ABOUT THE
HEALTHCARE DATA INSTITUTE

The Healthcare Data Institute is the first international think tank dedicated to Big Data in the health sector.

An Orange Healthcare initiative, the Healthcare Data Institute was launched in partnership with other companies representative of the Big Data health ecosystem: government and regulatory agencies, pharmaceutical companies, leading figures from the medical world, start-ups and insurance companies.

HEALTHCARE
DATA INSTITUTE

CONTACT
Quentin ROSET
office@healthcaredatainstitute.com
+33 (0)1 42 21 19 59

21, rue Jasmin
75016 PARIS - FRANCE

@HCDATAINSTITUTE
healthcaredatainstitute.com

HEALTHCARE
DATA INSTITUTE

INTERNATIONAL THINK TANK
DEDICATED TO BIG DATA IN HEALTHCARE

BLOCKCHAIN FOR BETTER CARE

OCTOBER 2017

(Frisoni et al., 2011) Virtual imaging laboratories for marker discovery in neurodegenerative diseases. G. B. Frisoni, A. Redolfi, D. Manset, M-É. Rousseau, A. Toga & A. Evans. Nature Reviews: Neurology August 2011 5; 7(8) pp 429-38. doi:10.1038/nrneurol.2011.99.

(CARDIOPROOF, 2016) The CARDIOPROOF Project. N.p., n.d. Web. 05 Apr. 2016. http://www.cardioproof.eu

(Watanabe et al., 2015) "Blockchain contract: A complete consensus using blockchain." IEEE 4th Global Conference on Consumer Electronics (GCCE). IEEE, 2015.

(Lietaer, 2001) "The Future of Money: Creating New Wealth, Work and a Wiser World" (Century, 2001).

(Bauwens et al., 2015) "Sauver Le Monde : Vers une économie post-capitaliste avec Le peer-to-peer". Bauwens, Michel, and Bernard Stiegler. Paris: Ed. Les Liens Qui Libèrent., 2015. Print.

End of writing: end of October 2017

THANKS TO THE CONTRIBUTORS

- **Head of the working group: David Manset,** Be-Studys
- **David Houlding,** Intel
- **Dr John Sotos,** Intel
- **Valère Dussaux,** Intel
- **Jan Rowell,** Intel
- **Philippe Genestier,** Orange
- **Sajida Zouahri,** Orange
- **Issam Ibnouhsein**, Quantmetry
- **Karl Neuberger,** Quantmetry
- **Me Cécile Théard-Jallu,** Avocat Associé, De Gaulle Fleurance & Associés
- **Edwin Morley-Fletcher,** Lynkeus

BIBLIOGRAPHY

(Wolf 2015) Wolf, Gary. "The Quantified Self." Antephase RSS. N.p., n.d. Web. 11 Nov. 2015. http://antephase.com/quantifiedself

(UnPatients, 2015) "You Should Get to Know You - UnPatients." UnPatients. N.p., n.d. Web. 11 Nov. 2015. http://unpatient.org

(Warren et al., 2007) Warren, T. Solomonides, C. del Frate, I. Warsi, J. Ding, M. Odeh, R .McClatchey, C. Tromans, M. Brady, R. Highnam, M. Cordell, F. Estrella & R. Amendolia. "MammoGrid - A Prototype Distributed Mammographic Database for Europe" Clinical Radiology Vol 62 N° 11 pp 1044-1051. ISSN 0009- 9260 November 2007, Elsevier publishers.
And R. McClatchey, D. Manset & T. Solomonides "Lessons Learned from MammoGrid for Integrated Biomedical Applications" Proceedings of the 19th IEEE Symposium on Computer-Based Medical Systems (CBMS 2006) pp 745-750. ISBN 0-7695-2517-1 IEEE Press. Salt Lake City, USA. June 2006.

(Foster et al., 2001) I. Foster, C. Kesselman & S. Tueke, "The Anatomy of the Grid – Enabling Scalable Virtual Organisations", International Journal of Supercomputer Applications, 15(3), 2001.

(Skaburskas et al., 2008) K. Skaburkas, F. Estrella, J. Shade, D. Manset, J. Revillard, A. Rios, A. Anjum, A. Brandon, P. Bloodsworth. T. Hauer, R. McClatchey & D. Rogulin. "Health-e-Child: A Grid-enabled Platform for European Paediatrics". Journal of Physics Conference Series Vol. 119 Paper 082011 ISSN 1742-6596.

(MD-Paedigree, 2016) "Model-Driven European Paediatric Digital Repository." CORDIS Portal. European Commission, n.d. Web. 05 Apr. 2016. http://cordis.europa.eu/project/rcn/108228_en.html

(Redolfi et al., 2009) A. Redolfi, R. McClatchey, A. Anjum, A. Zijdenbos, D. Manset, F. Barkhof, C. Spenger, Y. Legre, L-O. Wahlund, C. Barattieri, GB. Frisoni. "Grid Infrastructures for Computational Neuroscience: the neuGRID Example". Future Neurology. November 2009, Vol. 4, N°6, Pages 703-722, DOI 10.2217/fnl.09.53. Future Science Group publishers 2009.

BLOCKCHAIN
FOR **BETTER CARE**

INDEX

for exchanging value. With the ongoing regional hospitals grouping in France (i.e., GHT), for instance, public-health policy and care centers are converging and will soon produce key quality and performance indicators. This will imply interoperable information systems, accurate information sources, transparency, and traceability. Blockchain may well become an unavoidable technology to achieve this endeavor.

CONCLUSION

Contributor: David Manset, Be-Studys

Blockchain technology exhibits several interesting characteristics, indeed. Simply put, it brings trust where there is none, thanks to a cryptographic trick and decentralized consensus. In doing so, it also makes its information system resilient to external attacks and internal failures. It therefore makes it an ideal candidate to remove trusted third parties in multi-centric collaborations requiring transparency, traceability, and information robustness.

Nevertheless, one still has to consider it as a rather immature technology and nothing close to a magical wizard doing everything we could dream of. For instance, blockchains are not databases. They should not be used to store raw data, nor can they achieve DBMS-like performances, to date. They are also not high-performance transaction engines. Runtimes range from several seconds to minutes, so they are not useful in high-frequency trading as-is. There are different flavors of blockchains, as well as different types of consensus algorithms. The most secure and trustworthy ones are based on Proof-of-Work, but this also is computationally very demanding, over time. Last but not least, blockchain technology leverages regular cryptographic algorithms, and therefore remains quantum unsafe.

On the legal front, blockchain technology requires statutory recognition in all countries, which is not the case as of now. Indeed, while the technology offers algorithmic reliability and ensures non repudiation of transactions, it does not make it a legally probative tool. Blockchain technology also cannot replace human interactions, which is specifically necessary for patients to give informed consent. Many unresolved questions which will soon find a focal point with the entry into force of the GDPR, in Europe.

However, the blockchain still holds the potential of becoming a generalized authentication register and automated contracts generator for the healthcare industry. Besides the advances it will bring to the development of a transparent, traceable, and trustable decentralized ledger of consent and associated data transactions, blockchain technology could also lead to experiments with a novel type of social business model, involving the usage of specific protocols

PART 1

BLOCKCHAIN BASICS

TECHNICAL DEFINITION OF BLOCKCHAIN

Contributor: Valère Dussaux and Jan Rowell, Intel

Transactions among independent organizations and individuals have traditionally been recorded through centralized methods or intermediaries. These can range from centralized internal databases to clearinghouses such as those used by billing services or stock exchanges.

The blockchain is a disruptive technology that allows for the fully distributed, decentralized recording of transactions without the need for an intermediary. The concepts behind blockchain technology are not new – in fact, many were formulated in an influential 1976 paper published by the Institute for Electrical and Electronic Engineers.

The blockchain technology originated as part of the bitcoin digital currency system, which was first described in 2008 by an individual or a group using the pseudonym Satoshi Nakamoto. However, the blockchain technology can be used to create distributed ledgers – distributed records of transactions – that can record any item of value without the need for a central authority or administration.

1. OVERVIEW: DISTRIBUTED DATABASE, DIGITAL LEDGER

Like the Internet itself, which no single entity "owns," blockchain technology can be thought of as enabling an open, distributed, yet secure database or accounting ledger – owned by no single site, but available equally to its participants – for recording transactions. Running on a network of nodes over the Internet, blockchain networks can be public, private, or consortium-based (i.e., hybrid).

Blockchain networks use cryptographic methods to maintain the security and privacy of the distributed ledger. Participants in a blockchain ledger can submit transactions to add, remove, or modify records in the database according

Orange and the Clermont Ferrand Teaching Hospital: Patient recruitment associated with identity of mobile devices, on SIM card

Contributor: Philippe Genestier, Orange

In all healthcare applications, identification/authentication of users must comply with specific regulatory requirements. In particular, for healthcare professionals, the Shared Information Systems Agency (ASIP) recommends the use of Health Professional Cards (CPS) or another strong authentication mechanism such as an SMS OTP. These authentication methods have constraints in terms of implementation (the need for a CPS card reader, or a complicated user process in the case of a SMS OTP) that are fairly significant and greatly discourage access to medical applications on mobile devices.

So Orange, in conjunction with the Clermont-Ferrand Teaching Hospital, has proposed and trialed the Mobile Connect Santé solution. This involves a strong authentication mechanism standardized via GSMA (Mobile Connect) enhanced by a link between the identity of the health professional shown on the CPS and the identity of the mobile device loaded on the SIM. The user process has therefore been hugely streamlined in providing access to the health application covered by the trial on mobile devices without CPS card readers: the user was simply asked to enter a personal code on the mobile device, and the association mechanism then used that code to find that user's unique health professional identity.

called MyHealthMyData (MHMD www.myhealthmydata.eu). MHMD will serve the purpose of topping up this privacy-preserving information system with full transparency and traceability over space and time.

Now, think of such a ledger deployed at the European scale, enabling (anonymous) consents and data transactions, browsable at anytime, anywhere, and by anyone, yet containing no sensitive information. Imagine a place where individuals, research groups, pharmaceutical businesses, and healthcare professionals can easily search for and mobilize large volumes of data on demand while ensuring patients' clear consent and privacy at all times, regardless of their geographical locations, data complexity, and data protection laws.

This is the author's objective: to create such a solid technological backbone, supporting information systems' resilience, and acting as an operational GDPR-compliant infrastructure where data transactions are informed and controlled by informational self-determination and privacy-by-design/default principles. Such a foundational base will open new avenues to innovative (smart) contracts (Watanabe et al., 2015), incentivizing data mobilization under strict regulatory control, while facilitating dynamic consent collection and data preparation.

Besides the advances that blockchain technology shall bring to the development of a transparent, traceable, and trustable distributed ledger of consent and associated data transactions, it could also lead to experiments with a novel type of social business model, involving the usage of specific protocols for exchanging value. In fact, this would result in creating a new sort of virtual currency, experimenting with the creation of a health-dedicated complementary money, used for giving value to transactions in different ways within the healthcare area. At the state-of-the-art in the "transitional money systems, which can be used as crutches to re-educate atrophied collective behaviour patterns" (Lietaer, 2001), the intent is to investigate the potential use of shared economy and open value accounting in healthcare (Bauwens et al., 2015).

to a set of rules that are guaranteed to be enforced by the ledger itself. Once a transaction is accepted into the blockchain and recorded in the ledger, the data becomes immutable and cannot be tampered with, revised, or repudiated. This is one of the key characteristics of the blockchain.

2. LINKS IN A CHAIN

Blockchain technology gets its name from the way it builds historical transactions. Unlike traditional double-entry bookkeeping, the distributed ledger's transaction records are collected in blocks that are time- and date-stamped and chained together in chronological order. Each new set of transactions is time-stamped and added as a new block to the end of the current chain.

Each valid block in a blockchain thus contains a reference to the previous valid block, creating a chain of blocks that captures the history of a transaction. Each block contains a record of all the previous transactions, as well as a link to the immediately previous block. The series of transactions formed by a blockchain is shared by all participants in the ledger.

3. CRYPTOGRAPHIC FOUNDATION: ENCRYPTION, KEYS, AND DIGITAL SIGNATURES

Before adding a transaction to the chain, the blockchain technology uses consensus mechanisms based on robust cryptographic algorithms to determine whether the proposed transaction is legitimate or not.

Cryptographic signatures, along with the use of public and private keys, help ensure the correctness of the transaction record. These methods also help guarantee that once a transaction is committed to the blockchain, it cannot be un-committed. Distributed consensus algorithms ensure that all participants see the same series of transactions even if bad actors try to compromise the system.

4. HARDENED SECURITY AT THE ENDPOINT

With such a secure foundation, blockchains themselves have thus far proven impervious to attacks by bad actors. However, the computers that run blockchains are subject to the same risks as other systems on the Internet. Previous, highly publicized reports of Bitcoin being hacked are actually instances of breaches at endpoint nodes in the blockchain network, and at the application or client level.

Increasingly sophisticated malware seeks to infect lower stacks in the software, including BIOS, operating system kernels, and firmware. Hardware-enhanced security capabilities can improve endpoint security for blockchains and other applications. Hardware-enhanced security armors the security software stack down to the silicon, protecting all elements of the stack from malware. For example, Intel® Software Guard Extensions (Intel® SGX) provides new CPU instructions that software developers can use to better protect the confidentiality and integrity of sensitive data and code. Intel has also developed an open-source platform, the Sawtooth Lake Distributed Ledger Platform (SLDLP), that can be used for building, deploying, and running distributed ledgers.

5. TECHNICAL BENEFITS AND IMPACT

Distributed ledgers based on blockchain technology present several advantages over record-handling methods that rely on centralized databases. For example, connections between counterparts are simplified because each participant has a copy of the data. Data is recorded on an unbroken, secure, tamper-proof blockchain, which maintains the historical record and facilitates compliance with regulatory requirements.

The participants (or nodes) in a blockchain event each have their own copy of the stored data in what can be considered a secure, permanent, shared database. This ensures redundancy and fault tolerance for the distributed network.

Changes to the data are validated by participants collectively, and updated across the network almost immediately. In this way, blockchain technology serves as a machine for creating trust, allowing a group of users who have no particular confidence in each other to collaborate without having to go through a neutral central authority.

Blockchain for biomedical research – The MyHealthMyData H2020 Project

Contributor: David Manset, Be-Studys

Based on: 2017 – Big Data and Privacy: Fundamentals of Digital Trust Toward a Digital Skin. D. Manset. In L. Menvielle (ed.), Connected Health: New Challenges for The 21st Century. Edited by Palgrave MacMillan, 2017. In Press.

Anticipating the complex needs of GDPR in sensitive data protection and privacy matters, a first network of hospitals and research centers was developed in the 2000s, in the EU FP5 MammoGrid project (Warren et al., 2007), which made it possible to share sensitive medical data across renowned European centers in pioneering breast cancer research, utilizing the so-called Grid (Foster et al., 2001). In doing so, initial developments were achieved in anonymizing medical information (i.e., DICOM file headers and images, diagnostic reports) and in securely sharing, indexing, cataloguing, and curating data. Following on with an even more ambitious scope, Health-e-Child (Skaburskas et al., 2008) then pursued the development of this distributed platform, interconnecting several more centres and addressing three major pathologies in pediatrics, thus leading to an interesting strategy. The solution that emerged allowed sourcing and preparing sensitive data from the inside and applying proper anonymization onsite, under the strict supervision of data managers, who could perform quality control, quarantine, or even stop the sharing at any time. The verified data was then uploaded to the 'demilitarized zone' server, which synchronized the contents with the other connected centres. This architecture also made it possible to more deeply penetrate local information systems, by connecting to their routing systems, proprietary RIS, PIS, or PACS databases.

Today, the EU FP7 MD-Paedigree (MD-Paedigree, 2016), EU FP7 neuGRID (Redolfi et al., 2009), EU FP7 N4U (Frisoni et al., 2011), and EU FP7 CARDIOPROOF (CARDIOPROOF, 2016) projects further exploit and extend this initial network with a total set of 15 centers feeding dedicated scientific data catalogues.

Much as VISA developed a network of institutions accepting and supporting VISA payment cards, the intent of these projects is nowadays to further extend this network and keep on feeding research platforms by providing access to much more data. In the coming three years, the authors, in collaboration with involved project partners, will therefore propagate this legacy network to give life to a sustainable blockchain-enabled transactional platform, so-

BUSINESS NEEDS IN HEALTHCARE

Contributors: David Manset, Be-Studys;
Edwin Morley-Fletcher, Lynkeus

Our society is digitally transforming. As foundational pillars of our governing system, the healthcare and insurance sectors are moving from siloed, slow-changing monopolistic and yet complex information systems, to decoupled, rapidly growing and heterogeneous data landscapes. Facilitated access to healthcare information systems, reduced costs of genome sequencing, and the unprecedented volume of connected devices flooding the market are as many signs of our emerging ubiquitous and interconnected "big data powered" society. This globalisation inexorably is leading us toward the question of our "quantified self" (Wolf G., 2015). In other words: How much personal data to share with society? What are the associated risks and benefits? What is the actual value of our data? Who owns the data? (UnPatients, 2015). Several questions which must be pondered with care and under the lights of good practices, laws, and finally concerned individuals, organizations, and information systems.

Healthcare, especially in France, is a complex ecosystem made of actors of different natures with sometimes orthogonal objectives. It is a field that requires more and more transparency in its processes, be it for the sake of informing policies, benchmarking practices, or above everything else, saving lives. Blockchains can therefore play a key role there, at interoperating information systems, opening healthcare business processes, and strengthening trust among the actors of the value chain. Moreover, healthcare in Europe will soon see a revolution with the application of GDPR. Blockchain technology can also help in solving issues surrounding access, management, and processing of sensitive data, as well as in providing traceability and transparency in the entire process, from the patient to the healthcare professional. Blockchains may contribute to breaking silos of healthcare information towards a more connected and open data environment.

The following two example initiatives show how blockchains can help solve compelling requirements in biomedical research and healthcare applications.

Through the unique blockchain architecture, the permanence of its data records, and other capabilities, blockchain technology and distributed ledgers create a means to increase the efficiency and transparency of any transaction-based environment. The use of blockchains may also help lower transaction costs. It is no wonder that blockchain technology and distributed ledgers are generating excitement across a myriad of potential business applications, and well beyond the field of cryptocurrency.

References:

Whitfield Diffie and Martin E. Hellman, New Directions in Cryptography: Invited Paper, IEEE Transactions on Information Theory, November 1976, https://www-ee.stanford.edu/~hellman/publications/24.pdf

Bitcoin: A Peer-to-Peer Electronic Cash System, 2008. https://bitcoin.org/bitcoin.pdf

For an introduction to this technology, see Intel SGX for Dummies: Intel SGX Design Objectives, https://software.intel.com/en-us/blogs/2013/09/26/protecting-application-secrets-with-intel-sgx

For a deep dive on Intel SGX, refer to Victor Costan and Srinivas Devadas, Intel SGX Explained, https://eprint.iacr.org/2016/086.pdf

BLOCKCHAIN MODELS: PUBLIC, PRIVATE, CONSORTIUM

Contributors : Philippe Genestier and Sajida Zouarhi, ORANGE

The blockchain infrastructure can take a number of different forms, depending on the context. Several implementation solutions exist, each meeting specific requirements and criteria. The various types of blockchain can be categorized as follows:

• **Public blockchains:** in this type of system, anyone can implement a transaction and block validation node (all that is required is the installation of the node software on a PC). The most well-known examples are Bitcoin and Ethereum. In this type of blockchain, the validator peers do not know each other and user confidence is based on the size of the community of validators, and on an incentive mechanism whereby honesty is the most profitable behavior. The downside is that the validation time for transactions and blocks is fairly long because of the mechanisms implemented (i.e., proof of work), which means that certain uses of the technology are not possible.

• **Private blockchains:** in this case, there is only a single validator, which provides very good performance in terms of validation time, because there is only one validation, and no need for a consensus process. The trade-off is that this is another example of the traditional situation, where there is a single third party to be trusted. For example, the solution proposed by Chain.com is of this particular type. This kind of infrastructure is not really a "blockchain" because it does not make it possible to guarantee that the data cannot be changed, or that it will not be corrupted by the third party. If the nodes belong to the same entity, then there is no need to replicate the blockchain on all nodes (other than to ensure redundancy) because if the third party wishes to modify or corrupt the register, it has control over all of the nodes. To save on costs, it makes more sense to go back to a centralized register rather than overuse storage capacities. In other words, it would be better to continue using a private database managed by the third party. This then comes back to the current traditional system, with the only difference being the structure of the data – in the form of blocks.

PART 3

BLOCKCHAIN APPLICATIONS FOR HEALTHCARE, SOME EXEMPLARS

vacy regulations, will need to adapt itself to these requirements, to the extent necessary.

Beyond the legal issues raised above, three main types of legal questions seem to be at stake when considering the blockchain:

- How to reduce risks (cyber risks, cyber fraud, data privacy breaches, etc.)?
- How to ensure trust in the system (through an appropriate certification, traceability of documents, governance, etc.)?
- When considering the placement of products on the market based on clinical trial results, how to ensure compliance with freedom of trade in view of the advantage that could be brought by a specific local or regional regulation adopted for the benefit of the blockchain?

Conclusion

Blockchain technology will need to respond to major legal issues in order to become an effective alternative technology for the collection of patient's consent.

As we may observe today, the blockchain and smart contracts may presumably be used to simplify clinical trials' procedures, but not to replace them.

Defining an efficient legal environment around the blockchain does not mean regulation at all costs, but rather a realistic regulation that will allow blockchains' promises and advantages to mature for the benefit of all. These include less fraud, reduced losses, and increased reliability of clinical trial results; more efficient and personalized practice of medicine; an incentive for private initiatives; a greater fluidity and transparency in the exchange of health data between professionals and patients and other stakeholders, hence lower healthcare costs; and more. Let's allow time for this innovative technology to take shape and develop itself, and when the appropriate time has come, assess how to regulate it adequately and set up governance and controlling mechanisms that shall be in charge of following up on these regulations…

- **Consortium blockchains:** here, validation is performed by several entities, but they are chosen and approved by the consortium. This means that we still have the trust aspect distributed over several entities, but without the constraints associated with resource-intensive consensus mechanisms such as proof of work used by Bitcoin, because the selection of validators makes it possible to reduce the risk in the system and therefore streamline validation processes. This type of blockchain can be used where the technology is implemented within an ecosystem of entities that all have a common interest in decentralizing a specific data-management process that can be linked to their area of activity. The consortium can take different forms and can involve a mix of companies, institutions, associations, and organizations of different types, and even smaller structures, provided they can make available the necessary IT resources (down to one physical person).

BLOCKCHAIN TECHNOLOGY – WHERE DO WE STAND?

Contributor: Issam Ibnouhsein and Karl Neuberger, QUANTMETRY

Many blockchain technologies have been developed in recent years, the most famous being Bitcoin, Ethereum, and Hyperledger. The following table compares them:

	Bitcoin	Ethereum	Hyperledger
Date of introduction	January 2009	July 2015	December 2015
Private / Public	Public	Public / Private	Private
Main application	Transactions (Bitcoin)	Smart contracts	Corporate applications
Cryptocurrency	Bitcoin	Ether	None
Verification	Proof-of-work: SHA-256	Proof-of-work: Ethash, Proof-of-stake	Pluggable consensus framework
Transaction time	≈10 min	≈14 sec	Custom
Confidentiality	No	Smart contracts: Yes Public blockchain: No	Yes

The **Bitcoin** blockchain is a transparent public ledger where all transactions are recorded, introduced in 2008 and developed since 2009[1]. This permissionless blockchain is the world's largest to date, with about 5300 servers and the most developed virtual territory, with over $1bn invested in Bitcoin firms. It allows fast peer-to-peer transactions and worldwide payment with low processing fees.

This blockchain uses the SHA-256 hash function as proof-of-work to secure the network. Its main drawback is the very limited set of possible script instructions. Therefore, the Bitcoin blockchain can perform only a small set of operations, mainly transactions of a currency-like token, but is secure and resilient.

1. https://en.bitcoin.it/wiki/Help:FAQ

Blockchain technology is based on the anonymity of stakeholders through the use of private and public keys. The system will therefore need to further structure itself in order to match the abovementioned identification requirements and provide the appropriate technological warranties to prevent fraudulent signatures, be it on the part of investigators, false patients, or other actors.

• *How to prove that the investigator's preliminary interview has been conducted properly and that all necessary information has been provided to the patient?*

Providing patients with appropriate information before they may consent to participate in a trial is a crucial step in the recruitment process and contributes to the validity of the trial's results. How can we combine this step with the fact of directly coding the consent form on the blockchain? Will the interview take place in front of a computer and the coding be performed by the investigator (or on the investigator's behalf) in the presence of the patient? Will there be a third-party trustee to ensure compliance with existing healthcare regulations? How will this trustee be designated? Following which training programs, to be provided by whom? Which will be the controlling and appeal authority in case of conflict? etc.

• *How to conciliate this way of using the blockchain with data protection regulations ?*

A direct coding of patient data brings patients even "closer" to the blockchain perimeter and susceptible to having their personal data made available. The question about such personal data being disclosed through the blockchain is therefore even more crucial than for blockchains' primary function as a simple register. To some extent, certain laws currently applicable, including French law, authorize the disclosure and use of personal health data provided they have first been anonymized by using pre-authorized techniques (no more individualization, correlation, or inference is then permissible per the WP29's anonymization guidance 05/2014 of April 10, 2014[22]). Does the anonymity supposedly ensured by the blockchain comply with these requirements which are specific to the data-privacy context? We saw above that the answer is negative, as the blockchain user may finally be identified even if it is difficult to do so. Considering the GDPR, we also see that the general tendency is towards a more stringent protection of personal data, both inside and outside EU borders, and we may presume that the blockchain technology, and not data pri-

22. https://webcache.googleusercontent.com/search?q=cache:PIBuim8Hvn8J:https://cnpd.public.lu/fr/publications/groupe-art29/wp216_en.pdf+&cd=2&hl=fr&ct=clnk&gl=fr

4. THE BLOCKCHAIN AS AN AUTOMATED GENERATOR OF SMART CONTRACTS

Let's now imagine the direct coding of patient's consent through the blockchain, i.e., no separate traditional consent-collection format would be used before the consent is coded on the blockchain. In other words, the patient's consent would be directly coded as a smart contract which would automatically generate his or her approval to be recruited for and participate in the clinical trial.

How could we then transpose the existing legal framework to the blockchain universe? Should it evolve? There are many questions to consider. For instance:

• *How to authenticate the patient's identity and his/her signature?*

Under French law, an electronic document has the same legal value as a document in paper format, provided its author can be duly identified and that this document can be established and stored in a way that guarantees its integrity (article 1366 of the French civil code). Likewise, an electronic signature is awarded the same legal force and embodies the consent of the signatory in the same manner as a hand-written signature, provided that a reliable identification process is used in relation to the document to which it relates (article 1367 of the French civil code). Note that resorting to a certified third-party service provider to authenticate the signature process is necessary for the presumption of validity of an electronic signature to exist. Similar rules apply at EU level.

The matter is of importance when we look at a recent decision in the United States against the electronic signature business leader DocuSign[21]: a bankruptcy court in California sanctioned an attorney and ordered him to complete a local e-filing course because he did not maintain copies of filed documents that included the original "wet" signature. Instead, the attorney relied solely upon the popular DocuSign e-signing technology when submitting legal documents in support of his claim (as is done in many commercial situations in the US and globally). The court determined that while DocuSign is appropriate in many business settings, overall it does not constitute a replacement for original signatures on legal documents and the like.

21. http://www.natlawreview.com/article/attorney-sanctioned-over-use-docusign-signatures-original-signature-means-original
http://norcalrecord.com/stories/511025237-bankruptcy-court-judge-rejects-docusign-signatures-as-authentic-sources-sanctions-attorney
https://www.law360.com/articles/818913/docusign-leads-to-sanctions-for-calif-bankruptcy-atty

The **Ethereum** was launched in July 2015 by the Ethereum Foundation, a Swiss non-profit[2]. This is an alternative to the Bitcoin technology, specifically targeted for smart contract users, with its own cryptocurrency (the Ether). Applications run on a custom-built blockchain, thus providing a global infrastructure that can transfer value and ownership of assets. Developers can create markets, registries of debts, or promises, and move funds in accordance with instructions given in the past.

The Ethereum blockchain uses a different hash function (Ethash) and supports Turing-complete script execution: any script can run. Another difference is the block time: set to 14 to 15 seconds for Ethereum, compared to Bitcoin's 10 minutes. This implies faster transaction times. However, the $50 million theft involving a DAO smart contract that occurred this summer raises security concerns.

Healthcare applications may be developed over the Ethereum blockchain. This is the case of myHealthIRL: a decentralized application where individuals can keep their own health records safe, maintain ownership, and then choose to share the data with healthcare providers or anyone else (e.g., a research pool).

The **Hyperledger Project** is a community of software developers building open-source blockchain frameworks and platforms for business, started in December 2015 by the Linux Foundation[3]. It is led by several contributors, including R3, IBM, and ABN AMRO, and will not develop its own cryptocurrency.

Currently, two projects are being incubated. The first, called Fabric, is the result of IBM's proposal merging with Digital Asset Holdings' proposal. This implementation of a blockchain technology is intended as a modular architecture for developing applications. The second project is Sawtooth Lake, Intel's modular blockchain suite, which supports both permissioned and permissionless deployments, including a new consensus algorithm: Proof of Elapsed Time (PoET).

Potential applications in the healthcare industry are being explored by the Hyperledger Healthcare Working Group (HLHC Working Group), formed in October 2016 with members such as Accenture, IBM, and Hashed Health. Its purpose is to foster technical and business-level conversations about promising applications for blockchain, and identify opportunities for near-term collaborations.

2. https://www.ethereum.org

3. https://www.hyperledger.org

Other notable blockchain technologies:

IBM: The IBM blockchain service on Bluemix is built on top of Hyperledger Fabric v0.5. It delivers a four-node development and avoids creating a network from scratch. A "Starter Developer" or "High Security Business" network can be developed.

Sidechain: A sidechain is a completely separate blockchain that runs in parallel to a main blockchain. Tokens can be transferred or synchronized between the two chains. Several sidechains, such as Blockstream, have been developed to provide further applications to the Bitcoin blockchain, among others.

Enigma: Enigma is a new encryption system that has not been launched yet. This decentralized cloud platform uses blockchain technology and should enable anonymous participants to securely share information with a third party, with a strong guarantee on privacy.

15 [access], 16 [rectification], 18 [limitation] and 21 [opposition] subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes… "

and "3. Where personal data are processed for archiving purposes in the public interest, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18, 19 [notification of rectification or erasure or limitation], 20 [portability] and 21 subject to the conditions and safeguards referred to in paragraph 1 of [Article 89] in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes."

Of course, without prejudice to any other required warranty imposed to data controllers and data processors, including obtaining the consent of the data subject where imposed by data privacy legislation, a minimum measure would be reinforcing the level of information of the data subject on the final registration of his or her personal data in the blockchain.

There is little doubt that eventually, the identification of blockchain users will become the standard for legally recognized blockchains as a proof of their reliability and compliance with applicable legal rules. At the same time, healthcare professionals will need to address the transparent nature of the blockchain to ensure that each transaction a user conducts is not linked or traceable back to the user (unless otherwise requested) in order to ensure privacy. From this point of view, there will need to be a way to make the ownership of the key effectively anonymous and each transaction untraceable except by the two transacting parties or the owner of the key. At the same time, all relevant parties may need to be identified in order to avoid the negative legal impacts of pure anonymity as identified above. In a private or consortium blockchain, for instance, this may be achieved through an appropriate contract between the relevant parties, stipulating among other issues, who shall act as the data controller or data processor and what is the scope of the data privacy rules to be followed.

All applications using a blockchain technology register data (including users' public keys and certain metadata) on a permanent basis and store them on numerous nodes outside the control of the individual to which this key belongs.

Erasing, rectifying, or "forgetting" this data would suppose that at least half the nodes work together in order to rebuild the blockchain as it existed before the data was added or withdrawn. During this reconstruction phase, data would no longer be up to date and the blockchain could not be used.

Erasing data therefore seems incompatible with blockchain technology, which stores the data in registers without erasing it. Indeed, the blockchain is not designed for data to be erased: each of the blocks composing the blockchain is supposed to constitute an indelible mark (hence the interest of blockchain in the field of product timestamping). Nothing would prevent some blockchain protocols from allowing for a history editing process, but this seems contrary to the supposed intangibility offered by the blockchain.

Are blockchains therefore intrinsically unlawful, from the standpoint of data privacy rules?

This purely legalistic approach of simply condemning a technology seems too absolute. Flexibility needs to be ensured, both on the legislation and the blockchain sides.

To this end, the following provisions of the GDPR may be used as a foundation:

Article 17, under which the right to be forgotten (or to erasure) may be restricted "… for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the [erasure] right is likely to render impossible or seriously impair the achievement of the objectives of that processing."

Article 20, under which the right to data portability "… shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller."

Article 21, under which the right to object to the processing may be restricted if "the processing is necessary for the performance of a task carried out for reasons of public interest."

Article 89, under which "(…) 2. Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles

ANALYSIS MATRIX FOR USE-CASES AND USAGES

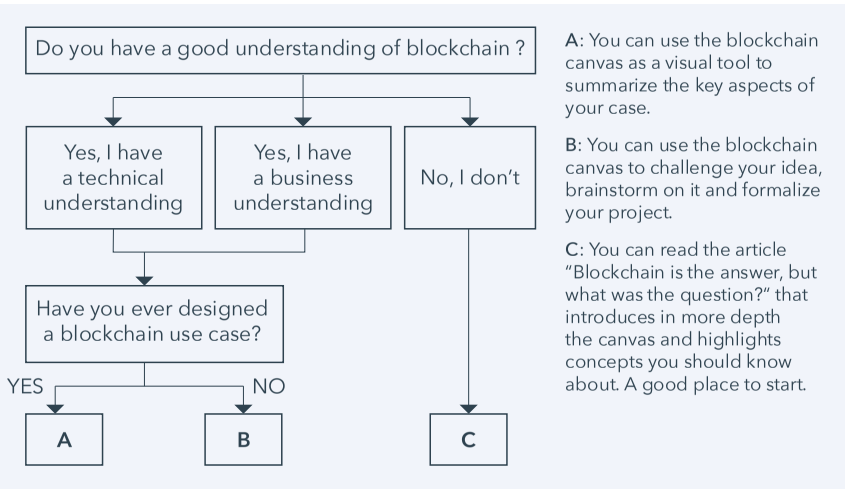
Contributor: Sajida Zouarhi, ORANGE

In this section, the intent is to provide a canvas that highlights the core components of any blockchain-based usages and helps readers decide whether to opt for blockchain. You can approach the blockchain canvas in numerous ways depending on:

- your familiarity with blockchain technology (high or low)
- your familiarity with blockchain use case (high or low)

The proposed canvas is a practical tool to check the relevance of the blockchain for a given use-case. It can help save precious time. It can also help understand and verbalize why the blockchain may be relevant to a given problem and a valuable ally in justifying the blockchain to coworkers. By answering the questions of the canvas in depth, you are actually writing your proposal, a document which you might very well share with your team, your manager or with the community. It is, however, important to understand that in some cases, you will not be able to fill all of the boxes. This may happen if your idea is too early stage.

How can the blockchain canvas be useful to me?



PROBLEM

Describe the problem that you are trying to solve.

ENTITIES AND CATEGORIES OF ENTITIES

- Specify the **quantity** and **diversity** of the entities. *For example: fewer than 30 (e.g.: private consortium), several hundred or several thousand (e.g.: Bitcoin).*
- Do they fall into the same category? *Examples of categories: companies, manufacturers, banks, institutions, associations, schools, private individuals, auditors, regulators, etc.*

DIVERGENCE OF INTEREST OF THE ENTITIES

- What is the status of the **trust** among the entities?
- What are the principal **causes of disputes**?
- Do the entities currently use a central authority or a trusted third party?

MOTIVATION OF THE ENTITIES

- What is the gain for the end user?
- What is the gain for the peers maintaining the network?
- Is the gain for the peers sufficient to discourage an attack or malicious behaviour?

SOLUTION

Describe the solution that you propose.

NETWORK PEERS

- Who are they?
- Are there more than one able to **write** or **view** data?
- Who among them are the validator peers?

DATA

Volume: Low/High

Criticality: Low/High

- Describe the type of your data.

VALUE

- Is your system based on (or does it use) a value system making it possible to **establish the link** between the blockchain and the real world?

TRANSACTIONS

Describe the transactions that will be performed on the blockchain.

NETWORK DYNAMIC

- What are the **rules** for **verification** and **validation** of a transaction?
- What is the rule for **consensus**?

TYPE OF PROCESSING

- Distributed **storage** (logs)
- Distributed **calculation** (conditions, use of oracles, contracts)

POINTS TO BE VERIFIED

- Indicate here the information that you are missing or the theories that you would like to verify. *For example: need for specific business expertise, need to identify the mose appropriate technology for your context.*

creet way.[17] Specialists also come to the conclusion that the public key, which is registered on the blockchain, is personal data in itself. Indeed, the concept of personal data is very broad, covering any information relating to an identified or directly or indirectly identifiable natural person.[18]

French and EU case laws tend to have an extensive understanding of this notion. For instance, they both consider IP addresses personal data, including dynamic IP addresses[19][20], even if an IP address alone does not allow the identification of the data subject. As soon as its correlation with other data allows identification of the person, then the IP address is considered personal data according to French and EU case laws.

In our view, the same applies to a blockchain user's public key: it does not allow for the direct identification of the user, but this identification may be achieved by using special technical means (e.g., tracing software) or third parties able to provide identification data to public authorities on the basis of the public key of the user (e.g., those regulated platforms which are bound to identify their clients pursuant to anti-bribery/money-laundering rules). The public key of the blockchain's user therefore does constitute personal data, and as a consequence, personal data is processed through the blockchain, which will be bound to comply with data privacy rules.

Besides, we need to distinguish between (i) the user accessing the blockchain through a private and public key and controlling his or her data, and (ii) the data subject whose data is contained in the blockchain in a structured or non-structured way – this data subject not being necessarily the user mentionned in point (i). If we focus on this second category of data subjects, we may assert even more strongly that personal data is present on a blockchain.

Then again, what about the compatibility of blockchains with data privacy rules, including data subjects' rights to have their data rectified, erased, or forgotten as now laid down by the GDPR?

17. Dalloz 2016, p. 1856, "Enjeux de la technologie de blockchain," by Yves Moreau, Professor at the Leuven University, Belgium

18. GDPR, article 4 http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=FR

19. French Supreme Court, First Civil Chamber – Decision no. 1184 of November 3, 2016 (15-22.595).

20. Decision of the EU Court of Justice of October 19, 2016, C-582/14.

3. THE BLOCKCHAIN AS AN AUTHENTICATION REGISTER

Let's imagine the collection of a patient's consent in the traditional way through an interview by the investigator, subsequently recorded, encoded, in a blockchain for registration purposes. The blockchain would then be used as a recording system to authenticate each patient's consent for participation in a given clinical trial.

This could demonstrate that healthcare professionals have complied with existing regulations (on how the interview of the patient was conducted, on whether the information provided to the patient was adequate, on whether consent was effectively collected, etc.). It may also guarantee data reliability, traceability, and ease of access.

However, to date, in this scenario, we still have no guarantee on a number of issues, such as the preservation of consent data integrity during the code transcription phase (who shall be authorized to conduct the coding, through which protocols, according to which language and security rules, under the control of which competent authority? etc.).

Also, blockchain use comes with a condition of transparency and intangibility in the content of blockchainized files (i.e., preservation of transaction history). How to reconcile this with applicable data privacy rules under which data controllers are bound to ensure the confidentiality of data subjects' personal data (especially health data that may be contained in these files) and data subjects' rights such as the right to rectify data, withdraw consent, and oppose data processing?[16]

The usual counterargument given to this is that the blockchain allegedly contains no personal data (generally hosted elsewhere, such as on a cloud server), only transaction footprints (hash), and works with the use

of a private key and public key, making user identification complicated unless users themselves initiate it. However, some blockchain specialists come to the conclusion that today the identity of a person may still be retrieved through a blockchain, hence the possible concern over personal data. In that sense, bitcoin is reputed to be an inefficient tool to carry out illegal actions in a dis-

16. This shall however be subject to the derogatory powers under Articles 9.2§4 or Article 89 of the GDPR as mentioned above.

PART 2

COLLECTION OF PATIENT'S CONSENT THROUGH THE BLOCKCHAIN: HIGHLIGHTS ON PRELIMINARY LEGAL ASPECTS

COLLECTION OF PATIENT'S CONSENT THROUGH THE BLOCKCHAIN: HIGHLIGHTS ON PRELIMINARY LEGAL ASPECTS

Contributor: Cécile Théard-Jallu, De Gaulle Fleurance & Associés
Date of preparation: October 15, 2017

Even though they undergo regular adjustments aiming at their constant enhancement, regulations governing the collection and processing of patients' consent in clinical trials have shown their inability to guarantee the total security of patient data, the perfect reliability of clinical trial results, or the adequate fluidity in the way patient data and trial results can be shared for the benefit of patients, medical professionals, and public health in general. In particular, current processes involved in the collection of patient consent may be seen as corruptible, non-transparent and not financially optimized. With its promise to create a new decentralized, and safe infrastructure, enabling the automatic registration of all kinds of transactions (such as a patient's commitment to take part in a clinical trial) in a more controlled, fluid, and fully transparent way, blockchain technology may well be the answer to the abovementioned difficulties. Let's have a look at what things already look like from a high-level legal standpoint.

1. THE SPECIFIC REGULATORY REGIME FOR THE COLLECTION OF PATIENT'S CONSENT IN CLINICAL TRIALS

In many countries, the collection of patient's consent to participate in a clinical trial is governed by a series of rules aimed at informing patients about the stakes of the trial and ensuring that they fully understand these stakes before expressly consenting to participate in the trial and to the related processing of their personal health data.

In particular, **blockchain technology raises the question of which jurisdiction has authority to handle situations triggered by use of blockchains,** considering that players may be located in different countries and subject to a variety of legal authorities.

A second crucial issue is how to identify the parties involved in those situations (e.g., parties to a contract, parties involved in a clinical-trial-related accident, or parties involved in an activity which does not comply with the regulations on clinical trials…). Indeed, the users of a blockchain are supposed to remain "almost" anonymous as in order to access their accounts (bitcoin, for example). The user needs to use a private key (the equivalent to a password), whose validity is checked by the network through the user's public key (using a cryptographic process). This private key will need to correspond to the public key. Although this does not constitute absolute anonymity preventing any future identification of the user, the complex pseudonymization mechanism operated through the blockchain is a serious hindrance to an easy identification and access to the user's identification data because among other reasons, the user keeps the control over the said data. This anonymity is often considered as an obstacle to the widespread adoption of blockchains.[14]

Another question is about which control mechanisms could be set up and how they should operate, evolve, and even be challenged, in order to guarantee that using a blockchain is reliable and secure, that fundamental principles of law are complied with during use, and that disputes are properly handled when these principles have been breached. New decentralized jurisdictions as well as arbitration have been proposed as the solution to these issues.[15]

At this very early stage of designing a legal landscape around blockchain technology and trying to identify its first legal impacts, let's have a look at the two main functions of the blockchain and see their legal consequences as well as the possibilities they offer regarding the collection of patient's consent in clinical trials.

A blockchain basically offers two key capabilities: the authentic registration of documents (see Section 3 below) and the automatic creation of "smart contracts" i.e. legal situations created through self-performing coded instructions when certain criteria are met (see Section 4 below).

14. *Blockchain et preuve*, Jérome Deroulez, Dalloz Avocat n°2 Février 2017 p.61.

15. Vitalik Buterin: *Blockchain and the future of courts*, www.bitcoinist.com, 27 avril 2016, http://bitcoinist.com/vitalik-buterin-blockchain-court/, in *Blockchain et preuve*, Jérome Deroulez, Dalloz Avocat n°2 Février 2017 p.61.

• **Luxembourg**, for its stock-exchange reporting services: Ethereum will provide a "digital signature" on all documents publicly disclosed by issuers, and new functionality will enhance security for issuers and transparency of LuxSE's certification service;[11]

• **Estonia** and its current experiment to secure the design and operation of a variety of public services such as e-residency, e-notary, or e-voting services, or patients' digital medical files;[12]

• **The Netherlands**, for the use of a blockchain-based digital ledger solution in the healthcare sector for communications between the country's health institutions, including hospitals and governement agencies.[13]

Private initiatives involving blockchain technology are more and more numerous. Interestingly enough, the blockchain resembles the Internet 20 years ago, when everyone thought it would be a new, lawless world. In reality, as for the Internet, one of the key issues for the success of blockchain technology will be regulation. Indeed, in our civilization, there is no place on earth, in the sea, or in space that is not governed by a rule of law emanating from a state or supra-state authority, and in most civil- or common-law countries, contracts must be attached to a state's legal system. Hence the following phrase, which we often hear about blockchain technology in relation to the coding of documents: "Code is law." This stands in opposition to another principle: "Law is code." If one wants the blockchain to become a sustainable technology, we think this second principle may not prevail over the first one and the "code" should definitely be "law."

The fact is that today, blockchain technology raises more legal questions than it answers. Indeed, as is generally the case for disruptive technologies, the blockchain is challenging established legal rules and posing challenges on a variety of topics, including intellectual property, data privacy, contracts, law of evidence, liability, insurance, international private law, and sectorial regulatory rules.

11. https://www.bourse.lu/blockchain-press-release
https://www.ethnews.com/luxembourg-stock-exchange-ethereum-secure-official-documents

12. https://news.bitcoin.com/estonian-health-records-secured-by-blockchain/

13. https://innovator.news/dutch-government-gets-legal-ok-to-use-blockchain-to-connect-healthcare-sector-fb070ad0fa8d

For instance, under French law[4], an interview of the patient shall be conducted by the investigator in order to provide the patient with a series of information about the trial (its purpose, methodology, duration, constraints and modalities, its benefits and risks for the patient, and the patient's right to receive specific care if his or her condition justifies it, while taking part in the trial). The patient shall then sign a form meant to expressly validate his or her consent to be recruited and for personal data, including health data, to be processed. The patient's consent shall be free, informed, and express. It shall be collected in writing for interventional trials with a given level of risks. Patient consent shall be collected again when a substantial change in the scope or conduct of the trial occurs. A new consent shall be sought in case the trial is renewed or extended, or if another trial is launched.

Patient's consent collection in medical trials is subject to strict data-protection rules. Among other provisions, the data manager shall ensure the security and integrity of patients' personal data as well as their individual data privacy rights, including the right to access and correct their own data, withdraw their consent, and oppose data processing.[5]

French law has recently been updated with a view to enhancing the patient-recruitment process (for instance, through an expanded intervention of ethical committees[6]). Beyond the procedure around the collection of patient's consent, the consequent use of patients' data will obviously be impacted by the more general legal landscape around the protection and processing of health data. For instance, under French law, if health data cannot be stored with adequate security measures by the healthcare center itself, it shall be entrusted to a duly authorized health data hosting company.[7] At the EU level, the new General Data Protection Regulation (GDPR) no. 2016/679 of April 27, 2016, which will automatically be enforceable in all European Member States' laws as of May 25, 2018, considers health data as sensitive data and forbids

4. In particular, articles L1121-1, L1122-1 and L1123-9 of the French Public Health Code.

5. Article 57 of the Act n°78-17 of January 6, 1978 as modified. Note that under the GDPR, these rights may be restricted (Articles 9.2, 9.3 and 17 of the GDPR).

6. Decree no. 2016-1537 of November 16, 2016 regarding researches on human beings
https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033394083&dateTexte=&categorieLien=id

7. Article L1111-8 of the French Public Health Code as recently updated by the Act no. 2016-41 of January 26, 2016 (among other measures, the French authorization process will soon be replaced by a certification process).

their processing unless it falls within a number of restrictively framed exceptions, including for the purposes of conducting clinical trials. More generally, it reinforces or creates rights for the benefit of data subjects and brings new constraints for data controllers and data processors within and outside the EU territory. Under certain conditions, these organizations will need to set up data registers, conduct privacy impact assessments (PIA) and other auditing measures, appoint data protection officers, give notice of data security breaches, and more. An overall obligation of privacy by design and privacy by default will need to be enforced. Severe sanctions may apply if the GDPR's provisions are breached: when non-compliant processing covers sensitive data such as health data, a fine of up to 20 million euros or 4% of the annual global turnover could be due, and operational measures such as compulsory suspension or interruption of data processing may also be meted out. Note the interesting rule under which each Member State will be entitled to derogate from the GDPR's rules with respect to the processing of health data (article 9.2 § 4) or the conduct of scientific research (article 89) by adding or maintaining specific conditions at a national level. In other words, EU Member States will have the possibility to protect further the rights of data subjects. Under article 89, data subjects' rights of access, correction, limitation or opposition may be restricted in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes of the research, and such derogations are necessary for the fulfilment of those purposes, subject to the adoption of the required warranties.[8]

8. http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679

2. HOW CAN BLOCKCHAIN TECHNOLOGY INTERACT WITH THIS LEGAL LANDSCAPE?

Today, there is no official legal recognition at a global or EU level of blockchain technology and the way it operates, in healthcare or other domains.

However, EU institutions are paying a strong attention to it with an apparent view to preparing coming regulations, for instance in the financial and banking sectors.

Legislation concerning blockchain technology is also being adopted at national levels. For instance, under French financial law, a first statutory recognition has been passed, in the form of an April 28, 2016, ordinance allowing for the entry of coupons in a shared electronic storage device for authentication purposes. The new Article L. 223-12 of the French Monetary and Financial Code hence defines a blockchain as a shared electronic recording system allowing the authentification of coupons' issuance and assignment operations. The Sapin II Act no. 2016-1691 of December 9, 2016, also authorizes the French government to legislate via ordinance on the use of shared electronic registers such as blockchains for the representation and transmission of unlisted shares or bonds. A draft ordinance has been published on September 19, 2017 and is on its way through the legislative procedure.[9]

Some governments have already started officially using blockchain technology for a variety of purposes, e.g.,:

• **The state of Delaware**, which is home to a majority of business incorporated in the USA, with its incentive plan to help businesses and state agencies use blockchain technology to distribute, share, and save ledgers and contracts, for instance in the data archiving domain. In July 2017, the governor of Delaware signed a bill into law making it explicitly legal for these entities to use blockchain technology for stock trading and record-keeping;[10]

9. https://www.tresor.economie.gouv.fr/Articles/2017/09/19/consultation-publique-projet-d-ordonnance-blockchain-titres-financiers

10. http://www.prnewswire.com/news-releases/governor-markell-launches-delaware-blockchain-initiative-300260672.html
https://corpgov.law.harvard.edu/2017/03/16/delaware-blockchain-initiative-transforming-the-foundational-infrastructure-of-corporate-finance/