



UnBLOCK the Chain

EDITORIAL, *C. LOVIS*

IS BLOCKCHAIN THE RIGHT TECHNOLOGY FOR HEALTHCARE? *K. LARDI ET AL.*

HOW BLOCKCHAIN WILL TRANSFORM HEALTHCARE, *A. CAHANA*

WHO STANDS TO BENEFIT FROM HEALTHCARE BLOCKCHAIN? *A. NORMAND*

BLOCKCHAIN SOLVES HEALTHCARE DATA OBSTACLES, *E. SCHEUER*

IS BLOCKCHAIN IMPACTING THE HEALTHCARE ARENA? *J. GRAAFF*

CAN BLOCKCHAIN SUPPORT ADVANCES IN RADIOLOGY? *M. MARENCO*

CAN BLOCKCHAIN CHANGE THE HEALTHCARE ECOSYSTEM? *K. KURIHARA*

BLOCKCHAIN FOR RADIOLOGY, *B. RAMAN & K. CHANDRASEKARAN*

BLOCKCHAIN AND GDPR COMPLIANCE FOR THE HEALTHCARE INDUSTRY, *D. MANSET ET AL.*

HEALTHCARE 2019: THE YEAR OF THE BIG DATA BLOCKCHAIN, *F. RICOTTA & R. LAIDLAW*

HOW TO ANALYSE PAST
PROFESSIONAL EXPERIENCE FOR
FUTURE SUCCESS, *M. VIRARDI*

HOW CAN AUTOMATION IMPROVE
OUTPATIENT CARE WHILE
REDUCING COSTS? *F. MACVEAN &
G. FITZGERALD*

PATIENT RESPONSIBILITY FOR
FOLLOWING UP ON TEST RESULTS,
ECRI INSTITUTE

ENCOURAGING HEALTH APP USE
WITH SENIORS, *E. GATTNAR*

A PATIENT'S JOURNEY IS
LIKELY TO INCLUDE SURFING
THE WEB: HOW CAN WE HELP?
C. ATHANASOPOULOU ET AL.

PATIENT SAFETY CULTURE,
L. RIBEIRO ET AL.

A MULTIMODAL SYSTEM FOR THE
DIAGNOSIS OF BREAST CANCER: THE

SOLUS PROJECT, *P. TARONI ET AL.*

THE EVOLUTION OF LEFT
VENTRICULAR ASSIST DEVICES,
M. PAPATHANASIOU & P. LUEDIKE

TRANSFORMING LIVES A DRONE
DELIVERY AT A TIME, *C. IRERE &
A. KABBATENDE*

HEAT WAVES: A CLIMATE CHANGE
CHALLENGE TO HOSPITALS'
RESILIENCE, *S. GANASSI*



Can Blockchain change the healthcare ecosystem?

Discovering the potential of Blockchain development; pursuing advantages of creating decentralised architectures.

This article presents an abstract concept and predictive benefit of applying Blockchain technology in the healthcare ecosystem. Some current working use cases show the potential short-term benefits of Blockchain database replacement.

Data sensitiveness by nature and by law prevents it to be shared freely among institutions—a silent obstacle—building barriers we find surrounding each of the clinical operations. Interoperability is a necessary element to enable the seamless distribution of medical data in order to provide patients with efficient treatment and eliminate miscommunication. From a medical viewpoint, Blockchain technology originally embraces some deployment features, in addition to, propelling digital-driven healthcare counterparts.

Who owns medical data?

Medical information is respectively administrated within the specific healthcare institutions, derived from a patient's data and diagnosis and is kept in its original format regardless of the standard within which similar categorised operations share it. It burdens the patients and healthcare providers, when they wish to visit other facilities, as data which can not be evaluated or analysed through consecutive formats is of no use or value. The Electric Data Interchange has revealed critical issues among different services that are harnessing information on a medical database with limited interoperation and a 'connected' environment. From a business point of view, this is a nasty arrangement that leads the customer/patient to reject their services and never come back again as a consequence.

Furthermore, what is worse, the data had been sold to third parties without the permission or agreement of patients and without ensuring any data safety provisions in some cases. Medical data is one of the most sensitive assets for an individual. From Pew Research analysis, "Americans Consider Certain Kinds of Data to be More Sensitive than Others" in 2014 (Madden 2014), over half of American respondents said they consider private health and medical information to have the highest sensitivity level among all their data.

Exponentially, with the enormous amount of data in healthcare, both the administration of this data and patient usability becomes significant. Blockchain technology is expected to disrupt the concept of privacy settlement from centralised ownership to empowering the individual management of personal data.

The asset in the case of Blockchain is that once you have received any medical information in the clinic and are diagnosed with a specific symptom, your medical record inherits a personal database and is encrypted in real time. As this output is not governed by any third party, it will be able to submit unbiased or altered information within the available environment.

The government has tried individual data authorities; My Health My Data (www.myhealthmydata.eu/) for example is a European project, aiming to create a transmittable medical information transaction by storing data on Blockchain.



Kohei Kurihara

President of Tokyo Chapter
Government Blockchain
Association

Co-Founder, CMO
CollaboGate
Tokyo, Japan

kurihara@collabogate.com

[@kuriharan](https://twitter.com/kuriharan)

[@gbaglobal](https://twitter.com/gbaglobal)

[linkedin.com/in/kuriharan/](https://www.linkedin.com/in/kuriharan/)

From the operational point, a Blockchain database is capable of retaining multiple adaptations in parallel among some medical institutions, by all means increasing effective access while releasing data management from centralised ownerships.

Who covers security costs?

The onslaught of data theft further burdens health-care providers with issues of liability concerning information ownership, the constant need to strengthen security teams and the increasing cost of compensation. This will continue to put great pressure on institutions that have large centralised data pools. In 2015, the Japanese Pension Service was hacked and 1.25 million files of personal data were leaked instantly, including sensitive personal information like people's pension IDs, names, addresses and birth dates, according to a report published in the Japan Times.

“THE PROBLEM BECOMES WORSE SINCE THERE IS ALREADY A SHORTAGE OF RADIOLOGY SUBSPECIALISTS IN THE US TO MAINTAIN SUFFICIENT SERVICES”

This incident happened as a result of an agency officer opening a suspicious file which then instantly infected the PC. All emails sent from there contained the virus and helped it spread infecting the entire administration core storage files simultaneously. When it comes to preventing a data hacking invasion from outside threats, it is not easy to predict; education and anti-virus software alone are not enough, a comprehensive safety plan requires serious scrutiny inside the management process. In accordance with the set protocols in any operation structure and the relevant data sharing regulations put in place, the owner of the information is held accountable and forced to pay attention and do the utmost to predict and protect the network against potential unknown attacks. In particular, medical data is one of the most valuable and sensitive sets of information and contains varieties of tangled asset records. Patients and healthcare providers are becoming more anxious demanding that their security service is perfect, in an effort to prove the best safety capabilities against

a hacking incident and potential targeting, otherwise risking to lose customer trust and ultimately any profits to their bottom line. Evaluating the security costs of implementing adequate measures strong enough to avoid critical assaults requires expertise and additional cost.

Recently, Korea's Myongji Hospital announced they signed an agreement with BICube, to collaborate on the development of a Blockchain-based medical information exchange system. In the recent announcement by the hospital, the main purpose of the agreement is to “Build a hybrid cloud that combines public and private clouds, and to secure the safety of online medical information exchange system by combining blockchain technology in the process of exchanging medical data through the cloud”, essentially to combine Blockchain technology and a cloud database (Myongji Hospital News 2014).

Managing medical information will require a great deal of expenses on behalf of the data holder, it is therefore preferable to adopt a decentralised operation system cutting cost in the long-run of all future endeavours.

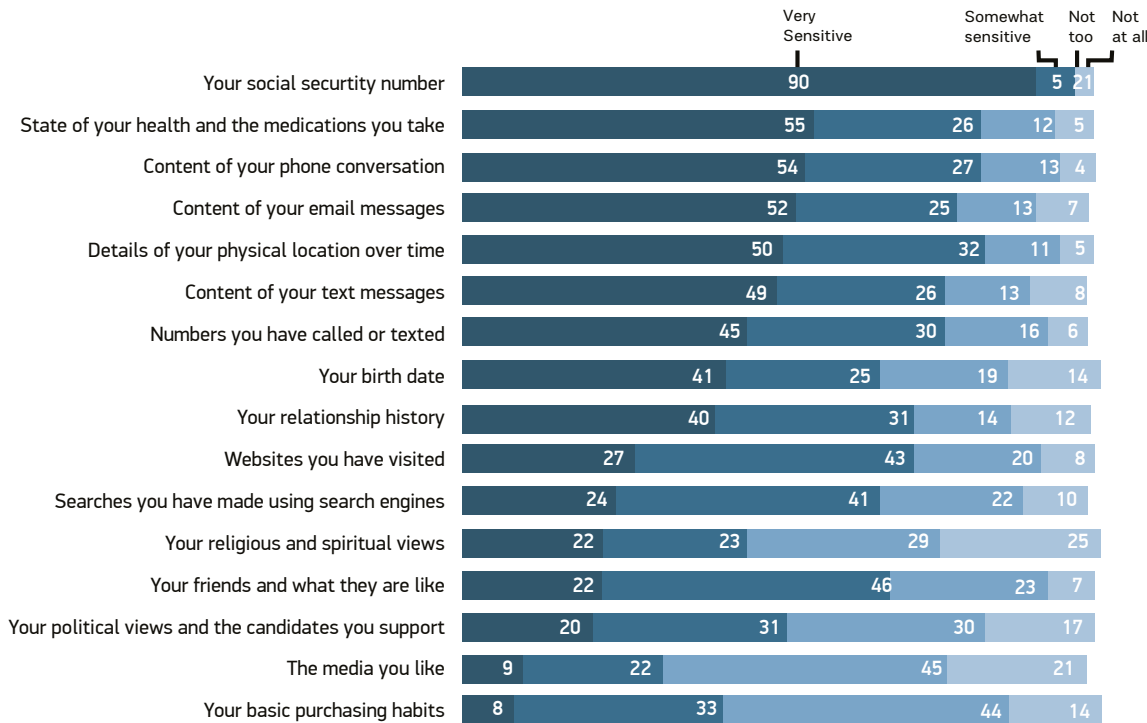
Who trusts the information?

Pharmaceutical supply chains are faced with immeasurable issues, in the meanwhile, from the top to bottom of their distribution, to take measures that will prevent contaminated drugs and errors in the mixture of drugs until they are ready and placed for sale in retail drug stores and pharmacies. According to a recent World Health Organization report, counterfeit drug production has been increasing; the top three countries where threats originate are India at 31%, UAE at 31% and China at 20% (Robles et al. nd).

A few years ago, there were serious incidents in Paraguay and Pakistan when a large number of patients were administered cough syrups containing contaminated agents while they were in the hospital. Although these incidents affected many people, manufactures and the hospitals were unaware and unable to provide tracking to the original sources of this supply chain. Despite the severity of the contamination, the complicated routes of the data could not allow officials to locate the precise factor of infections in order to provide timely treatment to the infected patients. Information asymmetry leads to ubiquitous consumption ratios and inescapable influences due to unknown nature of the structure, so that traceability is recognised as an imminent requirement in order to recall and clear the tainted drugs from the

Social security numbers, health info and phone conversations among the most sensitive data

% of adults who report varying levels of sensitive about the following kinds of info



Source: Pew Research Privacy Panel Survey, January 2014, N=607 adults, ages 18 and older.
PEW RESEARCH CENTER

entire distribution channels.

Pharmaceutical giant, Novartis has started to experiment with the use of Blockchain technology since 2016, even at the early stages of Proof of Concept, in an effort to demonstrate an imagined future with IoT harnessing services, storing temperatures and the ability to locate and identify counterfeit ingredients inside supply chain provisions.

Having the data to track elements of the distribution chain like the spots where the delivery truck has been routed through for example, or how and when the products are delivered to the final vendor will help to increase the accuracy and minimise the margin for outside tampering of products. Besides, the tamper-proof Blockchain database guarantees increased quality of trust compared to the current mostly handwritten documentation records while securing preventive storage against intentionally malicious attempts.

Who insures your healthcare security?

Medical insurance provides access for financial support while you are making payment with negotiating discounted prices and in some cases supported from third party payers and government healthcare systems. However, the insurance process gets more complicated through a series of identification and assessment requirements within each specific payment coverage and the potential of accepting or denying a patients claim. Currently, most insurance contractors spend significant time intervals, even when the patient has been diagnosed with a clear and acceptable healthcare symptom, because of congested administrative processes; and the patient is left to wait until the needed verification in order to receive treatment.

Healthcare data is continuously being refined through beneficiaries to be able to provide more

accurate information yet needs to be rethought by minimising the effect of human error. This entire verification system costs both in financial and human resources capital to complete, maintain and manage. Blockchain technology provides the tools to help decompose these complex procedures, improving the shortage of information and data, replacing them to integrate data flow in a single operation.

Actually, new healthcare organisation alliances have started out between groups of insurance providers. UnitedHealthcare and Humana, Optum, Quest Diagnostics and MultiPlan are now launching Blockchain pilot programmes, helping out payers to tackle complex bureaucracies within their organisations. These programmes focus on improving data quality and eliminating the administration procedures, to pursue cost efficient operation.

“ A DECENTRALISED
BLOCKCHAIN PLATFORM THAT
CONNECTS HEALTHCARE
FACILITIES, RADIOLOGISTS
AND AI ALGORITHMS, ENABLES
RADIOLOGISTS TO PREVIEW
AND PURCHASE VERIFIABLE
ALGORITHMS ”

According to healthcare IT news, insurance providers have received similar requests from dozens of payers. It takes a lot of time and money to reach out to providers on each 90-day cycle. Congested calls and emails delay those inquiries, heavy access traffic jams.

In this pilot, alliance members curated information to be shared, confirming the overlapping with other provider's data and highlighting the need to prevent the duplication of processes within each of them.

How to deal with patient images?

Medical imaging information is sensitive and crucial for both diagnosis and treatment. The patient retains ownership of the imaging data, and has secure individual rights against any service provider failing to protect the data from risk of leaking or malicious manipulation. In the US, the Health Insurance Portability and Accountability Act (HIPPA) defines the rule of privacy and medical data security; respectively

enterprises need to follow this enforcement, in terms of administrative privacy and medical data (Edemekong et al. 2018).

In 2015, there was a massive hacking incident that leaked more than 3.9 million patients' medical information nationwide by EHR vendor Medical Informatics Engineering. In this case, the electronic healthcare record vendor was suspected to be in violation of HIPPA rules and other state regulations, and held accountable for the breach of records including radiology patients.

In this case, the electronic medical record vendor was in direct violation of the process of operation to store information, and handle sensitive patient data. The problem becomes worse since there is already a shortage of radiology subspecialists in the US to maintain sufficient services. According to the Merritt Hawkins figure the number varies from the 2016 ACR Commission on Human Resources Workforce Survey in the article published in Diagnostic Imaging showing 28% of the radiology workforce is 56 or older (Kaplan 2016). In both cases, though, a significant number of radiologists are nearing retirement age. It is evident that there is a need for more resources to improve service delivery.

In order to solve this issue, the MDW project, a decentralised Blockchain platform that connects healthcare facilities, radiologists and AI algorithms, enables radiologists to preview and purchase verifiable algorithms to enhance their practice. Radiologists gain compensation once their report is accepted. This results in lower costs giving radiologists the ability to access high quality expertise.

There is a lack of talent to manage the current medical system structure. As such, it is unable to sustain the needs of healthcare overall and imaging in particular. These issues can be resolved with new technology like Blockchain. Blockchain databases can help secure the environment by following the regulatory requirements and by only distributing encrypted information more efficiently.

Who is aggressively betting on healthcare Blockchain?

From PwC's 2018 Global Blockchain survey, 49% of global healthcare companies have started Blockchain pilot programmes (PwC Global Blockchain Survey 2018). Even though this survey was conducted within a limit of 74 healthcare enterprises, other evidence suggests there is an increase in healthcare trials using Blockchain pilot programmes.

From the healthcare perspective, it tends to combine health privacy data with payment or other financial access. Some companies explore the technology as an alternative to the traditional process that requires endless paperwork and human centric enforcement. Blockchain companies are making a move to explore the potential of the healthcare market, adding significant value by cost cutting and providing simplified overall management.

How to build a decentralised operation system in healthcare?

In terms of healthcare areas, a decentralised network facilitates private data transformation from a centralised database to the individual end user or owner of the data, the patient. In accordance with the growth of health-tech and medical-tech innovation, data ownership has certainly come on the table, and solutions to tackle the sovereignty issues of ownership and privacy will ultimately be provided by new platforms. As a result, architectural concepts will have to be changed while information ownership and individual control will rely on the effective operation of these platforms.

Basically, when it comes to the application of Blockchain, it is important to involve all the stakeholders, visualise a consensus algorithm and incentive structure, and choose an appropriate governance and maintenance model. It is also important to consider some risks in advance that could possibly have an impact on governance or breach the rules.

However, the entire mechanism differs from the number of audiences and stakeholders; moreover, consensus algorithms influence the management block scales in consequences. Regardless of the technical aspects, government regulation is going to enforce Blockchain modeling unless it conflicts with enacted items on existing laws. Data privacy is controversial and on the table in a constant attempt to 'synchronise' governance and technology innovation. Ultimately, Blockchain systems will be utilised as

certification credits in order to prove data accuracy.

For example, the American Drug Supply Chain Security Act (DSCSA) outlines the steps required to build an electronic and interoperable system, capable of identifying and tracing prescription drugs distributed in the US market (Drug Supply Chain Security Act FDA). In order to protect consumers from contaminated products and otherwise harmful incidents, companies need to adhere to legal frameworks set in place for distribution. However, regulatory requirements are not the same between multilateral nations, so that it is now necessary to develop solutions such as Blockchain pipelines with the potential to securely service international healthcare delivery systems.

In conclusion, Blockchain is a decentralised database, potentially a tool that will be widely implemented in the next generation of our society to disrupt traditional healthcare ecosystems. However, we still have to fill knowledge and experience gaps by empirical operation and trials in various areas to determine how this technology can be further applied in healthcare and imaging as a natural extension.

From industry and government viewpoints, the inclusion of multiple stakeholders is the key element, even at the stage of discussion because Blockchain solutions must combine each player of the healthcare continuum if they are to produce meaningful value. ■

KEY POINTS



- ✓ Data ownership discussion becomes more serious by harnessing Blockchain-based operations
- ✓ Accurate traced information secures customer protection under the regulations
- ✓ Single pipelines are more cost effective than congested current operations
- ✓ First experiment, second create the standard, third follow with operation



REFERENCES

A new paradigm in health-care data privacy and security. MyHealthMyData.eu.

Drug Supply Chain Security Act (DSCSA). FDA US Food & Drug Administration. Edemekong PF, Haydel MJ (2018) Health Insurance Portability and Accountability Act (HIPAA). StatPearls Publishing.

Kaplan DA (2016) Is Radiology part of the physician shortage? Diagnostic Imaging.

Madden, Mary (2014) Americans consider certain kinds of data to be more sensitive than others. Pew Research Center.

Myongji Hospital, BICube to develop

Blockchain-based medical info exchange system (2014) Myongji Hospital News.

PwC global Blockchain survey (2018). PwC.

Robles, YR, Casauay JF, Bulatao BP (n.d.) Addressing the barriers to effective monitoring, reporting and

containment of spurious/substandard/falsely-labelled/falsified/counterfeit medical products through sustainable multi-stakeholder collaboration and community/consumer-based Interventions. Medicines Transparency Alliance, Philippines.