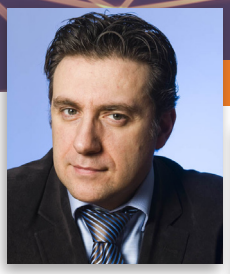
KEYRUS
insight into value

BLOCKCHAIN: CONCEPT AND APPLICATION DOMAINS

EXPERT OPINION



Frédéric Maserati | Consulting Director **Keyrus Management**

Maxime Leroux | Consultant **Data Scientist**

The Blockchain came into existence following the economic crisis of 2008 and the calling into question of the financial system, and it has its foundations in research into crypto-currencies, in other words, currencies denominated and operated by entirely digital technologies. According to the great technology gurus, the Blockchain harbours new potential for innovation and the disruption of dominant economic models. In that respect, the Blockchain is a revolutionary technology that makes it possible to develop and implement an "Internet of transactions". But what exactly is the point of it all?

The idea for the Blockchain appeared with the Bitcoin, the first crypto-currency, which is more familiar to the general public. However, in reality, we think that the Blockchain has more points in common with the TCP/IP protocol than with a crypto-currency. We have good reason for thinking this, since the Internet, and its famous TCP/IP protocol ("information highways"), made it possible to speed up the digital revolution, thanks, notably, to the dissemination of information in "peer-to-peer" mode.

Now, the Blockchain is to the transaction what TCP/IP is today to information, to communication… the Blockchain is set to produce "transactional highways" in peer-to-peer mode!

In theory, the Blockchain is a register duplicated and shared between all the nodes of a network; each node can be a user, or even a computer. To put things in even simpler terms, this register notifies and time -and date- stamps each exchange between each node in a "block". As soon as each "block" is full, it is linked up, one after the other, with the preceding blocks, such that everything is recorded in them… and visible to all… It is therefore both a time-and date-stamped, secured server, and at the same time, a secured peer-to-peer database.

Therein lies the disruption of classic transactional models as we know them. Indeed, regardless of the situation in which a company finds itself, and on almost every occasion, a trusted third party ensures and guarantees that a transaction has indeed taken place, and that it was executed only once (bank, notary, auditor,…). The Blockchain makes it possible for a transaction or exchange to have indeed taken place between several "parties"… so freeing itself from the presence of the trusted third party. The disruption here relies on distributed, secured disintermediation, organized in "peer-to-peer" mode.

To do this, the blocks are automatically piled up chronologically, time-and date-stamped, and of course, coded, with the whole thing having been "validated" by the "miners"… people like you and us (through one of the network's nodes) who make their computational power available so as to resolve the mathematical problem raised by the "chain of blocks". Resolving the problem thus amounts to "validating" the transaction, rather like a clearing house would do with payments. As the transactions are visible to all, the Blockchain therefore transforms itself into a formidable auditing tool, and this provides the foundation for trust between the parties involved.

In some ways, it is identical to the general ledgers of banking and financial institutions… but without the banks or the financial institutions. And around it goes. We find ourselves in a system based on trust… but without trusted third parties… how paradoxical! And how revolutionary!

WHY SO MUCH EXCITEMENT AROUND THIS?

If anyone and everyone can "transact" directly peer-to-peer with complete confidence, without intermediaries, and without trusted third parties, then it becomes possible to do away with platforms that skim wealth off (by way of examples: AirBnB, Uber,…). As a result, alternative models to Uber already exist: they are collaborative platforms, developed using Blockchain technologies, like ArcadeCity or Lazooz.org. After Uberization, the talk, from now on, is of the "Blockchainization" phenomenon!

Proof of this can be seen in the acceleration of investment in this area, and the incredible number of conferences and articles on it. The excitement has been growing since the Internet Gurus created much hype with their pronouncements on the possible applications of the Blockchain in the world of finance, the impact of which is estimated in terms of billions of dollars…

And, even if the main technical challenge involves the number of transactions processed per second -this being a challenge that the Bitcoin Blockchain appears to be unable to meet-, the use of private Blockchains is of great interest, since they can make it possible to adopt distributed approaches at a truly marginal cost.

The other reason for such excitement is the scalability of this technology. It is true that all Blockchains using the "Proof of Work" mechanism can be vulnerable to computer virus attacks of the "Goldfinger" type. These attacks consist of gathering together computational power equivalent to a little more than 50% of the total power of the relevant network (or of a group of servers, like those of the Pentagon, which are subjected to hundreds of daily attacks). Once this is achieved, the attacker is free to validate/invalidate certain transactions. The purpose of these attacks is to shake users' confidence in the technology, in this case, the Blockchain. But today, the Bitcoin is the world's most powerful network, with nearly 1200 Petahashes per second, which means that an attack with 51% is not impossible, but it would be terribly costly. Indeed, according to certain experts, you would need nearly 5 billion US dollars for 10 minutes' intrusion.

Moreover, since the Bitcoin is an open-source, worldwide project, a simple patch, followed by the rebooting of the network's nodes, would be enough to resolve the problem in a few minutes. In addition, it is possible for anyone to audit the source code without any great complexity.

A MULTITUDE OF BLOCKCHAINS

Given the universal nature of the Blockchain, one can appreciate that all sectors will be affected by the adoption of this technology. The number of processes likely to feel its impact is truly phenomenal. The banks were not wrong on this score. Acting either individually or in groups, they are exploring, and experimenting with, the Blockchain's possibilities, with a dual objective: to take advantage of its benefits, and incorporate the point-to-point logic in their model, so as to better withstand the arrival of new players using a natively distributed and disintermediated model, notably the FinTechs.

We are actually experiencing a Cambrian explosion, with the creation of hundreds of Blockchains conducive to experimentation. Today, anyone can create their own system, as the requirements for gaining access to this technology and getting started with it are simple and financially affordable.

So it is that we are seeing the appearance of private Blockchains, in which participation in the consensus (mining) requires permission. Despite the centralized arrangement of these private Blockchains, certain traits of public Blockchains, like the Bitcoin or Ethereum, remain: an architecture that is highly resistant because the database is distributed, a permanence to the system, since the data are immutable, and a uniqueness, with a single system: a "general ledger".

To sum up, on the one hand, there are public Blockchains, whose general ledger is open, and which are secured through the use of "proofs of work" that require computational power in order to obtain the right to make an entry in a block (mining), or "Proofs of Stake" that require certain particular digital assets to obtain the same right to make an entry.

On the other hand, there are also private Blockchains, whose general ledger is closed, and which require "permission" to access them. These private Blockchains are likely to mostly concern companies and the professional world, even if we may well witness a form of hybridization of public/private Blockchains in the coming years.

WHAT ARE THE BENEFITS OF THE BLOCKCHAIN? AND WHAT ARE THE ISSUES COMPANIES WILL HAVE TO FACE?

BENEFITS

TRACEABILITY AND TRANSPARENCY

Since every transaction is entered permanently, this ensures traceability (audit trail). By way of an example, Walmart is experimenting with the Blockchain technology with a view to increasing the traceability of its products. The technology allows it to have immediate and certified access to information relating to the production, distribution, and selling of its own-brand products

SECURITY

Thanks to the use of cryptographic methods, the Blockchain ensures that transactions are secure. Moreover, putting the information in a network ensures that the transactions can not be hacked. By way of an example, crypto-currencies take full advantage of this property by incorporating into the source code access to the past transactions relating to the unit of value, whilst at the same time protecting the identity of the individuals associated with the transaction. The theft of a person's identity during the execution of a transaction is therefore theoretically no longer possible.

SPEED OF EXECUTION

Thanks to a network-based infrastructure, the recording of information and access to it occur almost instantaneously. This is evidenced by the fact that the world of finance is currently experimenting with the use of the Blockchain with a view to facilitating intermediation between banks, clearing houses, and central banks. They see in this an opportunity to increase the efficiency of operations: speed of execution, reduction in resources required and in costs.

ISSUES

TECHNICAL NATURE; ACCESS TO, AND RELIANCE UPON, TECHNOLOGY

This subject remains highly technical and difficult for the great majority of people to grasp. However, with a process of evangelization and acculturation, numerous players (like Keyrus) are playing their part each day in developing new platforms, and ultimately new uses. The major Digital Service Companies like IBM are natively incorporating APIs to promote the integration and dissemination of the Blockchain technology.

HACKING AND INTEGRITY OF THE NETWORK

Although theoretically impossible to hack, certain applications, in the upper layers, connected to Blockchain infrastructures have recently allowed hackers to steal substantial quantities of crypto-currencies, questioning the integrity of Blockchain infrastructures. In reality, even if in that instance (a security flaw in a business application operating on the Ethereum public Blockchain) the Blockchain was not at fault, it has to be said that with any emerging technology, the learning phases are, more often than not, peppered with a multitude of pitfalls.

WHAT ARE THE CONCRETE APPLICATIONS? WHAT ARE THE USE CASES FOR THE BLOCKCHAIN?

To come back to the genesis of the Blockchain, we can now see more clearly why, philosophically, this technology (this exchange protocol) is in the process of "disrupting" many sectors.

It is thus still the case today that the architectural principle behind the Blockchain is based on quite a simple premise: to enable exchanges, transactions, to take place between 2 individuals, 2 entities, free of any involvement by any intermediaries or trusted third parties, who "betray" trust by abusing their dominant position in their ecosystem.

Since then, applications of the Blockchain have multiplied, extending well beyond the financial system, and ranging from the sharing economy, through smart contracts (those much-touted, self-executing and autonomous algorithms) and the digital vote, to the management of the logistics chain. The areas of application thus transcend economic sectors, and the Blockchain is already poised to transform all existing industries. This technology is set to radically change the organization of transport, the Supply Chain, advertising, the energy production and distribution sector, the real estate market, insurance... It is going to transform the future, taking us from the Internet of Things, to autonomous objects. It will enable the digital world and the physical one to be united... finally!

Smart Contracts promise to make objects unalterable, give them the means, if need be, of proving that they have been corrupted, and make them resistant to collusion. Through the Blockchain, it will be possible to give objects an identity and full autonomy. Objects will even end up "belonging to themselves", by managing, in the near future, to execute code on their own and autonomously.

Let us take the example of the driverless car: its future lies not so much in the fact that it moves around on its own... at its ultimate level, the model of driverless car will rent itself out, entirely on its own, and its users will pay only for their use of it, and will make such payment directly to the car itself, without going through any trusted third party. This is no doubt how the Uber and Lyft models will develop in the future.

WHAT ARE TODAY'S CONCRETE APPLICATIONS OF THE BLOCKCHAIN?

- **Financial sector & digital assets**

Beyond the Bitcoin, there are many potential applications in the financial sector. In 2015 the NASDAQ unveiled Linq: the very first platform for the issuance of private equity managed entirely using the Blockchain. Through this new system, private investors can trade in the stock of private companies. There is thus no need for certificates for the issuance of stock or the holding of shares in the companies: everything is digitalized and immortalized in the Blockchain. We refer to these as digital assets. Openchain and Chain are other examples of this. The first digitalizes all assets, whilst the second concentrates on the revolution in the financial system.

- **Digital identity & security**

oneName is an American start-up using the Blockchain to generate a digital identity which only the user will be able to use to log on for their various Web services. There will no longer be any need to memorize countless user names and passwords: only a single digital identity will be needed.

Estonia, a forerunner in this field, has, for a few years now, been running a digital identity project enabling its citizens to aggregate their personal information in a secure manner: this gives them a digital identity for voting purposes, medical references, a driving licence, etc. A more recent project, undertaken in partnership with the Tallinn stock exchange, will enable shareholders to vote at shareholder meetings – obviously without having to go to them.

For its part, the start-up FollowMyVote is banking on the digitalization of the electoral system. Observing the numerous problems experienced by several countries in terms of electoral fraud, this start-up is proposing to apply the Blockchain to ensure that the voting process is audited and traceable.

- **Health & pharmaceuticals**

The healthcare sector also abounds with potential applications. In the area of pharmaceutical industries, for example, the legitimacy, authenticity, and traceability of clinical results are paramount. BlockRX uses the Blockchain technology to ensure the traceability of the supply chain. Another use case in the area of healthcare is for medical records. By digitalizing them, information about the patient can be transferred more easily from one healthcare professional to another (with the patient's agreement, of course). Are we seeing the end of doctors' faxes and medical treatment forms? The interest within this sector is so great that, at the start of 2016, Phillips launched its own Blockchain research laboratory.

- **Insurance**

Another area of great interest for the Blockchain: insurance. Here, there are multiple possibilities, and we are still in for some surprises. For example, peer-to-peer insurance (e.g.: Dynamis) is putting an end to the usual, tripartite relationship between payers, insured parties, and insurers. It enables each individual to participate both in the pool of insured parties, and in the investment gains. By way of another example, parametric insurance (e.g.: Rainvow), for its part, enables the insured party to be compensated automatically when a certain event occurs, thanks to Smart Contracts. In this way, thanks to the interconnectivity of objects (IoT) and the programming of events, it is possible to record automatic insurance contracts. A striking example is the potential for insuring agricultural production against bad weather. Using sensors (of rainfall or temperature, for example), the payment of compensation (to the insured producer) will be triggered automatically, for example, after 2 months of drought (fictitious example).

- **Loyalty programs**

Loyalty programs will also undergo major upheavals with the arrival of the Blockchain. Today, the technology already makes it possible to record points earned and used by

members on the register on a rolling basis and in real time. Once participating partners are registered and connected up, all transactions (purchases and redemption of points) can be effected in real time. There will therefore no longer be any need to wait for your end-of-month points statement, or reach a minimum threshold before redeeming your points against a reduced selection of products; the purchase and redemption of points can occur simultaneously. Indeed, this is what is offered by loyyal.

But where the real revolution lies, in loyalty programs using a crypto-currency in a closed-loop model, is in the transferable nature of the Coin, versus the point. That is revolutionary. We "deverticalize" the relationship by "horizontalizing" it. As a result, we no longer address simply a loyalty program (with the relationship of the retailer towards the loyalty card, and of the card itself towards the customers), but rather, we interact with a customer community and promote exchanges even within that community. This constitutes a fundamental and comprehensive paradigm change.

- **Smart Contracts**

Smarts Contracts extend far beyond the insurance sector. Any agreement between two parties has the potential to be digitalized and automated. These so-called self-executing contracts give the various parties the assurance that, once the conditions have been fulfilled, the contract will be honoured, with no possibility for there being any fraud, bad faith, or interference with a third party. Indeed, this is what the Ethereum project is betting on.

- **Processes and information exchange**

Ultimately, any exchange between different parties can be managed by the Blockchain technology. Whether it involves digital money, proof of identity, an insurance payment, or a transfer to a supplier or customer, the logic remains the same: the process requires an exchange and the historization of transactions, and it must be traceable, efficient, transparent, and capable of being audited.

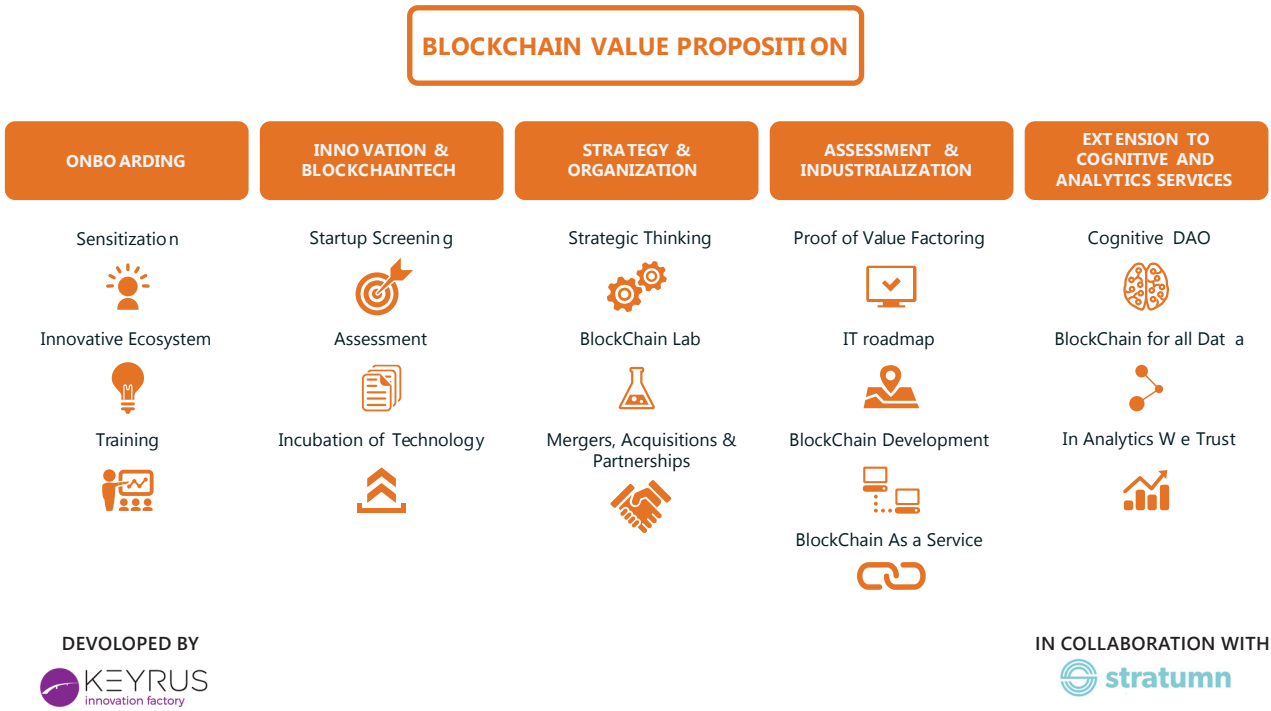
Considering the incredible disruptive potential of this technology and its applications, one thing seems almost obvious: faced with such potential, it becomes important for one to weigh up all the consequences of the Blockchain and its applications on one's business models, revenue models, growth models...

The Keyrus Group has built its own Blockchain ecosystem, and in doing so, it has developed an innovative offering capable of being deployed right from the strategic support stage, through to the integration of Blockchain projects in the technical sense. Keyrus has been assisting its clients with these initiatives for almost two years now: from the acculturation stage, through the identification of use cases, to developments and the integration of projects relying on Blockchain technologies.

Keyrus also takes care of the interconnection of Blockchain technologies with companies' existing Information Systems.

For more information on Keyrus's Blockchain offering: Blockchain@keyrus.com

KEYRUS BlockChain



Written with contributions from Camila Albigezi, Business Intelligence consultant, Philippe Grenier, BI Senior consultant, Timothée Cordier, BI Consultant, François Saloff-Coste, Special collaborator.

About the authors

Frédéric Maserati holds an MBA (from ESSEC). He has occupied several operational positions in Marketing and e-Business working for major banking groups. Today, he is developing several offerings around the Blockchain, Crypto-currencies, the commerce of tomorrow, and the bank of the future (with new approaches around Artificial Intelligence). He is increasingly interested in the impact of exponential technologies (NBIC) on new models.

Maxime Leroux is a consultant data scientist at **Keyrus** Canada. He is specialized in predictive modeling, data mining, machine learning and has a vast experience in big data technologies. He has worked as a quantitative analyst & data scientist in many industries such as banking, risk management, market finance, travel and loyalty programs. He has a master's degree in Applied Finance & is a Certified Professional Accountant.

About Keyrus

Keyrus, creator of value in the era of Data and Digital
An international player in consulting and technologies and a specialist in Data and Digital, **Keyrus** is dedicated to helping enterprises take advantage of the Data and Digital paradigm to enhance their performance, facilitate and accelerate their transformation, and generate new drivers of growth, competitiveness, and sustainability.
Placing innovation at the heart of its strategy, **Keyrus** is developing a value proposition that is unique in the market and centred around an innovative offering founded upon a combination of three major and convergent areas of expertise:

- **Data Intelligence**
Data Science - Big Data Analytics – Business Intelligence – EIM – CPM/EPM

- **Digital Experience**
Innovation & Digital Strategy – Digital Marketing & CRM – Digital Commerce – Digital Performance – User Experience

- **Management & Transformation Consulting**
Strategy & Innovation – Digital Transformation – Performance Management – Project Support

Present in some fifteen countries on 4 continents, the **Keyrus** Group has more than 2600 employees.
Keyrus is quoted in compartment C of the Eurolist of Euronext Paris (Compartment C/Small caps – ISIN Code: FR0004029411 – Reuters : KEYR.PA – Bloomberg : KEY : FP)

Further information at : www.keyrus.com

KEYRUS Marketing and Communication Department
155 rue Anatole France, 92593 Levallois-Perret Cedex – Tel. : +33 (0)1 41 34 10 00 - marketing@keyrus.com