WAVESTONE

BANKINSIGHT

THE BANKING NEWSLETTER
FROM WAVESTONE CONSULTING

OCTOBER/NOVEMBER 2016

BLOCKCHAIN
THE BIG BANG OF THE BANKING WORLD

OLIVIER SCHMITT
Associate Director

SUMMARY

SAFELY ELIMINATING INTERMEDIARIES

From time to time, everyone has envisioned a world where intermediaries are no longer necessary, and producers are able to have a direct relationships with their consumer.

With the advent of numerous online stores, trading, and second-hand websites could, to an extent, seem to meet this demand. But make no mistake, we are still going through an established intermediary, albeit a discreet one, who reassures us but still takes their cut.

Blockchain technology changes the intermediary because the power no longer resides in an institution, business or an entity, but in an informal community of stakeholders who trace, verify, and ensure contracts and transactions are secure.

This new shake-up of roles and powers could quickly challenge many established models.

Olivier Schmitt

Laetitia MERCIER de BEAUROUVRE
laetitia.mercier@wavestone.com

20 years ago, we couldn't even have imagined the internet...and yet, today we spend several hours a day online performing transactions that use online platforms, or applications that act as an intermediary to secure the transactions of goods against payments. What we were marveling at yesterday seems to be on the cusp of development with the arrival of *Blockchain*, which heralds the decline of the role of the intermediary («*Blockchain, or the sign of a changing world*»).

Blockchain is a technology for the digital storage and transmission of information, in a transparent and secure manner, without the involvement of any central controlling institution.

In concrete terms, *Blockchain* consists of a list of all the transactions made between users of the system since it was created. This register is decentralized, -that is to say, it is stored on the servers of its users- and works without intermediaries, thus eliminating infrastructure costs. Its security is guaranteed by a cryptographic protocol and is independently updated in real time by all users, allowing each user to verify the validity of the chain («*Blockchain: a New Model for Trust*?»).

This technology is already raising some questions that will, in time, become choices that society has to make: to what extent will we accept the replacement of historically trusted authorities (banks, governments, etc.) by computer programs? The answer to questions such as this will form the foundations of the use of *Blockchain* in the future («*Should You Have Limitless Faith in Blockchain*?»).

BLOCKCHAIN OR THE SIGN OF A CHANGING WORLD

Disruptive technologies are those that bring about great innovation.

Many see *Blockchain* as the next digital revolution, promising a radical change in society's model through redefining the role of an intermediary.

The shared trust that differentiates *Blockchain* carries the promise of a flatter structure for society. It could help with a meaningful redefining of the commercial and institutional models that we had thought immutable. This possibility carries with it as many hopes as it does concerns, and, for a substantial number of players, it's a matter of finding the right approach as they are playing a substantial role in designing the landscape of the future.

BLOCKCHAIN: THE EMERGENCE OF TRUST

Blockchain offers a new solution for the decentralization of records and automation of contracts, which raises questions relating to its security and its implementation on a large scale.

Originally, the Bitcoin *Blockchain* was the first way to conduct electronic financial transactions independently of the interventions of banks. In today's world, as a result of several banking crises, you can see the confidence that people previously had in institutions, is now focused on communities of users/providers.

However, reliability of this community model of trust continues to be questioned. Once reliability is confirmed, the elimination of the intermediary role will become theoretically possible.

The vastness of the potential scope of *Blockchain* doesn't assume that it can be relied upon for anything and everything, and above all without asking the question of which model to adopt and what governance to put in place. Not all uses require falling back on the mobilization of a large community.

PROMISE AND POTENTIAL

In the commercial and financial sectors, automation offers cost reduction possibilities and flexible transactions that would be of benefit to consumers, but more broadly the potential gains that *Blockchain* could offer affect a potentially limitless list of sectors and uses.

However, some processes could be automated without using *Blockchain*. It is, therefore, a question of conducting a full in-depth commercial, technical, and economic analysis in order to identify the relevant uses of *Blockchain*, by focusing on the overall direction before the business model.

The different paths studied are considered promising and are a testament to a collective energy that will bring as much benefit to businesses as they do consumers, However, the potential to completely eliminate the role of the intermediary will not necessarily be the result.

In the public arena, *Blockchain* is, amongst other things, an ideal way of implementing collaborative projects that are the product of the community model and therefore fixed to the concept of shared trust.

Meanwhile, governments could simultaneously be a potential user, promoter, project manager, and regulator of *Blockchain*.

Blockchain is therefore of interest in both the public and private sectors, and it remains to be seen whether it consists of a single target *Blockchain* and its variations or whether several different models could co-exist.

Anne GAUTRENEAU
anne.gautreneau@wavestone.com

BLOCKCHAIN: A NEW TRUST MODEL?

Championed by several technological revolutionaries, *Blockchain* is generating more and more discussion: it seems that everyone in the world is suddenly interested in it, and investment in the field is growing rapidly. Many businesses and other bodies are currently exploring the potential uses of this promising technology, which is, for all that, difficult for businesses to fully grasp.

However, it is not a new concept: *Blockchain* is the technology that the digital currency Bitcoin relies on, which emerged in 2009. So why the renewed interest? What are the characteristics of this technology and what uses could it lend itself to? What obstacles are there to overcome in order for it to be democratized?

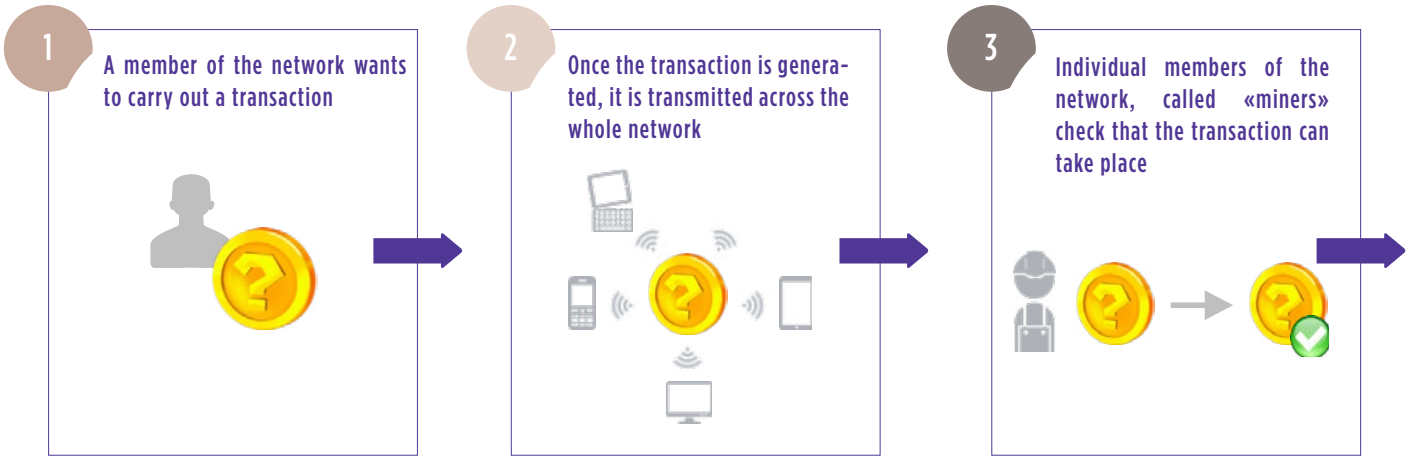
ALGORITHMS IN LIEU OF THE TRUSTED THIRD PARTY

Blockchain allows members of the same network to perform actions that store and transmit information, called transactions, in full confidence without the control of a central authority. The program is in the form of a record of all the transactions that have been registered since its creation and has two key characteristics:

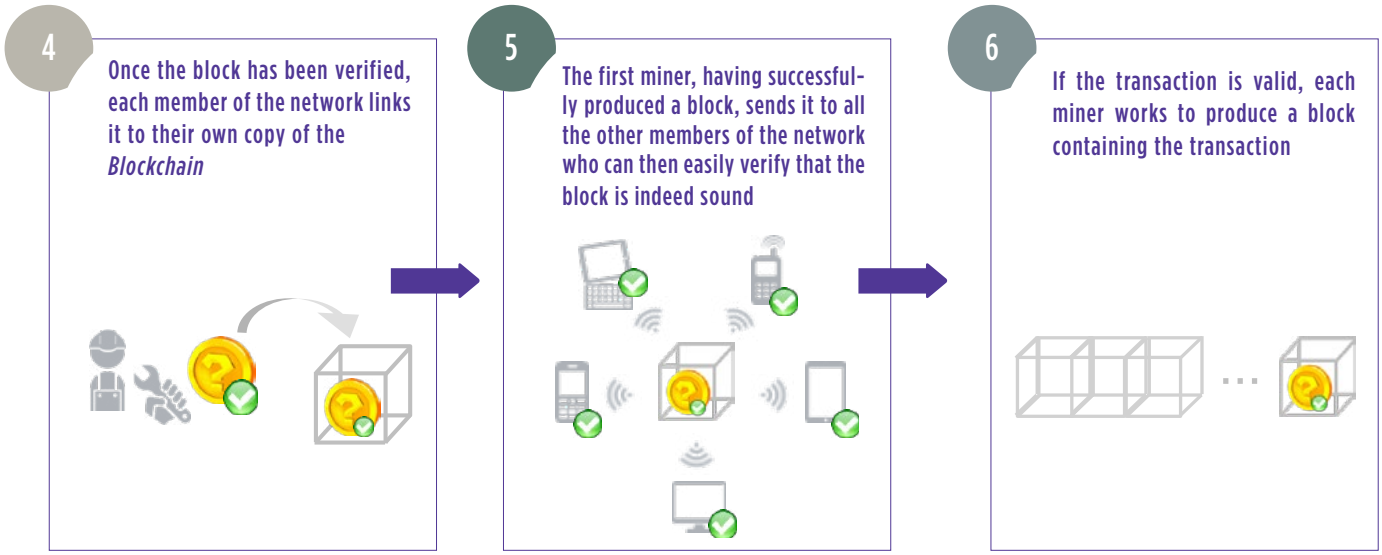
- **It is shared:** members of the network use a copy of the register, making it almost impossible to alter it without the agreement of the rest of the network.
- **It is safeguarded by the members of the network:** confidence in the system is guaranteed by the members of the network themselves; there is no central authority playing the role of trusted third party.

Within the register, transactions are grouped in chronological blocks. The diagram below helps demonstrate the process of creating a new block, and therefore the recording of a new transaction in the *Blockchain*.

An overview of the addition of a block to the *Blockchain*



The trusted third party is replaced by algorithms that allow all members of the network to easily verify that "miners" do not add, delete or modify a transaction when adding new blocks.



FROM SIMPLE STORAGE TO THE IMPLEMENTATION OF SMART CONTRACTS

Any situation requiring the costly or potentially fallible intervention of an intermediary is an opportunity to create a business case for using *Blockchain*. Banking, real estate. healthcare, transportation... all these sectors are affected and are currently considering the opportunities that *Blockchain* presents them with for improving upon, or replacing, existing models.

Currently, three categories of the application can be identified:

1. **Record keeping :** *Blockchain* is used as a storage repository for all the data that requires assurance by existence, their creation date, and their property rights, such as patents, medical data, etc.
2. **Digital transactions :** *Blockchain* is used to transfer things of value: real estate, crowdfunding, crypto-currency such as Bitcoin, etc.
3. **Smart-contracts :** *Blockchain* is used to develop and store smart-contracts. These are contracts between several parties that are rewritten in the form of computer code and run according to the terms and conditions they contain, without human intervention.

Stakeholders in the finance industry are particularly interested in *Blockchain*. There are many initiatives being conducted, sometimes by consortia, with the object of evaluating the potential uses of this technology in the sector and to define some standardized processes.

Although *Blockchain* was initially considered a public system, the majority of current thought is toward private *Blockchains* (belonging to a company) or hybrids (belonging to a group of partners).

PERFORMANCE, ENVIRONMENT AND REGULATIONS: OVERCOMING OBSTACLES

By way of example, the Bitcoin network is capable of recording around 7 transactions per second. compared with the 2000 transactions per second by VISA. In order to implement it on a large scale and develop new potential uses, *Blockchain* must prove that it can improve its performance.

The performance challenge is based on defining and calibrating the intrinsic operating parameters of *Blockchain*, depending on the use that you want to make of it (the size of the blocks, and the process for creating them).

Moreover, the process uses a lot of energy. The current electrical consumption of the Bitcoin network is, remarkably, equivalent to that of 280,000 American households.

Regulation is also proving to be an obstacle, the rapid development of the technology and its uses are leading to further questions being raised: how will the KYC (Know Your Customer) process be applied? What legal weight does a smart-contract have? Etc. Some ministries and parliamentary bodies are beginning to be seriously interested (see information on p.6)

It is rare for a new technology to raise so many questions. In the end, *Blockchain* is an excellent representation of what digital transition is: professionals, regulators, and IT specialists who are reflecting together on the uses that could be made of a new technological concept.

Matthieu GARIN
matthieu.garin@wavestone.com

Maxime ROCHE
maxime.roche@wavestone.com

BLOCKCHAIN REGULATIONS
in France

March 26, 2016

Bercy offers a framework for Blockchain experimentation for funding SMEs

Emmanuel Macron, the Minister of Economy, Industry, and Digital, announces, during the Assises du financement participatif (crowdfunding symposium), an adaptation of the financial regulations in order to permit Blockchain experimentation on commercial paper and mini-bonds.

June 14, 2016

The Assembly adopts the text of **the Sapin II law** in its first reading, authorizing the government to issue orders to take the legislative measures necessary for legal oversight of the "Blockchain" technology

Under the leadership of Assembly member Laure de la Raudière (Les Républicain - Eure-et-Loire), certain instruments, like unlisted shares or bonds, but also units or shares of collective investment undertakings, may use Blockchain on order.

June 24, 2016

€700 million released for Blockchain in the 3rd part of the Programme d'Investissement d'Avenir (future investment program)

Action 9.5 of the program involves funding very ambitious entrepreneurial projects through the structuring of a specific fund. Blockchain is clearly identified as an innovation that will benefit from this support with more than €700 million released.

July 8, 2016

The Senate adopts the Sapin II bill, with modifications, and maintains the authorization by government order

Despite the request to remove the amendment by Senator Pierre-Yves Collombat (RDSE), the text is adopted and indicates that "the government is authorized to issue an order to take the measures to adapt the law applicable to financial securities and transferable securities in order to permit representation and transmission, by means of a shared electronic record system, of financial securities that are not admitted for the operations of a central depository or delivered in a financial instrument settlement and delivery system."

July 18, 2016

The Conseil Supérieur de la Propriété Littéraire et Artistique (CSPLA - high council on literary and artistic property) commissions a report on Blockchain

At the Ministry of Culture's discretion, the CSPLA commissions a report exploring Blockchain while analyzing "the possible changes in controlling the use of works, in an environment of remote paperless services and a European and internationalized framework." The report resulting from this work is expected in spring 2017.

SHOULD YOU HAVE LIMITLESS CONFIDENCE IN *BLOCKCHAIN*?

The trust-guarantee argument is often raised in discussions about *Blockchain*.

In fact, *Blockchain* has built-in security: its decentralized and shared nature allows the system to be readily available, and its traceability is assured by the fact that all transactions are retained in the registry, and their authenticity is ensured by cryptographic mechanisms.

Despite all this, more and more attacks on *Blockchain* are being observed, with frauds often amounting to tens of millions of Euros.

So what level of confidence can we really have in this technology? Deciphering the attacks on *Blockchain* and learning from feedback on measures to be taken to improve confidence levels.

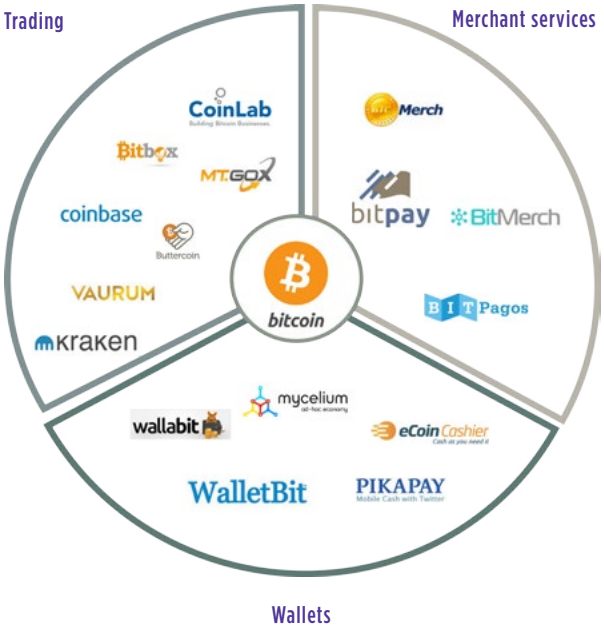
PROTECTING THE SYSTEMS AND APPLICATIONS THAT GIVE ACCESS TO *BLOCKCHAIN*

A member of a *Blockchain* network is identified by a pair of cryptographic keys: a private key which allows them to sign their transactions and receive completed transactions, and a public key which allows other members of the network to identify transactions that they have initiated or been involved in. Keeping the private key strictly confidential is therefore vital. However, the key is often kept on the owner's computer or phone, devices that are known for being easily hackable.

Also, more and more users are choosing to share their private key with intermediaries. It is clear that most attacks on Bitcoin, in reality, directly targeted these intermediary platforms It is therefore essential to prevent the misuse of private keys and more generally protect the entirety of users accessing the *Blockchain* network.

In the case of *Blockchain* relying on smart contracts, the amount of interaction with the external network can be extensive, because smart contracts rely on the verification of the input parameters, which are potentially external to the network. It is then no longer just a matter of securing the systems that access *Blockchain*, but also of securing systems accessed by *Blockchain* to verify the terms of a transaction.

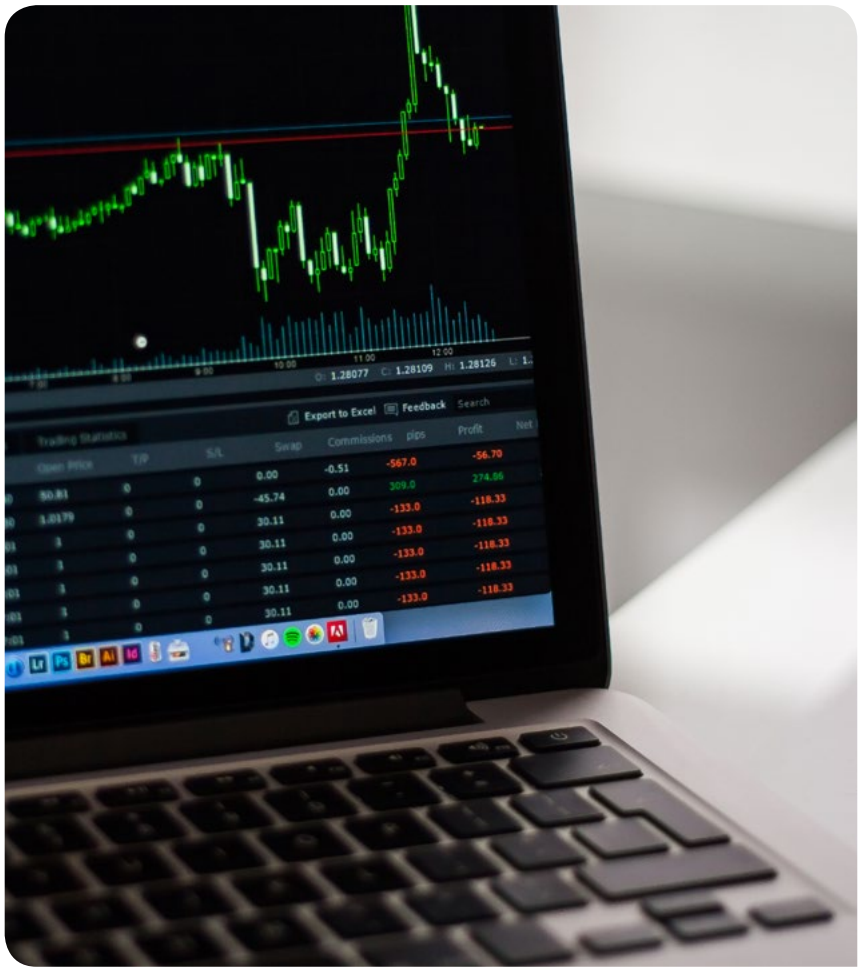
The Bitcoin ecosystem: examples of software that accesses *Blockchain*



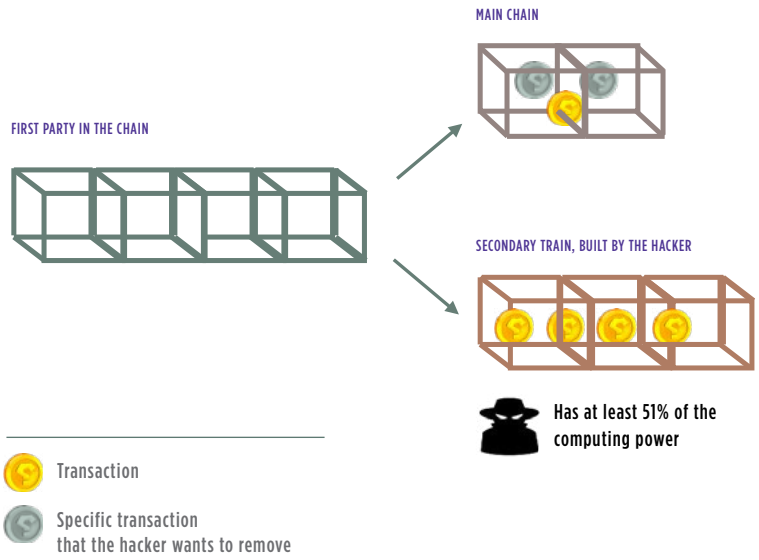
MONITOR THE PROCESSING POWER OF MINORS IN ORDER TO AVOID A 51% ATTACK

A 51% attack consists of having more than 51% of the computational power of the network in order to cancel, add, or change transactions made in a block. The idea is to create an alternative chain that is longer than the existing *Blockchain* in order to replace it. This is made possible by utilizing an essential element of *Blockchain*: where there are two co-existing chains, the longer one is deemed to be more legitimate.

This risk is greater in the context of private or hybrid *Blockchain*s, that are made up of a restricted number of users as it would therefore be easier to make up more than half of the processing power. Also, security measures should be put in place to detect this kind of attack: contractual commitments, monitoring and control mechanisms, etc.



Focus - a 51% attack, or the limits of the principle of consensus



EXPLANATION OF AN ATTACK

A hacker wants to rewrite the *Blockchain* in order to cancel certain transactions in a block

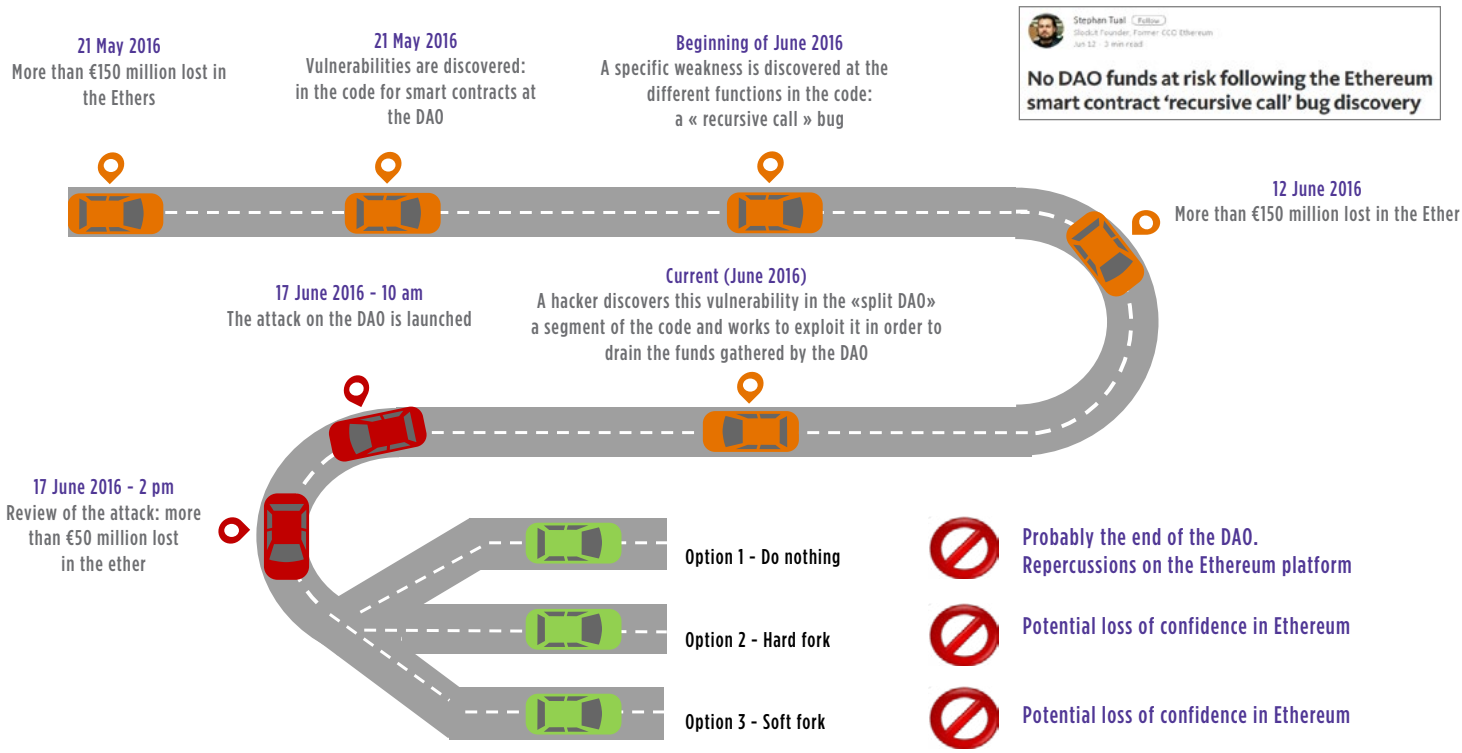
1. The hacker publishes the chain that they obtain on the network, once it is longer than the existing chain (which is possible because it contains more than 51% of the power of the network)
2. The hacker mines alternative blocks starting from the preceding block
3. The chain, being longer and exploiting the principle of consensus, replaces the existing chain and the transactions that it contained are cancelled.

SECURING THE CODE FOR SMART-CONTRACTS

A smart-contract is a computer program recorded in *Blockchain* which is automatically executed once the conditions of the contract are fulfilled.

The consequences of a coding error can be catastrophic and difficult to reverse, as evidenced by the DAO affair (an application based on *Blockchain* and offering participants a mutual investment fund). From a vulnerability found in the source code of the DAO smart-contract, a member of the network was able to drain the application's main account to the tune of 50 million dollars. These funds were partly recovered following an operation called «hard fork», something akin to a 51% attack.

Returning to the DAO affair, the application was based on the Ethereum platform.



This in itself was not an attack, because the contract was respected, it was only the design that was faulty. It is essential that the creation of cases that rely on smart-contracts is linked to the applicable security measures and safe development.

The *Blockchain* system is often regarded as secure by virtue of its design, but these attacks testify to the contrary. The nature of platforms accessing or being accessed by *Blockchain*, the complexity of the potential smart-contracts, or the number of miners on the network, are all elements equally capable of influencing the security of the service provided by *Blockchain*.

Matthieu GARIN
matthieu.garin@wavestone.com

Stéphane GOMEZ
stephane.gomez@wavestone.com

A REAL-LIFE APPLICATION OF BLOCKCHAIN

Interview with Philippe Ruault, Chief Innovation and Digital Officer at BNP Paribas Security Services.

1.HOW DID YOU FORESEE YOUR USE OF THE *BLOCKCHAIN* TECHNOLOGY?

We are currently working with the SmartAngels crowdfunding company on the creation of a securities management platform based on *Blockchain* technology. Its goal: to allow unlisted companies to issue securities and allow investors to invest in these secondary markets. It is due to be launched in October 2016.

2.WHY IS *BLOCKCHAIN* PARTICULARLY SUITED TO THIS APPLICATION?

Blockchain is a promising technology and we wanted to come up with a tangible use to implement it quickly. This platform seemed to be suitable for this «full-scale» test: the traceability and transparency of *Blockchain* are assets for shareholding, and the limitations of *Blockchain* in terms of performance are not an obstacle (the low volume of transactions on secondary markets).

3.HOW HAVE YOU TAKEN INTO ACCOUNT THE SECURITY ISSUES?

Our platforms are based on a private *Blockchain*; the miners are known and limited in number. For now, each customer has the same computing power, and there is no specific reward for the minors. Conventional security mechanisms are therefore adequate at this stage: secure development and a secure infrastructure. A potential future development to the business model (such as remuneration for miners) could incorporate additional security measures.

4.IN YOUR VIEW, WILL *BLOCKCHAIN* FUNDAMENTALLY INFLUENCE THE FINANCE SECTOR?

Blockchain possesses some interesting features that are suited to all the processes involved in the transfer of assets: powerful traceability, confidence in the records, etc.

However, let's not get carried away; it is essential to develop a regulatory framework and work to improve its performance: it is not currently possible to perform millions of financial transactions per day on a *Blockchain* system.

INTERVIEW BY EMILIE VAN LIERDE 06/10/2016

«Blockchain possesses some interesting features that are suited to all the processes involved in the transfer of assets: powerful traceability, confidence in the records, etc.»

Publishing overseen by: Olivier Schmitt

Chief Editor: Laetitia Mercier de Beaurouvre

Contributors: Anne Gautreneau, Matthieu Garin, Maxime Roche, Stephane Gomez and Philippe Ruault

Printer: Jolly - l'impression

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.