KEYRUS
insight into value

BLOCKCHAIN – TOWARDS A NEW REVOLUTION

EXPERT OPINION

By **Éric Lévy-Bencheton** | Blockchain Strategist - **Keyrus**

and **Frédéric Maserati** | Consulting Director - **Keyrus Management**

The Blockchain is a technology created with the bitcoin, which has become the world's 8th currency in terms of amounts exchanged. The Blockchain brings with it new promises of innovation in all sectors, but also of disruption of dominant economic models. By taking an interest now in its potential applications, we can be one step ahead of the next stage of the digital revolution and the advent of a "horizontal" society, without intermediaries or centralized authority...

The Blockchain is probably set to revolutionize transactions and exchanges; in the same way that Internet enabled peer-to-peer communication, in the years to come the Blockchain will provide the means for peer-to-peer transactions under a decentralized and autonomous rationale.

Whilst a degree of mystery still surrounds the real identity of the creators of the Bitcoin, having been around for 7 years now it has shown that it is possible to create a 100% digital currency and make it work over time, casting off the banking system and any central authority. This considerable feat ended up drawing attention to the technology underlying the Bitcoin: the famous "chain of blocks" or Blockchain, with a potential for disruption that generates as much concern as it does interest and enthusiasm around the world.

The stepping up of investment in this area and the incredible number of conferences and articles on it are proof of this. This excitement has grown notably following the hype created by Internet and Finance Gurus in the United States, first among them being Blythe Masters on the board of Digital Asset Holdings, who launched a cycle of conferences on the applications of the Blockchain to the world of international finance, with financial effects in the billions of dollars ... to say the least!

Thought out and built on the ashes of the 2008 crisis, the system carries in its genes a philosophy of trust (the trust machine)[1], established through massive collaboration between the network members and by advanced cryptography techniques. This trust was intended to make up for the shortcomings of a still failing global financial system.

UNDERSTANDING THE PRINCIPLES BEHIND THE BLOCKCHAIN

With the Blockchain, the pieces of information shared between the members of a network are stored on each of its nodes (each computer), instead of relying on a central point. The validation of the blocks is achieved by cryptographic means and through a logic of consensus, with 51% of the chain's nodes having to approve the information.

Not only does this register contain the full transaction history at all times, but it is tamper-proof and irrevocable, precisely because of the encryption technologies used and its replication at multiple points. Based on this brief description, three major benefits of the Blockchain can be outlined:

- the possibility of limiting the number of intermediaries and trusted third parties in exchanges;
- the possibility of guaranteeing the conformity, integrity, and traceability of a transaction or a piece of information without resorting to a superior/central authority;
- the absence of a dedicated infrastructure, the necessary computational power being provided by the participants' machines (nodes) and optimized by algorithms.

We have so far been talking about the Blockchain "in the singular", potentially implying that there is only ever one of them. However, there are actually numerous Blockchains (the Bitcoin's being one of them) and they adopt various

[1] *http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine*

models of governance and/or information-sharing: Private, Public, Mixed, Hybrid.

A Blockchain can carry "static" pieces of information such as Bitcoin exchange transactions, but can also carry self-executing programs called Smart Contracts because they can act as "self-supporting" and automatic contracts.

We are seeing the first uses of this appear, like for example agricultural insurance linked to the weather, with a Smart Contract that will automatically retrieve rainfall/sunshine information from a pre-approved source (*météo France* for example) and, when appropriate, would automatically effect payment of the agreed compensation between the parties.

We will also find ourselves talking about Autonomous Agent, which is a set of Smart Contracts and so a much more complex program. We see in this the promise of new forms of human enterprises, like decentralized organizations. "The DAO" (Decentralized Autonomous Organization)[2] is one of the first examples of this. The funding campaign for the DAO undertaken on Kickstarter raised 174 million dollars[3], which makes it the biggest crowdfunding project ever seen. The DAO can be seen as a distributed financing company in which those who have allocated funds to it can decide on the projects they will be able to finance via Smart Contracts, in exchange for a return on their investments.

On 17 June 2016 the DAO experienced a huge crash following a cyber attack. The "hacker" managed to exploit a flaw in the "smart contract" regulating the DAO, allowing him to siphon off, little by little, the ethers (Ethereum's currency or Token) held by the DAO. Nearly 3.6 million ethers were hacked in this way, representing more than 30% of the funds of the DAO![4]

We also readily see in this the emergence of new forms of artificial intelligence based on the principles of "plantoid"[5] AI as is shown by the incredible work of Primavera de Filippi[6], a researcher at the Harvard faculty of law.

WHY IS THE BLOCKCHAIN A REVOLUTION?

Certain people see in it the means for shifting to a large-scale collaborative economy and also new ways of exercizing democracy, like the new liquid democracy7. Others are banking on the promise of a drastic reduction in transaction costs thanks to the elimination of intermediaries; yet others see in it the opportunity to develop brand-new services and in doing so, take dominant positions on markets that are either entirely new or already exist – which is clearly a cause for concern on the part of those players already in place, and with good reason… Even if this emerging technology, that almost nobody understands, remains abstruse for most people, today we need to have the right level of abstraction to be able to discuss it, take an interest in it, and begin to imagine its impact on the models for today's and tomorrow's organizations.

Although the Bitcoin remains the only very large-scale application of the Blockchain to date, all observers are in agreement that this technology is disruptive in nature. According to some, its irruption could provoke a break on the same scale as the TCP/IP, the protocol at the origin of the Internet!

We are facing the second generation of the Internet, that of values and transactions, whilst the first generation was largely that of information and network communication (and hence a shift from the automation of the decentralized relationship to the automation of the decentralized transaction).

For all that, is it right to talk about a revolution? Beyond the fact that it needs much more than a technology to bring about a revolution, it is, in any event, too early to say. However, the social and economic context is favorable and, with the creation of a highly dynamic ecosystem, the conditions are right for there to be an increasing number of experiments. They already extend well beyond the realms of payment methods and even finance, even if it is in that sector that we are currently seeing the greatest number of initiatives and alliances with startups/fintechs working on the Blockchain.

FOUR MAIN CATEGORIES OF USE OF THE BLOCKCHAIN.

If we take stock of the initiatives and experiments currently underway, this reveals four major areas of use of the Blockchain.

1/ The facilitation of exchanges: cross-border payments, micropayments, and the exchange of unquoted stocks are the first identified cases. We can readily cite the case of the German bank Fidor, in association with the Ripple Labs startup, that put in place extremely low cost payment and currency exchange services for its customers. Two advantages of the Blockchain are being exploited here: its speed and its largely optimized costs. In this regard, Santander Bank is predicting a saving of 15 to 20 billion per year for the financial services industry from 2020.

2/ The notarization of instruments and documents: as we have seen, the Blockchain has the ability to store, and render tamper-proof, the evidence that a document exists on a given date. The Léonard de Vinci University at La Défense in Paris is experimenting with this paperless method to certify the diplomas it awards.

3/ The certified execution of workflows: the Blockchain enables each stage of a workflow to be published and publicly checked. Whether it involves an industrial quality control process or even a logistics process, the trusted workflow logic makes it possible to quite simply ensure

[2] *https://en.wikipedia.org/wiki/Decentralized_autonomous_organization*

[3] *https://daohub.org/*

[4] *When a member leaves the investment fund he triggers a function called splitDAO(). That gives rise to 2 problems. The first is that the member must provide his own code with the transaction. This code enables the DAO to be told where it must transfer the Ethers. This is a necessary function that is also part of Bitcoin. The second problem is that the Ethereum code is recursive. That means that when a function is launched, it can call itself a second time. And the bug occurs when the splitDAO() is called. When the call is made, it will call the code of all the recipients to transfer the Ethers. The code of the recipients will then call splitDAO() again before finishing the process. But with the bug, that provokes a repetition of the process, transferring more Ethers. Roughly speaking, the splitDAO() is triggered, and it calls the code of the "hacker", which calls splitDAO(), which again calls the code of the "hacker", and so on. Instead of sending the desired amount to the person who wishes to leave the investment fund, the process becomes an infinite loop depleting all the currency units of the DAO.*

[5] *http://theconversation.com/do-plantoids-dream-of-electric-arts-council-grants-52263*

[6] *https://cyber.law.harvard.edu/people/pdefilippi*

[7] *https://discuss.pirateparty.org.au/t/liquid-democracy-on-blockchain-and-in-parliament/527*

that all parties concerned have participated in the process in a definite, irrevocable manner and that this is known to all, simply and easily, as information is shared at every point of the network's nodes. Pharmaceutical laboratories are envisaging, for example, using the Blockchain to obtain the consent of patients to each new stage of a test protocol more quickly and thereby reduce the costs and length of the phases of clinical trials on new molecules.

4/ Digital deeds of title: the entry on a Blockchain's distributed register makes it possible to certify an individual's ownership and keep a trace of all transfers of a material or digital asset. With the assistance of the Bitland NGO, the government of Ghana is banking on these properties of the Blockchain to put an official land register in place at a lower cost. Digital artists are starting to use it to authenticate their works, control their dissemination, and protect their rights. This facet of the Blockchain technology marks a break with the first generation of the Internet that witnessed creators, the rights owners, seeing themselves deprived of their rights to the benefit of players like Spotify, Apple Music… without even mentioning the impact of piracy.

BLOCKCHAIN OF THINGS AND BLOCKCHAIN OF DATA

So as to take things further and open up new perspectives, notably with the Internet Of Things (or IoT), which seems to be an unstoppable wave in our digital societies, we can touch upon various examples in B2C (activity trackers, home automation…) or in B2B (sensors for monitoring fleet cars, sensors for all the parts of an aircraft…), where the IoT requires a capacity to carry out billions of transactions each day in an automated manner.

It appears imperative to us that a Blockchain of Things emerge, storing all these transactions, with Smart Contracts[7] regulating the relationships between these increasingly advanced objects. In fact, the IoT gives objects the possibility of performing transactions directly and fully autonomously. This vision of the IoT implies that the objects communicate and effect transactions between each other. The decentralized aspect of the Blockchain constitutes the cement enabling these objects to transact amongst themselves and retain the proof of this in a pre-defined frame of reference (Smart Contract), doing so entirely autonomously (AI) and securely. This current digital revolution corresponds to the digital economy shifting from "platformization" (putting people in direct contact with each other) to "Blockchainization" (putting "agents" in direct contact with each other).

Under a similar rationale, we place our trust daily in numerous organizations that store and use our personal data. In many cases, our informed consent is not really sought or approved.

The Blockchain of Data could be a solution for storing our individual information, but above all for managing (via the Smart Contract mechanisms) the rights granted and/or delegated to enterprises. Certain data could be free of charge, subject to certain conditions, others could be charged for when used, and finally a last category of them could be available for use solely by invitation.

PREPARING FOR THE BLOCKCHAIN TSUNAMI.

Given the universal nature of these categories, it becomes clear that all sectors, public and private, are concerned and will be affected, in one way or another, by the adoption and spread of Blockchain technologies. The number of processes likely to be affected is truly phenomenal. The banks were not wrong on this. Be it individually or collectively, as is the case within the R3 consortium[8], they are exploring and experimenting with the possibilities of the Blockchain, with a dual objective: of benefiting from its advantages (in terms of security, costs, and transparency) and of integrating the point-to-point logic into their own model, so as to better withstand the arrival of new players using a natively distributed and disintermediated model. The insurance world is doing likewise and is notably taking an interest in the possibilities offered by Smart Contracts.

The first suppliers of solutions for creating public or private Blockchains are beginning to appear. Startups are flourishing and attracting investors. In all sectors, we should therefore expect to see a surge in players proposing virtually free P2P services. Whilst they were disruptive 5 years ago with their platforms connecting people, the leading lights of the so-called sharing economy are not immune: the Israeli startup LaZooz.org and its English counterpart Arcade City fully intend to "uberize Uber" with its decentralized and self-managed car-sharing service based on the Blockchain…

The only way for an enterprise to prepare for the announced upheavals is to take an interest as of now in the Blockchain and its ecosystem. The first action to take is to identify the winning strategies to accelerate your transformation and stay one step ahead. That involves taking a fresh look at all the "nuts and bolts" of the organization and its value chain and, in a way, thoroughly reviewing the existing models before re-thinking them in terms of horizontal, decentralizing, and secured technologies in P2P mode as called for by Michel Bauwens[9].

This exercise can seem complex, but it is the surest way to precisely identify where the Blockchain can make a contribution and begin to experiment with it under a Proof of Concept rationale.

The philosophy behind this approach of becoming acculturated to the Blockchain and experimenting with it can be summed up in one sentence: "disrupt" oneself so as not to suffer the disruption. Internet promised instantaneous, immediate, and permanent information and communication in real time. The Blockchain will promise collaboration, transparency, decentralization, and the securing of all transactions in the broad sense…

E.LB. F.M.

[7] *These smart contracts are autonomous programs that automatically execute the terms and conditions of a contract, without the need for human intervention. The concept is not new, but the Blockchain makes it more secure and replaces the previously required trusted third party.*

[8] *With more than 40 major banks having joined it since its creation in New York in 2014, the R3CEV consortium acts for the financial industry developing and experimenting with standards and solutions based on the blockchain technology.*

[9] *http://www.editionslesliensquiliberent.fr/livre-Sauver_le_monde-9791020901835-1-1-0-1.html*

ABOUT THE AUTHORS

Eric Lévy-Bencheton has for some 20 years now been assisting his clients with their Marketing, Sales & Customer transformations, accelerated by Digital technologies. In the first instance, he developed sector knowledge in the banking field, which he then supplemented with experience in the Distribution, Telecoms, Energy, and Transport sectors. As early as 2011, Eric began to help his clients make the most of social media for Customer Relationship Management and published one of the first reference documents on the subject ("Social CRM – Towards Enhanced Customer Relationship Management"). He joined **Keyrus** at the beginning of 2015, attracted by the company's ability to utilize the Digital drivers of clients' transformations to serve their interests, and to accelerate those same transformations by exploiting their information capital. His role within **Keyrus** is that of Strategic Account Executive, essentially in the financial services field. Working with Bruno Teboul, SVP Sciences & Innovation, Eric leads the development of our offerings centred around the Blockchain technology.

Frédéric Maserati has worked for almost 20 years in the Retail Banking and Retail sectors. He has held several operational positions notably in marketing and e-business for several major banking groups. From 2011 in his capacity as Senior Manager in a Major Firm, Frédéric assisted numerous Banking and Distribution players with problem issues centred around payments, distribution, new user environments, and Big Data. He has also been involved in numerous market events like the Payforum and Banking & Innovation, in his capacity as an expert on Payment and Innovation. He joined **Keyrus** in 2015 as Consulting Director within **Keyrus Management**, where he is developing several offerings around the Blockchain, Cryptocurrencies, the commerce of tomorrow and the bank of the future, and new approaches centred around Artificial Intelligence. He is increasingly interested in the impact of exponential technologies on the new business models of banks and retailers.

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 15 countries on 4 continents, the **Keyrus** Group has 2500 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 insight into value
Marketing and Communication Department
155 rue Anatole France, 92593 Levallois-Perret Cedex – Tel. : +33 (0)1 41 34 10 00 - marketing@keyrus.com