WAVESTONE

RISKINSIGHT

LETTER FROM THE WAVESTONE CYBERSECURITY AND DIGITAL TRUST CONSULTANTS

BLOCKCHAIN: FINDING THE RIGHT BALANCE BETWEEN RISK AND INNOVATION

EDITO

Blockchain is presented as a revolutionary technology for digital trust. And it is! Usage cases are soaring, and all the activity sectors are getting to grips with them. Sometimes obvious, sometimes strange, even useless, these tests bring innovation to our daily lives and in the medium term.

The fundamentals of blockchain are theoretically solid and rely on cryptographic mechanisms which were developed and mastered many years ago. In light of this, their main point of weakness lies in the manner with which the implementation of Blockchain is realized. Recent attacks have highlighted these limits, in particular that which is aimed at the Ethereum chain and its famous “smart contracts”.

This RiskInsight letter aims to interpret these evolutions and their function, to explain the risks and the documented attacks to allow you to find the right balance between risk and innovation.

Gérôme BILLOIS
Senior manager Cybersecurity & Digital Trust

OVERVIEW

BLOCKCHAIN: A NEW MODEL FOR TRUST?

Described by some visionaries as a revolutionary (or disruptive) technology, today Blockchain is increasingly talked about. The entire world is interested in it, and investments in the field are multiplying: nearly 1 billion dollars was raised over the last 3 years, including 500 million dollars in 2015 (source: Magister Advisors).

Many companies and authorities are currently exploring the possible uses of this technology, which is promising but particularly complex for businesses to understand Meanwhile, the IT world is appropriating this technology: the major Cloud players like Microsoft, IBM, and Amazon, are pointing out "Blockchain-as-a-Service" offerings little by little, while numerous start-ups, like Ethereum, are innovating and proposing particularly advanced uses of Blockchain.

However, this concept is not new: Blockchain is the technology on which the Bitcoin cryptocurrency, which appeared in 2009, is based. So, why this renewed interest? What are the characteristics of this technology, and what uses can it favor? What are the obstacles to overcome and the security risks to be addressed so that it can become more widespread?

ALGORITHMS ARE REPLACING TRUSTED THIRD PARTIES

Blockchain is a technology that allows members of a single network to carry out information storage and transmission operations, called "transactions," confidently without any central control authority.

This technology appears in the form of a register containing all transactions recorded since its creation (in the case of the Bitcoin Blockchain, for example, it contains all financial transactions performed since the creation of this cryptocurrency). This register has two essential characteristics:

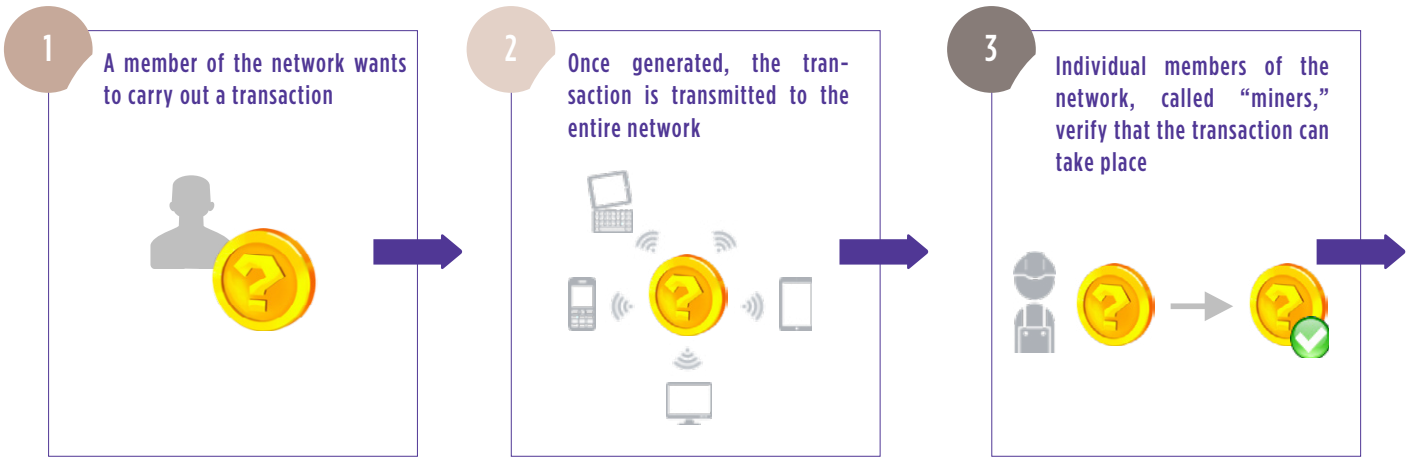
- **It is distributed:** all members of the network have a copy of the register, making it almost impossible for an individual to modify the register without the consent of the rest of the network;
- **It is made more reliable by the network's players:** the trust established within the system is ensured by the network members themselves; no central authority plays the role of trusted third party.

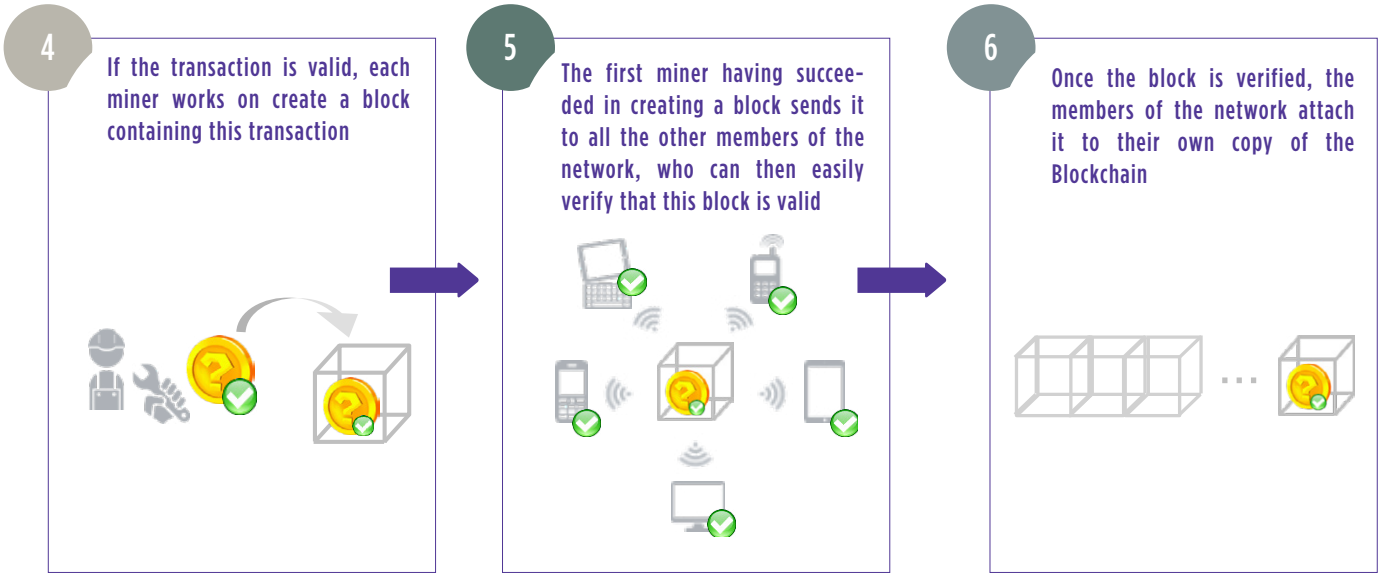
Within the register, transactions are grouped into "blocks" linked together in chronological order (in the case of the Bitcoin Blockchain, a block corresponds to around 10 minutes of transactions). The diagram below shows the process of creating a new block and therefore the recording of a new transaction in the Blockchain.

FROM SIMPLE SECURE STORAGE TO THE EXECUTION OF SMART "CONTRACTS"

Any situation involving a costly or fallible trusted third party is an opportunity to create a Blockchain use case.

Addition of a block to the Blockchain





The trusted third party is therefore replaced by algorithms allowing all network members to easily verify that the miners did not add, delete, or modify a transaction during the creation of new blocks.

Banking, insurance, real estate, healthcare, energy, transport... all sectors now feel involved and are currently looking into the opportunities offered by the Blockchain to improve or replace the current models.

There are currently three different categories of use cases:

1. **Record keeping:** A Blockchain can be used as a simple storage register for depositing data or digital fingerprints of documents whose existence y, date of creation, and ownership right, such as patents, artistic works, medical data, etc are to be ensured permanently and securely. Once these data are entered into the Blockchain, they are distributed to all the players of the network and can no longer be erased or altered.

Example: In Africa, nearly 90% of rural territories are not recorded in a reliable official land registry. So, how do inhabitants assert ownership or even have an address? To solve the resulting problems, the NGO Bitland based in Ghana took on the task of allowing individuals and legal entities who wish to record their ownership titles on a Blockchain, thereby acting as a digital land registry.

2. **Digital transactions:** A Blockchain can also be used in the transfer of value: real estate transactions, crowdfunding... and, of course, the use of cryptocurrencies (Bitcoin, Litecoin, Dogecoin, etc.). A Blockchain allows each transaction to be traced. Therefore, in the case of a cryptocurrency, for example, the movement of each unit of currency from its creation to the last exchange can be traced. In this way, miners can verify that the issuer has the necessary funds before recording a transaction in the Blockchain.

Example: SolarCoin is a cryptocurrency based on a tangible element: solar electricity. Created to encourage the production of clean energy, it allows anyone who so wishes to be paid in SolarCoins on the basis of the solar electricity generated by their photovoltaic system.

3. **Smart contracts:** A Blockchain can also be used to develop and store smart contracts, i.e., contracts between two or several parties. They are written in the form of computer code. This code is then run within the nodes of the Blockchain. Once these programs are recorded in the register, they can no longer be modified and will be run by the Blockchain without human intervention according to the terms and conditions of the contract.

Example: For example, on the Ethereum Blockchain, there are participatory and pooled investment funds. The members vote for projects in which they would like to invest, and the application, governed by smart contracts, automatically handles allocating the collected funds across the most popular projects, according to the predefined rules in the smart contracts.

Players in the finance world are particularly interested in Blockchain. For example, the start-up R3 put together a consortium of the world's 50 largest financial institutions around a project aiming to develop Blockchain use cases in the finance sector and to define standardized protocols for all international financial markets. In France, the Caisse des Dépôts has developed an "Innovation Laboratory" named LabChain, grouping together 30 major players in finance and other start-ups, with the objective of evaluating the potential uses of Blockchain while creating synergies and group initiatives on the subject.

In addition to these consortiums, many French companies are currently conducting their own initiatives. For example, Crédit Agricole has established a system on its CA-Store platform to provide payments in Bitcoin to developers who participate in the creation of bank applications for the group; another example is BNPP, which has, through a partnership with SmartAngels , set a goal to develop a platform based on Blockchain for issuing securities and crowdfunding for unlisted companies (see box for more details).

It is clear that most of the current discussions pertain to private Blockchains (specific to a company or public authority) or hybrid Blockchains (specific to a set of partners). However, Blockchain was initially designed as a public system: trust increases with the number of network members. The technical mechanisms of Blockchain must therefore be supplemented in order to adapt to this reality: identity verification required to be able to join the network, rules imposed on partners, limited computing power per miner, etc. These various factors must be defined for each use case.

PERFORMANCE, ECOLOGY, AND REGULATIONS: THE OBSTACLES TO OVERCOME

Until very recently, the only concrete application of Blockchain remained Bitcoin. To give an idea of the magnitude, the Bitcoin network allows around 7 transactions to be recorded per second, compared with 7,000 VISA transactions per second. Therefore, to succeed on a large scale and develop new use cases, Blockchain must be able to improve its performance.

Increasing the size of the blocks and decreasing the difficulty of the block construction process are some of the solutions considered for handling transactions more quickly. However, any change in the parameters is subject to compromise: for example, the construction of a block is intentionally complicated to prevent the network from being flooded with new blocks by several miners simultaneously. The challenge in performance lies in defining and calibrating the parameters intrinsic in Blockchain based on their desired use.

In addition, Blockchain is proving to be highly energy-consuming. To give an idea of the magnitude, some studies estimate the Bitcoin network's current electrical consumption at nearly 350 megawatts, i.e., the equivalent of the average consumption of 280,000 US households. There again, a solution could be to decrease the difficulty of constructing blocks (very high computing power is necessary, and several miners work in parallel). However, such a change would have no impact on the system's security, as will be discussed later on.

Another obstacle not to be overlooked: regulations, even though Blockchain often finds its interest on regulated activities. There were initial successes in recent years, as shown by the application of the KYC (Know Your Customer) process to the main cryptocurrency markets, but the rapid evolution of technology and use cases brings new questions. In particular, what is the legal weight of a smart contract today? None in principle, but no case law exists at this stage.

Rarely will a technology have resulted in so many discussions, debates, and questions. Certain French ministers and parliamentarians are beginning to take a serious look at Blockchain (see timeline). Blockchain is ultimately a very good representation of what the digital transition is: businesses, regulators, and IT specialists, working together to come up with new use cases based on a new technological concept.

Matthieu GARIN
matthieu.garin@wavestone.com

Maxime ROCHE
maxime.roche@wavestone.com

CAN WE HAVE UNLIMITED TRUST IN BLOCKCHAIN?

As explained in the previous article, the guarantee of trust is often an argument linked to the creation of Blockchain use cases.

Blockchain undeniably has intrinsic security qualities: its decentralized and distributed nature permits high system availability, traceability is ensured by storing all transactions in the register, and all transactions are secured by cryptographic mechanisms.

Despite everything, more and more attacks impacting Blockchain environments, and not only Bitcoin, are being seen. The recent frauds targeting this technology, such as The DAO and Bitfinex, very often amount to tens of millions of euros, an amount comparable with that of the most dreaded cyberattacks (Bank of Bangladesh, Carbanak, etc.).

So, what level of trust can truly be given to this technology? Deciphering attacks targeting Blockchain and feedback on measures to be taken to improve this level of trust.

PROTECTING SERVICES AND APPLICATIONS ACCESSING BLOCKCHAIN

Each member of a Blockchain network is identified using a pair of cryptographic keys: a private key, which allows each member to sign the transactions carried out and "benefit" from the transactions that are intended for the member; and a public key, which allows other members of the network to identify the transactions issued by the member and send any transactions to the member securely. Using a safe to illustrate this point, the private key allows it to be opened and have its contents removed. The public key only opens a trap door to add items in the safe, like a mailbox. The owner of the private key must be concerned about preserving it and shield it from any interest from a potential attacker. These keys are usually stored on a user's computer or telephone with the application that allows the user to access the Blockchain; these devices are known to be easily attackable. Specific malware has even appeared to steal these keys.

In addition, more and more users are choosing to entrust their private key to intermediaries offering services such as user-friendly access to the Bitcoin network. Most attacks impacting the Bitcoin network have not actually attacked the intrinsic operation of the Blockchain, but have targeted these intermediary platforms that manipulate the private key of their clients. Examples include attacks that have targeted the MtGox, Bitstamp, Bter, and, more recently, Bitfinex services.

It is crucial to protect the manipulation of private keys (storage, use, exchange, etc.) and, more generally, all services accessing the Blockchain network. This is especially essential given that the cancellation of a transaction is impossible in principle: once a transaction is recorded in a Blockchain, it theoretically cannot be modified or deleted when it is recorded.

In the case of a Blockchain relying on smart contracts, the level of interaction with the outside of the network may be significant. Smart contracts rely on the verification of "input parameters," potentially outside the Blockchain, allowing computer code to run. For example, in the case of a "sports betting" smart contract, the Blockchain verifies the results of a match at the website resultatsfoot.com and carries out a transaction accordingly. An attack on this website would probably be simpler than an attack on the Blockchain network.

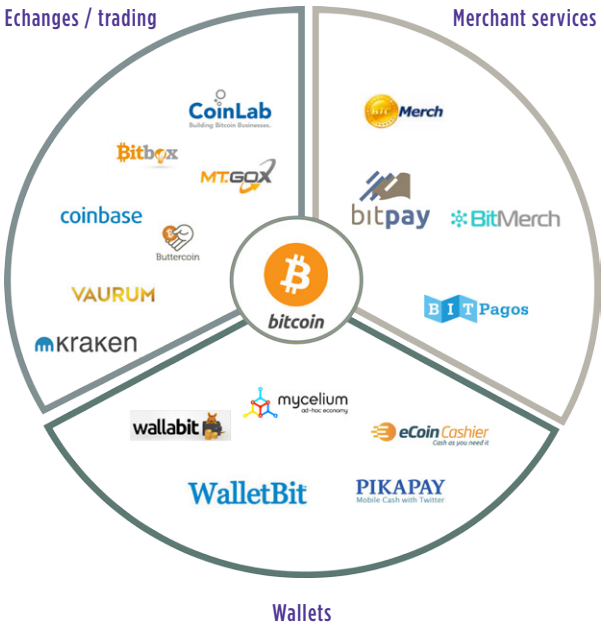
As such, for a Blockchain relying on smart contracts, an additional dimension must be taken into account: it is no longer a question of securing only the platforms accessing the Blockchain, but also those accessed by the Blockchain in order to validate the conditions of a transaction.

MONITORING THE COMPUTING POWER OF MINERS TO AVOID A 51% ATTACK

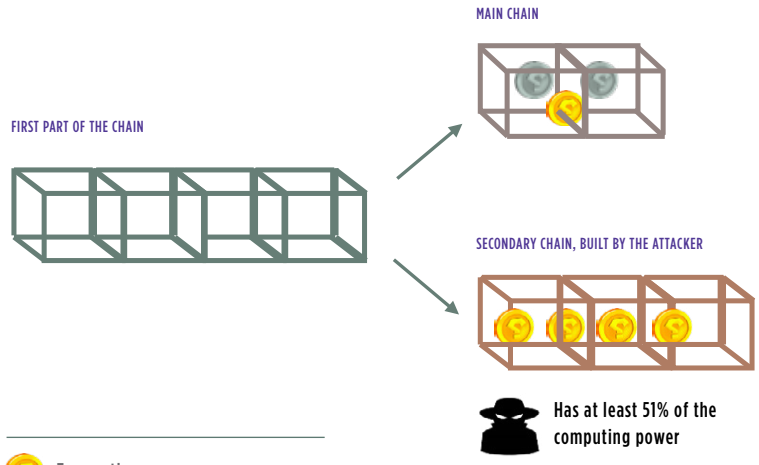
A "51% attack" involves controlling more than 51% of the computing power. During the construction of the Bitcoin Blockchain, its creator Satoshi Nakamoto had already identified that the integrity of a Blockchain is guaranteed provided that no single person, or a group working together, holds 51% of the computing power (source: https://Bitcoin.fr/public/Bitcoin.pdf).

Once this new level of control is reached, the attackers can re-write part of the Blockchain in order to cancel, add, or modify certain transactions in a block. In concrete terms, a group of miners can team up, start from a previous version of the Blockchain, and mine an alternative Blockchain. Given that this alternative chain has a greater computing capacity, it will catch up with and replace the legitimate chain, exploiting an essential parameter of the Blockchain: when two competing chains appear on the network, the longer chain is considered the legitimate chain.

Bitcoin ecosystem: examples of services accessing the Blockchain



The 51% attack, or the limits of the principle of consensus



EXPLANATION OF THE 51% ATTACK

An attacker wishes to rewrite the Blockchain in order to cancel certain transactions in a block

1. The attacker mines alternative blocks on the basis of the previous block
2. The attacker publishes the obtained chain on the network as soon as it is longer than the existing chain (which is possible because the attacker has more than 51% of the network's power)
3. Because the chain is longer, and using the principle of consensus, it replaces the existing chain, and the transactions that it contained are cancelled

In order to be able to carry out such an attack, the attacker must have more than 51% of the network's computing power

This attack is not just theoretical. For example, the largest cooperative of miners, GHash.io, very frequently approached 50% of computing power on the Bitcoin network, while the Reddcoin cryptocurrency suffered this attack in 2014.

Security measures must therefore support the establishment of any Blockchain in order to prevent or detect 51% attacks. This risk is especially great in private or hybrid Blockchains, made up of a small number of users and therefore able to provide more than half of the computing power more easily.

In this case, contractual commitments and monitoring and control mechanisms must be implemented between partners or members of a Blockchain in order to ensure that no participant holds more than 51% of the computing power.

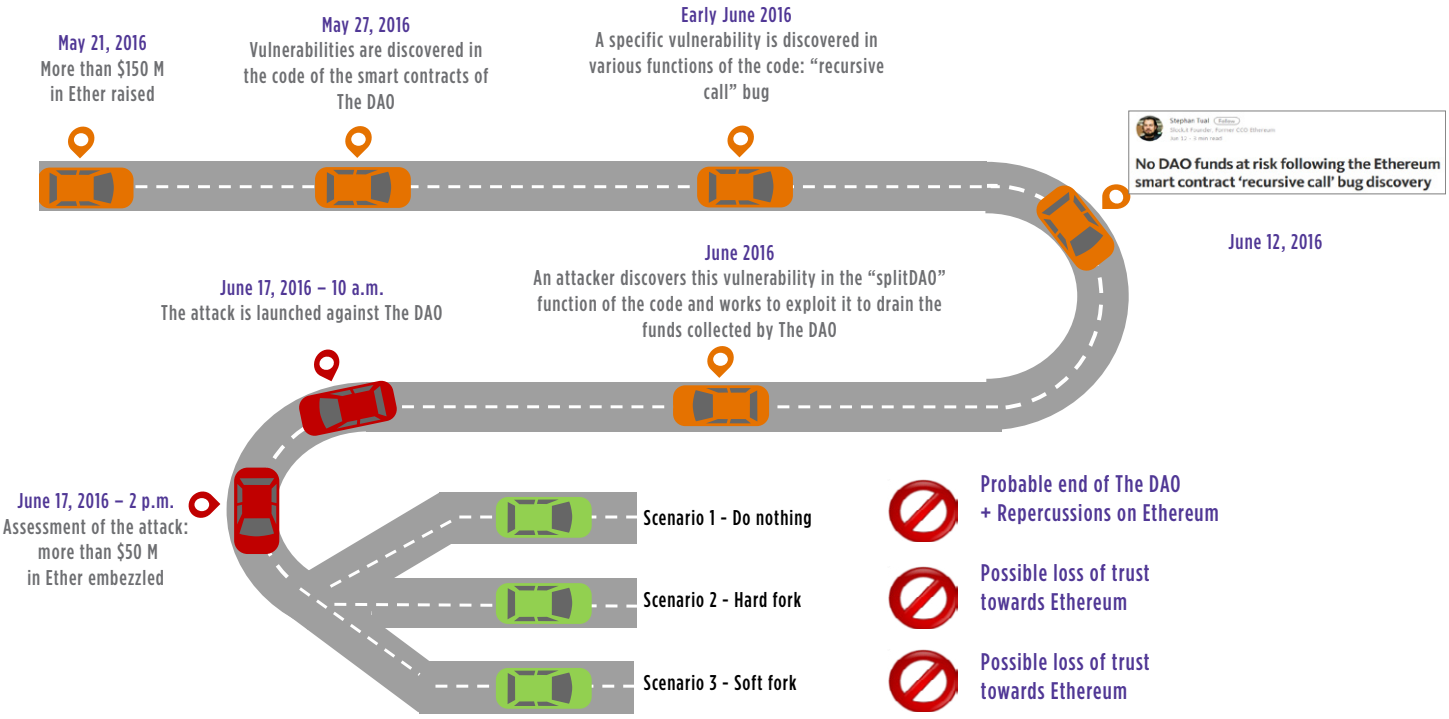
Note that alternative methods of operation of Blockchain are currently being discussed in order to combat this 51% attack. For example, proof-of-stake is a method giving preference to miners who are "rich" in cryptocurrency and not miners who have significant proof-of-work computing power.

SECURING THE COST OF SMART CONTRACTS

Smart contracts are computer programs recorded in a Blockchain. Once it is recorded in the Blockchain, such a program cannot be modified and will be automatically run once the contract's conditions are met.

The consequences of a coding error can be catastrophic and very difficult to reverse, as evidenced by the recent "TheDAO" case, an application based on the Ethereum platform. In this particular case, a member of the Blockchain discovered a vulnerability in the source code of the TheDAO smart contract. By running the smart contract with special settings, the member was able to drain 50 million dollars from the application's main account. These funds were recovered in part following an operation by Ethereum's developers, having jeopardized the Ethereum Blockchain ("hard fork" method akin to a concerted 51% attack).

An application of the Blacklist, THE DAO attack



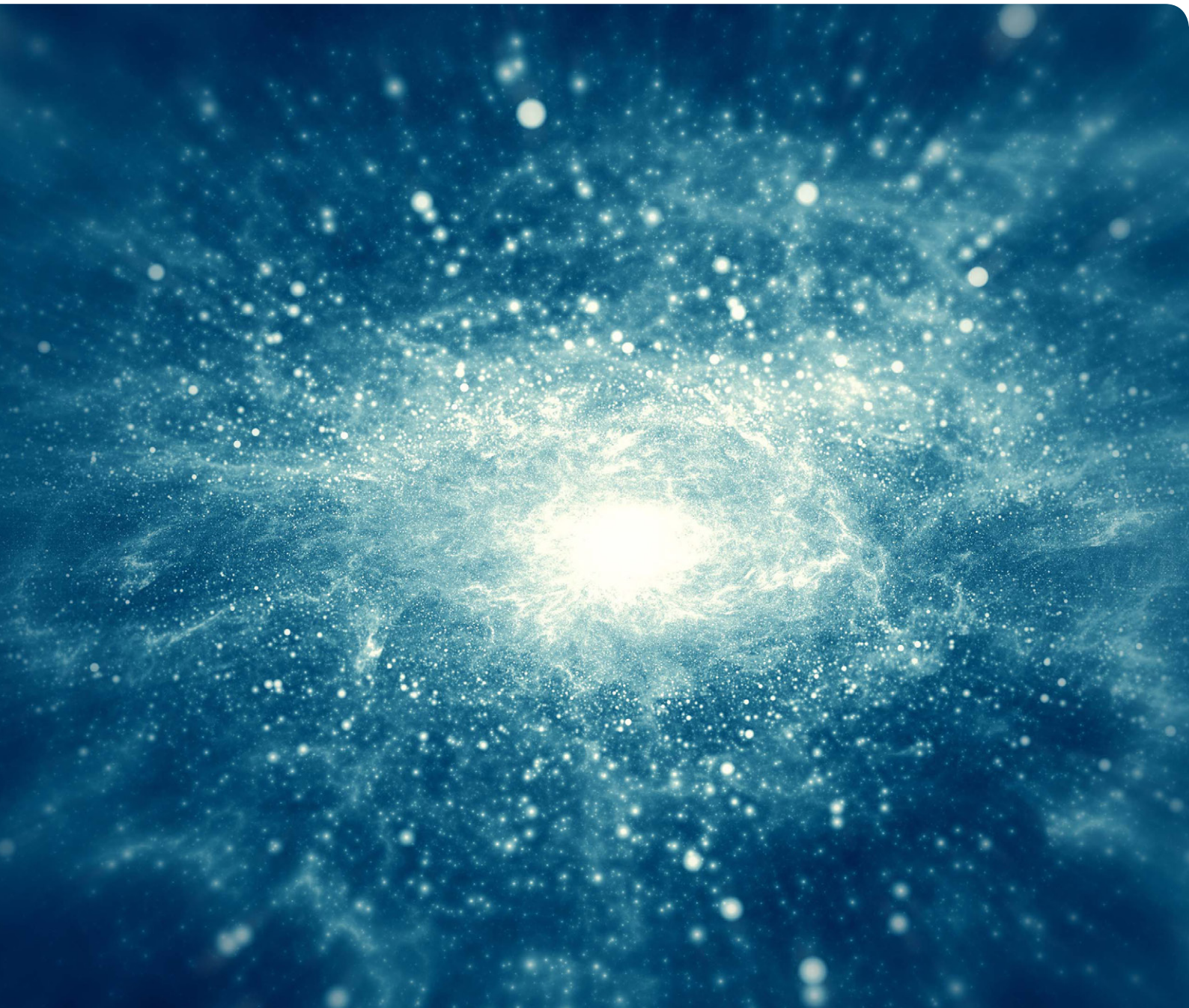
This was technically not an attack because the contract was respected. The contract's design had been flawed, and many discussions are underway about the true legal value of smart contracts. After all, the user "simply" ran a computer code to which all the members had agreed. However, the goal was contrary to the spirit of the contract...a concept that a computer code does not know how to assess! Many discussions are underway as to the true legal value of smart contracts.

The creation of use cases based on smart contracts must therefore be paired with application security measures: use of secure frameworks, raising developer awareness, systematic code reviews, etc.

Blockchain is a recent technology, often considered secure by nature. However, certain recent attacks prove otherwise. It must now be looked into, especially given that the security measures to be implemented differ according to the implemented use case. The nature of the platforms accessing Blockchain, the complexity of any smart contracts, and the number of miners in the network are all different types of factors that could influence the security of the service provided by Blockchain.

Matthieu GARIN
matthieu.garin@wavestone.com

Stéphane GOMEZ
stephane.gomez@wavestone.com



BLOCKCHAIN, OR THE ILLUSTRATION OF A CHANGING WORLD

Disruptive technologies are those that allow the expression of a great innovation.

And great innovations – those that profoundly change society – result from the meeting of technology and a particularly receptive state of society. Without this sociological parameter giving meaning and use to technology, there's no point to innovation.

The rather systematic parallel established between the premises of the public Internet and the current period of excitement around Blockchain reveal what many feel to be the next digital revolution, a disruption of transactions echoing the disruption of information embodied by the Internet: not a new catalog of uses emerging from a technological evolution, but rather the promise of a more radical change in the society model. This change is made possible by the distribution of trust and, ultimately, a more or less significant disintermediation of exchanges of all types.

This distributed trust that inherently differentiates Blockchain carries a promise of making society more horizontal. Depending on the public and private, national and international governance choices that will be made, we could see a rather profound redefinition of commercial and institutional models once thought to be unchangeable. This possibility carries as many promises as concerns, and, for many players, it means finding the right approach, between haste and procrastination, adopting one model over another, etc. for the sake of being part of the landscape of tomorrow.

BLOCKCHAIN, OR THE TECHNOLOGICAL RESPONSE TO THE SHIFT IN TRUST

As a technology, Blockchain provides a new response to the decentralization of registers and the automation of contracts and, as a corollary, naturally gives rise to questions about its security and the conditions of its large-scale implementation, which is quite simply the natural history of emerging technologies: more or less exaggerated hopes and obstacles to be overcome.

Originally, Blockchain was an underlying technology for exchanging Bitcoins. It was therefore the first way to conduct financial transactions without bank involvement. The mood after the 2008 financial crisis was important because the initiative found its audience and its uses thanks to a climate of lost trust towards traditional financial institutions. What we see today is a transfer of trust, traditionally given to institutions, towards communities of users/suppliers, in a movement to make society more horizontal. The success of platforms of any kind is a strong sign of this movement. The trust necessary before carrying out a transaction on one of these platforms is now more conditional on community feedback through widespread peer-rating systems than on other forms of guarantees.

However, this still raises the question of the reliability of this community trust model: does the rating that I'm referring to actually reflect a transaction actually carried out by the player? Is this transaction actually consistent with the reported characteristics? How can I be certain that the information has not been manipulated? It is in these questions that the novelty of the Blockchain's value proposition fits and perhaps the post-platform step: reliability and distributed auditability through consensus for a purely peer-to-peer model. Once these questions are resolved, the disappearance of third parties theoretically becomes possible.

However, the vastness of the scope of application of Blockchain does not assume that we will be able to use it for anything and everything, especially without asking the question of the model being adopted and the form of governance being implemented. All uses do not require resorting to "proof of work," which involves a large community and imposes a more than substantial energy cost.

PROMISES AND POSSIBILITIES

In the merchant sector, the promises of automation suggest the prospects of reduced costs and fluidity in certain transactions that could ultimately benefit consumers, but also assume a significant ability among commercial players to transform. The financial services sector, already heavily jolted by competition from fintechs, inevitably comes to mind. Beyond the mere subject of cryptocurrencies, for banks, the current objective is to appropriate the technology, without implementing the largely distributed model inherent in Bitcoin, in order to gain competitive benefits from it. Offering customers value-added services, such as almost immediate transfers of money and securities, would be less expensive since there is no human intervention in the process, thus defending its position as a third party and its competitive advantage. The same is true for insurers, which are opportunely looking into the potential gains offered by Blockchain thanks to the automatic execution of insurance policies or even the possible response to the problems of unclaimed policies. There could be an endless list of impacted sectors and uses, not to mention the uses that will emerge tomorrow that are unknown to us.

In any case, though, commercial projections around Blockchain should remain cautious. Certain processes may very well be automated without using Blockchain, and a technical and economic analysis will be necessary to make the most relevant choice. In banking, for example, a lending process can already

be automated without Blockchain. On the other hand, there could be additional benefits to having ways of submitting certified documents as part of this process, which could be supported by Blockchain mechanisms favorably and at a lower cost. A global, in-depth analysis of the technical, business, and economic aspects is therefore needed to identify real use cases. And, like any innovation, we must search for meaning before creating the business model.

Most of the experiments underway involve "private" Blockchains, which are therefore relatively at odds with the original Bitcoin Blockchain model. We should be rather cautious in choosing these models and not necessarily radically exploring one or the other. Although certain uses do not necessarily require using a large, diverse community of miners or implementing proof of work to secure the transaction, we can also ask ourselves, with a bit of caricature, whether this is a use specifically linked to Blockchain in this case. However, we also know that experiments will give us a change to step back and consider the subject, and the colossal investments currently made will undoubtedly allow us to establish beliefs, as long as no player or model establishes itself. The various opportunities currently being examined and tested are promising. They show considerable collective energy on the subject and suggest promises of gains for both companies and consumers. Yet, the promise of "absolute" disintermediation or the Uberization of platforms will not necessary result from it.

In the non-merchant sector, whether it is in the government or in civil society, the multiple promises are encountering rather profound aspirations from citizens of a more horizontal society, as evidenced by the growing number and the success of collaborative initiatives, as well as the larger or smaller scale experiences in participatory democracy.

The government finds itself in the position of a potential user, promoter, project owner, and regulator of Blockchain.

- User in the automation of complex and costly transactional mechanisms: uses for the tax authorities as well as anything pertaining to rights access could be considered.
- Promoter in the support of public and private initiatives: supporting a dynamic French ecosystem.
- Project owner and regulator of a future public Blockchain: supporter of a functional governance model at the national and international level.

Civil society could also see Blockchain as an ideal way of implementing numerous collaborative projects arising from the community model and therefore natively adhering to the concept of distributed trust. The vast field of exchanges of goods and services between individuals could cause a shift from a platform-type commercial model towards a purely community-based model tending towards a minimal cost for the user/member. It remains to be seen whether socially conscious consumers, attracted by this model, would be willing to consent to a more stripped-down transaction experience. It is difficult to contemplate a very rich customer experience in this type of model, unless we bet on a devoted community of developers, which is not out of the question. In addition, it seems complex to contemplate a massive use or to expand the concept to an activity requiring management of risks.

The other main promise of Blockchain to civil society involves all the possibilities relating to a more direct democratic expression, particularly through the voting systems currently being explored by various countries. Even closer, we can look at the controversies that have arisen surrounding the reliability and legitimacy of online petition systems, and we can imagine the positive role that a Blockchain implementation of a petition system could play to protect the petition and the petitioners.

Blockchain therefore presents an interest for both the private sphere and the public sphere, but it is still to be determined whether the target will be a Blockchain and its instantiations or the coexistence of different models.

A BREAKTHROUGH INNOVATION LOOKING FOR A GOVERNANCE MODEL

This quick, non-exhaustive overview examines the extent and depth of the implications of the advent of Blockchains. In his speech at the 2014 TEDxBerkeley Conference, Guy Kawasaki, a leading expert in innovation, aptly summed up the world-changing characteristics of a major innovation:

- Deep;
- Intelligent;
- Complete;
- Empowering;
- Elegant.

Blockchains definitely carry these attributes. It is also certain that the multiplicity of opportunities can only be expressed concretely in a configuration in which private and public players seize on the topic in an open, multidisciplinary approach.

From there, one or more governance models could emerge to allow new uses to flourish for the benefit of the greatest number.

Anne GAUTRENEAU
anne.gautreneau@wavestone.com

ABOUT WAVESTONE

Wavestone is a consulting firm, created from the merger of Solucom and Kurt Salmon's European activities (excluding retail and consumer goods consulting outside of France)

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

With 2500 employees across 4 continents, the firm is amongst the independent European leaders in consulting and is number 1 in France.

With over 400 consultants, Wavestone's has the largest EMEA strike force in terms of cybersecurity and digital trust.

AGENDA

05-08.10.2016

Les Assises de la Sécurité: Beyond the fortress and the airport, what security model after 2020? (Monaco, France)

17-18.11.2016

Zero Night Conference : Big Data (Moscow, Russia)

25-26.01.2017

International Cybersecurity Forum (Lille, France)

Discover our expertise
RISK INSIGHT

@Risk_Insight

Director of the publication : Frédéric Goux
Editor-in-chief: Gérôme Billois
Contributors: Matthieu Garin, Maxime Roche,
Stéphane Gomez, Anne Gautreneau
Printer: Axiom Graphics
ISSN 1995-1975

WAVESTONE

www.wavestone.com

Wavestone is a consulting firm, created from the merger of Solucom and Kurt Salmon's European activities (excluding retail and consumer goods consulting outside of France)

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

With 2500 employees across 4 continents, the firm is amongst the independent European leaders in consulting and is number 1 in France.