BLOCKCHAIN IN PRACTICE

WHAT ARE THE USES AND LIMITS OF THIS NEW TECHNOLOGY?

Financial services—in particular insurance—have been identified as the markets where Blockchain has the highest potential.

Insurance companies are well aware of this potential and are at the leading edge of research into the technology.

A survey conducted by MEDEF (France's largest employers' federation), in May 2017, shows that financial and insurance companies' interest in Blockchain is very real: 74% of decision makers have a strong interest in the technology, and 76% want to pilot Blockchain.

In its functioning, Blockchain is very different to many traditional technologies; it requires new technical skills to be used to its full potential. Wavestone has analyzed Blockchain and constructed POCs (Proofs of Concept) to better understand these completely new ideas, measure their potential, and assess their structural and applicational limits.

CONTACTS

LAURENCE AL NEIMI
laurence.alneimi@wavestone.com

NICOLAS MAI
nicolas.mai@wavestone.com

This publication has been produced with contributions from Islem BEN TAHER and Arnaud CHIKHANI.

STRONG OR LIMITED POTENTIAL?

Thanks to the innovative technological concepts associated with it, Blockchain offers very strong potential for insurance companies in three broad areas: record keeping, transactions, and smart contracts.

/ **Record Keeping**
Here, Blockchain's functionality meets the parties' need to keep records; it allows records to be stored transparently—in an unalterable registry.

This functionality allows all the relevant insurance players to access the same unfalsifiable information instantly—information that is updated in real time, guaranteeing traceability and efficiency.

/ **Transactions**
Because each member of the network has a complete, authenticated, and traceable, view of the transaction history, Blockchain makes it possible to perform digital transactions within a peer-to-peer network, in particular between partners within the insurance ecosystem. This feature offers scope for payments to be made or logistical operations to be carried out.

/ **Smart contracts**
Blockchain enables the storage and operation of smart contracts that can execute stored code automatically. This paves the way for process automation in areas like disaster compensation; possibly triggered by external data, delivered by an oracle—a trusted third party.

The immaturity of the technology

Today, large-scale deployment represents a considerable technological challenge. While experiments may work well in a controlled environment, with a well-controlled number of participants, difficulties nevertheless arise in large-scale use.

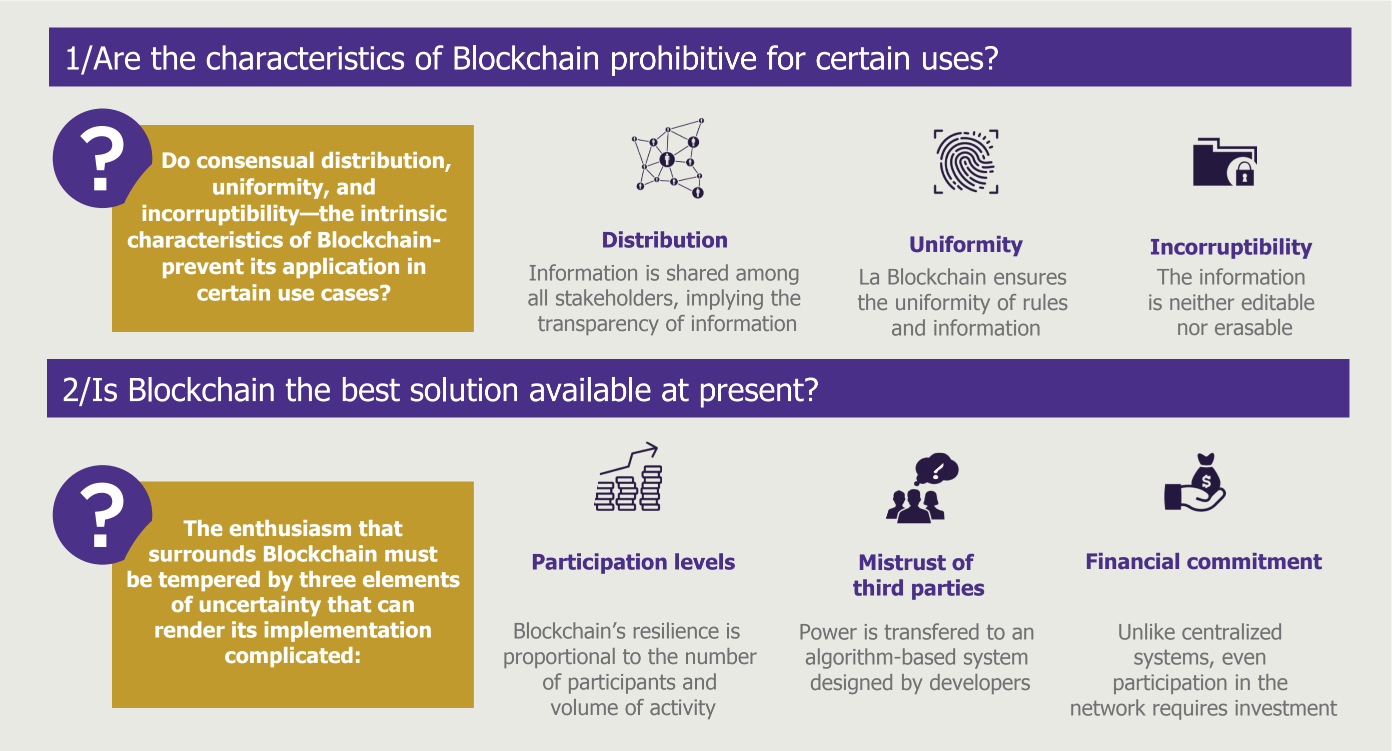
In addition, it should be kept in mind that the cost of mining (the required computational power x the processing cost) of a block increases with the size of the Blockchain, something that threatens the sustainability of mining activities. The difficulty of finding a new block has increased sevenfold over the past year[1], even though miners' transaction costs (in $US equivalent) have remained substantially the same over this period[2]. In general, the unit cost per transaction (miners' total revenue/number of transactions) has increased tenfold in the space of a year[3].

The challenge with this emerging technology, which can handle a range of new concepts, is the difficulty of understanding all its technological dimensions, as well as its ergonomics, if it is to offer a simple and attractive customer journey. To date, few experts have been able to master this requirement for dual competency.

And we note that developments in Blockchain's usage are currently, for the most part, confined to start-ups. In 2017, they were responsible for 70% of all Blockchain investments.

Lastly, where the issue is one of testing and understanding Blockchain technology, the use case doesn't particularly matter. Conversely, when the aim is large-scale deployment, it is fundamental, especially with respect to traditional solutions. To provide assurance in cases like this, we have established the **double filtre Wavestone** ®, which can help establish the suitability of a Blockchain project. Using the filter to evaluate the idea, allows the use case to be assessed.

Le double filtre Wavestone® permet d'évaluer la pertinence des cas d'usage Blockchain



1/Are the characteristics of Blockchain prohibitive for certain uses?

? Do consensual distribution, uniformity, and incorruptibility—the intrinsic characteristics of Blockchain- prevent its application in certain use cases?

Distribution
Information is shared among all stakeholders, implying the transparency of information

Uniformity
La Blockchain ensures the uniformity of rules and information

Incorruptibility
The information is neither editable nor erasable

2/Is Blockchain the best solution available at present?

? The enthusiasm that surrounds Blockchain must be tempered by three elements of uncertainty that can render its implementation complicated:

Participation levels
Blockchain's resilience is proportional to the number of participants and volume of activity

Mistrust of third parties
Power is transfered to an algorithm-based system designed by developers

Financial commitment
Unlike centralized systems, even participation in the network requires investment

[1] Source Blockchain.info (March 2018): https://blockchain.info/fr/charts/difficulty?timespan=1year
[2] Source Blockchain.info (March 2018): https://blockchain.info/fr/charts/transaction-fees-usd?timespan=1year
[3] Source Blockchain.info (March 2018): https://blockchain.info/fr/charts/cost-per-transaction?timespan=1year

Risks surrounding the technology

The entire Blockchain has numerous vulnerabilities—something that needs to be looked at closely. There are three major risks that make the approach particularly vulnerable.

- **The quality of the code in smart contracts:** Unlike a conventional program, smart contracts are unalterable. Programming them correctly is therefore critical. A flaw in the algorithm can enable them to be easily altered or misappropriated.
- **The governance of Blockchains:** the regrouping of miners in a mining farm can lead to a concentration of control. Between December 20, 2017 and March 20, 2018, three Chinese farms accounted for 56% of the computing power of Bitcoin's Blockchain.
- **The Blockchain Ecosystem:** the vulnerability of oracles and easily-attackable private keys is allowing Blockchain attacks to proliferate.

A regulatory framework under construction

France is aiming to be in the vanguard in here, and the Ordinance (a French statutory instrument) of April 28, 2016 put in place the provisions of Article L. 223-12 of the French Monetary and Financial Code permitting the use of a so-called DEEP ("dispositif d'enregistrement électronique partagé"—a shared electronic recording device), allowing the use of Blockchain technology for the transfer of mini-bonds. Then, Act No. 2016-1691 of December 9, 2016, known as the Sapin II Act, has allowed, again by means of an ordinance, Blockchain to be incorporated into the law applicable to financial securities. Lastly, following Ordinance No. 2017-1674, published on December 9, 2017, Paris has become the first financial center in Europe to define a framework for the transfer of ownership of financial securities by DEEP; it remains for the Council of State to fix the conditions applicable to the registration of financial securities in a DEEP; these will be applied by decree.

However, further moves down a regulatory route will require a thorough understanding of technological concepts and innovative uses. This state of affairs is similar to the way in which the internet was largely unregulated in its early years.
Being aware of this requirement, legislators are allowing experimentation to take place, something they themselves are taking part in.

In February 2018, France's Assemblée Nationale (the lower house of its parliament) launched two informational initiatives. The first focuses on uses not directly related to cryptocurrencies. The second focuses on cryptocurrencies and cryptoshares. The challenge is to find the right balance between regulation and prohibition, and to adapt the French legislative framework to the new financial behaviors of consumers and businesses.

BLOCKCHAIN AND THE GDPR?

The unalterable nature of the Blockchain is incompatible, in terms of principles, with the General Data Protection Regulation (GDPR) which comes into force in May 2018; there is a particularly poor fit with the GDPR's Article 17, which covers the right to have personal data erased.

A priori, as a result of this inalterability, the processing of personal data in a public or private Blockchain would be contrary to the regulation. A workaround has been put in place by several start-ups, such as BCDiploma—which stores and certifies diplomas. This solution aims to encrypt data with three keys: one for the student—and one durable and one permanent key for the institution. The encrypted data can only be read with the possession of these three keys. To make it impossible to access data, all that is required is for students who are storing their personal data to ask the institution to delete the durable key.

At the same time, Jean-Pierre Landau, the Banque de France's former deputy governor, is leading an initiative to develop guidance on changes to cryptocurrency regulations in 2018.

Using this approach, the personal data is not literally erased, but they become unreadable and access to them is impossible.

It is this type of issue that any future regulatory framework must address.

FROM PROTOTYPE TO REALITY: THE RIGHT APPROACH TO ADOPTING THE TECHNOLOGY WHILE ENSURING MASTERY OF THE TECHNOLOGICAL AND HUMAN DIMENSIONS?

Due to the newness of the technology and the lack of understanding of its potential, as well as the evolving regulatory framework, its mode of operation needs to be adapted, compared with traditional projects.

Large-scale deployment

The large-scale deployment phase has to be based on previous experimental work and developed hand-in-hand with the regulator. The POCs and experimental work must be used, in particular, to anticipate any difficulties in implementation.

Care must be taken to fit things into the existing legislative framework, and, as far as possible, to anticipate the future shape of regulation, in order to remain compliant with regulations.

The idea is to involve the regulator in large-scale deployment cycles in order to underpin the fundamental decisions that will have to be taken.

To cover for the possibility of the regulator's failure to engage in the process, or its silence on the matter, one option to anticipate the shape the of future legislative framework is to consider the regulator's overall philosophy: is it aimed at protecting consumers? Is there a desire to promote competition by applying light-touch regulation to the Blockchain technologies being used? Is the regulator seeking a balance between traditional and disruptive solutions? What are the stances being taken by regulators at the international level?

We can also obtain a host of clues by analyzing the various problem areas: have there been bad experiences with Blockchain that might lead the regulator to adopt a stricter framework?

WAVEVOTE®, AN ONLINE VOTING APPLICATION ON ETHEREUM

In order to experiment with this new technology, Wavestone has developed an online voting demonstrator based on the Ethereum Blockchain. The main objective was to address technical and functional constraints in order to best advise our clients on their own experimental work.

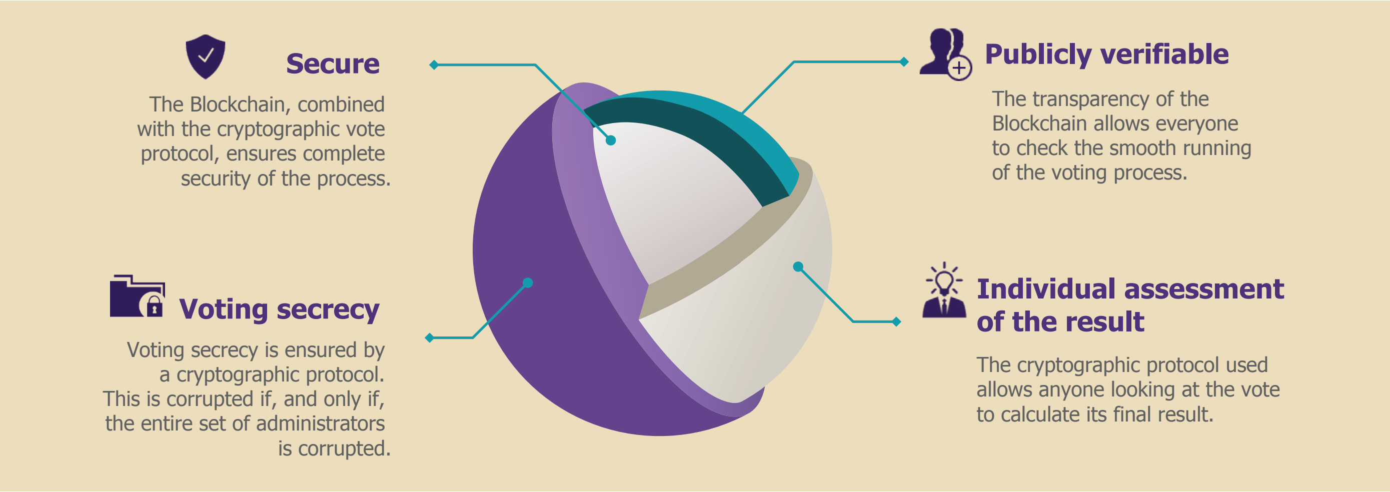
For ergonomic reasons, this demonstrator is transparent: it masks both the complexity of Blockchain and its cryptography.

Key results from the POCs

- 0 The cost of voting, excluding application creation and hosting (on servers) costs
- 1 Private blockchain
- 2 Main technical skills: back end (solidity, blockchain) and front end (interface)
- 4 Months of development

Pour être pertinent, le POC doit répondre à différentes contraintes pour assurer la qualité du vote

WaveVote®, an online voting application on ethereum



Secure

The Blockchain, combined with the cryptographic vote protocol, ensures complete security of the process.

Publicly verifiable

The transparency of the Blockchain allows everyone to check the smooth running of the voting process.

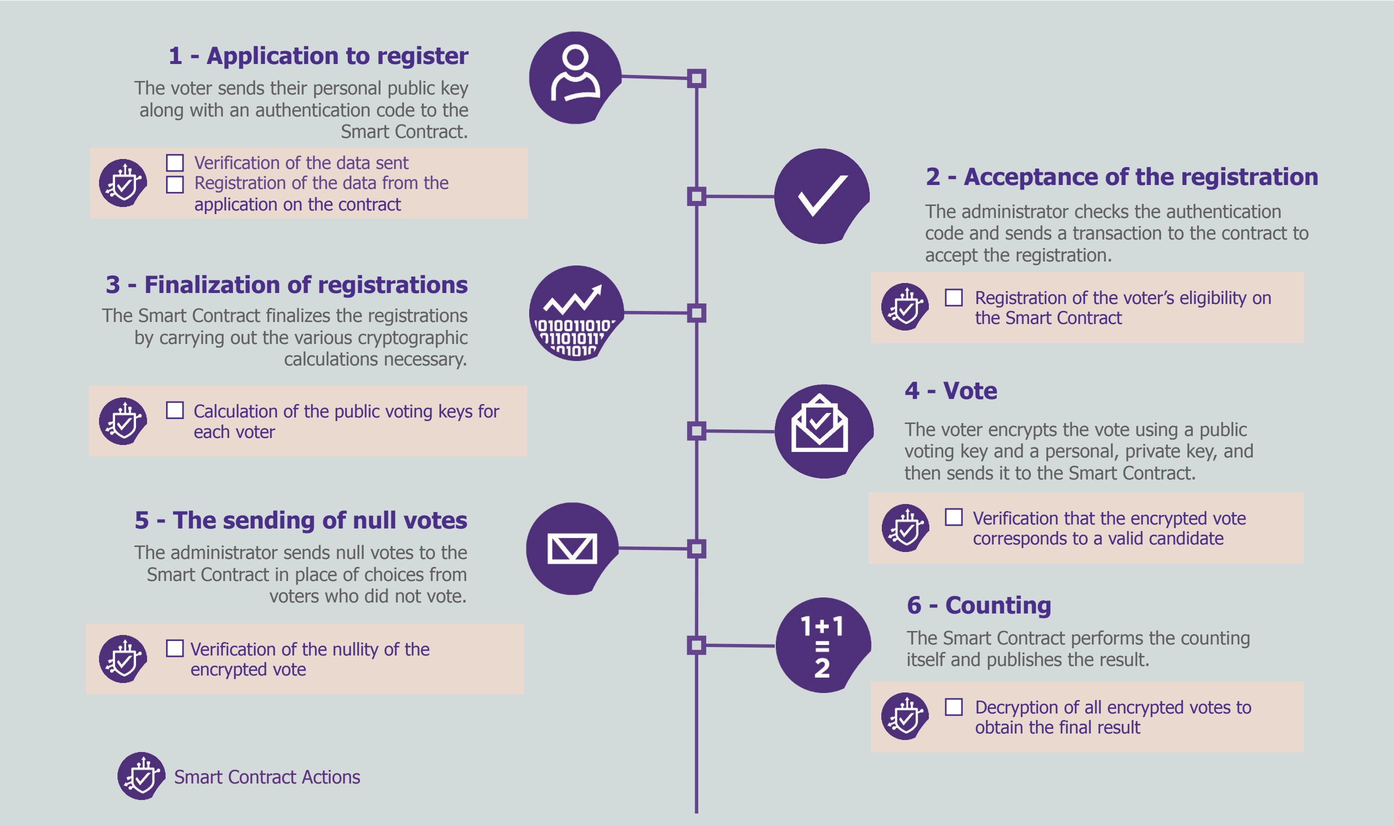
Voting secrecy

Voting secrecy is ensured by a cryptographic protocol. This is corrupted if, and only if, the entire set of administrators is corrupted.

Individual assessment of the result

The cryptographic protocol used allows anyone looking at the vote to calculate its final result.

Simplified functioning of the WaveVote® Demonstrator



1 - Application to register

The voter sends their personal public key along with an authentication code to the Smart Contract.

□ Verification of the data sent
□ Registration of the data from the application on the contract

2 - Acceptance of the registration

The administrator checks the authentication code and sends a transaction to the contract to accept the registration.

□ Registration of the voter's eligibility on the Smart Contract

3 - Finalization of registrations

The Smart Contract finalizes the registrations by carrying out the various cryptographic calculations necessary.

□ Calculation of the public voting keys for each voter

4 - Vote

The voter encrypts the vote using a public voting key and a personal, private key, and then sends it to the Smart Contract.

□ Verification that the encrypted vote corresponds to a valid candidate

5 - The sending of null votes

The administrator sends null votes to the Smart Contract in place of choices from voters who did not vote.

□ Verification of the nullity of the encrypted vote

6 - Counting

The Smart Contract performs the counting itself and publishes the result.

□ Decryption of all encrypted votes to obtain the final result

Smart Contract Actions

Limitations and difficulties encountered during WaveVote®'s development.

In its current configuration, the voting application cannot be scaled up; for example, for use in national elections. In fact, it faces a dilemma between being a public or private Blockchain:

1 **Public to ensure voting transparency**

Every citizen must be able to inspect and confirm the results of the vote. Such transparency in counting is not possible in a private Blockchain, where only administrators would have access to the results. Using a public blockchain solves this problem.

2 **Private to address technical limitations**

Voting activities (when not broken down) are too cumbersome to be integrated in traditional blocks. The administrator of a private Blockchain can choose to increase the size of the blocks so that they can support a transaction. But this is not possible on a public Blockchain.

Even at small scale, using a private Blockchain, we encountered several difficulties in developing this POC:

1 **Developments**

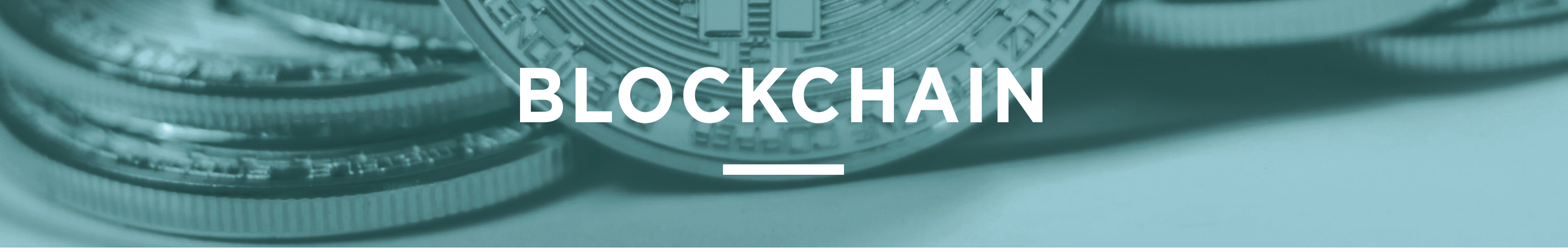
Because the technology is still young, the POC has been constructed without a development interface, and using a programming language that is still immature—something that makes the debugging of the program particularly complex.

2 **Gas**

Gas represents the computing power needed to mine a block on Ethereum. To protect the Blockchain, a gas limit per block is set in order to avoid «infinite» computation times. Although a private Blockchain was being used, it was not possible to increase the gas limit of a block. Additionally, gas breakdowns, when the computational power required exceeds the limit, are undetectable.

3 **Smart Contracts**

While Smart Contracts allow the integration of programs running in the Blockchain, their complexity remains limited. It is not yet possible to integrate sophisticated mechanisms into Blockchain.



BLOCKCHAIN

KEYS FIGURES

$587 bn

Valuation of cryptocurrencies at January 19, 2018—$814bn: their value peaked on January 7, 2018

$5,6 bn

Amount of funds raised via ICOs* in 2017

$2 bn

Cumulative Blockchain investments in 2017

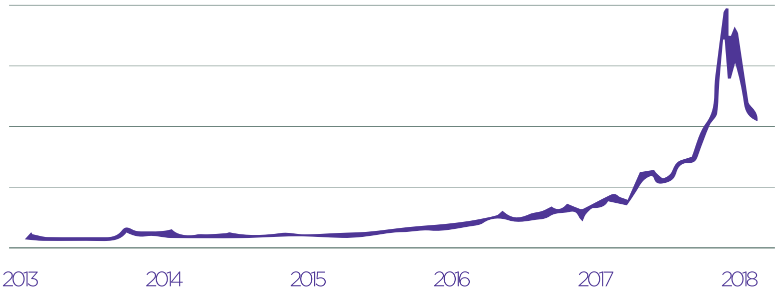
500

Number of startups, worldwide, developing Blockchain-based solutions in 2017

+ 2333%

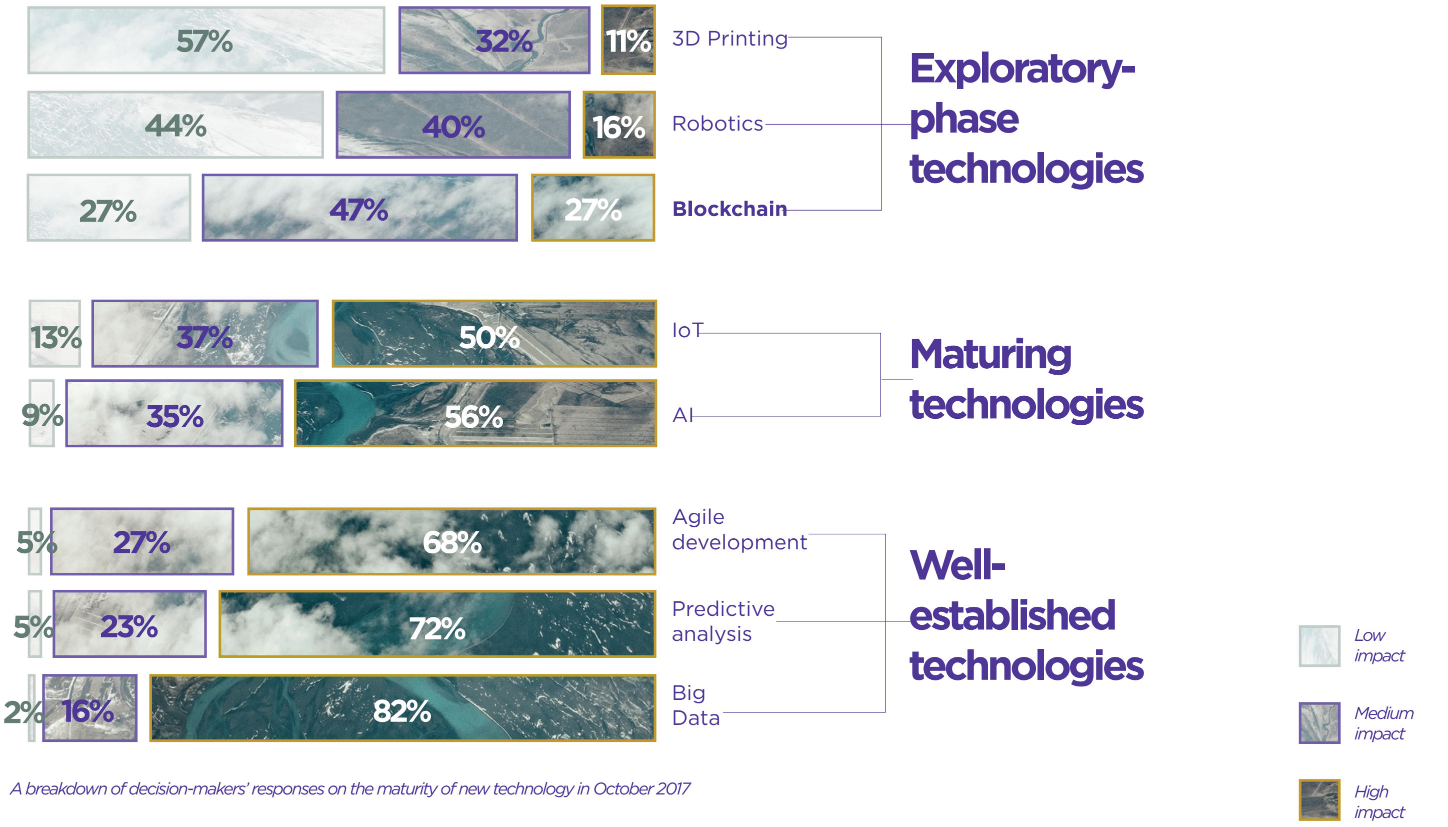
Investment growth in Blockchain between 2012 and 2017

* A ICO Initial Coin Offering is a fund-raising method that works by issuing exchangeable digital assets against cryptocurrencies



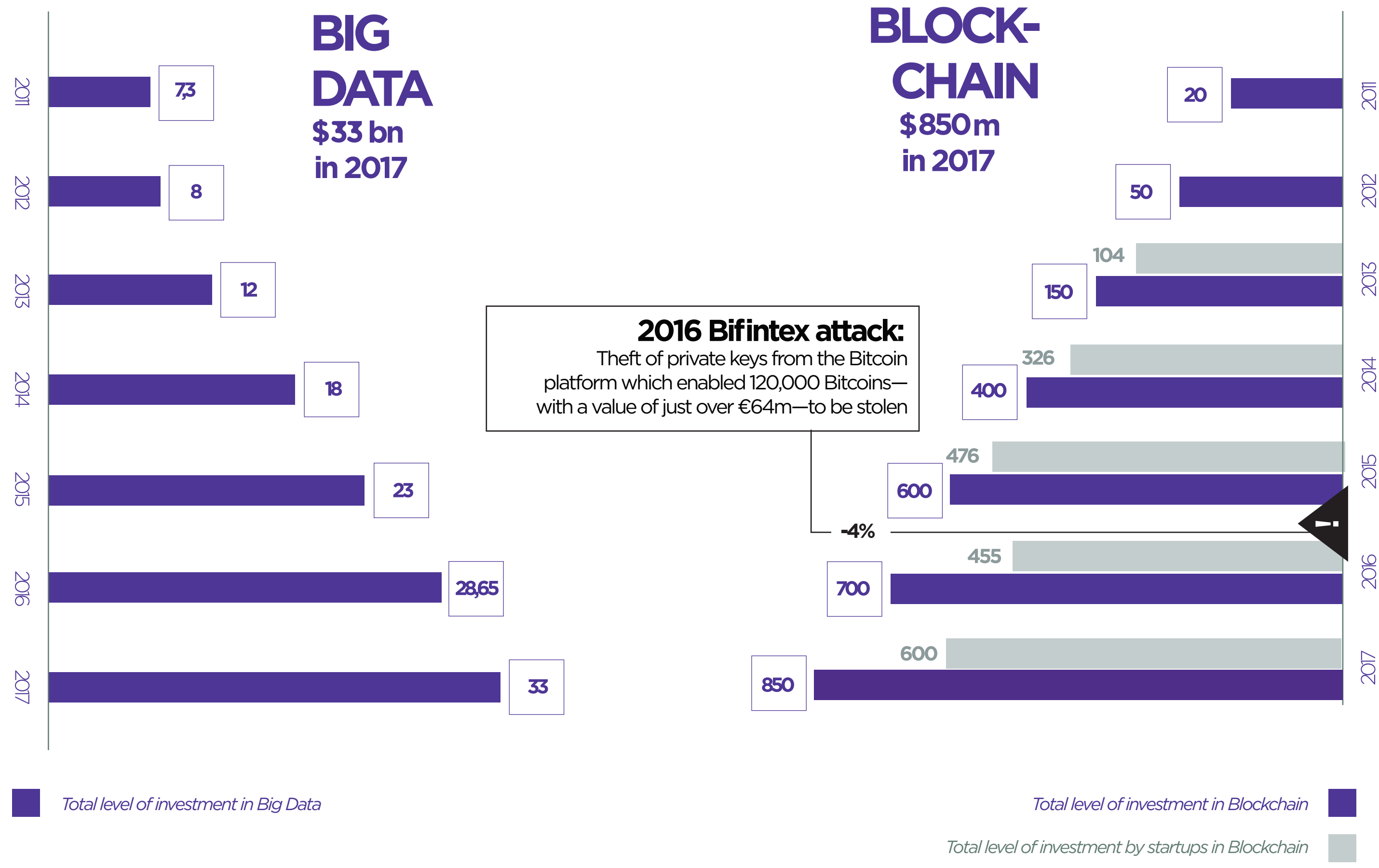
Changes, according to Google Trends, in searches for the keyword "Blockchain" – 14/03/2018

Decision makers are starting to see the potential of Blockchain...



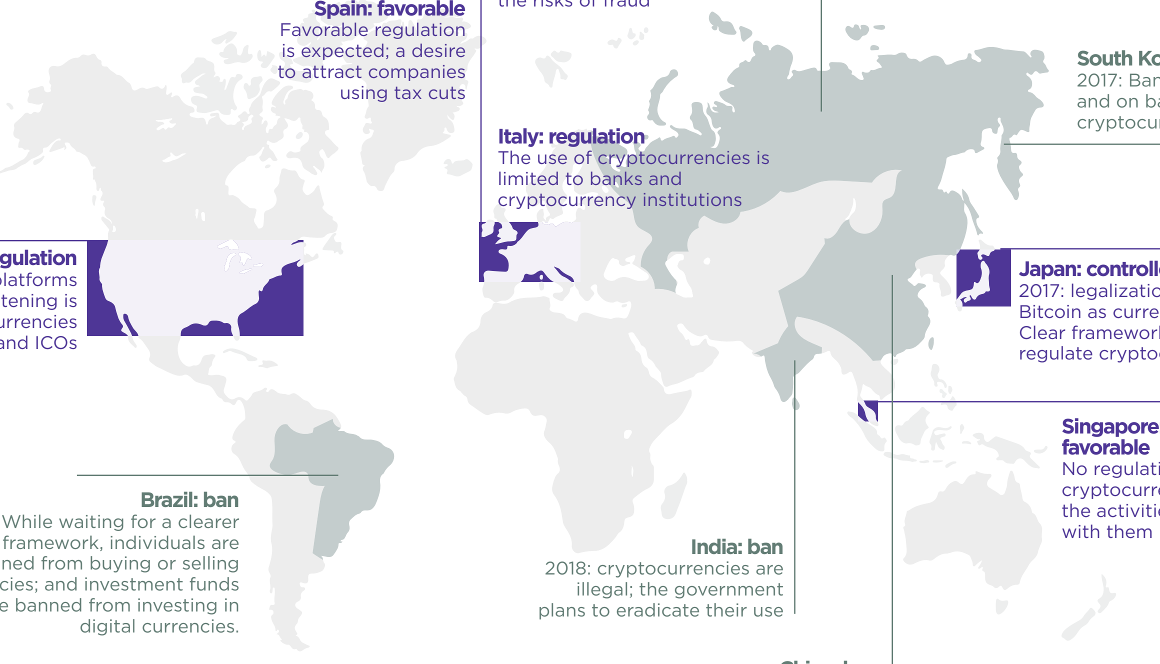
A breakdown of decision-makers' responses on the maturity of new technology in October 2017

Investments in Blockchain are seeing significant growth, but remain far behind more mature technologies



2016 Bifintex attack:
Theft of private keys from the Bitcoin platform which enabled 120,000 Bitcoins—with a value of just over €64m—to be stolen

At global scale, regulation is focused on cryptocurrencies



🟪 *Favorable regulation*

⬜ *Unfavorable regulation*

Spain: favorable
Favorable regulation is expected; a desire to attract companies using tax cuts

Germany and France: market opening and regulation
Advocating international regulation. Consultations are in progress. Further regulation is expected, in France, to limit the risks of fraud

Russia: very tight control
2014: cryptocurrencies are banned. The position is shifting toward regulation to better control risks. Plans to create a national cryptocurrency: the CryptoRouble

South Korea: ban
2017: Ban on ICOs, and on banks using cryptocurrencies

Italy: regulation
The use of cryptocurrencies is limited to banks and cryptocurrency institutions

US: tight regulation of trading platforms
Regulatory tightening is expected for cryptocurrencies and ICOs

Japan: controlled opening
2017: legalization of Bitcoin as currency. Clear framework to regulate cryptocurrencies

Singapore: highly favorable
No regulation of cryptocurrencies—only the activities associated with them

Brazil: ban
2018: While waiting for a clearer regulatory framework, individuals are banned from buying or selling cryptocurrencies; and investment funds are banned from investing in digital currencies.

India: ban
2018: cryptocurrencies are illegal; the government plans to eradicate their use

China: ban
2015: financial institutions are prohibited from using cryptocurrencies.
2017: ban on ICOs
Regulations on mining are in process

WAVESTONE IN BRIEF

Working at the interface between management consulting, and digital and technological-innovation consulting, Wavestone is built on a unique position in the market and a differentiating value proposition that is perfectly aligned with the challenges faced by companies and organizations in the digital age.

In a world where knowing how to transform is the key to success, Wavestone's mission is to enlighten and guide its clients in their most strategic transformation decisions—a mission that we pursue on the basis of three strongly held convictions:

- Innovation is no longer an option for companies: it is a daily imperative.
- Creating relevant business strategies requires, more than ever, the mastery of the technological dimensions of business.
- companies seeking to transform themselves want not only a consulting firm that can offer them concepts, but a partner capable of translating these concepts into concrete action.

Wavestone is working with a range of blue-chip clients, including major institutions and players who are leaders in their markets. The firm draws on some 2,500 employees across four continents, who operate in a synchronized manner—worldwide. A strength of expertise that makes Wavestone a leading independent consulting firm in Europe, and the number one in France.

L'ARGUS de l'assurance

WAVESTONE IS A PARTNER TO SEVERAL EVENTS THAT ARGUS ASSURANCE ORGANIZES

- **April 5: Blockchain and Insurance Morning**
  With Laurence Al Neimi, Senior Manager, Financial Services
- **April 11: Preventive Health and Welfare Morning**
  With Laurence Al Neimi, Senior Manager, Financial Services
- **May 29: Connected Homes Morning**
  With Patrick Durand, Senior Manager, Financial Services
- **October 16: Connected Vehicles Morning**
  With Patrick Durand, Senior Manager, Financial Services
- **July 3 and 4: Workshop on the Customer Experience**
  With Patrick Durand, Senior Manager, Financial Services

WAVESTONE

www.wavestone.com

Wavestone is a consultancy firm, formed by the combination of Solucom and the European businesses of Kurt Salmon (excluding consultancy for in the retail & consumer goods sectors).

Wavestone is one of the leading independent consultancy firms in Europe.

Wavestone's mission is to enlighten and guide its customers in their most strategic decisions through relying on its threefold functional, sectoral and technological expertise.