Trusted data sharing
enabled by blockchain technology

Peter Kieseberg (& Rudolf Mayer)
SBA Research
The big data revolution in healthcare

With its 150 exabytes of stored data worldwide per year, healthcare is a bright example of “data explosion” phenomenon.
Health data is abundant – and at risk

**5.6 BILLION DOLLARS/YEAR SPENT IN THE US TO PROTECT HEALTHCARE DATA**

**27.8 MILLIONS OF MEDICAL RECORDS BREACHED SINCE 2009**

**BLACK MARKET PRICES 10X HIGHER FOR MEDICAL RECORDS IN RESPECT TO OTHER INDUSTRIES**

**MORE THAN 193 MILLION PERSONAL RECORDS OPEN TO FRAUD AND IDENTITY THEFT IN 2015**
Patients are skeptical about data sharing

“Soon after you tell your doctor about an intimate medical problem, data about your condition are sold commercially to companies that have nothing to do with your treatment or billing”

Adam Tanner, “Our Bodies, Our Data”
Patients are skeptical about data sharing

Austrian E-Health ("ELGA") records proposed to be made available for research

➔ Patients unsubscribe from the service!
Blockchain: new ways for data sharing?

- Need to develop new mechanisms of trust and of direct, value-based relationships between people, hospitals, research centres – and businesses
- Many initiatives (Public and private, in the EU, US,..) currently addressing potential of applying blockchain to health data
- Great general expectations: “what Internet did to transaction costs regarding information, blockchain can do regarding trust”
- Assumption that what is needed for health data is a Distributed Empowerment system
- Leading to an open biomedical information network centred on the connection between organisations and the individual
Blockchain: new ways for data sharing?

- Blockchain ledger is the secure, non-editable record
- Stakeholders are equipped with a ‘wallet’
  - an encrypted identifier
  - his/her dynamic consent
  - his/her data access policy file
- This could lead to Personal storage clouds for ubiquitous individual data access through blockchain and advanced personal use
Various initiatives
Blockchain hype?


HIMSS Europe - Health IT Central – May 15th, 2017
# Blockchain value propositions for healthcare

<table>
<thead>
<tr>
<th>Health Information Exchange (HIE) Pain Points</th>
<th>Blockchain Opportunities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Establishing a Trust Network</strong> depends on the HIE as an intermediary to establish point-to-point sharing and “book-keeping” of what data was exchanged.</td>
<td><strong>Disintermediation of Trust</strong> likely would not require an HIE operator because all participants would have access to the distributed ledger to maintain a secure exchange without complex brokered trust.</td>
</tr>
<tr>
<td><strong>Cost Per Transaction</strong>, given low transaction volumes, reduces the business case for central systems or new edge networks for participating groups.</td>
<td><strong>Reduced Transaction Costs</strong> due to disintermediation, as well as near-real time processing, would make the system more efficient.</td>
</tr>
<tr>
<td><strong>Master Patient Index (MPI)</strong> challenges arise from the need to synchronize multiple patient identifiers between systems while securing patient privacy.</td>
<td><strong>Distributed framework for patient digital identities</strong>, which uses private and public identifiers secured through cryptography, creates a singular, more secure method of protecting patient identity.</td>
</tr>
<tr>
<td><strong>Varying Data Standards</strong> reduce interoperability because records are not compatible between systems.</td>
<td><strong>Shared data</strong> enables near real-time updates across the network to all parties.</td>
</tr>
<tr>
<td><strong>Limited Access to Population Health Data</strong>, as HIE is one of the few sources of integrated records.</td>
<td><strong>Distributed, secure access</strong> to patient longitudinal health data across the distributed ledger.</td>
</tr>
<tr>
<td><strong>Inconsistent Rules and Permissions</strong> inhibit the right health organization from accessing the right patient data at the right time.</td>
<td><strong>Smart Contracts</strong> create a consistent, rule-based method for accessing patient data that can be permissioned to selected health organizations.</td>
</tr>
</tbody>
</table>
Putting the patients in the loop

“Patients ownership of their data is an entitlement and civil right that should be recognized”

Right to data portability: “receive personal data in a structured, commonly used, machine-readable and interoperable format”

From patient being “the single most unused person in health care” to a new era of health care democratisation
MyHealthMyData at a glance

• Duration: November 2016 – October 2019
• 9 Research Partners
• 4 Clinical partners:
• 1 Legal consultancy: 1 Industry:
A long story of EU-funded research

• ... providing a lot of experience with health data
MHMD mission

CITIZENS’ EMPOWERMENT
Grant individuals ownership and control of their personal health data

DATA PRIVACY AND SECURITY
Ensure the strongest privacy protection and health data security

DATA VALUE ENHANCEMENT
Leverage the value of large biomedical datasets for medical care, research and business
How will MHMD do that?
(1) PERSONAL DATA ACCOUNTS

Individual data ownership and control

Personal storage clouds enabling individuals to access their data from any technological device through the blockchain and employ them for personal use.

Aggregate personal data from disparate sources (social media accounts, clinical data repositories, personal drives, wearable devices, etc.), in a single, user-owned account

• MHMD Mobile App
• Data providers like digi.me
TAKE CONTROL OF YOUR DATA

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad.
(2) MULTILEVEL DE-IDENTIFICATION AND ENCRYPTION TECHNOLOGIES

- Profile and classify sensitive data
- Identify most suitable de-identification and encryption techniques

*Encode and de-associate sensible data from the owners’ identity, still allowing the application of advanced analytics*
(3) DATA CATALOGUE
Finding specific data of interest

- Organise datasets so to provide a database overview
- Allow researchers to find what kind of data most suits their needs

http://maxpixel.freegreatpicture.com/photo-29398
Search the Data Catalogue

Data Providers

Data Types

Keywords

What's inside our data catalogue?

Data Providers
- Unit 1
- Unit 2
- Unit 3

Data Types
- Unit 1
- Unit 2
- Unit 3
- Unit 4

Diseases
- Unit 1
- Unit 2
- Unit 3
- Unit 4

Drugs & Chemicals
- Unit 1
- Unit 2
- Unit 3
- Unit 4
A secure, non-editable digital ledger where:

- **All transactions are confirmed by the network** as entries forming **blocks of transactions**
- **The whole network monitors the legitimacy of each transaction**, guaranteeing a **distributed control system**

**Applying the blockchain approach to health data guarantees secure access from anywhere on any device**
(5) SMART CONTRACTS

Encoding regulation and implementing it at the speed of light

Self-executing contractual states, based on the formalisation of contractual relations in digital form, that automate the execution of peer-to-peer transactions under user-defined conditions.

Regulate data transactions on the blockchain

- in compliance with the incoming GDPR regulation
- allowing to set use conditions and consent options for different stakeholders and purposes.
(6) SECURITY: PENETRATION AND RE-IDENTIFICATION CHALLENGE

Checking the ability of avoiding privacy & security breaches

- **Active self-hacking (1) and public hacking (2) simulations**

- **Testing external re-identification possibilities on**
  1) *synthetic datasets attributed to virtual patients*
  2) *patients consenting to being used as test-basis*

"Hacked..." (CC BY-NC-ND 2.0) by Christine Krizsa
Questions?

http://www.myhealthmydata.eu/

@myhealthmydata

rmayer@research.org