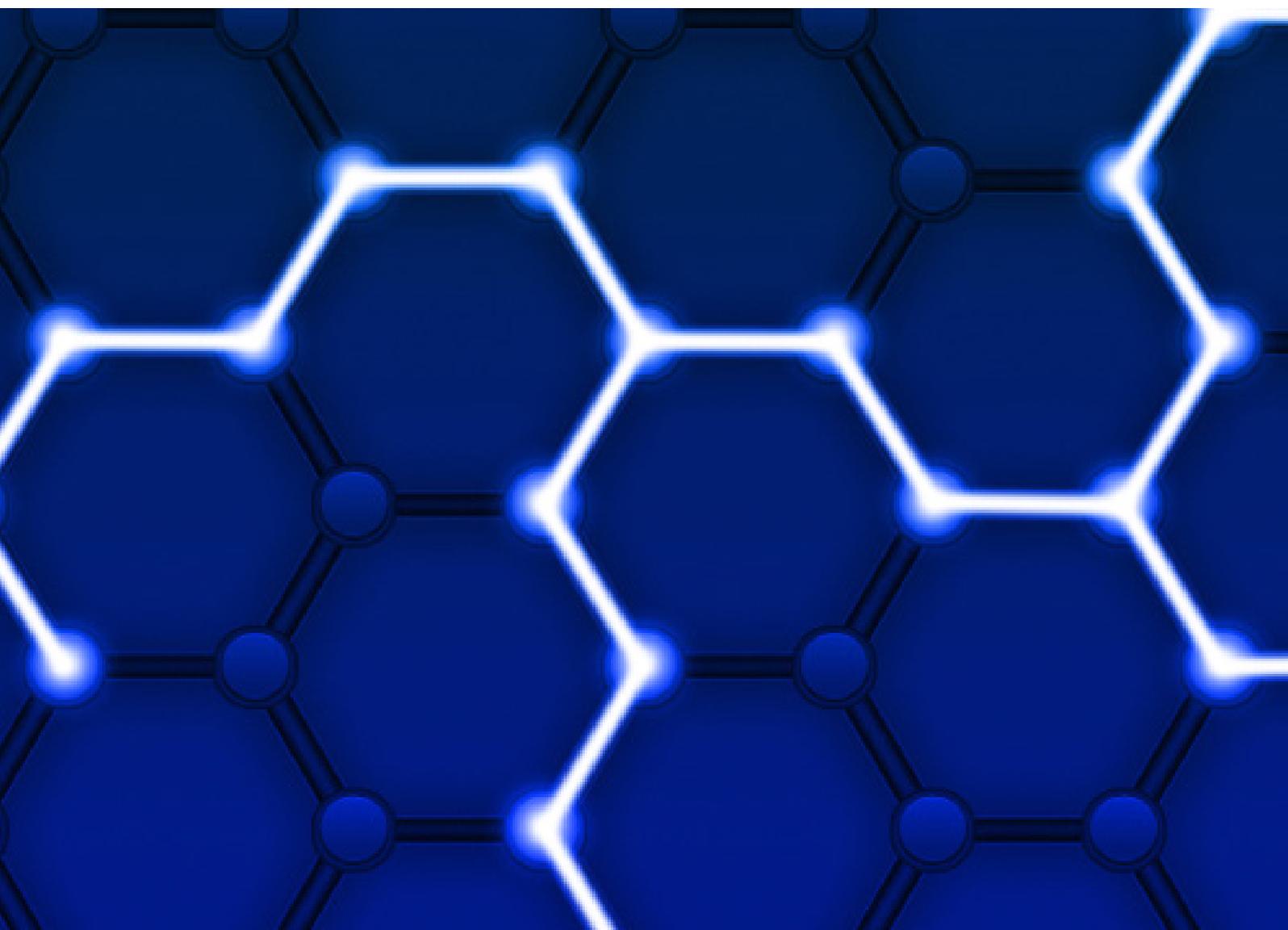


# ***BLOCKCHAIN :*** **FROM THEORY TO PRACTICE**

***The transformational challenges in adopting  
blockchain in large companies***



# Blockchain: from theory to practice

---

## The transformational challenges in adopting blockchain in large companies

October 2018

Cigref is a network of major French companies and public administrations set up in order to develop its members' ability to acquire and master digital technology. It is a key player and federating body in the digital society, thanks to its high-quality thinking and the extent to which it represents its members.

Created in 1970, Cigref is a not-for-profit body in accordance with the French 1901 Law of Associations. It counts among its members some 150 major French corporations and public administrations across all business sectors. It is overseen by 15 board members who are elected by the General Assembly. Its day-to-day work is carried out by a team of ten permanent members of staff.

 Intellectual copyright

All Cigref publications are made freely available to the general public but remain protected by the applicable laws on intellectual property.

Browse all our publications at [www.cigref.fr](http://www.cigref.fr) | Follow us on Twitter: [@Cigref](https://twitter.com/Cigref)  
Cigref, [21 avenue de Messine, 75008 Paris](https://www.google.com/maps/place/21+avenue+de+Messine,+75008+Paris), +33 1 56 59 70 00, [cigref@cigref.fr](mailto:cigref@cigref.fr)

# OVERVIEW

Blockchain is an extremely innovative information exchange protocol that cleverly combines known and well-understood technologies whose use can be disruptive in many sectors given the significance of its industrial potential by removing the disintermediation who today act as trusted third parties as well as by providing security and fast service while reducing costs.

While it may be considered a threat by some people since it removes middlemen or makes certain business models obsolete, or is seen as an opportunity by others to simplify exchanges, many agree that blockchain should bring about significant changes in inter-company relations, potentially revolutionising their business models.

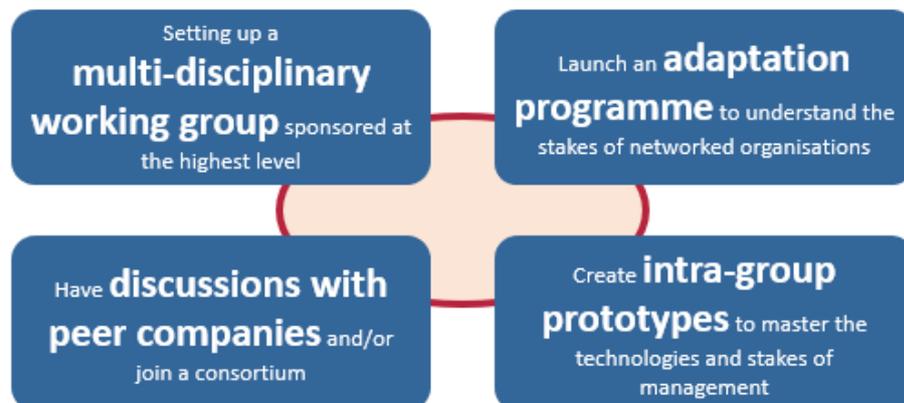
Although we present different types of blockchains, this document is intended to help managers and decision-makers understand this protocol's impacts and the challenges for business in culture, legal, management and technology.

It reinterprets the notion of "trusted third party" in light of the paradigm shift that blockchain involves: going from x2y2x (B2B2B, C2B2C, etc.) to x2x, or, in other words, how to go from a traditional hub-and-spoke exchange model to a collaborative network model where trust is no longer centralised in a (trusted) third party but distributed among all participants in a blockchain.

This document also focuses on two aspects:

- blockchain's legal approach so that lawyers and IT professionals can understand each other and work together.
- the impact on the IT function by explaining how blockchain can entail significant changes to the technical IT teams that implement it.

Finally, to put the theory into practice, we suggest decision-makers four possible ways to take action as soon as possible:



# ACKNOWLEDGEMENTS

We would like to thank Patrick LAURENS-FRINGS, CIO at CAISSE DES DÉPÔTS, who led this study as well as all members of the Cigref working group:

François BANOS - RENAULT	Jean-Yves LEONNEC - ORANGE
Alain BARBAY - MINISTÈRE DE L'INTÉRIEUR	Olivier LIGNEUL - EDF
Jean-Charles BASTOUL - MINISTÈRE DE L'INTÉRIEUR	Philippe LOMBARD - EDENRED
Jeff BETBEDER - LVMH	Olivier MALE - GENERALI
Pierre BLANC - CARREFOUR	Christophe MARQUAILLE - MINISTÈRE DE L'INTÉRIEUR
Marc BOGET - MINISTÈRE DE L'INTÉRIEUR	Marko MICHAUD - SCOR
David BOUCHER - NEXITY	Jean-Christophe MONTIGNY - MINISTÈRE DE L'INTÉRIEUR
Romain BRUNIAS - SAINT-GOBAIN	Emmanuel MONZIES - GROUPE PSA
Guillaume CHEVALLIER - GROUPE POMONA	Fabio OLIVEIRA - RENAULT
Arnaud FAISSOLLE - CARREFOUR	David QUANTIN - MATMUT
Nadia FILALI - CAISSE DES DÉPÔTS	Marc SANCIER - LABORATOIRES SERVIER
Nicolas FORGUES - AIR FRANCE KLM	Remy SAUDREAU - MINISTÈRE DE L'INTÉRIEUR
Pierre GACHON - RENAULT	Nicolas TARDY - MALAKOFF MÉDÉRIC
Franck HAVARD - GROUPE POMONA	Pierre TARIF - ENGIE
Laurent HEMERY - CNAF	Phonesyraphay THOUMAKED - MALAKOFF MÉDÉRIC
Michel HUTIN - ARKEMA	Frédéric TRAN DU PHUOC - SOCIÉTÉ GÉNÉRALE
Cédric KROURI - GROUPE ADP	Bastien VOITURIEZ - CAISSE DES DÉPÔTS

In particular, we would also like to thank Sylvie DE THÉSUT DUFOURNAUD, manager of the intellectual property and new technologies department at CAISSE DES DÉPÔTS, for her legal insights into blockchains.

This document was written by Frédéric LAU, Cigref Mission Director, with help from Laurent FRISCOUR, CEO of postme.io.

## Table of contents

Foreword .....	1
Introduction .....	2
<b>1. Blockchain: a particularly disruptive concept .....</b>	<b>3</b>
1.1. The decentralisation of telecommunications .....	3
1.2. The decentralisation of information .....	3
1.3. The decentralisation of transactions .....	4
1.4. The origin and recent developments of the blockchain protocol .....	4
<b>2. The different types of blockchains .....</b>	<b>6</b>
2.1. Public blockchains .....	6
2.2. Consortium blockchains .....	7
2.3. Private blockchains .....	8
2.4. The (current) choice of large companies .....	8
<b>3. Information exchange and transaction security as a new factor of business performance .....</b>	<b>9</b>
3.1. Ensuring the quality, traceability, and real-time availability of data .....	9
3.2. Providing objective proof of data's existence .....	9
3.3. Smoothing digital processes .....	10
3.4. Qualifying data upstream instead of downstream .....	11
<b>4. A paradigm shift .....</b>	<b>12</b>
4.1. Switching from X2Y2X to X2X .....	12
4.2. Third parties disappear, but not their function .....	13
<b>5. The challenges for large companies of adopting blockchain .....</b>	<b>14</b>
5.1. Cultural challenges .....	14
5.1.1. Understanding the benefits of the concept .....	14
5.1.2. Accepting a transaction system that is natively secure without control .....	14
5.1.3. Accepting and anticipating the consequences of the disappearance of the activities of trusted third parties concerned by blockchain .....	15
5.1.4. Partner actors .....	15
5.2. Governance challenges .....	15
5.2.1. Establishing a consensus between actors .....	15
5.2.2. Defining operating rules .....	15
5.2.3. Defining an economic model .....	15
5.3. Legal challenges .....	16
5.3.1. Dividing responsibility .....	16
5.3.2. Establishing regulatory and conflict management mechanisms .....	16
5.4. Technological challenges .....	16
5.4.1. A technological base accepted by all participants .....	16
5.4.2. Securing the development environment .....	16
5.4.3. Rethinking how we work .....	17

5.4.4. Tracking the development of a still-unstable ecosystem .....	17
6. Blockchain's legal approach .....	18
6.1. Getting into phase with the legal perception .....	18
6.2. Legal questions .....	19
6.3. The various challenges related to the legal aspects .....	20
7. Impact on the IT function .....	22
8. And Monday morning? .....	24

## Table of figures

---

Figure 1: Public blockchain .....	6
Figure 2: The promise of public smart contracts .....	6
Figure 3: Consortium blockchain .....	7
Figure 4: Private blockchain .....	8
Figure 5: Moving trust in the actors .....	11
Figure 6: Going from a hub-and-spoke model to a network model .....	12
Figure 7: Key questions to ask when creating a consortium blockchain .....	14
Figure 8: Stakes related to blockchain's legal aspects .....	20
Figure 9: The benefits of blockchain <i>vis-à-vis</i> the IT function .....	23

# Foreword

---

According to Michel Serres, "Man is this animal whose body loses its functions little by little".<sup>1</sup> Humans invented objects that, to be precise, have progressively "outsourced" their functions "outside" the body: the wheel imitates the rotation of the knee and hip; a hammer is an imitation of the hand and arm. Historically, several fundamental changes and innovations have been based on this mechanism of gain and loss: for example, printing as it relates to memory, and digital tools as they relate to space. Today, the digital revolution is taking this idea of "outsourcing" very far since all intellectual tasks are within automation's reach. It's the most extraordinary of objectifications.<sup>2</sup>

So what is left for humanity? Trust, perhaps? Anthropologically speaking, human beings are social creatures in the sense that we build and progress in and through relationships with others. As a result, we live in social ecosystems where we are interdependent with other human beings. Communication, cooperation, and collective actions are strengths that humanity has developed throughout our evolution to compensate for our biological weaknesses.

To survive, human beings must interact and cooperate with our peers by engaging in exchanges of goods and services. Transactions are the cornerstone of social and, by extension, economic interaction. Trust is at the origin of reciprocal concessions. To ensure that this trust is kept at its highest level, humanity has created an ecosystem of trust that includes jobs called "trusted third parties" subject to regulations that guarantee the integrity of the people or organisations that hold this trust.

This ecosystem of trust has its limits, which are intrinsically linked to humans ourselves. Blockchain is a new concept that relies on digital technologies that shake up the established order. It too will outsource functions and tasks related to trusted third parties to the point of changing profoundly how they work. Above all, it will create value for businesses who work in the trust market by changing the interactions with their partners independently of the company's business function by changing the information transfer processes that underlie transactions.

Blockchain is a new concept that demonstrates that a mechanism that does not require people can bring trust to a transaction through an unalterable protocol.

---

<sup>1</sup> Inria 2007 Conference - "*Les nouvelles technologies : révolution culturelle et cognitive*"  
<https://www.youtube.com/watch?v=ZCBB0QEmT5g> (in French)

<sup>2</sup> Objectification is the mental act that makes an abstract idea perceptible, expresses something, creates it, defines it, gives it a concrete form. By extension, objectification signifies the process by which knowledge tends towards objectiveness and takes on a universal value.

# Introduction

Before anything else, we must remember that a blockchain is not a "technological" innovation; it implements known, controlled technologies (data storage, cryptography, distributed systems (peer-to-peer), etc.). The clever combination of these technologies gives birth to this concept by defining an extremely innovative information exchange protocol.

Thus, blockchain is a protocol that can disrupt many sectors and concerns all companies. Its industrial potential is significant in that it removes all intermediaries who act as trusted third parties as well as reduces costs, provides security (a blockchain is considered inalterable), fast service (validation time is generally low, notably when consortiums are involved<sup>3</sup>).

For certain sectors, this is a threat (by the risk of removing intermediaries or making certain business models obsolete); for others, this is an opportunity (by simplifying exchanges with direct transactions). Finally, blockchain may allow us to implement true interoperability between connected objects (IoT).

Therefore, many people agree that this protocol should result in profound changes in inter-business relationships and within the IT department over the next few years. Some even state that it could cause a breakthrough on a scale comparable to the arrival of the web in the 1990s and revolutionise businesses' economic models.

This is why Cigref undertook a study and gathered a working group on the subject. This working group's goal was:

- On the one hand, to help a CIO explain, in appropriate language, to an executive the stakes involved in blockchain and why they should pay attention to it.
- On the other hand, to raise awareness among CIO and their teams of the stakes to give them the tools to understand it and support business units in their reflections on use cases.
- Finally, to identify and capitalise on existing initiatives.

This document is not intended to explain blockchain protocols in detail. These are very clearly explained on websites such as Blockchain France (in French)<sup>4</sup>.

Although the subject is new, the working group prioritised discussions that centred on feedback on potential use cases or existing experimental projects instead of technical discussions with experts on the topic.

<sup>3</sup> Wait time can vary (depends on the block's propagation and validation time) depending on the protocol: while it is near-instant for certain consortium protocols, it can take several seconds or minutes between Ethereum and Bitcoin.

<sup>4</sup> <https://blockchainfrance.net/>

# 1. Blockchain: a particularly disruptive concept

In 1494, Luca PACIOLI<sup>5</sup> (1447-1517) invented and codified "double-entry bookkeeping" in a work entitled "*Summa de arithmetica, geometrica, proportioni et proportionalita*"<sup>6</sup>. Even today, this reference work is considered as the single model for representing the accounts of all economic organisations.

**It is this model, used by all, that blockchain threatens to disrupt.**

In the history of the internet, two major disruptions have occurred: the decentralisation of telecommunications and the decentralisation of information. Blockchain, with the decentralisation of transactions, promises to be a third chapter in line with the previous two.

## 1.1. The decentralisation of telecommunications

In 1974, the TCP/IP protocol was formalised by Vinton G. CERF and Bob KAHN<sup>7</sup>. It allows to decentralise telecommunications by meeting the goal of being free from the telecommunications operators, which were very centralised at the time.

The US Defense Department experimented with this protocol in its multi-node network ARPANET<sup>8</sup> based on NCP<sup>9</sup> to homogenise and build a robust network to withstand possible aggressions against communication centres. But it wasn't "officially" adopted until 1 January 1983, the military reserving for itself MILNet, the military version of ARPANET<sup>10</sup>, and leaving civilians with a version of ARPANET that, in 1985 with the NSFNet<sup>11</sup> programme, resulted in the internet we know today.

## 1.2. The decentralisation of information

On 12 March 1989, Tim Berners-Lee filed a document at CERN called "Information Management: A Proposal"<sup>12</sup> that proposed a distributed information system using hypertext technologies to link CERN's scientific documents.

This document defined the basic protocols of the web: HTTP (to locate and link documents) and HTML (to create pages). The first website to apply these protocols was the CERN website in 1990: info.cern.ch. But it was really in 1994, with the first website directory Yahoo and the Netscape browser (1993), that public browsing of web servers took off.

<sup>5</sup> [https://en.wikipedia.org/wiki/Luca\\_Pacioli](https://en.wikipedia.org/wiki/Luca_Pacioli)

<sup>6</sup> <http://cerebro.xu.edu/math/Sources/Pacioli/summa.pdf>

<sup>7</sup> <http://www.cs.princeton.edu/courses/archive/fall06/cos561/papers/cerf74.pdf>

<sup>8</sup> <https://en.wikipedia.org/wiki/ARPANET>

<sup>9</sup> [https://en.wikipedia.org/wiki/Network\\_Control\\_Program](https://en.wikipedia.org/wiki/Network_Control_Program)

<sup>10</sup> <https://en.wikipedia.org/wiki/MILNET>

<sup>11</sup> [https://en.wikipedia.org/wiki/National\\_Science\\_Foundation\\_Network](https://en.wikipedia.org/wiki/National_Science_Foundation_Network)

<sup>12</sup> <http://info.cern.ch/Proposal.html>

### 1.3. The decentralisation of transactions

Blockchain is the third chapter, after the decentralisation of telecommunications and then information, that seeks to define a set of protocols that allow us to consider a decentralisation of transactions in a transparent and secure way without a central control authority.

### 1.4. The origin and recent developments of the blockchain protocol

The disruption caused by blockchain lies in the ability to remove exchange intermediaries **without control but with trust**, which would directly impact the various transaction monopolies that exist in the banking, healthcare, insurance, real estate, education, music, or even government sectors.

Blockchain promises a breakthrough, indeed a revolution "in development", but with extraordinary potential. French companies, and especially Cigref companies, don't see it as a utopia.

We must not repeat past errors such as the misunderstanding of the internet's impact on the French economy described in 1994 in the report by Gérard Théry<sup>13</sup> on "les autoroutes de l'information"<sup>14</sup>. This report recognised the internet's existence, but felt that it had no future because, among other reasons, its cooperative operating model was not designed to offer commercial services. Or, Jeff Bezos founded Amazon in the United States in the same year, which became the world leader in commercial services on the internet in less than 15 years!

In 2008, while the sub-prime crisis was getting underway, and a crisis of trust in the American banking system was developing, Satoshi Nakamoto<sup>15</sup> published the bitcoin blockchain protocol under MIT Licence. This protocol provides an elegant and clever solution to the problem of **the online exchange and validation of transactions in total confidence in a decentralised way**. In 1998, American Nick Szabo<sup>16</sup>, a computer scientist, legal scholar and cryptographer designed a decentralised digital currency mechanism called "*Bit Gold*", but the technology was not yet ready.

In 2009, Satoshi Nakamoto started the first application based on this protocol to create the **cryptocurrency** bitcoin. This application reflects a libertarian spirit that tries to free itself from banking and financial organisation in a form of decentralised collaboration for exchanges and transactions.

In October 2015, the magazine *The Economist* revealed to the public the significance of blockchain and ran its cover story<sup>17</sup> on "*The trust machine: the technology behind bitcoin could transform how the economy works*".

<sup>13</sup> [https://fr.wikipedia.org/wiki/G%C3%A9rard\\_Th%C3%A9ry](https://fr.wikipedia.org/wiki/G%C3%A9rard_Th%C3%A9ry) (in French)

<sup>14</sup> [Http://www.ladocumentationfrancaise.fr/rapports-publics/064000675-les-autoroutes-de-l-information](http://www.ladocumentationfrancaise.fr/rapports-publics/064000675-les-autoroutes-de-l-information) (in French)

<sup>15</sup> <https://bitcoin.fr/satoshi-nakamoto/> (in French)

<sup>16</sup> [https://en.wikipedia.org/wiki/Nick\\_Szabo](https://en.wikipedia.org/wiki/Nick_Szabo)

<sup>17</sup> <http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine>

## Blockchain: from theory to practice

---

The transformational challenges in adopting blockchain in large companies

While it suffered from a rather negative reputation in 2016<sup>18</sup>, bitcoin was the first successful implementation of a decentralised consensus structure with the lack of any regulatory authority. In blockchain, we can see the operational reflection of Lawrence Lessig's saying, "Code is Law"<sup>19</sup>.

In the last two years, the development of the blockchain concept has not only been borne by cryptocurrencies, which may have raised doubts about the concept's sustainability, but also by **the appearance in many different sectors of the first "scaled" applications** (the Banque de France's MADRE project<sup>20</sup>, food traceability in mass retail<sup>21</sup>, the B3i consortium in the insurance sector<sup>22</sup>, and, very recently, the World Bank's issuance of bonds<sup>23</sup>, etc.)

---

<sup>18</sup> <https://bitcoin.fr/bernard-debre-demande-linterdiction-des-bitcoins/> (in French)

<sup>19</sup> <https://framablog.org/2010/05/22/code-is-law-lessig/> (in French)

<sup>20</sup> <https://blockchainpartner.fr/comprendre-projet-blockchain-de-banque-de-france/> (in French)

<sup>21</sup> [https://www.challenges.fr/entreprise/grande-conso/carrefour-lance-la-premiere-blockchain-alimentaire-d-europe-pour-une-tracabilite-totale-des-produits\\_571731](https://www.challenges.fr/entreprise/grande-conso/carrefour-lance-la-premiere-blockchain-alimentaire-d-europe-pour-une-tracabilite-totale-des-produits_571731) (in French)

<sup>22</sup> <https://b3i.tech/home.html>

<sup>23</sup> <https://www.latribune.fr/entreprises-finance/banques-finance/pourquoi-la-banque-mondiale-a-emis-la-premiere-obligation-sur-la-blockchain-789401.html> (in French)

## 2. The different types of blockchains

### 2.1. Public blockchains

Public blockchains are almost all developed and maintained by communities of independent developers (in Open Source) and seek a complete disintermediation of historical trusted third parties.

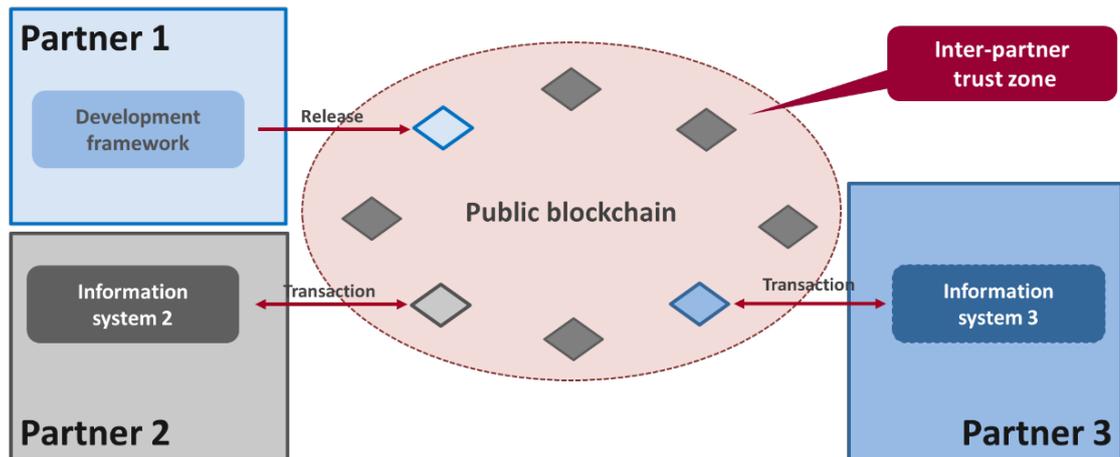


Figure 1: Public blockchain

They promise to support micro-services in the form of "smart contracts<sup>24</sup>" that seek to amplify the breakup of value chains as happened when apps appeared on smartphones.

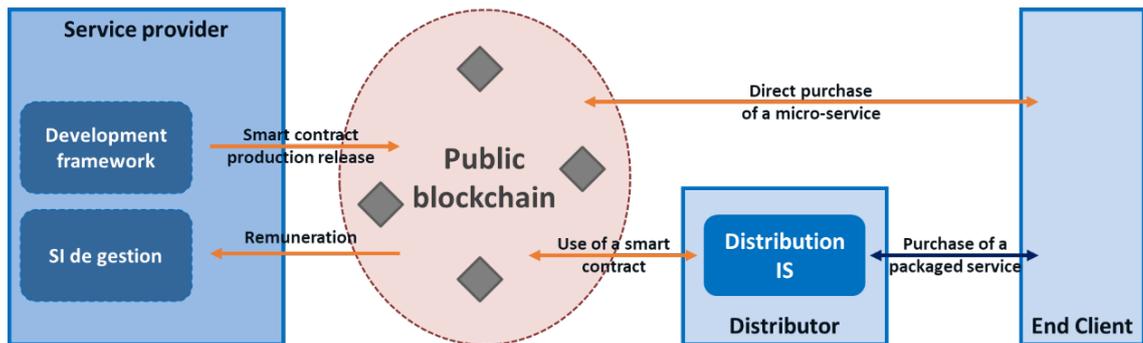


Figure 2: The promise of public smart contracts

Public blockchains stand out by the fact that they rely entirely on the trust that we can place in the computer code that underlies the exchanges. We can highlight the strong resilience of the bitcoin blockchain that has existed for nine years now.

Legal thinking is beginning to formalise concerning blockchain:

- for example, through the French "eIDAS"<sup>25</sup> regulation of 23 July 2014 that establishes a common base for secure electronic interactions between citizens, business, and public authorities,

<sup>24</sup> A "smart contract" is an autonomous programme (in the form of a web service, for example) that, once started, automatically executes the conditions defined previously and written in the blockchain (Blockchain France definition)

<sup>25</sup> <https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-reglement-eidas/>

The transformational challenges in adopting blockchain in large companies

- as well as the French decree of 28 September 2017 concerning the presumption of reliability of the signature method since blockchain implements **cryptographical procedures similar to electronic signatures**,
- or areas of **compatibility or convergence with the GDPR** (General Data Protection Regulation).

However, the transnational character of transactions, particularly in the case of public blockchains, can result in **legal insecurity**. Indeed, whether in common law<sup>26</sup> or civil law<sup>27</sup>, the legal environment and interpretation is not uniform.

Beyond the legal uncertainty, and despite the ongoing debates and studies, it's above all the novelty of the blockchain concept that has led to **low take-up among companies of public blockchains** and causes them to turn to consortium or private blockchains. However, we have observed that companies that have matured in this area tend to create an increasing number of links with public blockchains given their transversal and universal nature.

## 2.2. Consortium blockchains

Consortium blockchains rely on software developed by public blockchains, but **instance them in environments that we can call "privatised"**.

Indeed, unlike public blockchains where anyone can download the blockchain programme, mine<sup>28</sup> transactions and perform direct exchanges, the nodes of a consortium blockchain are implanted *a priori* inside consortium members' datacentres and source software updates can be inspected by the consortium *a priori*.

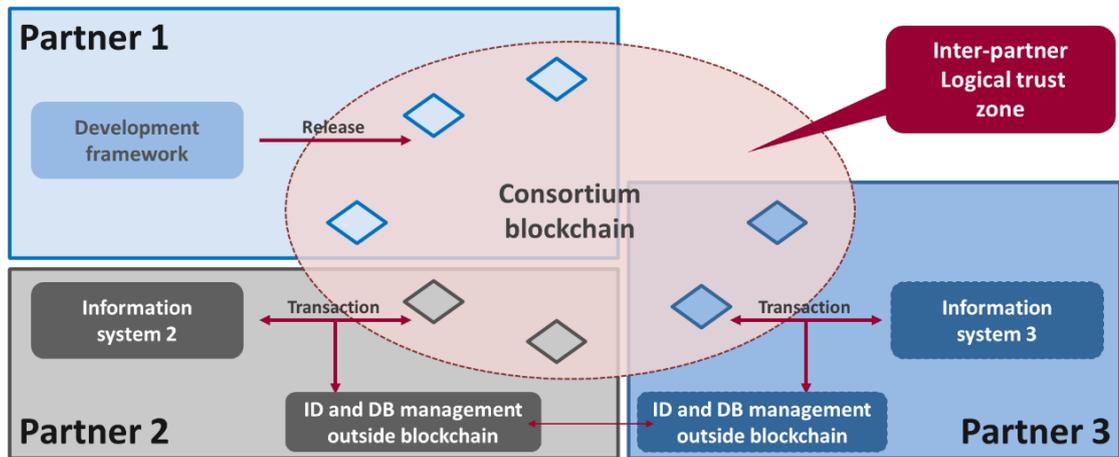


Figure 3: Consortium blockchain

The main advantage of consortiums can be found in the B2B world where this kind of blockchain **simplifies marketplace systems** and potentially reduces transaction costs.

In a legal aspect, consortium blockchains offer an acceptable security potential that must nevertheless be **formalised in a consortium agreement** that covers all legal risks, beginning with those borne by the former trusted third parties.

<sup>26</sup> The legal system that applies in English-speaking and Commonwealth countries

<sup>27</sup> The European legal system based on codified law derived from Roman law

<sup>28</sup> Mining is the use of computer processing power to process transactions, secure the network, and allow all system users to stay synchronised (Blockchain France definition)

The transformational challenges in adopting blockchain in large companies

In a technical aspect, setting up a hybrid architecture that mixes traditional and blockchain architecture created a **technical trusted space** at low cost by capitalising on blockchain's potential in an environment that is secured in a traditional manner (notably for managing identities, databases and inter-partner flow exchanges).

### 2.3. Private blockchains

Technically, private blockchains are consortium blockchains but **applied to different units within the same company or organisation**. The advantages of implementing these systems lie in **simplifying and smoothing** intra-business exchanges by substituting the control nodes of shared systems.

The first application the working group observed in companies concerned synchronising repositories and financial data.

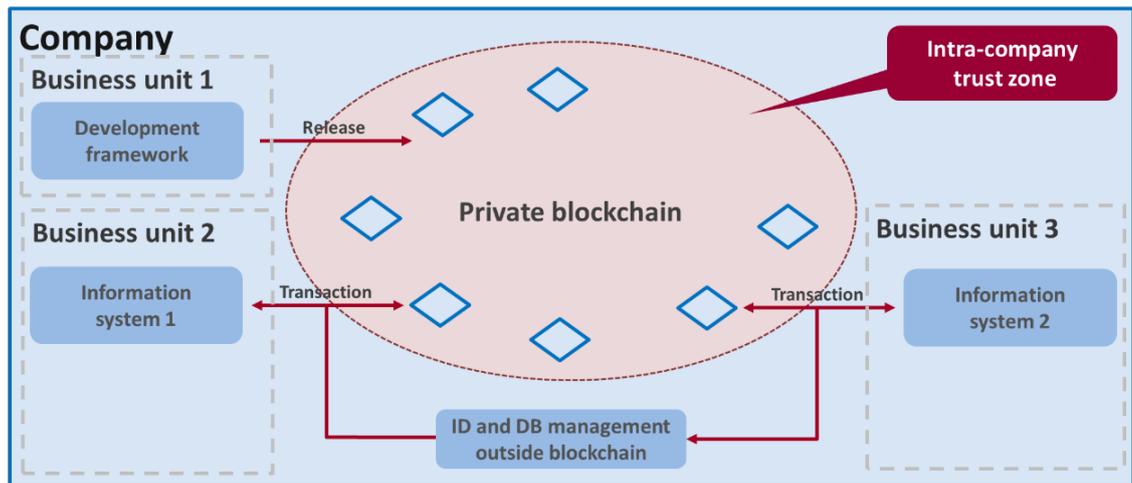


Figure 4: Private blockchain

### 2.4. The (current) choice of large companies

Given the lack of a secure legal environment for public blockchains, **nearly all projects at large companies are currently based on either private or consortium blockchains**. This allows businesses to enjoy the benefits of simpler inter- or intra-company transactions, currently concentrated in "back office"-type transactions.

Note that these companies, while benefiting from the savings these blockchains bring, cannot expect a competitive advantage within their ecosystem since **all consortium participants have the same advantage**.

These systems, whose scale is by definition limited, also have the drawback of not being able to bring the company into contact, through the blockchain, with all of the populations and economic actors in the B2C universe. This technical-legal-regulatory mechanism that should allow this relationship with the wider public remains to be invented, and to transpose the benefits of trust distributed "at scale" in the economic universe beyond simple cryptocurrencies like bitcoin.

## 3. Information exchange and transaction security as a new factor of business performance

### 3.1. Ensuring the quality, traceability, and real-time availability of data

Blockchain is not a concept that responds to all of a company's problems: a traditional database can fulfil many use cases. However, if this database must be read- and/or write-accessible by many actors who do not trust each other, then a blockchain fulfils this use case perfectly.

The principle of a database has stayed the same for decades. In an increasingly connected society where the exchange of information becomes a new factor of performance, transparency, and productivity for businesses, this tool works very well when isolated. When it comes to link with it, trust comes into question, particularly the issue of **data reconciliation**.

In the classical information exchange model, data intended to be shared among partners relies for a moment on asymmetrical transactions that results in a dissymmetry of information between the various parties. To create symmetry, participants add layers of synchronisation. This synchronisation's complexity is overcome by intermediaries that play the role of trusted third parties (for example, clearing houses in the finance industry) who use computing protocols such as EDI<sup>29</sup> with open and/or proprietary formats. **Information symmetry is the victim of this defence paradigm where everyone protects their data for staying its integrity.**

Blockchains allow for remove the transactional processes with these third parties: the same transaction is used simultaneously for negotiation, payment and delivery of information, insuring a near real-time availability of the data and the traceability of its ownership<sup>30</sup>.

### 3.2. Providing objective proof of data's existence

With blockchains, this paradigm of defence where everyone protects their data to insure its integrity is replaced by a new paradigm of **decentralised trust**, where data is unchanging and transparent among the various participants of a transaction and a process. This concept also offers a **traceability and auditability independent of the data**. Blockchain provides **objective proof** of the existence of data through a consensus around the data's status at a given moment that no one can question (thanks to the use of mathematical formulas and cryptographic protocols). Notably, it allows for a timestamp.

In the near future, we can imagine the emergence of decentralised applications that will remove the traditional notion of information transmission in favour of the secure sharing of information.

<sup>29</sup> EDI: Electronic data interchange. An electronic protocol (defined in the 1980s) that allows for the exchange of data about transactions through networks and standardised formats (for example, XML, EDIFACT, etc.).

<sup>30</sup> See the Paris Europlace report "Les impacts des réseaux distribués et de la technologie *blockchain* dans les activités de marché" (in French)  
[https://www.paris-europlace.com/fr/file/2867/download?token=h3\\_Q1t6V](https://www.paris-europlace.com/fr/file/2867/download?token=h3_Q1t6V)

**Use case: Information symmetry**

When a buyer receives an invoice from their supplier, and they accept this debt since it matches the goods delivered according to the conditions set out in the contract, the seller **does not automatically have this information** and is unable to use it. At the moment the buyer accepts the invoice, **information becomes asymmetrical**. The seller performs an epistolary action to capture this information by matching<sup>31</sup> third-party information in their accounts after accounting for client payments. This asymmetry of information requires time and resources to **reconcile the information in partners' systems** (banks, credit organisation, etc.).

In this example of invoicing, suppliers can use this **information symmetry** concerning an invoice's status by using blockchain's abilities. Through a smart contract, a buyer who approves an invoice registers this information **directly in the blockchain**. This information becomes available immediately, and potentially to other third parties connected to the blockchain, such as a factor<sup>32</sup> or a credit insurer. The exploitation of this **information symmetry between all actors could allow** the seller to obtain instant financing for his or her invoice **while reducing processing costs**.

### 3.3. Smoothing digital processes

One of the goals of dematerialisation projects is to **make processes smoother by reducing human control**. But if these processes are not secure enough, digitising them can cause a loss of data integrity, especially in an environment where partners have little trust for each other.

As we saw earlier, blockchain is a protocol that builds trust in the reality and truth of a piece of data shared between several actors. It offers real-time, automated proof that a digital process was successful, making audits much easier.

In a traditional digital process, participants send dematerialised data that is processed sequentially by each participant. In this approach, trusted third parties define the management rules of data validation/qualification at each step and intervene when the data is generated and viewed by each participant, as well as in the data's traceability.

In a decentralised process, once the data has been produced or changed, it is duplicated throughout the network and made available to all those who would like to track it. **Thus, each network participant has exhaustive, raw, timestamped and inalterable information**. Generating data that circulates independently of a central organisation in a way that is secure and can be viewed by each of the participants of a same process makes it smoother and meets the needs of flexibility in defining the management rules that govern the relationships between actors derived from a multitude of use cases. A trusted third party cannot programme this transaction diversity into a centralised tool; they are confronted with inevitable exceptions.

<sup>31</sup> An accounting transaction that is often used to verify that invoices have been paid correctly

<sup>32</sup> Factoring can be defined as the convention by which a specialist organisation, called the factor, buys the debt a company holds from its clients and takes on the collection itself. Using factoring allows a business to collect on its debts quickly without waiting for payment periods to end. The factor is paid various commission fees and covers any losses if the client does not pay their invoices.

## Blockchain: from theory to practice

The transformational challenges in adopting blockchain in large companies

**Use case: Sharing management rules brings more automation to the exchange of information**

In the invoicing process described above, the tax dematerialisation resulting from the use of EDI messages encourages **data automation**.

When actors send invoices in this electronic format, they can **reduce this document's processing costs** despite the initial investment needed to set up this bilateral exchange. However, managing exceptions or unexpected cases require using more conventional exchanges with a paper invoice, which limits the use cases for this electronic invoice.

With blockchain, not only is it possible to **industrialise invoicing** in a bilaterally structured data format, but we can also **share multilaterally** with other third parties while allowing each actor in this document's life cycle to bring their own management rules in an autonomous way. Blockchain allows this invoice data sharing automation to account for each actor's business specificities.

For example, the buyer can define an **acceptance workflow** where several departments can **inspect the accuracy** of invoice data thanks to structured data, or the factor can accept to finance an invoice according to certain conditions agreed to with the seller while obtaining an **automatic payment routing** for the invoice to avoid double payment.

### 3.4. Qualifying data upstream instead of downstream

In traditional systems, all transactions are validated at each exchange by the trusted third party and synchronised/verified by the parties to the transaction. Using a third party between the various actors centralises and concentrates the trust and efforts of the exchanges on this intermediary.

With blockchain, not only does the transaction happen directly between the parties without an intermediary, but the information is synchronised between the parties to the transaction by design. Blockchain creates a "sphere of trust" by moving the trust of the trusted third party to the stakeholders.

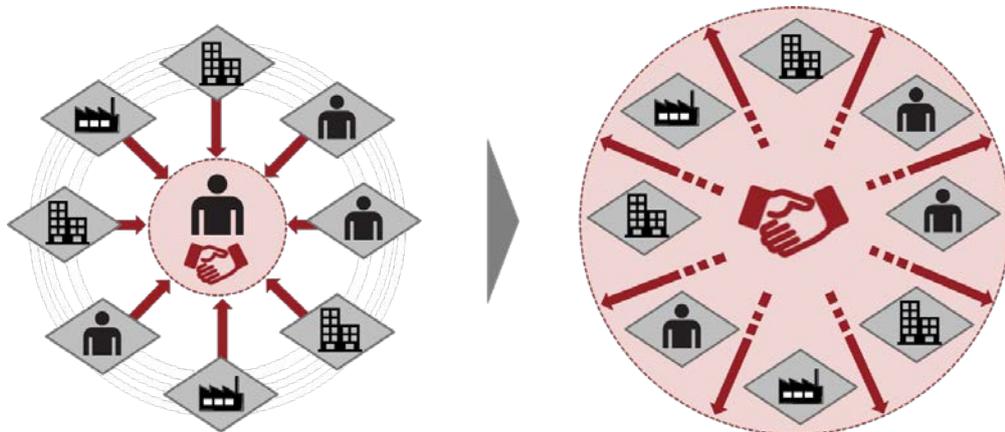


Figure 5: Moving trust in the actors

Thus, viewing available and accurate transaction data at any given time is no longer a problem. Businesses can then concentrate their efforts on implementing tools and processes to secure transaction data as far upstream as possible of their registration in a decentralised information system.

## 4. A paradigm shift

### 4.1. Switching from X2Y2X to X2X

Going from theory to practice is not easy on an issue as complex as blockchain given the extent to which traditional thinking is called into question. As we have seen previously, this mainly concerns the notion of the "trusted third party" that everyone has completely integrated into their lifestyles without questioning the basis for it.

For everyone, the government's role is natural in guaranteeing their identity, banks' role is natural in guaranteeing that their bank account matches real money, which the bank guarantees really belongs to us. In a certain way, we have integrated the role of all sorts of intermediaries in all aspects of our lives to guarantee our rights, from the most basic to the most complex.

Questioning the need for trusted third parties is a result of the same logic that produced the internet and the web for data. The internet allows a networked dialogue without going through central nodes, and the web is the natural extension in data exchange management. By comparing the blockchain revolution to the web revolution, we can see that it is not just another collaborative technology, but the extension of an established collaborative philosophy applied to transactions.

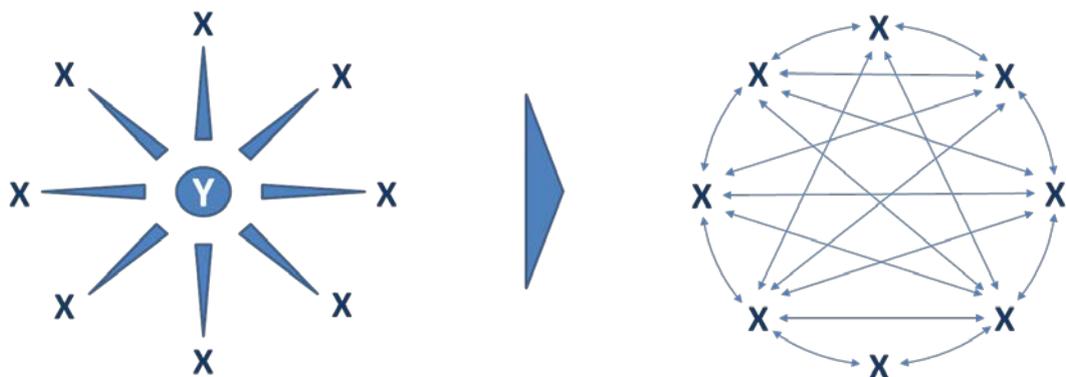


Figure 6: Going from a hub-and-spoke model to a network model

If the blockchain promise is fulfilled at a large scale, potentially all of these transactional systems that operate on a hub-and-spoke basis are concerned:

- In the B2B2B (B for business) sphere, the centrality of **clearing systems**, whatever their nature (in particular, we are thinking of payment systems in general), can be called into question.
- In the C2B2C sphere, we are seeing an "Uberisation of Uber", meaning a **direct transactional relationship from customer (C for customer) to customer**.
- In the C2G2C sphere, it's the systematic need for the government (G for government) as the guarantor of citizens' rights (C for citizen) which is potentially undermined **with the emergence of extranational communities that can guarantee citizens' rights**, starting with identity.

Taken to the extreme, there is theoretically no limit to the disappearance of trusted third parties except for those that the law or consumers themselves set up depending on the level of trust

they place in the system. This is why we could say that blockchain allows for a sort of final form of the collaborative economy.

## 4.2. Third parties disappear, but not their function

However, we shouldn't exaggerate the disappearance of trusted third parties. While the actor who holds this trust at the time of the transaction is destined to disappear, **the function they represented will certainly be moved to the margins** by being divided amongst the various actors or by being concentrated into a single one to provide a certain number of guarantees:

- Before anything else, we must **have trust in the programme that manages the blockchain**. In a public blockchain, the fact that it is governed by open-source communities makes it legally non-opposable by companies. This is one of the reasons there are now so many private and consortium blockchains.
- When the blockchain is **initialised, the first level of trust concerns the blockchain itself and its first block** (genesis) on which its ability to respond to the stakes of actors' trust depends.
- **On the identity level**: there must be an external actor who can ensure that the other actors are who they say they are and have the rights to access the data.
- **Data management**: blockchain is a transactional process that stores some data, but it is not a database as such. Therefore, it may be necessary to **have external databases to support the processes**.
- **The link with connected information systems**: for example, for financial exchanges in regulated currency, the blockchain stores, secures, and guarantees the traceability of transactions but not the monetary flows that are linked to them, which will flow through marketplace payment systems.
- **The link with the real world**, for example:
  - The transactions covering the exchange of physical objects (in supply chains, in transactions of the buying/selling of objects, etc.): the challenge is to have a **certifying third party that guarantees the integrity between the object itself and its digital representation** in the blockchain in the form of a certificate (for example a certified car registration that represents a physical vehicle)
  - **Document management**: while blockchain will preserve a document's signature (the hash<sup>33</sup>), the document needs to be stored somewhere and, therefore, **the document (content and location) must be guaranteed by a third party**.
  - **Event management**: thanks to certified third parties ("oracles"), we can irrevocably introduce **external information** recognised as "true" by all parties **that can trigger a management rule**. For example, to determine if a person has died and, in this case, trigger a testament smart contract, or to trigger compensation from an insurance policy indexed to a weather event.

<sup>33</sup> A hash is a chain of characters obtained by applying a mathematical formula to the content of an object. A hash has the particularity of being unique: if the object to which it is associated ever changes, the result of the calculation changes too.

## 5. The challenges for large companies of adopting blockchain

*In this chapter, we look at the case of implementing private or consortium blockchains.*

For companies, there are many challenges in adopting blockchain. In four aspects, cultural, management, legal, and technology, we will detail the main elements to consider.

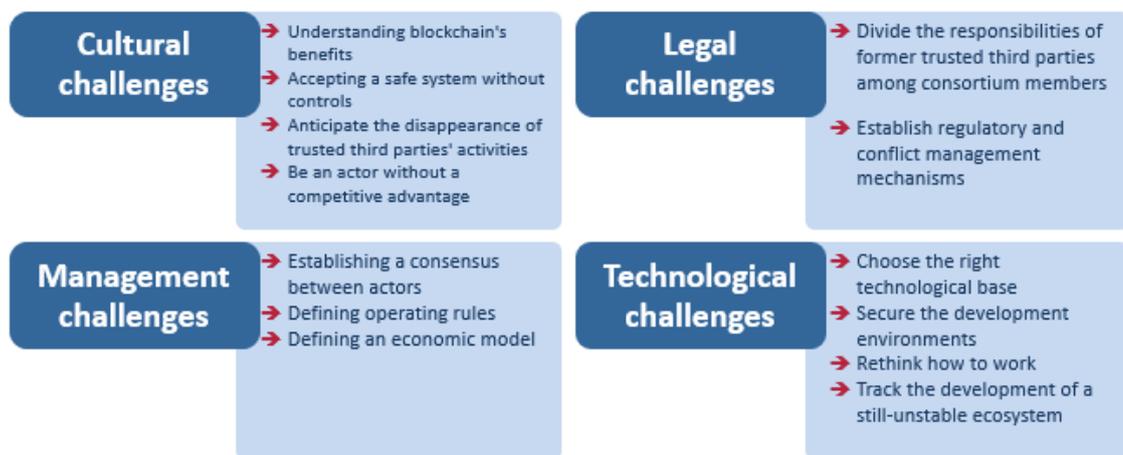


Figure 7: Key questions to ask when creating a consortium blockchain

### 5.1. Cultural challenges

#### 5.1.1. Understanding the benefits of the concept

Blockchain is an assembly of technologies that are well-known and understood. It can replace processes that currently work but, by optimising them, it offers data uniqueness and security.

Two types of reactions currently predominate:

- Those who think that blockchain can **replace all transactional systems**: it only manages the certification of the transaction, not all of the prerequisites the transaction requires (see section 4.2)
- Those who think "it's too good to be true!" and who **have not understood the breakthroughs blockchain brings**.

So, first, there is the challenge of **explaining in a simple and convincing manner blockchain's opportunities and scope of validity**.

#### 5.1.2. Accepting a transaction system that is natively secure without control

Today's information systems are designed to guarantee and secure transactions by central actors (purchasing, finance, HR, etc.) whose function it is to do so. **Designing an exchange system without a central intermediary guaranteeing transaction is not easy to accept.**

### 5.1.3. Accepting and anticipating the consequences of the disappearance of the activities of trusted third parties concerned by blockchain

The removal of intermediaries due to blockchain will cause the activities that were guaranteed transactions to disappear. Socially, this could cause complicated situations resulting in resistance or opposition.

However, this could be an **opportunity to redeploy skills internally** and/or train employees to meet new challenges for the company. But here as well, this requires **appropriate support**.

### 5.1.4. Partner actors

Finally, all participants in a consortium blockchain must **accept that there is not necessarily a competitive advantage in being a member of a consortium**.

Indeed, blockchain's simpler transactions are intended to **benefit all actors**.

## 5.2. Governance challenges

### 5.2.1. Establishing a consensus between actors

Implementing a blockchain shakes up traditional logic as well as marketplace systems that require a trusted central third party to whom we delegate a certain number of powers (regulator, closed economic consortiums, etc.). With blockchain, we **switch to more open modes where we will have to find consensus** between actors and professions.

The challenge is to set up **appropriate governance** that requires, above all, that blockchain participants (particularly for consortiums) **agree to a highly collaborative operating mode** with a **simplified chain of processes** since all that concerns traditional data verification, auditing and security disappear.

### 5.2.2. Defining operating rules

While blockchain's main innovation is to bring a philosophy of decentralised consensus and information sharing to all levels of thinking, it is vital to set out a few rules:

- **For decision making**, particularly in terms of technology ("Code is law").
- To define what data is visible or hidden and to **determine what we do not want others to see**.

### 5.2.3. Defining an economic model

We must also **define the economic model of cooperation** by answering a certain number of questions, notably:

- How are the costs of developing smart contracts spread?
- Given the technical commitments each consortium member makes for the blockchain nodes to function, what are the mechanisms for funding infrastructure (for example, everyone pays for their infrastructure vs. setting up an incentivising equalisation system)?
- etc.

### 5.3. Legal challenges

#### 5.3.1. Dividing responsibility

As we saw previously, by moving trust to all actors, blockchain removes intermediaries, but not their functions (see section 4.2). Consortium blockchains will need to **divide the responsibilities of the former trusted third party among the consortium members** (for example, identity management, compensation for fraud, error management, etc.).

This division asks blockchain participants for an **unnatural understanding** of all of the functions performed by the historical trusted third party and to transpose it into the new system.

#### 5.3.2. Establishing regulatory and conflict management mechanisms

With the lack of trusted third parties contractually guaranteeing the regulations and conflict resolution methods with each party, **the rules that the consortium stakeholders accept in case of conflict must be defined beforehand**. An easy solution could be to appoint an external third party to guarantee that the rules are applied.

### 5.4. Technological challenges

#### 5.4.1. A technological base accepted by all participants

Although blockchain is an assembly of known technologies, it is necessary to **choose the right technological base** from among a plethora of offers. This means choosing the right tools that will support a blockchain application's entire life cycle and all of the standards that these tools will have to respect. Choosing a sustainable technological base is critical since **it cannot be changed**. However, while there is currently no portability system, experiments are ongoing on possible interoperability between blockchains (consortium/consortium, consortium/public, public/public) that could limit the risk.

Another major point is to **define common standards** in identity management, data and document synchronisation for elements that must be managed outside the blockchain by design, as well as the choice of infrastructure and exchange protocol between consortium partners.

**There must be an agreement among the consortium on the technologies used**. Without underestimating the difficulty of convergence, these technological choices can be a problem given the diverging IT strategies among participants.

#### 5.4.2. Securing the development environment

Securing the tools is just as important as which ones you choose, particularly for the development environment.

This is what will allow you to develop smart contracts **that will be irrevocable once deployed in the blockchain** ("*Code is Law*"). Therefore, they must be secure, and so must actor(s) that will use them (consortium partners or external partners?) as well as the code generated (who approves the code? who is responsible?).

The user acceptance process is thus critical given that, **while it is complicated but possible to change certain functions of a smart contract via certain mechanisms** (to correct a bug, for example), **it is impossible to roll back past transactions that exploit a flaw**.

## Blockchain: from theory to practice

---

The transformational challenges in adopting blockchain in large companies

### 5.4.3. Rethinking how we work

Another challenge involves control over a distributed environment: **Are we ready to let actors with whom we are not used to working get involved with our own technologies?**

For IT production teams, this is not the same way of working. They must become part of a **network with these actors**, certain aspects of production will no longer need to be done, and certain internal management information systems may be replaced.

### 5.4.4. Tracking the development of a still-unstable ecosystem

Developing a coherent technological ecosystem around blockchain is also a strong technological challenge in both development and production. **This ecosystem is currently being developed:** many actors currently offer development environments, and we are seeing service providers specialised in administering blockchains, code audits, administration and node control. The risk for companies here is **no longer having control of the trusted environment** that they were looking to put in place with blockchain by depending on outside actors.

There are other unanswered questions about a blockchain's sustainability, interoperability, and scalability.

## 6. Blockchain's legal approach

One of the most surprising issues in implementing blockchain is the need for an unprecedented and vital collaboration between legal scholars and IT experts.

### 6.1. Getting into phase with the legal perception

It is important for legal scholars and IT professionals to understand each other to be able to work together. While blockchain may fit certain articles of recent French laws such as Article 120.1 of the Sapin II law for the registration and circulation of unlisted company shares where blockchain can be considered a "shared electronic registration system", there is no real definition appropriate to the legal world.

A few definitions used in business within the reach of legal scholars

*"Blockchain is a transparent information storage and transmission technology that seeks to perform peer-to-peer transactions in a secure and decentralised manner that relies on the use of a decentralised ledger of digital data shared between multiple parties."*

*"Blockchain is a technical protocol that uses an open or closed peer-to-peer network accessible to all users used for transactions through a system of exchange values (cryptocurrency) performed in an irreversible and unchanging manner that establishes an exhaustive, certified ledger of transactions (events)."*

From a legal standpoint, a good understanding of peer-to-peer networks must include explanations of:

- **Organisation rules:** to identify who does what and who is responsible for what. For public blockchains, there is no uniform international law; for consortium blockchains there must be contractual rules, and it falls under internal organisation for private blockchains.
- **Applying laws and rules in case of dispute:** what are the international treaties (WTO, Vienna, etc.) concerned?

It is the same for exchange value systems (cryptocurrencies); there also needs to be explanations for:

- **The opposability of the currency:** how is the exchange done with cryptocurrencies? By what mechanisms?
- **The currency's volatility:** in November 2016, a bitcoin was worth 514 euros; today it is worth over 5,000. We must be very aware of changes in value during transactions.
- **The fact that the currency/reward guarantees the sustainability of a consortium or public system.** This is what makes trust solid in blockchain.

Explanations must also cover the notion of an exhaustive and certified ledger of transactions which has a very significant value for a legal expert and for legal acts:

- **The ledger's reliability:** The notion of trust or control is at stake.
- **The ledger's sustainability:** How to handle the issue of the right to be forgotten?

The transformational challenges in adopting blockchain in large companies

- **ID management:** What security for identifiers and personal data if the keys risk being defective in 5 to 7 years?

Unlike the three previous notions, smart contracts are very meaningful to lawyers who can translate a contract's commitments and obligations. These smart contracts **give order** to transactions, translate the **conditions of execution** and manage the **various parties** to the transaction. What is also interesting is that smart contracts, once programmed, **execute automatically** and perform the transactions to which the parties agreed according to the agreed conditions.

#### Use case: What blockchain brings to legal practices

Blockchain is called a "**trustless**" technology, whereas trust is the main subject of a legal negotiation. To what extent can we trust a partner, and at what level of problems do we negotiate compensation or a commitment of responsibility? Therefore, this notion of "**sphere of trust**" is very interesting from a legal standpoint because it allows us:

- On the one hand, to seek a **homogeneous treatment** by the end user (the lawyer) by allowing them to take control over contracts and their legal costs, to standardise the practices and overcome the lack of trust toward certain actors.
- On the other hand, to have the possibility of **making the execution of the contract conditional** to a vote of several actors, with options for a quorum, without needed to know them and without losing trust, or conditional to objective events: duration, registration on a ledger or the execution of a task.
- Finally (and above all), a **true tracking of execution** and control over the consequences of a contract for the parties.

## 6.2. Legal questions

Many experiments are currently underway, revealing new legal questions that mainly concern public blockchains:

- **On actors' identity:** in consortium or private blockchains, the various actors are known and identified according to established rules and managed by controlled systems. But in public blockchains, how can we be sure of the reliable, opposable nature of users' identity?
- **On personal data:** a public blockchain is a decentralised environment where you cannot know who owns the data. Therefore, it is not possible to have information on where the data is located or about the user's consent, for example. Currently, there are no sure answers about the respect for the GDPR in a public blockchain environment.
- **On territoriality and applicable law:** the environment's decentralisation, the fact that we do not know where the actors and data are located, begs the question of the impact of the transactions' transnational nature. At a French and European level, a legal environment can be adapted, but, beyond that, it becomes complicated.
- **On responsibility** and the executable nature of corrections in case of a "bug". In a consortium, a contract defines the responsibilities of each actor in the blockchain. For private blockchains, we can also rely on the company's regulations. However, for public

The transformational challenges in adopting blockchain in large companies

blockchains, the current practice is to try to get a maximum of actors on-board with a correction with no guarantee.

### 6.3. The various challenges related to the legal aspects

Challenges	Blockchain		
	Private	Consortium	Public (in 2-5 years)
Management	● Internal	● Contractual	● Core
Trust	● Ethics rules/labour contracts	● Consortium rules/partnership contract (consortium contract)	● Protocol and miners
Reliability	● Internal or service provider technical capacity	● controlled by the consortium project committee	● Lack of detected anomaly (DAO)
Opposability	● Internal	● Between consortium members or their contracted clients	● To be determined according to legal acts (1)
Responsibility	● Internal (2)	● Contractual (2)	● Currently none (DAO) but could be covered contractually for certain users
Guarantees	● Internal technical qualifications	● Contractual	● Number and spread of miners
Applicable law and court	● Court of the place of establishment or damages	● Contractual jurisdiction clause	● At this stage, unresolved due to the difficulty in identifying territoriality
Sanctions	● Internal: disciplinary	● Contractual: penalties, damages, and interest	● For users: "at their own risk"
Preservation of personal data (DCP)*	● Internal archiving rules	● Contract clauses: avoid DCPs as much as possible	● Indefinite preservation of identifiers
User information*	● Internal charters, rules of ethics, information notices	● Terms of use	● None

(1) Not all legal acts require the same level of reliability: i.e. electronic signature level  
 (2) Needs analysis on the concept of processing manager



Figure 8: Stakes related to blockchain's legal aspects

**Governance:** whatever the type of blockchain, actors have different stakes, even within the same company, and it takes time to define the management and decision-making rules.

**Trust:** by definition, trust in the blockchain is "dehumanised" in the sense that it does not rely on human actors but on computer code. In the case of public blockchains, this translates into a requirement of infallibility, otherwise trust breaks down between actors who do not know each other. In consortium or private blockchains, the rules that govern the trust between actors must be defined together. Legally, this can be complicated depending on the extent to which everyone knows everyone else.

**Reliability:** this stake essentially concerns everything the legal actors will consider in terms of risks.

**Opposability:** in a public blockchain, the opposable nature depends on the possible legal acts (for example, legislation regarding electronic signatures). In a consortium, opposability will be covered in a consortium contract/agreement. Private blockchains are not concerned by this stake.

For the stakes of responsibility, guarantees, applicable law, sanctions, preservation of personal data and user information, public blockchains seem less appropriate from a legal

The transformational challenges in adopting blockchain in large companies

standpoint. All of these stakes are often covered by contracts or legal provisions. However, for public blockchains it is difficult to know which legislation applies (for example, the place of transaction on an international network).

**Responsibility:** public blockchains are not concerned by this problem since the various actors currently do not bear any responsibility. With private or consortium blockchains, while it may seem simple to get together, it is not easy to agree on each actor's responsibilities in terms of development, testing, confirming identity, etc.

**Guarantee:** this stake concerns contractual aspects that are not covered by public blockchains

**Applicable law and sanctions:** these issues are controlled when agreements are possible, i.e. for private or consortium blockchains.

**Preservation of personal data:** this issue is not exclusive to blockchains, but generally it is not yet legally resolved for blockchains (in particular concerning the GDPR).

**User information:** there needs to be an actor that takes a customer viewpoint and informs users of the blockchain's risks and guarantees. This is the case currently within companies and, therefore, taken into account in consortium and private blockchains, but not in public blockchains.

## 7. Impact on the IT function

We have the habit of thinking about a technology essentially in the context of how it is used. However, often this use can entail significant changes in the technical teams that implement them.

For blockchain, and particularly public blockchains, it seems that an entire set of operating activities initially under IT teams' responsibility are handled natively by the protocol and distributed architecture. Concerning the transaction system itself:

- The **certification of the transaction** is inherent in the blockchain concept. The central clearing information systems and inspections by partner information systems are made obsolete, and there is no longer a need for mutually accountable information systems to record double-entry transactions.<sup>34</sup>
- Since the blockchain protocol bears the functions of a self-managed virtual machine, **code changes are no longer managed** by the technical teams of each blockchain participant.
- The real-time replication of transaction data on the networks' nodes makes an entire set of existing functions obsolete, like **managing transaction backups, redundancy, and business continuity**.
- The blockchain also manages **perimeter security and the interconnections between IT partners** natively, which greatly simplifies the needs in these areas.

Nevertheless, there remain issues that IT teams must continue to process. For example, as we saw previously, blockchains do not currently manage **identities and data**, which implies managing these elements separately and **in a traditional manner**. This despite the fact that great research efforts are being directed toward managing identities and data with blockchains themselves (many blockchain communities are working to natively manage data and identities, but this is not guaranteed).

**Servers must still be supervised to guarantee entry points to the blockchain** (node endpoints) and, above all, to perform **software upgrades** on these nodes (for bug corrections): a node that has not been upgraded on a server can be excluded from the protocol. **Server upgrades must still be managed in a traditional manner**.

Currently, **the main pitfall concerns development management**: unlike current mature development environments that provide effective frameworks, current blockchains provide very regressive frameworks that cause drops in productivity and development security, although publishers are working harder and promise effective frameworks within two to five years.

That which is true for public blockchains is less so for consortium blockchains, and the table below presents a comparison of the benefits between a traditional IS management, consortium blockchain management, and the promises of public blockchains.

---

<sup>34</sup> In double-entry accounting, the basic principle of the accounting system used by all companies, an entry is made in two accounts (at least): an account debited and an account credited.

The transformational challenges in adopting blockchain in large companies

Activity	Traditional IS	Blockchain	
		Consortium (current)	Public (in 2-5 years)
Transaction certification	Central clearing IS + control by partner IS	Managed natively	Managed natively
Development	Effective frameworks	Currently frameworks in their infancy	Mature frameworks
Application server management	Version management and configuration of all layers	Standard HW + OS management Virtual machine version	Managed natively
Application server supervision	Traditional supervision	Managed natively	Managed natively
Transaction backup management	Traditional backup	Managed natively	Managed natively
Interconnection management between partner IS	Traditional flow opening	Traditional flow opening	Managed natively
Redundancy and business continuity	Traditional redundancy	Managed natively by the blockchain	Managed natively
Scope security	Traditional security	Node inclusion to be planned	Not concerned
Data and identity management	Traditional management	Traditional management	Managed in the future?

No benefit    
 Low benefits    
 Significant benefits    
 Great benefits

Figure 9: The benefits of blockchain *vis-à-vis* the IT function

## 8. And Monday morning?

Given public blockchain's current lack of maturity for business use, we encourage companies to focus their efforts on the emerging consortium blockchains (and private blockchains, which are ultimately just a special case of consortium blockchain).

What is new in this scope is the level of transversality that is required immediately of anyone who takes the initiative:

Setting up a  
**multi-disciplinary  
working group** sponsored at  
the highest level

→ An internal transversality that requires gathering a working group that is multidisciplinary from the outset, including business developers, back office managers, computer scientists and legal experts as well as lobbyists and communications officers.

New uses can only be identified by confronting the technology with the stakes of simplifying transactional processes (associating the back offices) in a value creation philosophy (business development) and with a sharp sense of legal issues (see section 5.3 above).

→ External transversality that requires discussion with peer companies and, more widely, the actors of the company's ecosystem. A consortium blockchain's value proposition only comes from its ability to simplify transaction systems by eliminating the historical trusted third parties from them.

Have **discussions with  
peer companies** and/or  
join a consortium

Launch an **adaptation  
programme** to understand the  
stakes of networked organisations

→ As such, the most important challenge is probably the **cultural challenge** that consists of conceiving a transactional ecosystem without a central trusted third party while controlling the shift of its attributes to the ecosystem's margins: who will manage identities? How will we manage

data synchronisation? Who will guarantee the digital integrity of the description of physical assets? We all have the habit of thinking about transactional universes as hubs and spokes. The challenge is to design organisations as a network without a specific guarantor.

→ Finally, a good way to start is to "get your hands dirty" with the technology in-house by developing a few uses with private blockchains, for example regarding repository data management. For example, it's easiest to do "assisted runs" to get used to the technology and, above all, the challenges of governance in a distributed organisation.

Create **intra-group  
prototypes** to master the  
technologies and stakes of  
management



## **ABOUT CIGREF**

### **KEY PLAYER IN THE DIGITAL SOCIETY**

Cigref is a network of major French companies and public administrations set up in order to develop its members ability to acquire and master digital technology.



### **NETWORK OF MAJOR COMPANIES**

Created in 1970, Cigref is a nonprofit organization. It counts among its members some 150 major French corporations and public administrations across all business sectors, all users of digital services.



### **DIGITAL PLAYER**

It is a key player and federating body in the digital society, thanks to its high-quality thinking and the extent to which it represents its members.



### **TO SERVE ITS MEMBERS**

15 Board members, elected by the General Assembly, ensure its governance. A team of 10 permanent members leads the activities.