WAVESTONE

BLOCKCHAIN
HOW TO RETHINK TRUST

BLOCKCHAIN : DISRUPTIVE INNOVATION OR OVER-HYPED DEVELOPMENT?

You'll have been hard pressed not to have read at least one article about *blockchains* and their potential benefits! Having said that, apart from a small group of experts, it's an area that is still little understood. In between a stream of press releases—really marketing announcements dressed up as news of innovations—and white papers, that tackle the subject from the very specific angle of fundamental computer-science research, statistics, and cryptography, it can be difficult for decision makers at major companies to set a sensible way forward.

To illustrate the thinking, let's take the analogy of medical research, where the development of new solutions is very carefully managed. As a thought experiment to see whether *blockchains* are a fully developed technology, we can compare it with a new drug. A number of questions come to mind naturally, like: what disease is the drug intended to treat? Where are we in terms of testing? And is the product sufficiently mature for marketing authorization?

Let's take a look at where *blockchains* are, in terms of these questions.

AUTHOR

JONATHAN GÉRARDIN
jonathan.gerardin@wavestone.com

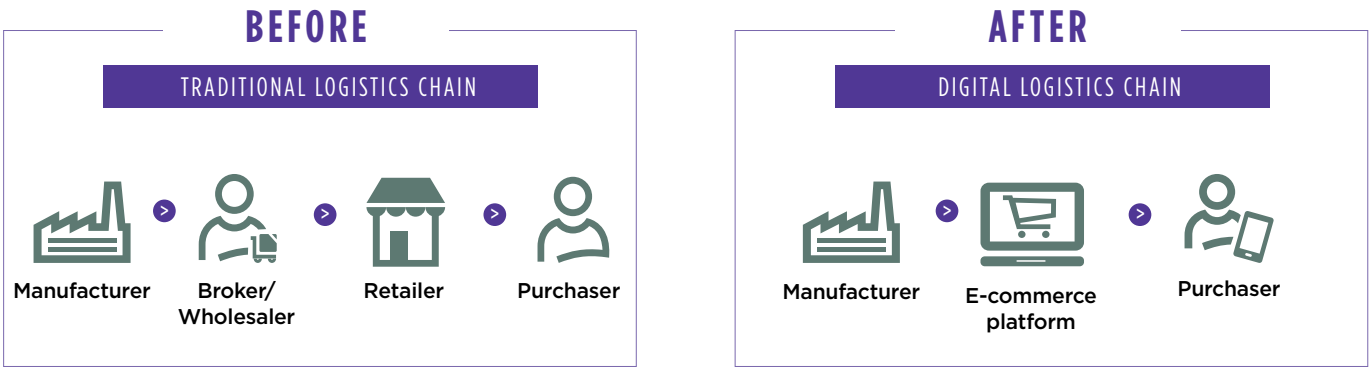
IS IT POSSIBLE TO CREATE AN ELECTRONIC CURRENCY WITH NO CENTRAL ORGANIZATION TO GUARANTEE IT?

Over the last two decades, the rise of the internet has led to major economic upheavals, especially those driven by the disappearance of former intermediaries. A number of sectors using third parties who specialize in the commercialization of products and services have been deeply affected. Tourism and distribution are good examples.

These well-known intermediaries have gradually been replaced by new, hyper-generic players, offering trading platforms based on advanced technologies, which have created the digital giants we know today: Amazon, Apple, Google, and Facebook. They have thrived as a result of being willing participants in massive disintermediation, which has been driven by the considerable costs reductions associated with their models, as well as the offer of faster and more flexible transactions.

The focus of this disintermediation process has been on simplifying supply chains, removing intermediaries between suppliers and customers.

The disintermediation process



Yet the dematerialization phenomenon has significantly reinforced the role of one type of intermediary. When we make an online purchase, we rely on a trusted third party, responsible for guaranteeing the reliability, security, and auditability of the payment: payment bodies, like the banks, Paypal, and so on. Their role is to ensure that payment transactions between buyers and sellers are properly executed, while also ensuring the integrity of the system as a whole. Where dematerialized (not physical) payments are involved, technically speaking, the sums of money can be duplicated as easily as copying a file. Certain precautions must therefore be taken to ensure that confidence in the monetary exchange system remains intact.

The topic of "double spending" is a text-book IT problem, which has come to prominence as a result of the widespread use of dematerialized methods of payment. The challenge is to ensure that transactions are as fast and flexible as those we make with physical currency.

Since the rise in popularity of bank cards in the 1980s, no solution to this problem has been found that doesn't involve relying on a trusted, third-party intermediary with responsibility for verifying and effecting payment transactions.

With the explosion of e-commerce in the 2000s, the problem was eventually considered to be insoluble, until 31 October 2008, that is, when **the White Paper, *«Bitcoin: a Peer-to-Peer Electronic Cash System»***[1] was published. In it, **Satoshi Nakamoto** presented an electronic-money solution, and demonstrated that the «double spending" problem could be solved without the use of a trusted third party.

Picking up our medical analogy again, "double spending" is the disease that Bitcoin proposed to treat; and it was, in fact, the first time a *blockchain* had been used.

1- Bitcoin P2P e-cash paper - Cryptography mailing list - Satoshi NAKAMOTO - October 31st 2008 - http://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html

BLOCKCHAINS : WHOSE TECHNICAL VIABILITY IS DEMONSTRATED DAILY—USING BITCOIN

A *blockchain* is a registry of binding transactions operating with no central authority.

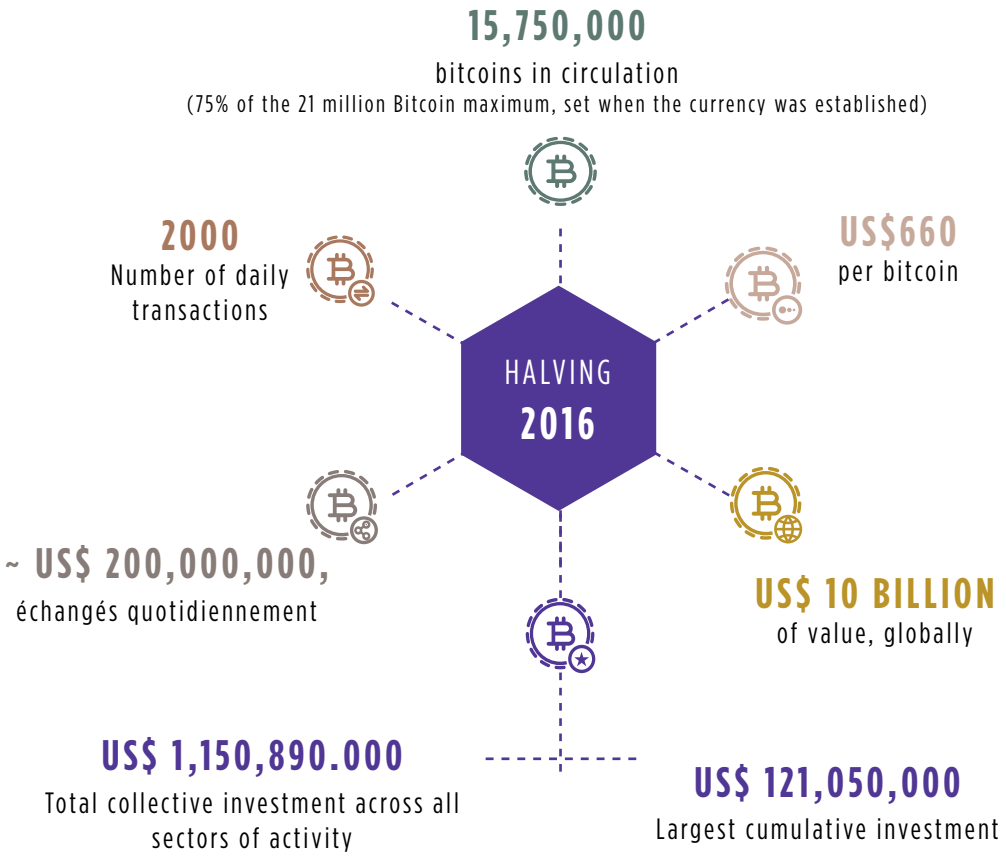
Over a period of eight years, Bitcoin has proved the robustness of Satoshi's system, and its *blockchain* continues to grow. The model, therefore, is a long way from being simply a theoretical proposition: today, it is **an operational system for the management of worldwide electronic transactions, using an approach that is not based on trust in a central authority.** In summary, we can say that: in vivo trials have shown the drug to be effective, and the large-scale testing phase has been successful.

To better understand the road taken, Bitcoin's position on 9 July 2016[2] is shown in the diagram below.

July 9 2016 is a symbolic date for Bitcoin. The reward associated with the mining of a new block (a validation operation for a group of transactions) is halved every 210,000 blocks, something known as Halving. On this occasion, the reward went from 25 to 12 bitcoins. The next milestone will be on 26 June 2020, when the reward associated with mining a new, valid block will be reduced to six bitcoins.

And although, initially, the *blockchain* was nothing more than a technical solution allowing Bitcoin to function, it is, in fact, a genuine alternative system to relying on a central authority to guarantee a registry of transactions—of any type. Compared with traditional systems, ***blockchains*** **claim to offer greater processing efficiency, more flexibility, and reduced operating costs**. What's more, these benefits are possible as a result of the elimination of trusted third parties (disintermediation).

Bitcoin at July 9 2016



2- Source : Bitcoin Magazine Halving Infographic - https://bitcoinmagazine.com/articles/the-halving-then-now-a-bitcoin-magazine-infographic-1468082535

CAN *BLOCKCHAIN* BE A DISRUPTIVE INNOVATION, BEYOND ELECTRONIC COINS?

As in every industrial cycle, an innovation is accompanied by an ecosystem of companies, organizations, and entrepreneurs, who want to transform technical progress into new products or services. ***Blockchain*, then, could potentially transform any sector whose product or service is based on trus**t. The number of players has continued to grow, be it "generalists," where the basic service is trust («Trust as a Service»), or specialists providing niche services.

But, so far, apart from electronic currencies, the search for an application where the *blockchain* could offer advantages compared with traditional solutions, has not yielded any obvious areas that were ripe for transformation.

Taking our drug analogy, we could say that the reproducibility of a *blockchain*'s beneficial effects is still to be demonstrated. While waiting for such a demonstration, marketing authorization would not be granted, and experimentation with the drug confined to the laboratory.

HOW TO MOVE FROM TECHNOLOGICAL INNOVATION TO ESTABLISHED COMMERCIAL USE?

The *blockchain*'s fundamental technical principles are mature, and the model has a demonstrable value. However, **there is still some distance to be traveled to find the right applications, and transform technical progress into innovative new products or services capable of widespread adoption**.

Recent news highlights the current challenges that market pioneers are

A sample of the *Blockchain ecosystem*

1 GENERALISTS

« *TRUST AS A SERVICE* » PLATFORMS

Ethereum, Rootstock, Tendermint, Lisk, Eris...

2 NICHE SPECIALISTS

FINANCIAL SERVICES

Payments, loans, wealth management, crowdfunding

Blade, BitNet, BitPay, Ripple, BitBond, BTCpop, LoanBase, AlphaPoint, KolBanx, WelFund, Harvestr...

IDENTITY

Authy, BlockSeer, NetKi, OneName, ShoCard...

INSURANCE AND MICRO-INSURANCE

Augur, EverLedger, WeKeep, Consuelo, Riskebiz...

LEGAL SERVICES, INTELLECTUAL PROPERTY

BitProof, CoinSpark, Mamoru, Proof of Existence, Stampery...

currently coming up against. The most popular *blockchain*s are being used in the area of electronic currency; and these are naturally looked upon by other players with a degree of envy. More than ever, security requires the involvement of specialists to provide protection

- In March 2016, Shapeshift, an electronic currency exchange platform (which like a foreign-currency service, allows exchanges between Bitcoin, Ether, Litecoin, and other currencies) was the **victim of a hacking attack perpetrated by one of its own system administrators**[3]. Hacking resulted in the theft of $230,000, the platform being out of service for a month, and an urgent need to reconstruct its infrastructure.

  As a result of the incident, the company's basic security procedures had to be strengthened, particularly with regard to procedures for secure communication between employees, as well as the means of access to the servers hosting the platform.

- In June 2016, «the DAO», active on the *blockchain*, Ethereum, was the victim of a hacking attack costing 3.6 million Ether. "The DAO» is the trading name of a Decentralized Autonomous Organization, i.e. an organization whose articles (rules, governance, and means of decision making) are applied through smart contracts (software extensions permitting operations on the *blockchain*, according to conditions defined in a contract). The objective of a DAO is to eliminate the use of documents and people, in order to create a structure that functions in a decentralized way.

"The DAO" could be considered as an investment-fund management organization for a set of projects, whose operation is based solely on smart contracts.

One of the DAO's smart contracts found itself vulnerable to **a security flaw due to an implementation error**[4], which was then exploited.

This hacking attack immediately resulted in the collapse of the Ether's valuation, which fell from $21.5 to less than $13, in the space of a few hours. Even with this fall in value, the amount stolen still represented a value of more than US$60 million. At the end of July, after several weeks of discussions, the Ethereum community effected a hard fork (an operation resulting in the creation of a new *blockchain* based on an existing history, but modifying some of the rules of operation), in order to recover the stolen funds.

It is important to emphasize that the security vulnerability exploited was not related to the implementation of the Ethereum *blockchain*, but only to that of a smart contract, which was designed by a third-party. The design of smart contracts, and their development, are activities that should be considered critical, and systematically subject to specialist audits.

Ultimately, it is the hard fork decision made by the Ethereum community that will have the greatest long-term impact. This event demonstrates that the history and the rules applicable to a *blockchain* , supposedly unalterable, can be modified voluntarily, if enough miners decide to associate their resources with the decision (note: in a hard fork, two *blockchain*s coexist in parallel, and participation in one or the other becomes a choice for each participant).

3- https://info.shapeshift.io/blog/2016/04/19/timeline-shapeshift-hacking-incident
4-http://www.securityinsider-solucom.fr/2016/06/ethereum-x-dao-retours-sur-lattaque-de_30.html

THE ISSUES WITH *BLOCKCHAIN*, FOR LARGE ACCOUNTS, ARE NOT TECHNICAL

From a less sensationalist point of view, there are important issues still to be addressed if a *blockchain* is to be used effectively and easily beyond a limited population of specialized start-ups, which are more inclined to risk-taking.

The integral **transparency** of the most popular *blockchains* is an obstacle that some organizations may consider insurmountable. Looking beyond public networks, *blockchains* may be propagated by more restrictive models, both completely private ones, or those where management has been delegated to trusted third parties. Each of these variations is necessarily based on a compromise in terms of security or decentralization, by recreating a new form of trusted third party. Nevertheless, these private or semi-private *blockchains* seem to be good solutions for sharing information between several organizations. The prior trust between the participants allows certain adjustments to technical configurations, helping to improve the *blockchain*'s security (the principle and difficulty of transaction-validation operations, number of transactions per second, etc.).

The take-up and use of a service by multiple parties will, sooner or later, lead to divergences between stakeholders. Although, technically speaking, a *blockchain*'s protocol sets the rules by which it operates, it can be confronted with situations that are too complex to be managed solely by algorithms. The example of the exploitation of a security breach at «The DAO," or the discussions about the evolution of the Bitcoin protocol - to increase the number of possible transactions per second on that *blockchain* - are both examples that illustrate the **need for governance**. In the absence of such mechanisms, the fragmentation of the current market will continue to produce *blockchains* optimized for specific uses which are not interoperable. At the point where a dominant *blockchain* generalist manages to conquer the market, the use of intermediaries will be required to link the various *blockchains* together. The main objective, simplification through disintermediation, is therefore a long-term goal, which will depend on the degree of standardization and the consolidation of the ecosystem.

To continue our comparison with the medical world, the risk/benefit analysis of a *blockchain*, compared with traditional solutions, may seem rather negative, given what has been discussed. The experiments highlight a set of brakes that the research is attempting to address.

OBSERVER OR ENTREPRENEUR: WHICH IS THE RIGHT STANCE?

To summarize: the basic technical principles of the *blockchain* have demonstrated it to be capable of operating at large scale when used in **electronic-money-type applications**. Some of the limitations intrinsic to *blockchains* have also revealed themselves: limits on the number of transactions per second, energy consumption, latency, etc. Some of the current experiments aim to identify workarounds for these constraints, although it's difficult to predict what the results will be. And other investments are fueling an ecosystem of start-ups, which is growing in scale every day. **The objective is to identify applications where *blockchains* can make a concrete difference, disrupting traditional solutions**. It is in this second area that the uncertainties are strongest, but this is also where the greatest hopes and expectations lie, something generating intense speculation.

For a CIO, a CTO, or an innovation manager at a large account, there are three possible courses of action. Choosing one depends on a cocktail of considerations that are specific to each organization:

- The degree of management and operational control over the *blockchain*, and, more generally, the ability to map business issues to technological considerations;
- The corporate culture with respect to innovation: the appetite for risk and the resources allocated to R&D activities;
- The organization's ambitions in its market: whether it wants to be an innovator or a "steady as you go" organization.

The **first approach** is to actively pursue a **watching brief**, in terms of **business and technical** plans, the market, but also the **regulatory framework**.

In 2016, in France, the government began to shape a regulatory framework for companies and institutions. June 2016 saw the first reading of the Sapin II Bill, with plans to allow the use of *blockchains* in specific, regulated applications. In March 2016, Emmanuel Macron, then the French Minister of the Economy, Industry and Digital Technology, announced a modification to the regulations, in order to allow *blockchains* to be tested on the cash markets. The field of application may next be extended to unlisted securities.

The **second approach** is that of **experimentation around a variation on the use of electronic money** (see page opposite). Potential applications can be found in areas where physical currency is used in a dematerialized way; examples are: the creation of exchange markets, transaction registers, or automatic funds transfers between a number of organizations - without a central authority.

- Readily available solutions exist to create prototypes for these types of application. **The main difficulty lies in the identification of business problems that lend themselves well to such operations.**

Unsurprisingly, central banks, regulators, and large banking players have seized on the possibilities and have been testing them for several months now:

- **Financial sector players** are the most active in this area and taking steps to pool their resources via the international consortium, R3

(which involves Société Générale, BNP Paribas, and Natixis) and the innovation lab launched by Caisse des Dépôts[5] which brings together AXA, BNP Paribas, *Blockchain* Solutions, BPCE Group, Cellabz, CNAM, CNP Assurances, Crédit Agricole, Croissance Plus, Paymium, and the Finance Innovation Competitiveness Cluster.

- **Banque de France is conducting its experiments through an interbank operational project**[6] to exchange, and share, information and data with the various players in the financial system. The first area of application involves the sharing of a French financial market database, the SEPA Creditor Identifiers repository.

The **third approach**, which is the most complex, is that of a ***blockchain* experiment** in the form of a **technical solution enabling a new mode of operation** or a new service.

To be able to identify such cases, which necessarily involve innovation, we are strongly of the view that there is a need to:

- put in place of a participatory approach to innovation, involving both business and technical managers;
- gain a thorough understanding of both the traditional architectures and the internal functional mechanisms of *blockchain*, in order to ensure a truly viable solution.

The overarching challenge is **to find the right decentralized control mechanism, before recording a new transaction, or data, in the registry.**

SPOTLIGHT ON...

WHY ELECTRONIC CURRENCIES PROVIDE POTENTIAL APPLICATIONS FOR *BLOCKCHAIN*?

Regardless of the circumstances surrounding the creation of the first *blockchain*, and its natural association with Bitcoin, electronic currencies have certain characteristics that mean *blockchains* can offer particular resilience in these types of applications.

For an electronic currency exchange to be considered as valid, the issuer must possess the amount of currency they want to be credited. The public nature of the register of transactions allows all participants autonomous control of the validity of the exchange. Each new transaction recorded in the *blockchain* has thus been validated, and remains verifiable, by all participants, in a transparent and decentralized way.

For electronic currency, the mechanism for checking the validity of a transaction is based only on the data present in the *blockchain*.

To conclude our medical parallel: if a blockchain were a medicine, considering the information presented, the national medical regulator might conclude:

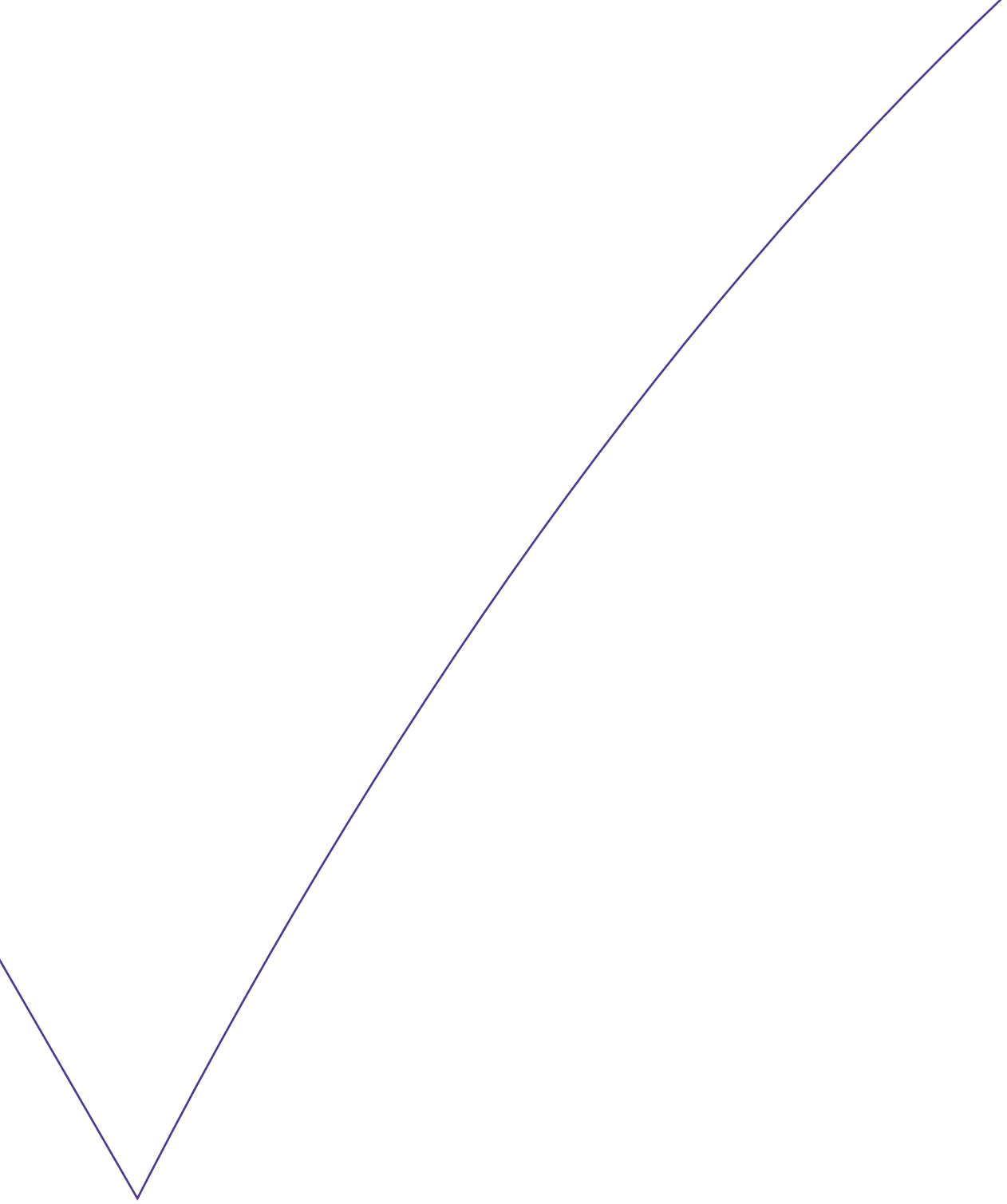
- That a blockchain is a solution aimed at treating the disease of "double spending," outbreaks of which have been caused by the emergence of electronic currencies; and that the most effective treatment found, to-date, is the use of a «trusted third party» (payment institutions: banks, Paypal, etc.).
- This drug is effective in vivo: the results have been demonstrated by a successful large-scale testing phase: Bitcoin.
- For other, related illnesses that affect transactions between individuals, the reproducibility of a blockchain's beneficial effects remains to be demonstrated. For these conditions, the risk/benefit analysis of the use of a blockchain, compared with the use of a conventional «trusted third party», might seem rather negative at present.

And for all of the above reasons, this medical product cannot be considered for marketing authorization at present, and requires further analysis and research. However, its use by specialists is permitted for treatment of some cases of the disease, caused by the use of «trusted third parties», and associated with electronic currencies.

This publication will be complemented by a more technical one, aimed at architects, analysts, or R&D professionals who have a need to explore the subject in greater depth in order to carry out tests within their organizations or evaluate the risks and benefits of the use of a blockchain, compared with other, traditional solutions.

5- http://www.caissedesdepots.fr/lancement-dune-initiative-de-place-sur-la-blockchain-avec-11-partenaires

6- https://www.banque-france.fr/sites/default/files/medias/documents/communique-de-presse_2016-12-15_la-banque-de-france-mene-une-experimentation-de-blockchain-interbancaire.pdf



WAVESTONE

www.wavestone.com

Wavestone is a consulting firm, created from the merger of Solucom and Kurt Salmon's European Business (excluding retails and consumer goods outside of France). The firm is counted amongst the lead players in European independent consulting.

Wavestone's mission is to enlighten and guide their clients in their most critical decisions, drawing on functional, sectoral and technological expertise.