FOR USAGE

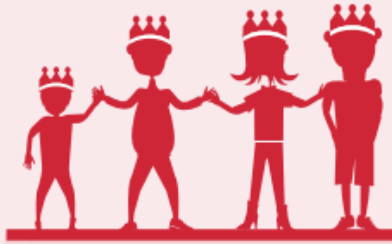
health bank

HEALTHBANK COOPERATIVE



INDIVIDUAL USERS

- **In:** health data platform, timeline, consent management
- **Out:** no fees apply



PREMIUM USERS

- **In:** health data platform, timeline consent management, premium functions
- **Out:** premium service fee

USER CONTENT

HEALTHBANK INNOVATION AG

HEALTHCARE PROVIDERS

- **In:** healthbank platform services (health data management)
- **Out:** data licensing fee

RESEARCH INSTITUTIONS

- **In:** healthbank platform services (marketplace for health data)
- **Out:** brokerage & data licensing fee

End-to-end encryption

healthbank lets the user generate a fully random private key

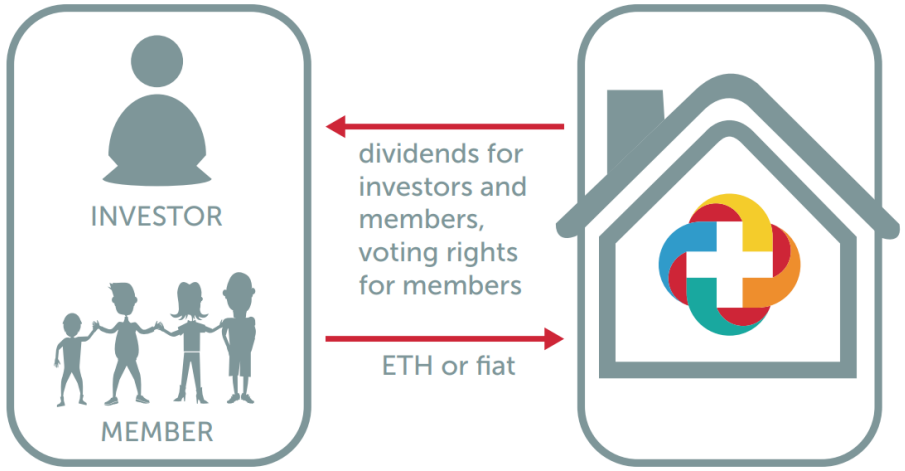
the healthbank application creates a public key from that private key, so others can share data with the user, and the user can share data with others; ”

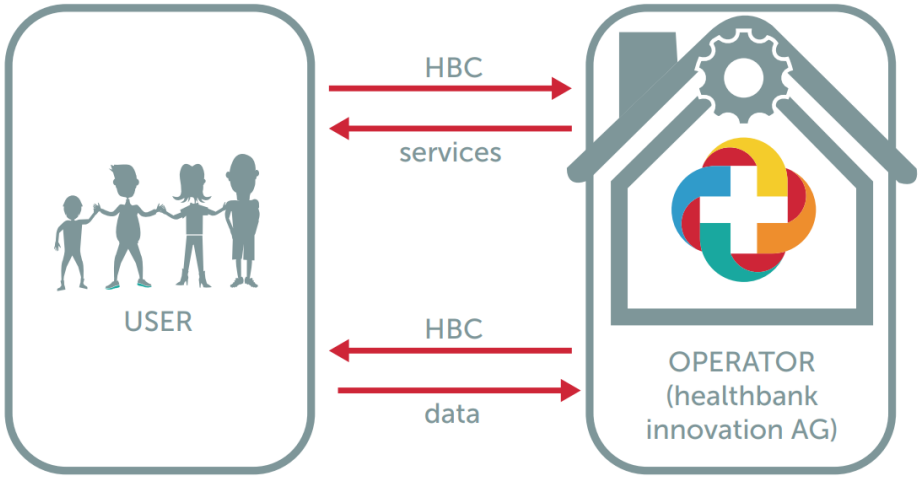
The data will be fully encrypted whilst maintaining the speed of all transactions, using a synchronous key;

Only the member with the corresponding private key can read this synchronous key, and therefore is able to decode the subset of data that users are willing to share.

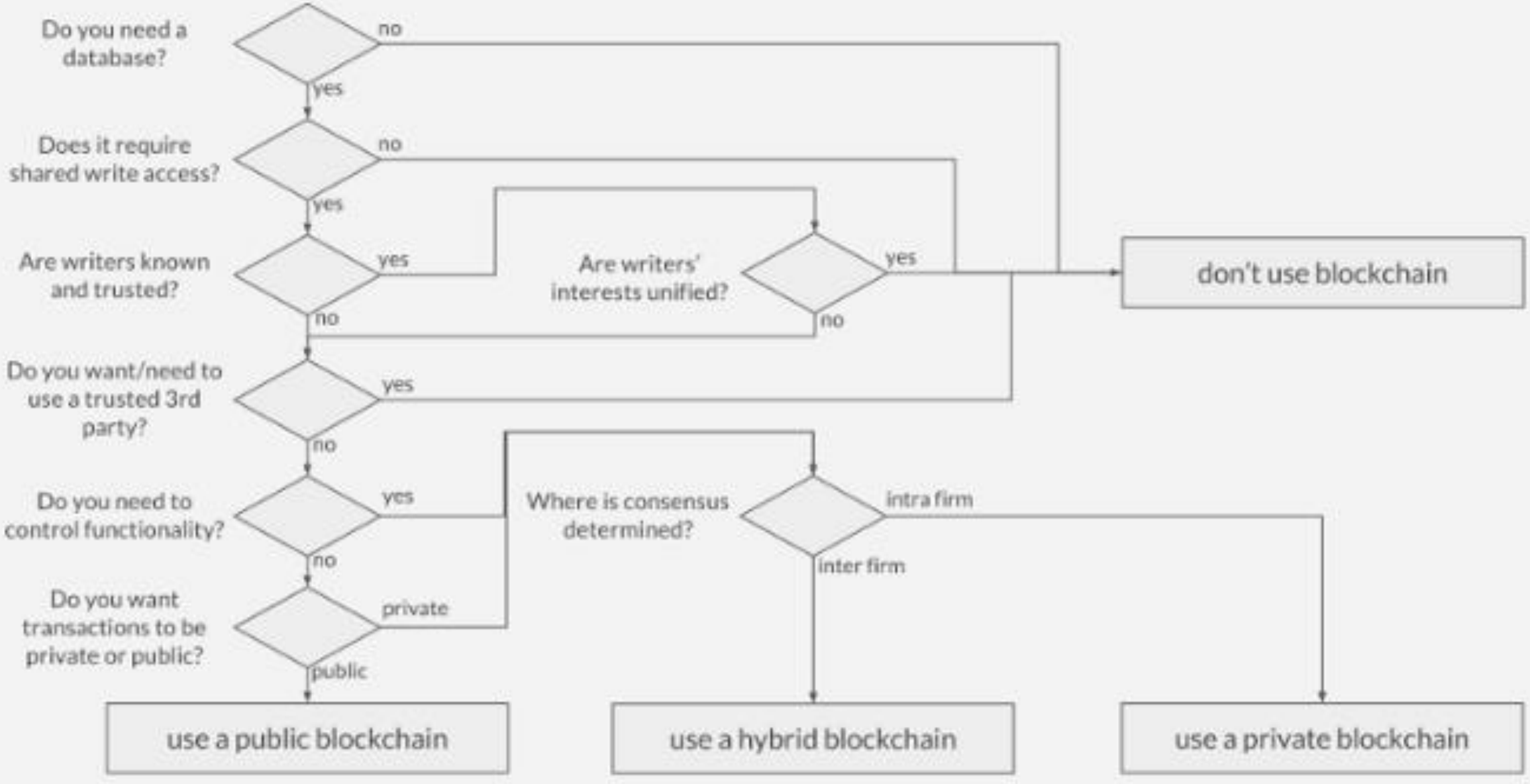
No data shall leave users’ devices without being encrypted.

An ideal (simplified) workflow





A set of criteria for considering blockchain solutions



Are you working with digital assets and can you create a permanent, authoritative record of the digital asset?

Yes (EHRs)

Is there value in an immutable record? Or is an immutable record a requirement?

Yes, immutability is surely a value in specific use cases (access control and auditing, e.g. claims management, drugs authenticity).

Do you require high performance rapid transactions?

Not necessarily – depend on use cases

Do you intend to store large amounts of non-transactional data as part of your solution?

No, large volumes of data from images and genomics will continue to reside on dedicated databases**.**

Do you want/need to rely on a trusted party?

Yes, given roles and liability as set forth in relevant regulations (see GDPR)

Are you managing a contractual relationship or value exchange?

Yes. Here blockchain could help in reducing unnecessary friction and cost in the supply chain or during payments.

Are there multiple stakeholders involved in the process/value chain?

Yes (hospitals, GPs, doctors, nurses, payers, health institutions, patients)

Do you require shared write access?

Yes, as many (if not all) members of the network will need to input into the ledger

Do contributors know and trust each other? Are relevant interests aligned?

No, there are many mis-aligned incentives between healthcare professionals, hospitals, payors, patients, families and regulators,

Do you need to be able to control functionality? (e.g., node distribution, permissioning, engagement rules, etc.)

Yes, to express/enforce policies

Should transactions be public?

No, in most cases.

Blockchain opportunities

Blockchain opportunities

The blockchain/DLTs might be helpful a complex environment such as healthcare where:

a) Multiple actors (professionals, nurses, patients, payors, researchers)…

b) …need to access and exchange data in a secure manner…

c) …while respecting relevant regulations…

d) …ensuring data integrity …

e) …interacting with external stakeholders (research centers, biomedical industries…)

f) …without necessarily trust each others

Blockchain and DLTs can hopefully support such a process offering a way to:

- Filling the **«trust gap»**
- **Automating** data exchange, business processes, and relevant policies' enforcement
- Ensure regulatory **compliance**

Key topics for the discussion

- Use cases – experiences, issues, and challenges, with current data management models
  - Example during the TC: microbial biodiversity digital sequencing for pandemics/epidemics control and sharing of information (reference to the Convention on Biological Diversity)
- Creation of value for justifying public and private investments
- Specific research use cases
- Where blockchain **cannot** be used /doesn’t help
- Contribution to the report