RESEARCH DATA ALLIANCE

Blockchain Applications in Health WG @P14

Regulatory and legal issues related to
Blockchain in health
and 'decision tree' improvement

Helsinki, 25th October 2019, 9:00-10:30

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

research data sharing without barriers
rd-alliance.org

BLOCKCHAIN APPLICATIONS IN HEALTH WG

AGENDA

1. **Introduction to the WG and to the second WG's report on "legal and regulatory issues",** Edwin Morley-Fletcher, co-chair
2. Presentation on **"Security, Privacy & Legal aspects of Healthcare**
3. **Big Data Analytics within the General Data Protection Regulation",** Lorenzo Cristofaro (Panetta&Associati, Legal firm)
4. **Q&A**
5. **Presentation on the 'decision tree' for blockchain solutions** and discussion on **participants' use cases,** Mirko de Maldé (President of the Blockchain Government Association Italy)
6. **Q&A and open discussion**
7. **Next steps:** looking forward the conclusion of the WG activities and producing a set of **comprehensive guidelines**

Background leading 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 blockchain in healthcare and of compliance isues with advanced data protection requirements
- RDA P12 (Gaborone) first official meeting of the WG **(**discussion on potential uses and challenges coming from crytpocurrencies such and “tokenomics”)

Working Plan and GOALS of the WG (18 months)

- **P13 First report** on the *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 and the ‘decision tree’ model)

First Report on the State of the Art @P13

The report provided hints to:

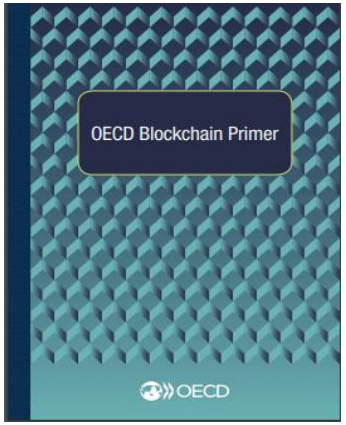
- **analyse and compare** usages of the blockchain in healthcare, implementations of blockchain architectures, associated legal and socio-economic impacts and perspectives,
- assess **incremental and disruptive innovation** and relevant innovative business models,
- understand the connection with other technologies for creating **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.

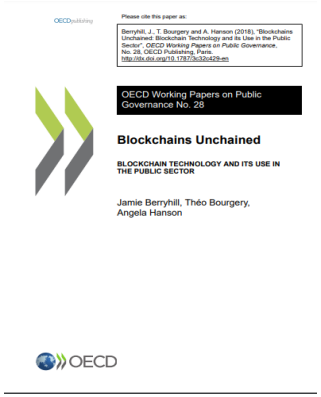
Second Report on Regulatory and Legal issues @P14

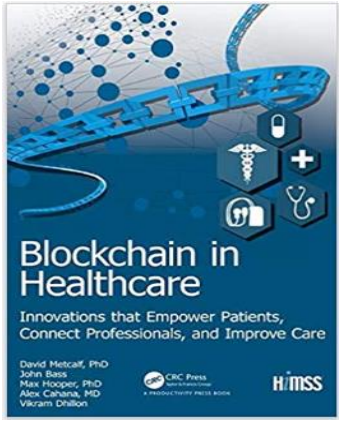
This report aims at giving a first hint to:

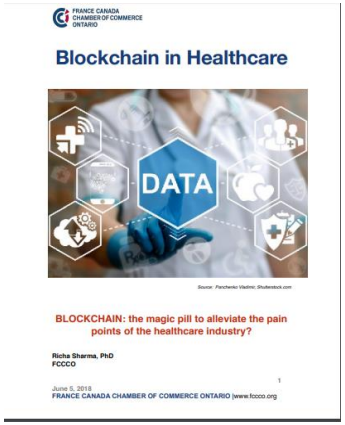
- Understand **the legal framework** and relevant data protection rules and standards with regard to Health data and Blockchain usages, with special regard to **GDPR** provisions
- Highlight the main **challenges and opportunities** related to applying Blockchain in Health from a legal perspective
- Present some **regulatory-compliant solutions** for Blockchain applications in Health

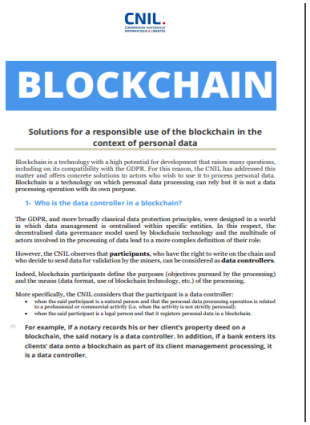
Plenty of official publications on Blockchain, and Blockchain in Healthcare



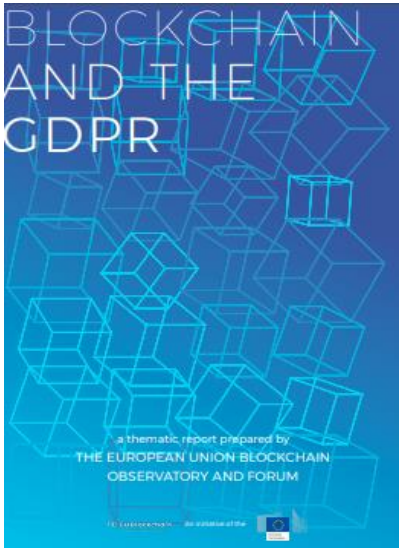


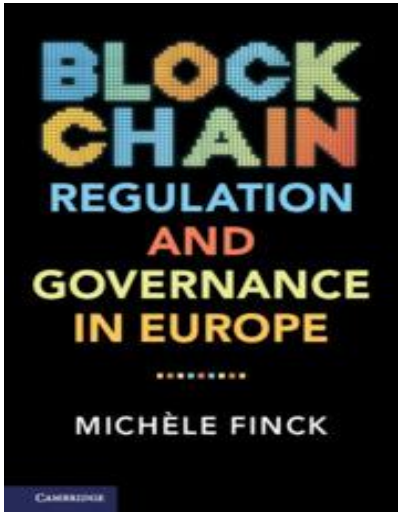






Plenty of studies on Blockchain and the GDPR





General properties of a blockchain

An example of blockchain-based platform for health data (main features 1)

- MyHealthMyData is a blockchain system, permitting to access the Off-chain data stored by multiple hospital repositories and by individuals.
- The blockchain is the concertation layer, recording what transactions happen and specifying under what conditions and with what type of consent.
- The authorised access to data or data computation is enacted through the relevant Smart Contracts.

An example of blockchain-based platform for health data (main features 2)

- Any registered user can browse the central Catalogue, which is ingesting and indexing all the needed metadata, fostering an integrated system for dataset search, and providing statistical representations and analytics.
- Output privacy ensures that no sensitive information is revealed within the Catalogue's queries results.
- The blockchain is the digital space where the execution of the researcher's request can be enacted triggering the process automation based on Smart Contracts.

No personal data are registered on the blockchain. Still specific actions follow automatically the exercise of individual rights (1)

RIGHT	CONSEQUENT AUTOMATED ACTION
Access (obtaining confirmation as to whether or not personal data concerning the data subject are being processed and, in case, access to such data and to all relevant information regarding the processing)	A transaction is registered on the blockchain which indicates that access was requested for a specific data item. The extraction and delivery of the data will then take place off-chain (under the responsibility of the competent controller).
Rectification (obtaining without undue delay the rectification of inaccurate personal data)	A specific smart contract is activated in order to prevent any party to the Project, including particularly the Stakeholder, to access the inaccurate data, while allowing to collect and process only the amended Datasets.
Erasure (obtaining from the controller, when certain conditions laid down by Art. 17 of the GDPR are met, the erasure of personal data concerning him or her without undue delay)	The right to erasure is achieved by 'breaking the link', *i.e.* deleting the entries, in the Local mapping DB, so preventing anyone from being able to associate a data source identifier and the relevant blockchain identifier. As a result of this, a smart contract will forbid anyone from accessing the data on the Platform, thus guaranteeing a result whose effects are reasonably completely equivalent to those of material cancellation (which will obviously will be carried out off-chain with no delay, insofar at least one of the conditions set forth by Art. 17.1 is satisfied)

No personal data are registered on the blockchain. Still specific actions follow automatically the exercise of individual rights (2)

RIGHT	CONSEQUENT AUTOMATED ACTION
Restriction of processing (obtaining from the controller restriction of processing, meaning that the personal data shall, with the exception of storage, only be processed, *inter alia*, with the data subject's consent or for the establishment, exercise or defense of legal claims)	Where the processing is restricted in the cases set out by Art. 18.1, a specific smart contract will be executed to prevent all Stakeholders from carrying out any kind of processing, with the exception of storage, unless (i) the data subject has given his/her consent, or (ii) for the establishment, exercise or defence of legal claims.
Notification (the controller shall communicate any rectification or erasure of personal data or restriction of processing to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it)	The measures described above in regards of the request of rectification or erasure of personal data, or restriction of processing, ensure that the relevant legal effects are appropriately extended to any user of MHMD blockchain, thus meeting notification requirement which, however, shall apply only where this does not prove impossible or does not involve a disproportionate effort.
Portability (receiving the personal data provided to the controller in a structured, commonly used and machine-readable format and, where requested, having such data directly transmitted to another controller)	The same actions described above in regards of the right of access shall apply, mutatis mutandis, to the requests of portability. The duty to provide the data subject with the data in a structured, commonly used and machine-readable format lies exclusively with the controller (namely the Hospital for Clinical Data, or the Platform Operator for Individual data).

An inconvenient truth

- Big Data and AI are difficult to apply in medicine, especially in rare diseases, where data driven solutions are most needed.
- The risk of data breaches increases with the number of copies shared.
- What happens after the data download is no-more under control of the blockchain.
- Rather than simply publishing health data either as pseudonymous or anonymous data, in MHMD the preferred solution has been to publish synthetic data.
- Synthetic data are fully artificial data, automatically generated by making use of machine learning algorithms, based on recursive conditional parameter aggregation, operating within global statistical models.

Differentially-Private Synthetic Data

- Synthetic data typify the case of “personal data [which are] rendered anonymous in such a manner that the data subject is not or no longer identifiable” (Recital 26 GDPR).
- Especially Differentially-Private Synthetic Data Generation provides an until-now lacking mathematical foundation to privacy definition.
- Scalable quality-control systems and iterative approaches allow to generate synthetic data being even more informative and robust than the original ones, leading to statistically equivalent sets, at a vastly lower cost.

The other privacy enhancing direction is Health Data Computation without accessing the data

- Secure Multiparty Computation allows a set of distrustful parties to perform the computation in a distributed manner, while each of them individually remains oblivious to the input data and the intermediate results.
- Another solution, based on MORE Homomorphic Encryption, has been awarded the Innovation Radar Prize 2019 in the category Industrial & Enabling Tech, increasing its security with an additional obfuscation layer based on polynomial evaluation maps.
- The third available tool is using federated learning with untrusted “black-box“: a ML request is distributed to the data providers and local computation results are then securely aggregated, repeating this cycle to obtain training iterations and model validations.