HealthManagement.org
The Journal

LEADERSHIP • CROSS-COLLABORATION • WINNING PRACTICES

VOLUME 19 • ISSUE 1 • 2019 • € 22 ISSN = 1377-7629

UnBLOCK the Chain

Blockchain and GDPR compliance for the healthcare industry

Permissioned blockchains for healthcare data sharing management

In times of rising concerns about data privacy among services providers and consumers, the arrival of the new GDPR alongside cutting-edge technologies can help to better act and benefit the healthcare industry.

David Manset
Head of Research and Innovation
Be-Studys (Almerys group)
Geneva, Switzerland

david.manset@be-ys.com

@dmanset

Laura Bernal
Marketing and communication
Be-Studys (Almerys group)
Paris, France

Master's degree in entrepreneurship and management
Paris 1 Panthéon-Sorbonne

laura.bernal@almerys.com

Mirko Koscina
Research Project Manager
Be-Studys (Almerys group)
Clermont-Ferrand, France

PhD student in information security
École Normal Supérieure (ENS)

mirko.koscina@almerys.com

Octavio Perez Kempner
Research Engineer
Be-Studys (Almerys group)
Clermont-Ferrand, France

PhD student in information security
École Normal Supérieure (ENS)

octavio.perez@almerys.com

@octaviopk

Concepts like traceability, compliance, access control, and risk control and assessment have always been of utmost importance for the healthcare industry. Not only from an economic point of view but also because the associated involved responsibility and management are difficult to handle.

Over the last years, researchers have identified many use cases within the Blockchain ecosystem to tackle such problems. Moreover, patient data management, clinical trials, and even drug traceability are currently being studied as use cases for Blockchain (Quora 2018), posing new challenges for a promising 2019.

One of the biggest challenges has to do with the arrival of the new European General Data Protection Regulation (GDPR), which came into force in May 2018. The GDPR was introduced to protect and empower EU citizen's data privacy and to better deal with the asymmetry between organizations that handle and work with personal data and individuals control over their data. In this context, some principles or rights conferred by the regulation such as the right to be forgotten may clash at first with the usage of distributed ledger technologies (DLT), due to their permanent nature. To correctly assess the risks related to the GDPR-DLT relationship and to better determine how the two of them can be used together to address existing problems, common ground and clear definitions should be established first.

To start with, a distributed ledger is a type of data structure which is replicated, shared, and synchronized across multiple devices that may operate geographically distant from each other. In this scenario, governance over the data in a distributed ledger is achieved using a consensus mechanism among the parties that hold a copy of the ledger. In this context, consensus refers to a protocol that ensures that parties agree to a specific state of the system as the valid one.

According to the definition given by the Hyperledger project, a distributed ledger relies on three essential components:

- A data model that captures the current state of the ledger.
- A language of transactions that can change the ledger state.
- A protocol used to build consensus among participants around which transactions will be accepted, and in what order, by the ledger.

With the above in mind, a Blockchain can be defined as a type of DLT with specific characteristics that differentiate it from other types of distributed ledgers. It is an append-only ledger organized as a chain of blocks that relies on a peer-to-peer network to perform its management, updates and operations. Roughly speaking, blocks are merely containers for transactions and they can be linked to an existing chain of blocks allowing it to grow. As a data structure, a Blockchain has two distinctive features which are block timestamps and hash pointers that link the last block of the chain to the previous one in such a way that any modification made on a block compels

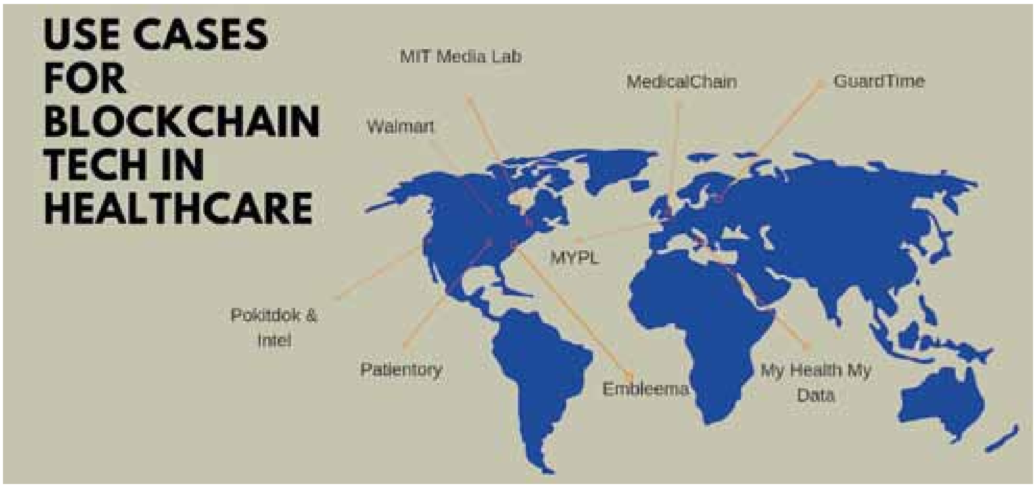

Figure 1. Use cases for blockchain tech in healthcare. (Hello tomorrow, 2018)

the regeneration of the following blocks in the chain.

Together, timestamps and hash pointers can provide a tamper-proof capability to a Blockchain and this, in turn, allows it to achieve a high level of security thanks to the immutability guarantees of its data structure. This immutability feature makes the Blockchain suitable for accounting, financial transactions, and asset ownership management and transfer. For instance, the idea of the so-called “Internet of Value” (Leonard 2018) is based on those use cases.

Alongside immutability, a very close concept is that of compliance. Since it is possible to create tamper-proof (or immutable) records using a Blockchain even in scenarios where parties may not fully nor partially trust each other. This also makes a Blockchain suitable for attestation of compliance. A Blockchain can be very useful when one needs to attest compliance, for example, in relation to the manipulation of certain data.

Another relevant aspect is that of the Blockchain's network being permissionless (open, everyone can join) or permissioned (closed, permission is needed).

In scenarios where partially or fully trusted parties want to work together or need from each other, a permissioned Blockchain is better suitable. In such scenarios, since parties are known to each other, they can be identified and thus can be granted or revoked with permission.

Permissioned Blockchains have contributed to the Blockchain adoption in closed ecosystems and business applications. Some examples include the PlasticTwist project that creates a new circular economy based on an ERC20 cryptocurrency implemented on the top of a permissioned ledger to encourage plastics recycling across Europe and the joint effort between Maersk and IBM to develop TradeLens, a supply chain system supported by the permissioned Blockchain Hyperledger Fabric.

Moreover, the European Blockchain Observatory and Forum has published a technical report which recommends, in case of needing to store sensitive data, to use private and permissioned Blockchains. In particular, achieving privacy is very challenging and the current absence of mechanisms to keep user’s privacy in permissioned Blockchains is turning highly relevant.

Illustrating such a possible scenario, MyHealth-MyData (MHMD) is a project carried out by a consortium of companies that connects hospitals and research centers in Europe to enable the sharing of medical data (from medical records to radiology images) in a private Blockchain network. MHMD is a European project with the ambition to become the first research data network focused on linking organizations and individuals to the health ecosystem. This initiative encourages hospitals to pseudonymize their data for research while giving individuals control of their health data. MHMD wants to become the reference data “marketplace”, providing verified information to value networks in the health ecosystem.

MHMD is a scenario in which the proposed blockchain (private and permissioned) grants the possibility of sharing any kind of sensitive health data example: behavioral data, clinical data, biological data, imaging data (CT, ultrasound, MRI, X-ray, scintigraphy), bacteriological / parasitology data, IoT data among others. (Hello Tomorrow 2018)

Here, the health ecosystem which is composed of European citizens, hospitals, research centers and businesses is faced with two contradictory requirements. On the one hand, the principle of open science defined by the European Commission as a new approach to the scientific process based on cooperative works, sharing and using all available knowledge at an early stage in the research process with new ways of diffusing knowledge by using digital technologies and collaborative tools (European Commission 2018). On the other hand, the GDPR regulation and its application to health data compliance.

> “HEALTH DATA RELATES TO PHYSICAL OR MENTAL HEALTH, PAST, PRESENT OR FUTURE, OF A NATURAL PERSON THAT REVEAL INFORMATION ABOUT THE HEALTH STATUS OF THAT PERSON”

In order to succeed, however, challenges arising from the GDPR must be addressed. A major one is to enforce the privacy of the citizens while allowing the organizations to continue their clinical research (public interest) and to respect the law. Since GDPR, health data has a more precise definition, health data “relates to physical or mental health, past, present or future, of a natural person that reveal information about the health status of that person.” (Aumage 2018)

Due to this and the introduction of new individual’s rights such as the right to be forgotten, one has to be very careful with the immutability property of a Blockchain, when dealing with personal data. To solve these paradoxical matters, in-depth analysis and evaluation of the data cycle have to be carried out to correctly understand how to attest compliance at the same time as being able to empower citizens over the control of their own data.

MHMD’s approach to this is to ensure that looking at the transactions stored on the Blockchain it is impossible to know the parties involved in a transaction (i.e., unlinkability) nor the concerned data. This property increases the overall level of privacy of the resulting system. For this purpose, a privacy-preserving consensus algorithm was designed based on PBFT (Liskov s.d.), so-called “proof-of-privacy”, that relies on Okamoto-Schnorr's blind signature scheme (Tatsuki Okamoto s.d.). This, together with the fact that the data lifecycle is managed through a catalog in a way that it can be indexed and referenced in the Blockchain by storing a hash value of the indexed data items. This process allows the MHMD Blockchain to maintain the records of available data and its associated history without the need to record the private data itself, the latter remaining off chain. Using one-way cryptographic algorithms to describe data and transactions results in an anonymous ledger, which also prevents from statistical inference to locate data or individuals thanks to k-anonymity like models. Following two years of intense prototyping, a GDPR-compliant permissioned Blockchain is now under deployment in pioneer hospital and research centers in Europe, to validate the concept. ■

KEY POINTS

- ✓ Blockchain and the European General Data Protection Regulation.
- ✓ Permissioned Blockchains.
- ✓ Solutions based on “proof-of-privacy” for the Healthcare industry.

REFERENCES

Aumage, B. &., 2018. Global data hub. [Online] Available at: https://globaldatahub.taylorwessing.com/article/health-data-and-data-privacy-challenges-for-data-processors-under-the-gdpr [Accessed 26 December 2018].

Chaparro, F., 2018. Business Insider. [Online] Available at: https://www.businessinsider.fr/us/cryptocurrency-bitcoin-markets-tumbled-early-in-the-year-but-this-has-happened-before-2018-1 [Accessed 26 December 2018].

European Commission, 2018. Europa.eu. [Online] Available at: https://ec.europa.eu/programmes/horizon2020/en/h2020-section/open-science-open-access [Accessed 26 December 2018].

European Commission, 2018. Open Science. [Online] Available at: https://ec.europa.eu/programmes/horizon2020/en/h2020-section/open-science-open-access [Accessed 26 December 2018].

Hello tomorrow, 2018. Blockchain et données patients.

Leonard, S., 2018. ripple. [Online] Available at: https://ripple.com/insights/the-internet-of-value-what-it-means-and-how-it-benefits-everyone/ [Accessed 26 December 2018].

Liskov, M. C. a. B., n.d. USENIX. [Online] Available at: https://www.usenix.org/legacy/events/osdi99/full_papers/castro/castro_html/castro.html [Accessed 12 December 2018].

Njui, J. P., 2018. EWM. [Online] Available at: https://ethereumworldnews.com/bitcoin-btc-under-6k-total-crypto- [Accessed 26 December 2018].

Quora, 2018. IMB. [Online] Available at: https://www.ibm.com/blogs/blockchain/2018/12/what-are-the-use-cases-for-blockchain-tech-in-healthcare/ [Accessed 27 December 2018].

TatsuakiOkamoto, n.d. Provably Secure and Practical Identification, Japon: s.n.

Vries, A. d., 2018. SciendeDirect. [Online] Available at: https://www.sciencedirect.com/science/article/pii/S2542435118301776 [Accessed 26 December 2018].