# Blockchain as a method of securing the process of collective decision-making through voting.

*Under the kind direction of Stéphane Dalbera, Atopos.*

> The interesting thing about cryptography is that we can begin to create institutional models that are no longer based on the fallibility of human authority but are strictly based on code, mathematics and encryption. We can begin to build an institutional reality where checks and balances are protected by firm promises, fundamental mathematical constructs that are simply impossible to break because of the properties inherent in the functioning of information.
>
> Santiago Siri, Democraty Earth Foundation

Many observers agree that we we are entering a period of crisis of confidence in the services offered by the Internet.

Security breaches, breaches of privacy, public opinion manipulation, cybercrime, cyberwar, etc. are nowadays issues that are widely covered by the media outside insider circles.

The time for blind belief in the benefits of the Internet revolution and fantasies seems over.

This crisis of confidence is not specific to the digital sector, it is spreading throughout all the strata of our societies. It manifests itself in the political field, in the media field, so that the era in which we live is now called the post-truth era. (*post-factual era*).

This crisis is already having many consequences in the political field as well as in the economic field where trust is the cornerstone of investment and accession.

Public opinion, legislators and industry players are beginning to appreciate the full extent of the work that is coming up to emerge from a period that may soon be considered as the Wild West.

The work of rebuilding trust, which is only beginning to crumble, will in the coming years be one of the sectors with the greatest potential for growth and innovation. *Du marché de la sécurité au marché de la confiance* (Y.ECHED et O. ARGAUT 2003)

It is in this context that we intend to focus here on the impact that a widely publicized technology could have because at the heart of cryptomonnaies: the blockchain.

If this approach has emerged in the BitCoin movement, it is above all a decentralized approach to contract security with very large potential uses.

Secure and decentralized voting services offer a wide scope for creating new modes of interaction around one of the major challenges of any structured society: decision-making.

In this work we will analyze the perspectives opened by the use of the blockchain as a tool to secure collective decision-making. Through the imperatives demanded by these decision-making processes, we will attempt to assess the blockchain's ability to meet them.

We will also attempt to assess the cost of using the blockchain for collective decision-making with particular attention to environmental criteria.

Finally, we will illustrate our point with ongoing projects or proofs of concept and provide prospective leads.

# Table des matières

# Summary

Our societies are facing a crisis of trust, and companies, institutions, associations and other actors in the public sector are already suffering the consequences.

These harmful effects are multiple, ranging from economic scandal with the financial losses involved, to the general public's disinterest in a cause, or, more generally, in citizen participation.

These institutions are closely monitored and must protect themselves by acting with greater transparency and public consultation.

Voting is the queen form of participation; although it represents the most embryonic form of democracy, it remains the easiest solution to implement on a large scale.

The blockchain appears as a potential solution to these problems, when it frames this participation process.

The blockchain is a distributed registry in which information is stored in blocks and validated using different cryptographic and consensus methods. It offers security guarantees and its limits are identified.

While many experiments and proof of concept demonstrate the general public's interest in these issues, the prospective leads are even more numerous and the blockchain could be the driving force behind this change. These experiments make it possible to consider companies involving the consumer, decentralized associations whose shares are subject to permanent voting by their supporters or public institutions managed in real time by citizens.

Many challenges and problems make the blockchain reasonably unusable in its large-scale state, particularly the energy challenge.

The ways to respond to this environmental challenge are the implementation of blockchains implementing the proof of the issue (less costly energy block validation technique) and the different forms of standardization.

# Acknowledgements

This paper was made possible thanks to the assistance of several people to whom I would like to express my deep gratitude.

First of all, I would like to express my gratitude to the director of this brief, Mr Stéphane Dalbera, for his patience, his availability and above all his judicious advice, which helped to feed my reflection.

I would like to express a special gratitude to Virgile Deville, whose advice and criticism guided my thoughts.

# Terms and definitions

1. La blockchain

2. Modalité de sécurisation

3. Prise de décision collective

4. Vote

# Definition: blockchain

A blockchain, or chain of blocks, is a technology for storing and transmitting information without a control body.

Technically, it is a distributed database whose information sent by users and internal links to the database are checked and grouped at regular time intervals into blocks, all secured by cryptography, and thus forming a chain.

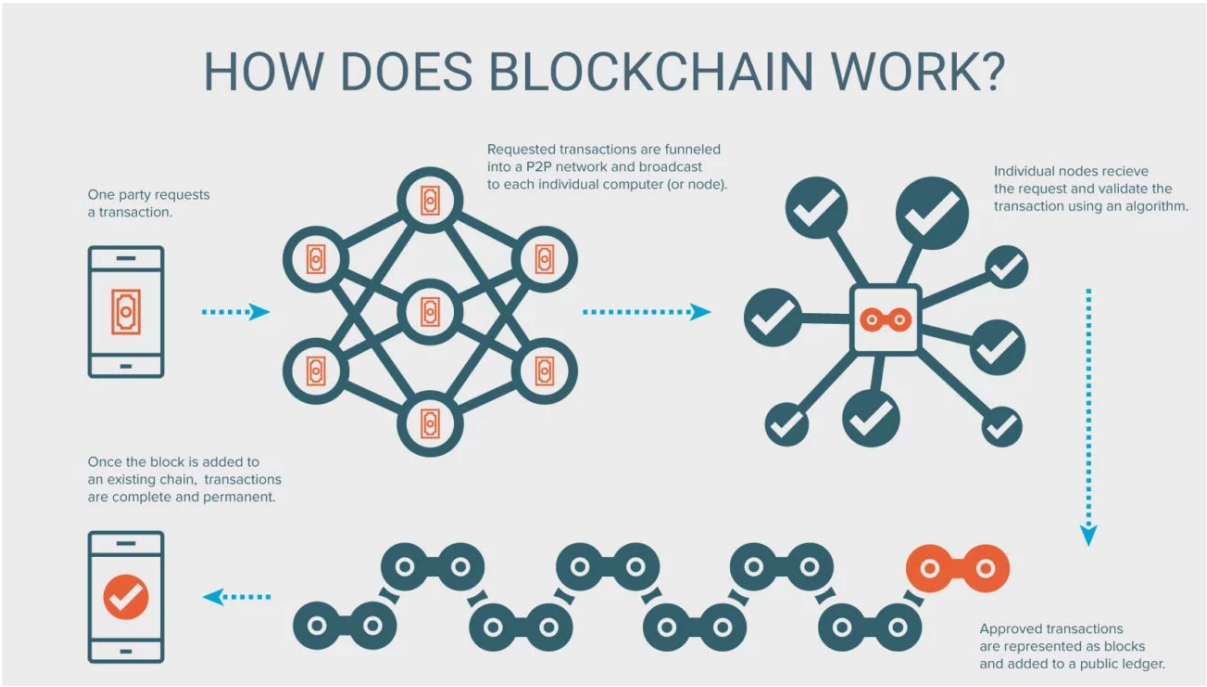
By extension, a block string is a distributed database that manages a list of records protected against falsification or modification by storage nodes.


A blockchain is therefore a distributed and secure registry of all transactions made since the start of the distributed system.

There are public blockchains, open to all, and private blockchains whose access and use are limited to a certain number of actors.

A public blockchain can therefore be assimilated to a public, anonymous and unforgeable accounting ledger.

> you have to imagine "a very large notebook, which everyone can read freely and without charge, on which everyone can write, but which is impossible to erase and indestructible."
>
> Jean-Paul Delahaye, Les blockchains, clefs d'un nouveau monde



# Definition: security modality

We understand the methods of security as the different methods and means deployed in order to secure.

The security action is initiated by the application of security techniques in the IT sense.

Information system security (ISS) or simply computer security, is the set of technical, organizational, legal and human resources necessary to implement measures to prevent unauthorized use, misuse, modification or misappropriation of the information system.

Security is a major challenge for companies and all the players around them.

- Its long-term goal is to maintain the trust of users and customers.
- Its medium-term objective is to ensure the coherence of the entire information system.

> "The information system represents an essential asset of the organization, that must be protected. IT security is about ensuring that an organization's hardware or software resources are only used within the framework provided."
>
> *JF Pillou, Tout sur les systèmes d'information*

Information systems security has the following objectives:

| Objective | Explanation |
|---|---|
| Availability | The system must operate flawlessly during the intended use ranges and guarantee access to the services and resources installed with the expected response time. |
| Integrity | The data must be the data expected, and must not be accidentally, unlawfully or maliciously altered. In other words, the elements considered must be accurate and complete. |
| Confidentiality | Only authorized persons may have access to the information intended for them. Unwanted access must be prevented. |
| Traceability (or "proof") | It must be ensured that access and attempted access to the elements in question are traced and that these traces are preserved and usable. |
| Authentication | User identification is fundamental to managing access to relevant workspaces and maintaining trust in exchange relationships. |
| Non-repudiation and imputation | Once the security objectives have been determined, the risks to each of these elements can be assessed according to the threats. |

The overall level of security of information systems is defined by the security level of the weakest link. Precautions and countermeasures should be considered in accordance with the vulnerabilities specific to the context to which the information system is intended to provide service and support.

This requires an estimate:

- The seriousness of the consequences in the event that the risks materialize.
- The likelihood of the risks (or their potentiality), or their probability of occurrence).

# Definition: collective decision-making

Collective decision-making is a situation where individuals are brought together in a group to solve problems.

Decisions made collectively tend to be more effective than decisions made individually. However, there are situations in which group decisions lead to poor judgment.

In social psychology, collective decision-making can be defined as:

> "a convergence of cognitive and visual interactions, planned or opportunistic, where people agree to come together for a common goal, within a defined period of time, [...] in order to make decisions"
>
> Abdelkader Adla, Aide à la Facilitation pour une prise de Décision Collective: Proposition d'un Modèle et d'un Outil

Collective decision-making is a broad field of study in which several disciplines are interested, such as social sciences, political sciences, computer science, marketing and management, each of which has its own perspective on the issue.

From the point of view of social psychology more specifically, theoretical applications and consequences are numerous and varied in different fields such as team management, jury situations, politics, etc. There are different types of collective decisions, each with very specific psychological modalities and processes, such as polarization, group thinking and the effect of common knowledge.

# Definition: vote

Voting (from the Latin *votum* meaning "vow") refers to a method that allows a group to make a common decision.

Formal or informal organizations of all kinds (economic, political, associative, etc.) use this practice. The practice of voting aims to give legitimacy to the decision by showing that it does not come from an isolated individual. Before the vote itself takes place, it is common for a period of discussion or debate to be set aside to allow each voter to present or read the arguments, in order to provide the best possible justification for their decision.

Voting is generally governed by an electoral process also known as "voting" or "election".

# The implications of the vote:

| Principle | Explanation |
|---|---|
| Decidability | The primary purpose is generally to be able to decide on a position, whether it is a position to take a decision, or a position not to take a decision; this is particularly the case for a referendum. |
| Voting uniqueness | Generally speaking, we want the vote to be unique: to allow everyone to be fairly represented, we must not allow an elector to vote several times, i.e. to be over-represented. |
| Representativeness | The vote must be representative of the opinion of the whole. In some systems, the votes of each voter are weighted by a share of participation. |
| Secrecy and transparency | Depending on the election, one may wish the vote to be secret, in order to prevent corruption of the vote, or on the contrary, public, in order to force an assumed position. |
| Verifiability | In order to remove any doubt about the legitimacy of the election, when an issue exists, we want the election to be verifiable, in other words, awe want everyone to see that there is no cheating. The aim is to ensure that the people and materials involved in the organisation are not diverted to the benefit of specific interests. |
| Attractiveness | Some commercial organizations promote votes with the unspoken aim of encouraging participation in an action that without saying it is an act of purchase. This is particularly the case for votes to purchase by "value-added service numbers" also known as premium rate telephone calls. |
| Non-participation | To avoid that a decision is taken by default or to compensate for certain contingencies, it is customary to allow non-participation, for example through abstention or a nil or blank vote. |
| Quorum and majority | To give greater legitimacy to decision-making, the voting method may be correlated with a quorum system, i.e. a minimum number of members present at a meeting without which a deliberation within the meeting cannot be valid |
| Rapidity | In a vote where a positive result is expected, it is customary to ask first who is against and then who abstains. Those who do not speak out are then assumed to be in favour of the decision. This has a double advantage: it avoids having to count the many pros, while maximizing their number. |

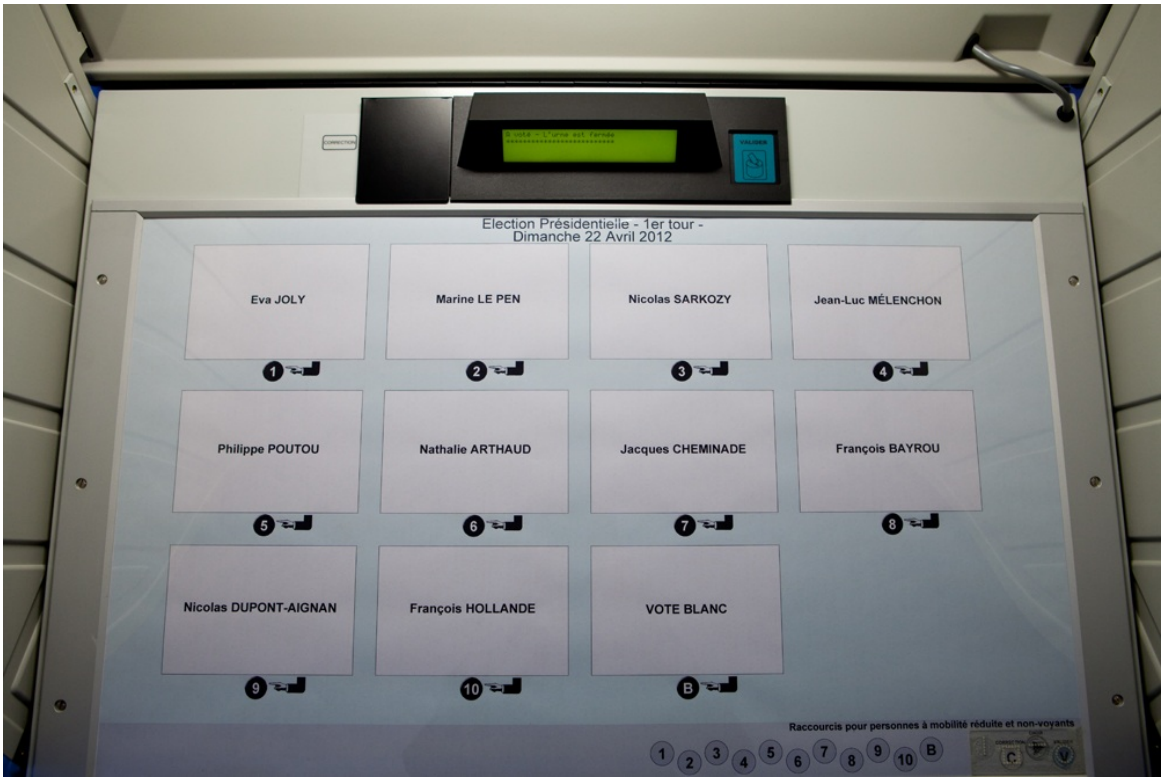
# Expression modalities:

- Secret ballot: A secret ballot, also known as a secret ballot, consists of giving an opinion on several proposals, anonymously.
- Show of hands: A show of hands vote consists of raising your hand to give your opinion between several proposals. It allows a quick decision making, because the counting is almost immediate. But this requires that all voters be present at the same time. The procedure can begin with an acclamation vote, where the volume of each option is estimated, as in the Spartan assembly or at the conclusion of presidential primaries in the United States. Voting by show of hands does not guarantee the confidentiality of the vote, this voting system guarantees a form of transparency in representative democracies.


>

> Hands up voting, source French National Assembly

- Public vote: A public vote, also known as a roll-call vote, consists of calling each member of a meeting in turn to cast his or her vote publicly. This is then recorded in the register of deliberations and it is then possible to publish the vote of each of the participants in the vote.
- Postal voting: it consists in sending the ballot paper in advance by post; an identification number ensures that a person only votes once, while maintaining the secrecy of the vote.
- Voting by proxy: Proxy voting allows the principal to appoint a proxy to vote in his or her place.
- Replacement vote: Substitute voting allows those who vote for candidates or lists that do not have elected representatives because they have not reached a quorum to allow their votes to be carried over to another candidate.
- Electronic voting: Electronic voting is an automated voting system, including elections, using computer systems. This generic term actually refers to several concrete situations. For example, it may correspond to the computerization of the voting process allowing remote voting, i.e. voting from home, or from anywhere in the world and thus avoiding travelling to polling stations.



>

> A French electronic voting machine, source Saint-Pol-sur-Mer Town Hall.

- Vote by key: It consists of voting using a physical key on a dedicated desk.

---

## The particular case of Internet voting is not a specific one.

Internet voting, which is part of the mode of action of electronic voting, has long been criticized on the grounds that its main disadvantage would be the absence of a voting booth (there is no guarantee that citizens are alone in front of the computer when they vote, nor can they verify it). However, this insurance is also absent during public voting, by post, by show of hands. It is also impossible to ensure that the principal's wishes have been respected in a proxy vote.

# A. The requirement of secured collective decision-making tools and their impact potential

# Les origines de la crise de confiance et l'aspiration à la transparence

## L'ère de la post-vérité

«Post-vérité»: c'est le néologisme que le dictionnaire de l'université d'Oxford a choisi de nommer mot international de l'année 2016. Il provient du livre *The Post-Truth Era de Ralph Keyes*.

> Cette notion est généralement associée aux affirmations fantaisistes et mensongères de Donald Trump et à ceux qui ont voté pour lui, issus des classes populaires de la société américaine. Mais, en réalité, la responsabilité de l'ère post-vérité revient aux professionnels des classes moyennes qui ont préparé le terrain à son récent triomphe. Universitaires, journalistes, «créatifs» et traders: tous ont contribué à l'avènement de la «post-vérité» ; même les politiciens de centre gauche, pourtant durement touchés par le succès du courant anti-factuel.
>
> *Andrew Calcutt, The Conversation*

Déjà en 1964, dans Vérité et politique, Hannah Arendt se posait la question de l'objectivité de l'histoire. Dès la première phrase, en évoluant l'opinion et l'interprétation, elle engage la réflexion sur le terrain de la supposée subjectivité de l'historien.

Cette remise en question et ce questionnement, légitime, ont ouvert la porte à une remise en question plus profonde. Il existerait un pan entier de la réalité qui ne serait appréhendable qu'à travers le regard subjectif de l'observateur.

Dans la seconde moitié des années 1990, les industries créatives ont réussi à générer une croissance spectaculaire à travers le développement de l'image de marque ou «branding«. Le «branding» est devenu beaucoup plus important que l'activité banale de conception, de développement et de fabrication d'un produit.

Au lieu de commercialiser un produit en le présentant comme utile, ces créatifs ont entrepris de lui donner une âme, une conscience et une morale.

Au tournant du siècle, le gouvernement se préoccupait déjà moins de «la vérité» que de la façon dont «les vérités» pouvaient être (dé)tournées. Ceux que l'on nomme des «spin doctors» ont investi le devant de la scène. La guerre en Irak en est un excellent exemple.

Les faits ont été relégués au second plan.

Dans cette perspective, toutes les revendications sur la vérité sont relatives à la personne qui les fait ; en dehors de nos propres particularités, aucune position ne permet d'établir la vérité universelle. C'est l'un des principes fondamentaux du postmodernisme, un concept qui a pris son envol dans les années 1980 après la publication de La Condition postmoderne: rapport sur le savoir de Jean-François Lyotard.

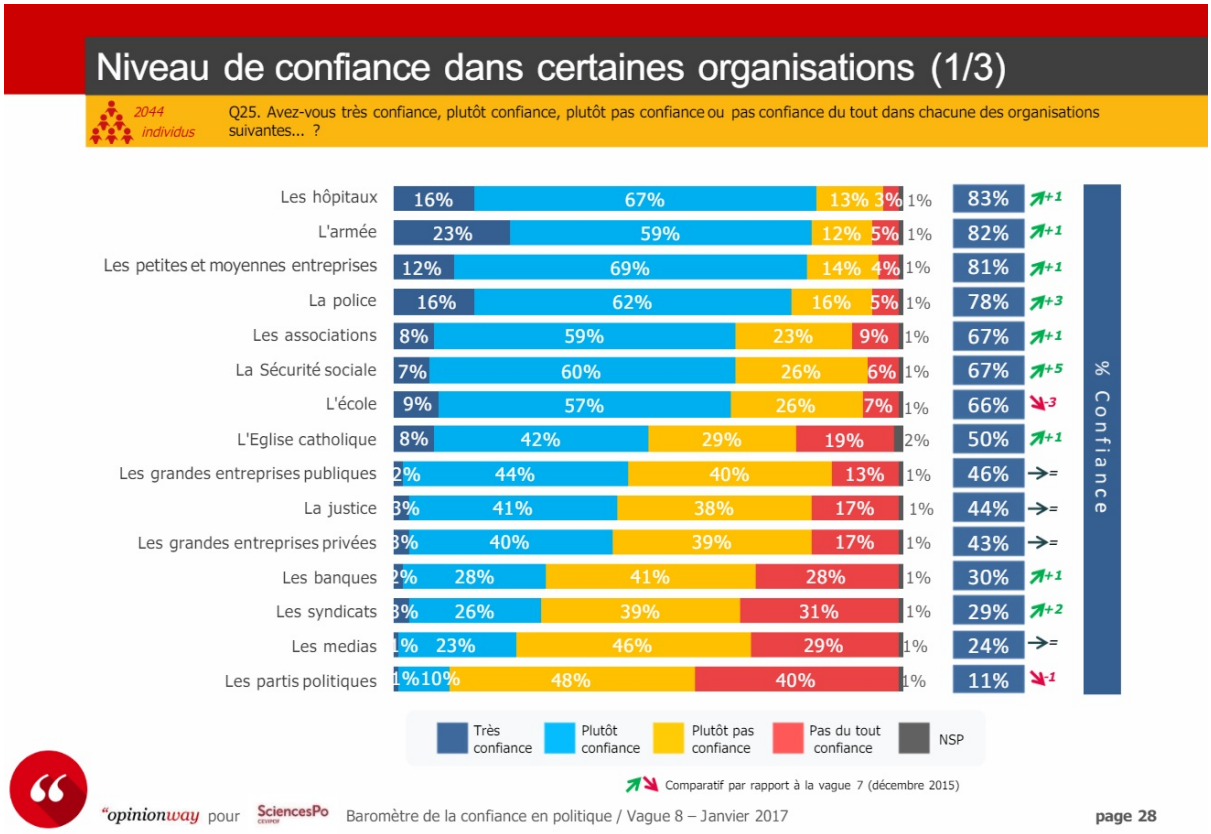
Le postmodernisme n'a pas créé les fondations de l'ère «post-vérité».

Ces fondations ont été creusées par le détournement malhonnête d'un certain nombre de concepts évoqué par le post-modernisme alliés aux révélations de scandales politiques, économiques et écologiques au cours de ces cinquante dernières années.

A l'origine parfois méfiant ou suspicieux, le grand public est devenu hyper-critique quant aux faits.

Internet a amplifié cette réaction en maintenant ce public dans des sphères de confirmation sur les réseaux sociaux ou via les médias qu'ils consultent.

Aujourd'hui il apparait comme un défi pour les entités s'adressant à ces citoyens d'appréhender ces cercles idéologiques et leur influence sur le message qu'elles véhiculent.




>

> Source Étude Cevipof Sciences Po

Comme nous pouvons le voir sur l'infographie ci-dessus, les grandes entreprises privées, les banques, les syndicats, les médias et les partis politiques sont parmi les moins dignes de confiance pour le grand public.

Nous traiterons dans ce mémoire essentiellement des institutions publiques, des entreprises privées et des associations.

Il serait vain de tenter de lister toutes les manifestations de cette crise de confiance ni même ses origines qui sont sujettes à controverses. Néanmoins, il convient de constater que celle-ci existe indubitablement, en témoignent les nombreux articles de presse sur ce sujet, et que son existence impose de repenser profondément le rapport au monde des entreprises, associations, et États en intégrant ses nouveaux impératifs de transparence.

# Une aspiration à la transparence

Pour répondre à la problématique de la transparence, une solution semble apparaître: «montrer patte blanche».

Les entreprises engagées dans des actions de communications doivent prendre conscience qu'elles sont hyper-scrutées et qu'elles doivent engager das actions pour prouver leur bonne-foi.

Nous entendons par là de faire usage le plus possible de la preuve, la plus irréfutable possible et d'instaurer la transparence comme un principe fondamental de la communication nouvelle des entreprises, des états et des entités émettrices de messages envers le public.

Pour accompagner cette restauration de la confiance, des outils technologiques ont vu le jour: plateforme participative, management holacratique, consultation publique. Le besoin en transparence est d'ailleurs bien compris par certains acteurs, par exemple, ces outils font partie des propositions attendues par les collectivités dans le cadre des grands appels à projets urbains tels que "Inventons la Métropole du Grand Paris".

Mais pour que ces nouvelles méthodes ne soient pas un palliatif, il faut qu'elles mettent en place un réel système vertueux et orienté sur le long terme.

> Pour cela, ces systèmes doivent être conçus de manière ouverte (Open Source) mais également respecter des principes de sécurité par conception (security by design) et de protection de la vie privée (privacy by design).

## La confiance partagée: l'émergence du «trustless»

La blockchain intègre ces attentes et les dépasse: elle pose le concept de non-nécessité de la confiance (trustlessness). À l'origine, ce mot désignait une personne ou une ressource à laquelle on ne pouvait pas faire confiance. Mais dans le cadre de la blockchain, le terme «sans confiance» (trustless) signifie qu'il existe des mécanismes en place par lesquels toutes les parties dans le système peuvent parvenir à un consensus sur une vérité canonique.

Le pouvoir et la confiance sont répartis (ou partagés) entre les parties prenantes du réseau (par exemple, les promoteurs, les mineurs et les consommateurs), plutôt que concentrés dans une seule personne ou entité (par exemple, les banques, les gouvernements et les institutions financières).

# Du statut de la preuve au vote

Si la transparence nécessite d'apporter la preuve de sa bonne foi, la preuve mérite que l'on s'intéresse à son statut et aux conséquences qu'elle fait peser sur le vote.

## Qu'est ce qu'une preuve?

Une preuve est un élément matériel (ex. : document contractuel, attestation) qui démontre, établit, prouve la vérité ou la réalité d'une situation de fait ou de droit. La preuve est également une opération par laquelle on contrôle l'exactitude d'un calcul ou la justesse de la solution d'un problème. C'est bien cette double nature qui nous intéresse ici au regard de la question du vote.

## Le vote et la preuve

Le rapport entre le vote et la preuve est comme nous l'avons évoqué, duale. Parce que la preuve doit être présente autour du processus de vote et autour du vote en tant qu'acte matériel.

Preuve entourant le processus:

- Fiabilité
- Traçabilité

Ce processus doit être réfutable, c'est-à-dire qu'il doit présenter des éléments tangibles et objectifs permettant sa potentielle disqualification ou non. Si le processus ne présente des critères de réfutabilité potentielles, il est jugé corrompu a priori.

Preuve entourant le vote:

- Authenticité
- Intégrité
- Confidentialité

> La confidentialité est une question épineuse dans le cadre du vote car elle n'est requise que dans le cas du vote à bulletin secret. Bien que ce soit une manifestation du vote plus rare, ce type de vote pourrait être le plus critique.

En effet, le vote à bulletin secret a pour but de garantir que le votant n'a pas été corrompu, ou ne pourra subir de coercitions en conséquence de son vote. Il est difficile de garantir l'intégrité du processus tout en assurant la confidentialité du vote. Pour cette raison, ce type de vote est moins utlisé.

Dans le processus démocratique actuel, l'identité du votant est contrôlée par l'existence d'une liste préalable, et la présentation d'un document d'identité attestant de l'état civil. Il s'agit d'un très classique recours à un tiers de confiance. En effet, l'État joue un double rôle ici: il atteste de l'état civil de la personne et délivre une preuve matérielle, disposant d'outils de lutte contre la falsification afin d'attester de cet état civil. Il délivre également la liste des personnes légitimes à s'exprimer dans le cadre du scrutin.

Cette confusion des rôles fait reposer une lourde responsabilité sur l'organe étatique, car il est à la fois juge et partie: il doit garantir la sécurité du processus, en étant le bénéficiaire du résultat de celui-ci, et en déterminant les processus de validation, de contrôle et de méta-contrôle .

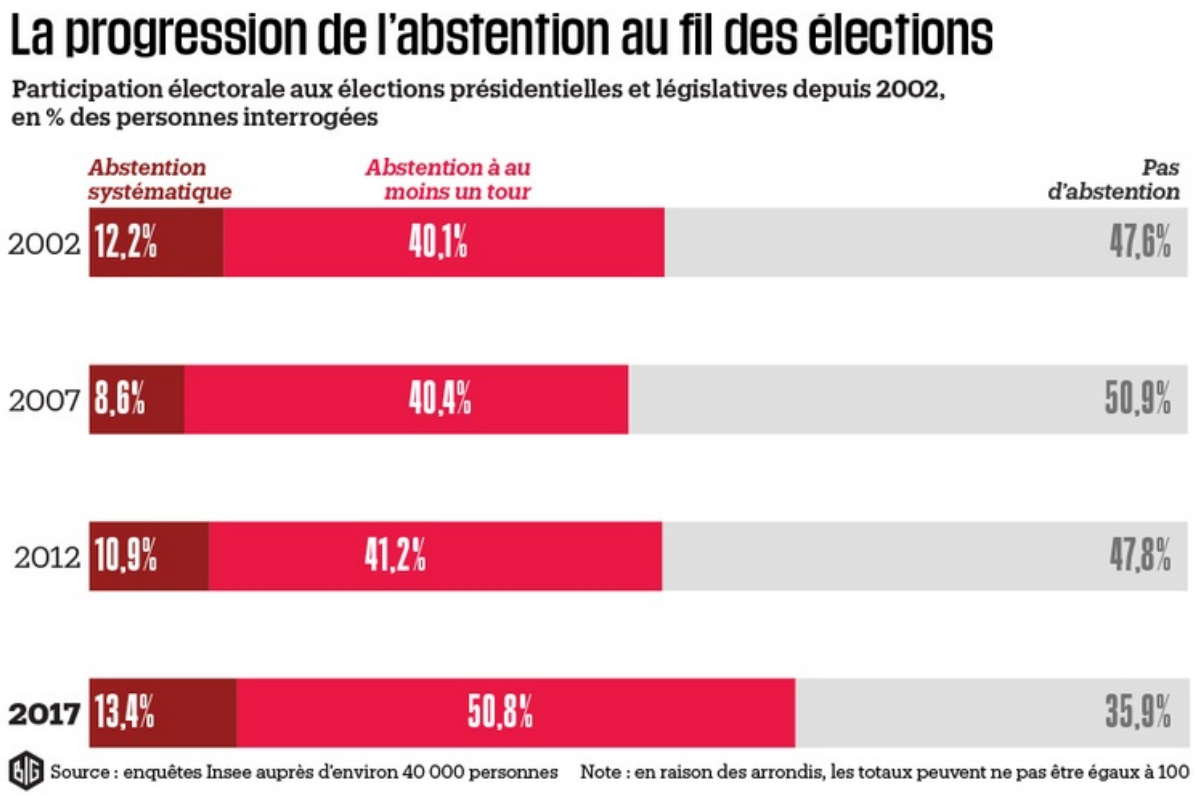
# Les domaines d'enjeux

La sphère publique, au sens arrendtien, est agitée des nombreuses problématiques que nous avons illustrées précédemment. Dans cette dimension publique, le vote est la forme d'expression reine : elle permet la consultation du plus grand nombre au moindre effort.

Le vote dans la sphère publique invite à s'interroger sur la représentativité en matière de prise de décision, de disponibilité physique des votants, de la transparence du processus démocratique, de l'intégrité et de la traçabilité.

De nombreuses implémentations du vote sont connexes au sein des institutions publiques, des associations, des entreprises dont la gestion se veut collaborative. Par conséquent, les réponses apportées à ces besoins peuvent être proches, voir similaires.

Par exemple, la participation aux élections nationales en France voit sa participation chuter d'année en année:




>

> L'abstention en France depuis 2002, source INSEE

La blockchain, parce qu'elle supprime en partie le besoin de confiance, pourrait rassurer le grand public dans son acte de participation et pourrait constituer un moteur de ré-engagement de ce dernier.

## Les différentes formes de vote dans la sphère publique:

## Le vote dans les conseils d'administration:

Ils ont pour champ de compétence l'administration des institutions, associations, entreprises ou un établissement public.

L'organisation, le fonctionnement et les prérogatives du conseil d'administration sont fixés par le statut de l'institution et dépendent du droit des sociétés. (Art. L.225-36-1 C. com.).

En général, les statuts prévoient la périodicité des réunions et les modalités de convocations des administrateurs.

Un conseil d'administration doit théoriquement se tenir dès lors que la situation de l'entreprise l'exige. Or, la tenue de celui-ci est *de facto* conditionné à la disponibilité physique des parties prenantes.

Les décisions sont prises par le vote au sein d'un conseil d'administration, en général à main levée. Ce qui implique la confiance dans le déroulé honnête de celui-ci, la traçabilité n'étant assurée que par le tiers de confiance qui le rapporte.

- La participation de la personne morale au conseil d'administration: Si une personne morale est membre d'un conseil d'administration, elle désigne une personne physique pour la représenter. De la délégation de ce vote découle un doute: le délégataire est dans la capacité de dépasser ou d'outrepasser les choix préalables du ou des délégants.
- L'intégration du salarié: Le projet de loi sur la croissance des entreprises, dit loi Pacte, prévoit de renforcer la présence des représentants salariés dans les conseils d'administration (Projet de loi PACTE article 62, alinéa II).

  Ce projet de loi introduit une plus grande participation des salariés comme vecteur de croissance économique selon le Rapport d'étude d'impact du projet de loi relatif à la croissance et la transformation des entreprises.

## Le vote dans la consultation publique

- Dans le cadre de la pétition: La pétition consiste à apporter son soutien à une cause en la ratifiant. Bien qu'elle n'appartienne pas directement au vote, elle partage avec ce dernier de nombreux attributs qui font que nous pouvons traiter les deux sujets conjointement sans perdre en pertinence.
- Dans le cadre de l'administration du bien public: L'administration du bien public en toute transparence est une préoccupation majeure de ces dernières années. Elle se pose à deux niveaux ; le premier concerne la prise de décision et implique la concertation. Le second implique la gestion continue du bien et sa gouvernance. Les biens publics sont multiples et les propositions les concernant peuvent provenir des citoyens mais également des institutions.

## Le vote dans la gestion collaborative:

- La co-gestion avec les utilisateurs: Le crowdfunding désigne tous les outils et méthodes de transactions financières qui font appel à un grand nombre de personnes afin de financer un projet. Les manifestations de soutiens provenant des utilisateurs de ces outils sont de deux types: un soutien financier qui consiste en une transaction dont le montant représente un pourcentage d'un objectif, et l'acte de transaction qui représente un soutien en tant que tel. Le montant de la transaction ne représentant qu'une échelle du soutien.
- Du besoin spécifique des associations:

  Les associations peuvent recourir à la consultation du public par le vote dans plusieurs cas:

  - Choix des projets associatifs
  - Allocations des budgets
  - Désignation des administrateurs
  - Détermination des processus opérationnels

> L'action des associations est soumise à la confiance de ses donateurs. De nombreux scandales ont illustré que cette confiance était parfois abusée menant au mieux à un désintérêt pour la cause défendue, au pire à un lynchage médiatique discréditant durablement les actions entreprises.

## Les promesses de la blockchain:

Le recours a la blockchain dans ces méthodes de prises de décisions par le vote permettrait:

- Une plus grande représentativité par l'intégration d'un grand nombre d'acteurs (dans les limites d'échelle permise).
- Une indépendance quant à la disponibilité physique des votants. Particulièrement avantageuse dans le cadre d'organisations internationales ou éclatées.
- Intégrité de la décision, par des processus de lutte contre la falsification.
- Traçabilité de la donnée.
- Transparence des décisions et des processus.

## En synthèse

| Acteur / Forme de vote présent | Conseil d'administration | Management Participatif | Consultation publique | Élection des administrateurs et représentants |
|---|---|---|---|---|
| Institution | ✓ | ✓ | ✓ | ✓ |
| Association | ✓ | ✓ | ✓ | ✓ |
| Entreprise | ✓ | ✓ | ✓ | ✓ |
| Établissements public | ✓ | ✓ | ✓ | ✓ |
| Grand public | ✗ | ✗ | ✓ | ✓ |

> Tableau récapitulatif des formes de vote présents au sein d'un acteur.

# B. Blockchain as the potential heart of this change

Companies, institutions and associations are going through a crisis of trust. They are now being examined, analysed and the slightest slip-up can have costly consequences. While participation through voting is an easy first step towards reconciliation, it is not enough. Indeed, the general public is now demanding reliable and transparent processes to enable control by as many people as possible. The blockchain appears as an opportunity to restore confidence and as an engine for re-engagement with these organizations.

# What is the blockchain?

The term blockchain refers to both the system and the technology behind it.

The blockchain is known mainly to the general public as the technology used by Bitcoin.

Invented in 2008, the Bitcoin is originally a prototype designed to demonstrate the possibility of creating a cryptocurrency whose mechanism is based on a distributed register distributed among multiple nodes of a network.

Due to their intrinsically open-source nature, encryption algorithms are an additional argument for confidence in this system.

If the Bitcoin has benefited from such media exposure, it is because it is a limited volume currency that is outside the current benchmark. But above all, it is a currency that challenges the role of banking institutions and states as trusted third parties and legitimate entities to issue and regulate money.

## The three pillars of the blockchain

The blockchain is based on three pillars: two are technological, namely asymmetric cryptography and distributed systems, and the third is sociological.

## 1. Cryptography

It is based on the concept of a key. There are two types of keys: symmetrical and asymmetrical.

The former have been known since antiquity and the latter were first introduced in the 1970s.

The second is essential to blockchain technology because it ensures the authenticity of the sender of the message. The sender uses his private key to code a message that the recipient can decode with the sender's public key. The symmetric encryption method has the advantage of being inexpensive in terms of computing power, and of remaining very secure. Unfortunately, it has its limitations:

> The disadvantage is that to encrypt an n-bit message, you must first have exchanged an n-bit key with the recipient of the message, and this by an absolutely secure means, otherwise encrypting becomes unnecessary.
>
> Claude Shannon, Communication theory of secrecy system

Instead of this method, asymmetric encryption is preferred, which makes it possible to bypass the obstacle of the common key for all stakeholders. Indeed, in the context of asymmetric encryption, two keys are present: private and public. The key that is chosen private is never transmitted to anyone while the key that is chosen public is transferable without restriction.

This technique allows:

- Encryption

  One of the roles of the public key is to enable encryption. It is therefore this key that a first subject will use to send encrypted messages to a second subject. The other key - the secret information - is used to decipher. Thus, the second subject, and only the second subject, can read the messages of the first subject.

  The knowledge of one key does not allow the other key to be deduced.

- Origin Authentication

The use by one of the subjects of his private key on the condensate of a message will allow the latter to verify that the message comes from the expected interlocutor and to prevent usurpation:

```
  he will apply the public key that his interlocutor provided him on the condensate (encrypted condensate w
ith the private key of the other subject) and thus find the original condensate of the message.

  It will therefore be sufficient for him to compare the condensate thus obtained and the actual condensate
 of the message to know if his interlocutor is really who he claims. It is on this mechanism in particular
that the digital signature works.
```

## 2. Distribution

The Internet happens to be one of the most beautiful proofs of a distributed system, no need for a single telecommunications operator so that anyone, anywhere in the world, can connect to the Internet.

## 3. Distributed consensus

To understand the concept of distributed consensus, the example of an operation to combat drug traffickers seems to us to be the most appropriate.

Imagine a city fighting crime, especially a powerful cartel. As part of an operation to combat drug trafficking, all the police forces in the region are working together to destroy criminals.

The different police organizations must all attack together to take advantage of the surprise effect. Otherwise they would be overwhelmed and traffickers would risk taking advantage of the confusion to escape.

They therefore had to coordinate the date and time of the attack, and, as they could not all meet, they delegated the role of messenger to some in order to limit the comings and goings.

Unfortunately, in such a corrupt city, no one can be trusted and some police officers are actually undercover criminals whose objective is to thwart the attack.

For example, one of them may tell half of the police forces that they must attack at a given date and time, and the other half that they must withdraw, a disorganization that will not allow them to benefit from the surprise effect and numerical superiority.

The great novelty brought by the blockchain is to propose a system that allows to get rid of this hierarchical authority.

In essence, each police force can only send one order at a time, associated with a timestamp.

Most importantly, however, the orders are aggregated to each other and then encrypted, forming a chain stored in a "transaction ledger", which is redistributed to all the police services involved.

A chain is thus formed, containing a hash of all previous orders.

Thus, if a messenger receives the information "The search will take place tomorrow at 4:00 p. m.", and decides to pass it on to only half of the others and send a different schedule to the other half, he will change the value of this hash.

As other messengers share information with all police forces involved, it will be possible to determine inconsistent chains and identify corrupt ones simply by comparing the value of hashes.

This of course implies that the number of honest messengers is greater than the number of corrupt ones.

## Consensus methods:

| Consensus type | Description | Advantages | Disadvantages | Blockchain type |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| Proof of work (PoW) | Miners' computers are made available to solve a complicated mathematical problem. The first one to find a solution wins the reward for the next block in the chain. | Secure, proven and robust. | High electricity and computer equipment consumption. | Public |
| Proof of stake (PoS) | Transaction validators must pledge possession of cryptomone to receive a reward. If a node is malicious, it may lose its pledge to honest validators. | Low consumption of energy resources. | Little tested on a large scale. | Public |
| Practical Bizantine Fault Tolerance (PBFT) | Consensus whose list of validators is known at the outset and can tolerate up to 1/3 of compromised nodes (disconnected or malicious). | Fast and efficient group consensus building. No fork or chain reorganization. | | Private |
| Proof of authority | Consensus whose list of validators is known at the beginning and which validates a block in turn. This type of consensus can tolerate up to 49% of malicious or disconnected nodes. | Quick group consensus. | | Private |

# What are smart contracts?

## Principle

The Ethereum blockchain has a unique capacity compared to other blockchains, It can be programmed using a specific language: Solidity. It is a "complete" programming language (turing-complete), i.e. it allows to execute all the functions used to develop a modern application.

This allows you to schedule commitments on the Ethereum blockchain. These can be simple, such as initiating a transaction, or more complex, because they consist of several actions in series or parallel.

When the conditions for the execution of these commitments are met, these contracts are automatically executed on the blockchain, taking into account all the conditions and limitations originally scheduled.

A service contract between two entities can easily be modelled as a smart-contract.

The first wishes to remunerate the second in payment of the service, this contract is formalised in the Ehthereum blog by the creation of a smart-contract type commitment. The corresponding amount is then pledged on the blockchain. When the service is provided, the commitment automatically verifies that the conditions set have been met and, if necessary, pays the sum pledged. In the event of failure to comply with the provisions of the contract, the pledging party shall be reimbursed the sum.

The transactions carried out are public, this is the principle of disclosure. The proper execution of the contract can thus be verified, any party who has the source code of the contract can verify that the contract has been registered.

The blockchain provides high security, one of its limits is the vulnerability to attack of 51%. Voir sécurité de la blockchain.

The data that is recorded in the blockchain is recorded in an immutable way: the history is kept since the beginning. A commitment is irrevocably recorded in the blockchain.

Offlining a blockchain would require stopping all nodes of the block simultaneously, which is virtually impossible. It is therefore a system that can be considered reliable.

> In short, smart-contracts make it possible to enter into agreements between two parties without one of them being able to hinder its execution, but also decentralized applications.

## Limits

This raises the question of the validation of the execution conditions. Indeed, since it interacts with the physical world, smart-contract sometimes has to have material capacities. There are two possibilities for this:

- Internal execution condition: When the execution conditions do not require physical interaction with the environment, the conditions are recorded in the blockchain. The contract is executed as soon as the conditions are met and the execution date is reached.
- External execution condition: When the conditions of execution are external to the blockchain such as the performance of a service, the occurrence of an event... etc., the use of a trusted third party, called "oracle" is necessary. It is delegated to him the observation of these foreign events and the writing of the conditions in the blockchain.

The main limitation inherent in blockchain technology is the slowness of the network, in return for its security.

## As part of the vote:

Example with the use of an oracle service:

The use of an oracle service requires a significant number of participants. Each protagonist votes for the result he or she considers to be accurate and the result is entrusted to consensus. One example is the Oraclize project. In the context of the vote, this implies entrusting a number of proposals to the consensus that determines the valid elements.

A proposal is in this case a classic smart-contract whose conditions set the framework for its application. Once these conditions have been validated, the contract is scheduled for execution.

This system has a limit and requires particular vigilance. Indeed, the interruption of the contract (and therefore of the execution of the proposal) is in practice impossible, unless this interruption condition was foreseen from the outset.

# Proof of work vs. proof of stake

We have seen earlier that a blockchain is a distributed registry that is encrypted and replicated in all nodes of the network, which contains the order chains that allow, through consensus building, to manage trust without an external institution.

## Concerning proof of work:

Proof-of-work English. Short for PoW.

We have seen earlier that the string consists of a set of data blocks containing information and a time stamp. With each transaction, these blocks are integrated into the chain.

In order to guarantee its integrity, this chain is encrypted and must be certified.

To certify the transaction, powerful computers made up of networked nodes perform cryptographic calculations.

The overall certification work is called "proof of work".

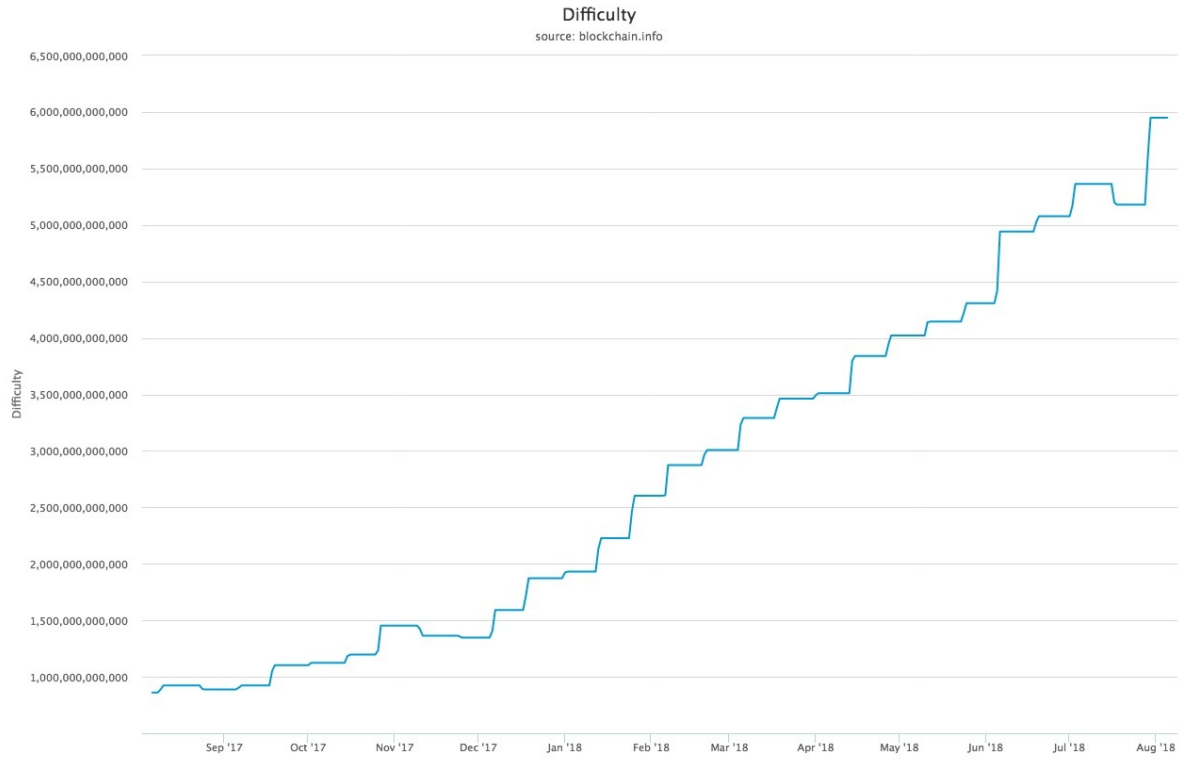
The machines (or institutions) that do this work of certifying English "minors" are called *mining*.

The cryptographic object created by the minor is proof of the time spent at certification, it constitutes proof of work.

It is essential to ensure the real nature of the work of stakeholders in order to preserve consensus.

The result of an invention by Adam Back, inventor of the Hashcash protocol, it avoids easy cloning, which would have the consequence of being able to control the blockchain retroactively.

The mechanism is even more sophisticated: at regular time intervals, the difficulty increases.



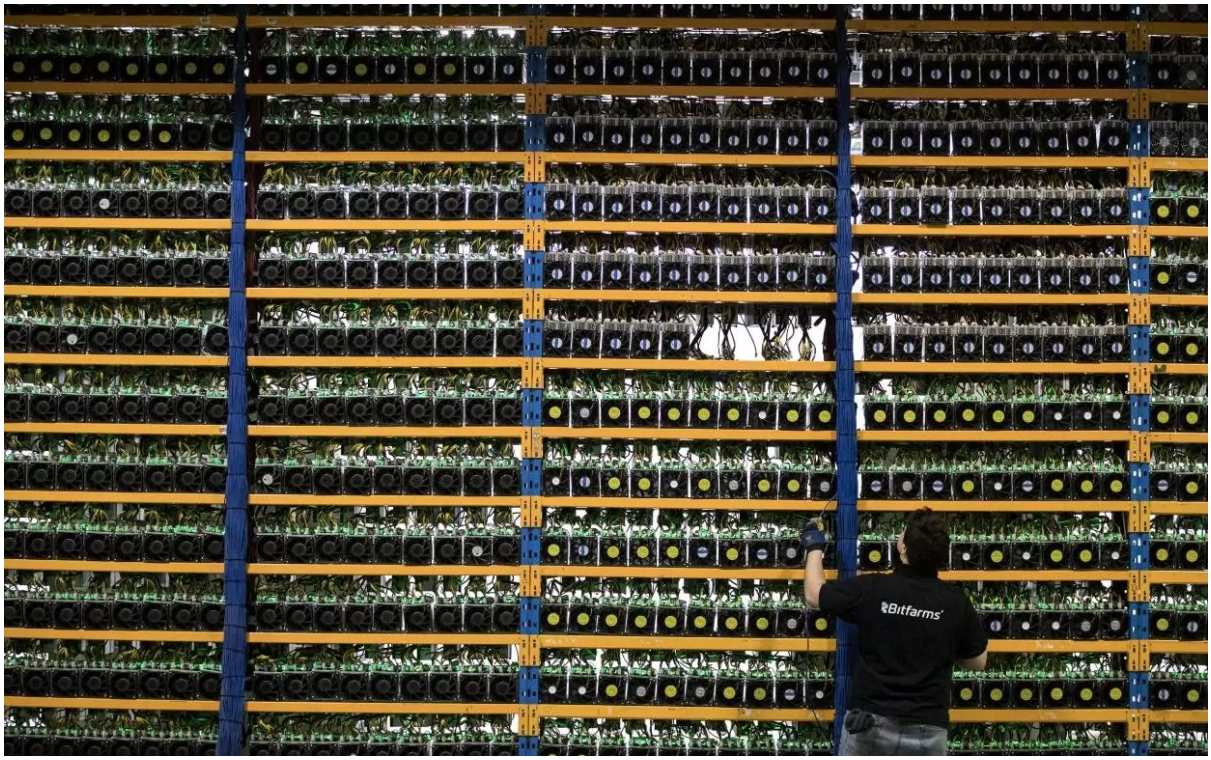
> Graph illustrating the relative measure of difficulty in finding a new block. The difficulty is periodically adjusted according to the hash power deployed by the miner network.
>
> Source: blockchain.com

Competition is the method used to motivate for certification, so the first minor to validate a new block will be rewarded.

For bitcoin, the certification task was originally accessible to private individuals through the use of graphic cards, whose power for the type of calculation required for certification was higher.

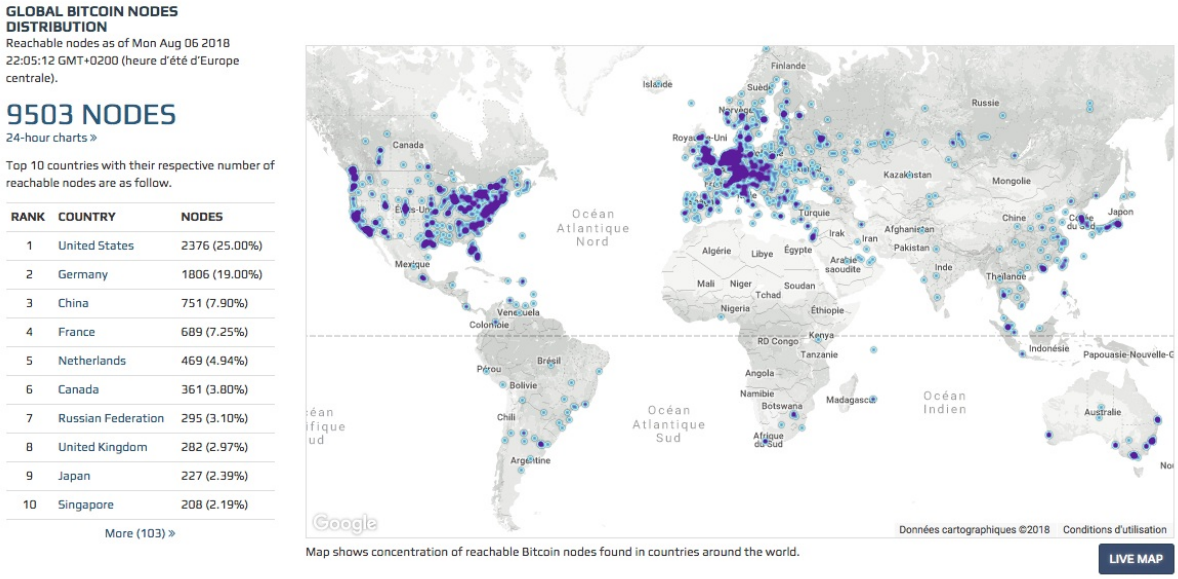
Since then, specific miners have appeared to carry out the proof of work and the general public graphic cards are neglected because they are not competitive.

Because as the size of the chains increases, so must the computing power. This interdependent relationship has driven individuals out of the certification race and institutions have now taken over.




> The bitfarm computation farm
>
> Source: bitfarms.io

In August 2018, there were 9,503 Bitcoin blockchain processing nodes worldwide.




> Global bitcoin nodes distribution
>
> Source: bitnodes.earn.com

Mining services are available in the cloud through cloud-mining, which nevertheless remains a model more oriented towards companies or large organizations than towards individuals.

## Regarding the proof of stake:

## Selon Usman W. Chohan, Proof-of-Stake Algorithmic Methods: A Comparative Summary

The proof of the issue is a different algorithm than the proof of work to obtain a distributed consensus.

In crypto-currencies based on evidence of stakes, the creator of the next block is chosen by various criteria (e. g. random selection combinations, wealth or age). These criteria depend on the economic stake of a validator in the network.

As a proof of work (PoW), the algorithm rewards participants who solve cryptographic puzzles to validate transactions and create new blocks (i. e. mining).

In public block chains based on evidence of issues (e.g., the upcoming implementation of Ethereum's Casper), a set of validators take turns proposing and voting on the next block, and each validator's voting weight depends on the size of its repository (i.e., its stake).

Significant benefits of the proof-of-investigation method include safety, reduction of centralization risks and energy efficiency.

There are two types of algorithms for proof by stake:

- Chain proof of the issue:

  In chain-based proof, the algorithm chooses a validator at random for each time slot (e. g. every ten seconds), and assigns this validator the right to create a single block, and this block must point to a previous block (normally the block at the end of the longest chain). Thus, over time, we observe a growth in a single chain.

- Proof of the Byzantine-Fault-Tolerant (BFT) type of issue: In the BFT proof of bet, the assignment is made at random and the validator is given the right to propose blocks. The agreement on the canonical blocks is made through a multi-round consensus where each validator votes for a specific block. At the end of this process, an agreement is reached between all validators on whether a block belongs to the chain or not.

## Advantages of proof of stake over proof of work:

Proof of stake provides an undeniable advantage over proof of work: the amount of electricity required to secure a block chain is reduced.

The cost of the Bitcoin and Ethereum mechanism is estimated at more than $1 million in electricity and computer equipment per day. The subject is therefore crucial for the future development of the blockchain.

(Voir Quid de ses impacts énergétiques)

Lower raw material consumption implies a lower need for motivation, and therefore a lower cost per transaction and better participation of the network.

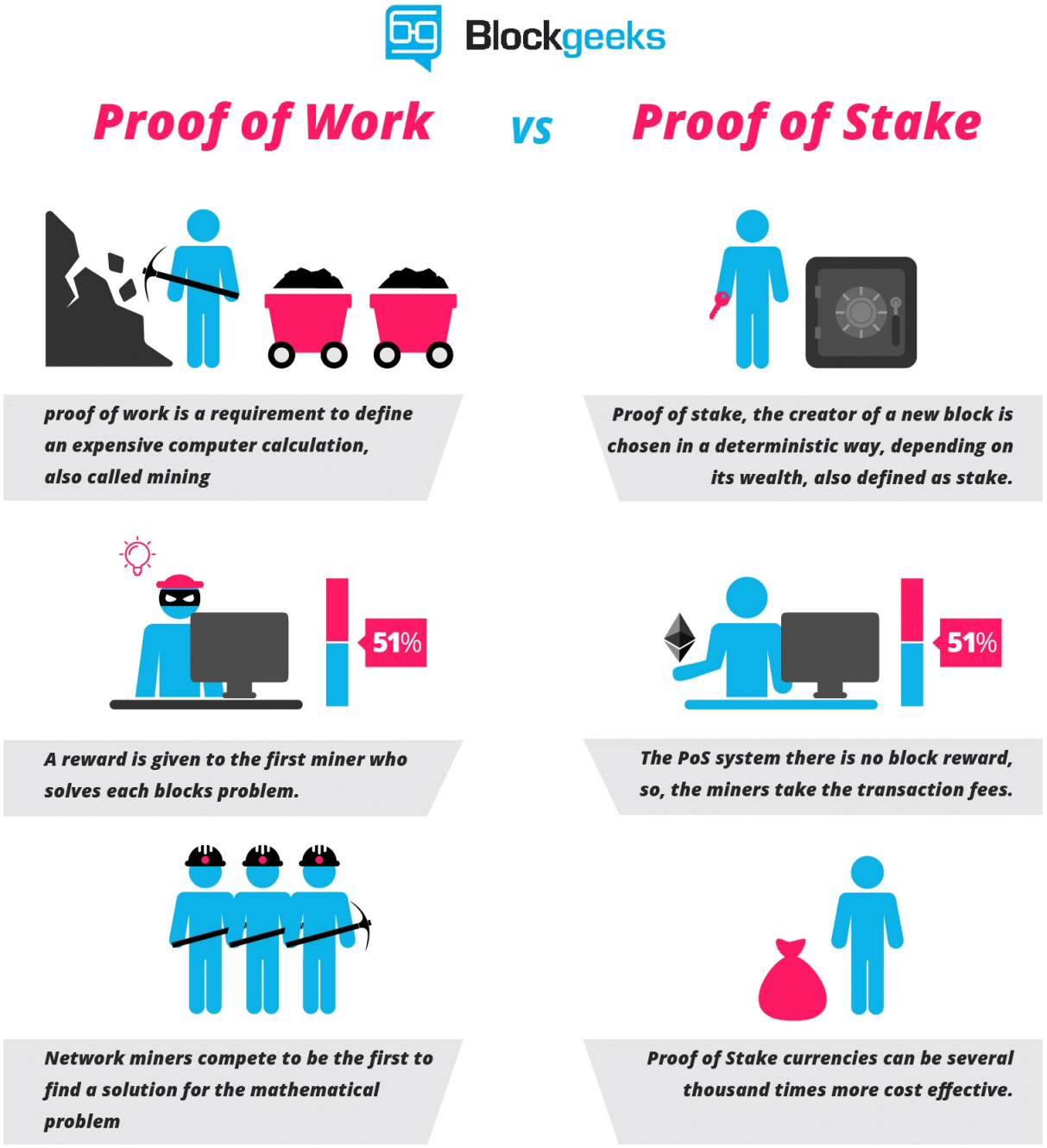
This opens the door to a better regulation of the abuses that can affect the blockchain, such as the phenomenon of the selfish miner or the activities of cartels trying to centralize the blockchain.

The proof of the stakes introduces a reduction in the risks of centralisation. Random selection of a validator limits the interest in developing large infrastructures and allows small actors to survive.

An additional benefit of using a proof-of-concept validation is the increase in the cost of a "51% attack" dramatically compared to the proof-of-work method. Thus the safety of the blockchain is reinforced.

> «taking part in a 51% attack is like burning your ASICS mining farm».
>
> Vlad Zamfir, Ethereum Foundation researcher

## Comparative computer graphics of the two methods:




The proof-of-investigation method offers undeniable advantages over methods currently in use, better safety, lower consumption and greater decentralization. Unfortunately, alternative validation methods are still in the development stage. The various problems of size and frequency of adding blocks, the purpose of mining and the concentration of mining capacity are challenges that developers will have to solve if these methods are to be considered as viable alternatives.

# Private blockchain vs. public blockchain

| | Public blockchain | Private blockchain |
|---|---|---|
|  Usage | Manage simple traces (hash). Beyond that is less relevant given its cost of data manipulation and its limitations in managing confidentiality. | Manage exchanges that are richer than just traces. The absence of transaction fees allows for a larger size of stored data. The management of access rights and confidentiality can be better controlled. |
|  Security | The more users, the more security is guaranteed. Generally, consensus is guaranteed by proof of work. | Only validator nodes are allowed to validate a transaction. A consensus of n% (e. g. 2/3) of the validating members is required. |
|  Confidentiality | The data flows in a transparent way. Unless disclosed, the holders of the addresses are anonymous. | Only authorized actors have access to transactions. |
|  Scalability | Between 3 and 7 transactions per second but one transaction can contain several thousand hashes. | 1,000 transactions per second or more. |
|  Accessibility | "Permisionless": like the Internet, accessible to all. | Access to consortium members only. |

> Comparison of private and public blockchain
>
> Julien Maldonato and Rémi Foult dans La Blockchain, panorama des technologies existantes.

# Identification management and confidentiality

On the Bitcoin and Ethereum blockchain (before 2017), the identification of a user can be discovered. It therefore does not ensure the confidentiality required for a secret ballot vote..

Indeed, the nature of the public block chain means that each transaction that takes place will be published and linked to a publication of a public cryptographic key. This key is encrypted so that a person looking at the history of the block chain would not be able to identify the actual identification of the individual behind this key.

This anonymity could be preserved if this public key were used only once. But if this key is used several times, it is possible to determine that the same individual is hiding behind this public key.

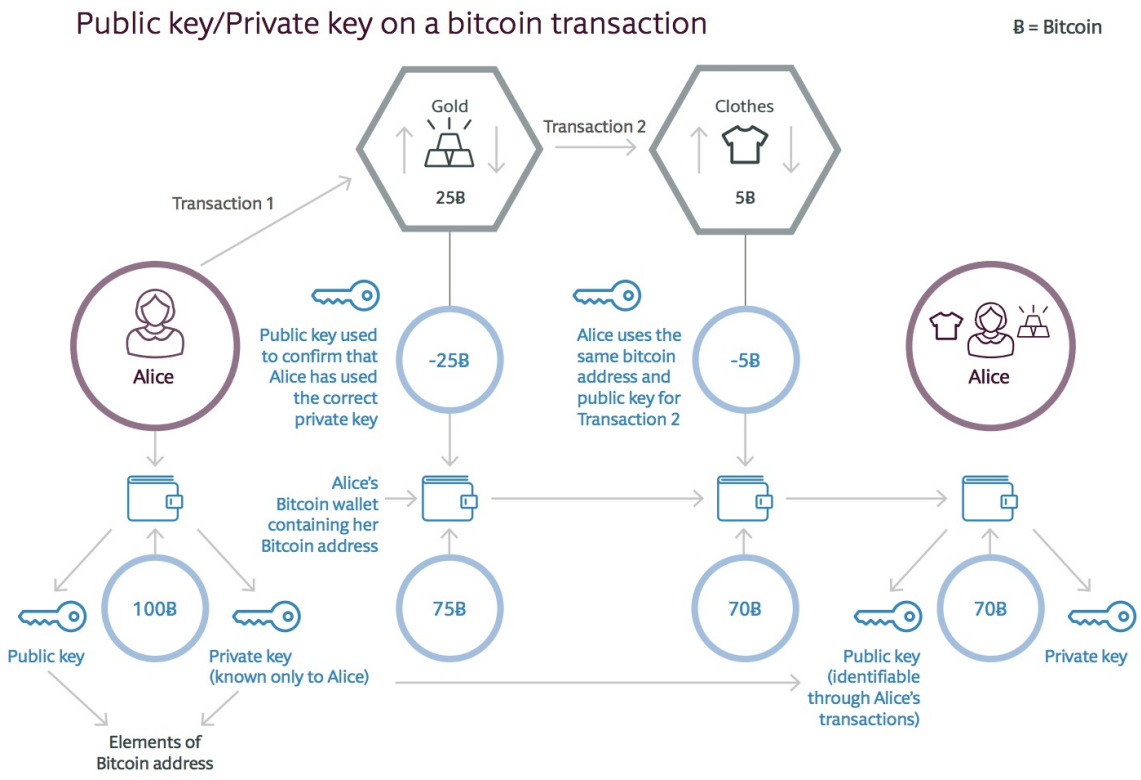



Diagram showing the possibility of linking a user to multiple transactions on the Bitcoin blockchain

Of course, the purpose of the public key is to distinguish one user from another on the network to ensure that the transaction is assigned to the right author.

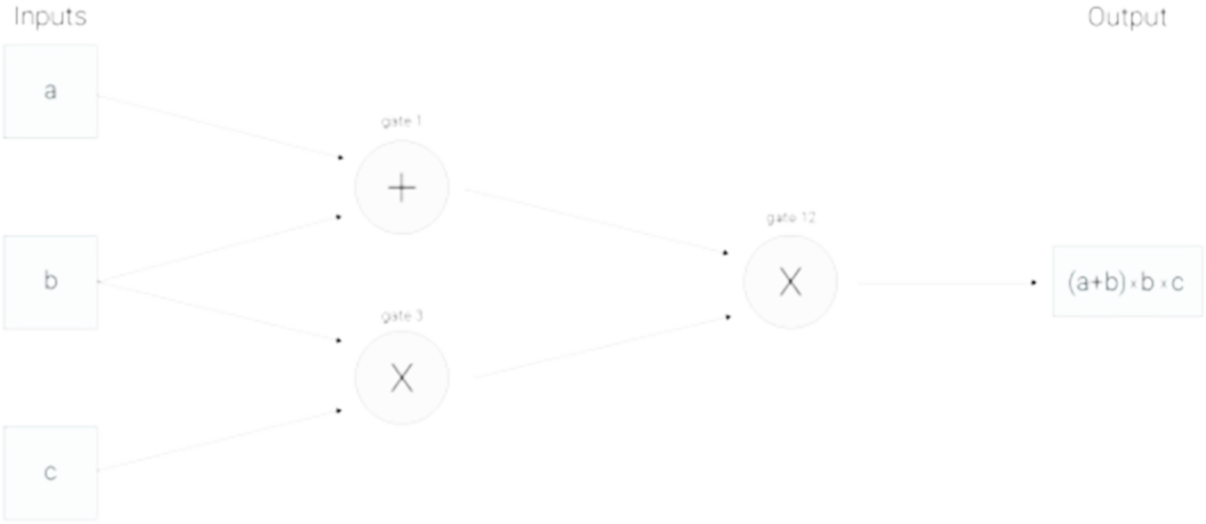
One solution to this problem is to use the Zero knowledge proof (ZKP) method of proof.

The most widespread form at present is zk-SNARKs (zero-knowledge Succinct Non-Interactive ARgument of Knowledge), native to Ethereum since the Metropolis (Byzantium Fork) update on 12 October 2017 and native to Zcash. Another form of ZKP is also found on the Monera blockchain, which implements a circle signing system: Monero Ring Confidential Transactions (RingCT).

In order to have "unconscious privacy" in Zcash, the function determining the validity of a transaction according to the network's consensus rules must return the answer on whether or not the transaction is valid, without revealing any information about the calculations performed on it. This is done by coding some of the network's consensus rules in

zk-SNARKs.

At a high level, zk-SNARKs work by first transforming what you want to prove into an equivalent form on the knowledge of a solution to certain algebraic equations.




> Demonstration of the arithmetic circuit for calculating (a+b)*(b*c) using zk-SNARKS
>
> Source: Zcash about zk-SNARKS

Looking at such a circuit, one can consider the input values a, b, c as "moving" from left to right on the wires to the output wire. The next step is to build what is called a Rank 1 Constraint System (R1CS) to verify that the values move "correctly". In this example, R1CS will confirm, for example, that the value that comes out of the multiplication gate where b and c are entered is b*c.

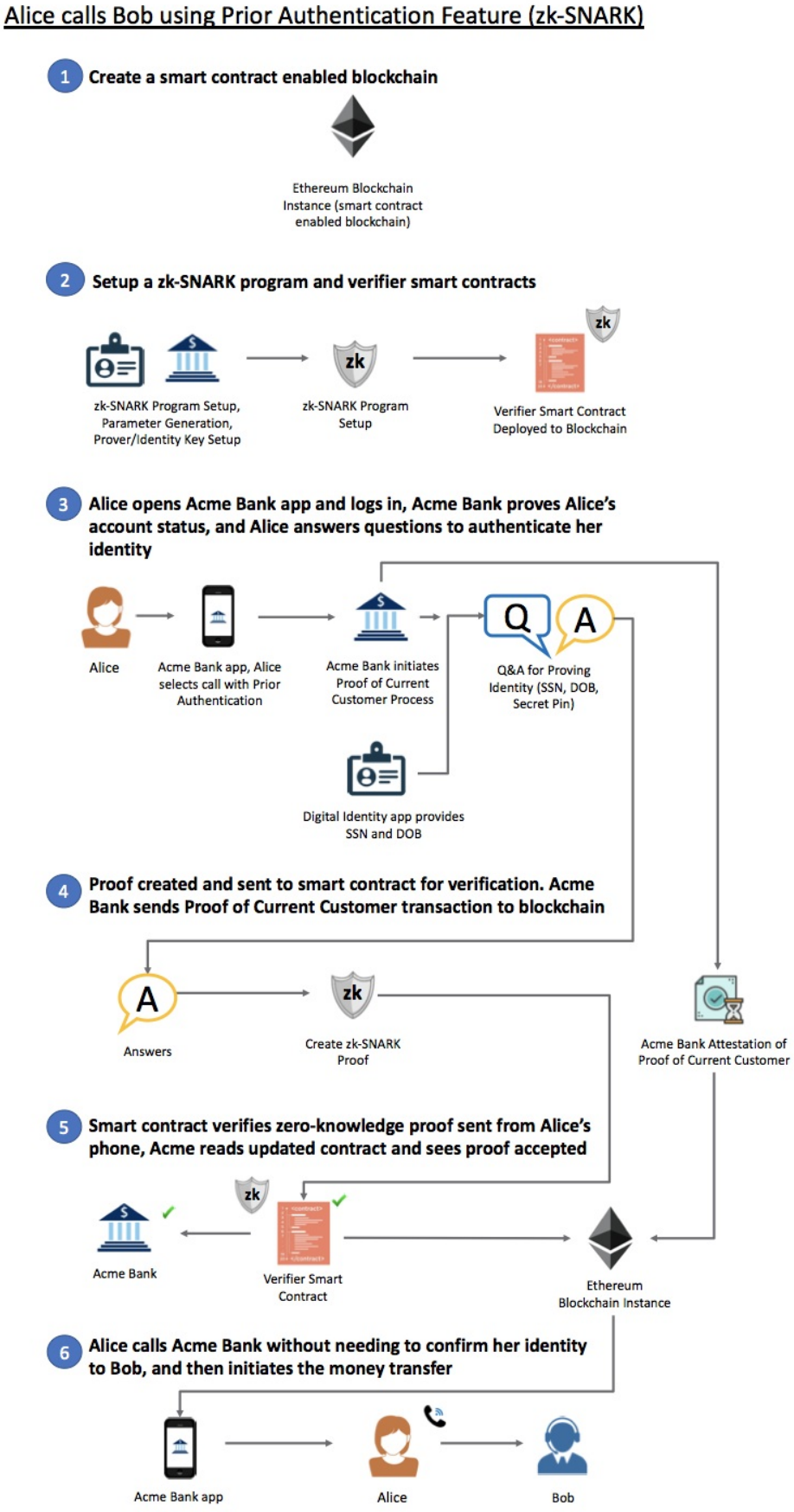
In this R1CS representation, the auditor must check many constraints - one for almost all the wires in the circuit. This method uses a representation of the circuit called the Quadratic Arithmetic Program (QAP). The only constraint that needs to be checked is now between polynomials rather than between numbers. Polynomials can be quite large, but that's okay, because when an identity doesn't hold between polynomials, it won't hold on to most points. Therefore, it is sufficient to verify that the two polynomials correspond to a randomly selected point in order to correctly verify the proof with a high probability.

In concrete terms, this means that it is possible to obtain a transaction without sharing information.

To better understand how zk-SNARKS works in practice, let's look at an example of "how Alice can transfer money from one of her bank accounts to another, without providing Bob at Acme Bank with information to guarantee her identity".

For this scenario, we will need four entities:

- Alice - an individual who wishes to prove his identity without transmitting it
- Acme Bank - Trusted third party for bank account attestations, and a trusted third party for the installation of zk-SNARK.
- Bob - Acme Bank Call Centre Representative
- Self-Sovereign Identity Solution - Provider of digital identity data to Acme Bank App, and a trusted third party for the installation of zk-SNARK.


Alice calls Bob using Prior Authentication Feature (zk-SNARK)
1 Create a smart contract enabled blockchain
Ethereum Blockchain Instance (smart contract enabled blockchain)
2 Setup a zk-SNARK program and verifier smart contracts
zk-SNARK Program Setup, Parameter Generation, Prover/Identity Key Setup
zk-SNARK Program Setup
Verifier Smart Contract Deployed to Blockchain
3 Alice opens Acme Bank app and logs in, Acme Bank proves Alice's account status, and Alice answers questions to authenticate her identity
Alice
Acme Bank app, Alice selects call with Prior Authentication
Acme Bank initiates Proof of Current Customer Process
Q&A for Proving Identity (SSN, DOB, Secret Pin)
Digital Identity app provides SSN and DOB
4 Proof created and sent to smart contract for verification. Acme Bank sends Proof of Current Customer transaction to blockchain
Answers
Create zk-SNARK Proof
Acme Bank Attestation of Proof of Current Customer
5 Smart contract verifies zero-knowledge proof sent from Alice's phone, Acme reads updated contract and sees proof accepted
Acme Bank
Verifier Smart Contract
Ethereum Blockchain Instance
6 Alice calls Acme Bank without needing to confirm her identity to Bob, and then initiates the money transfer
Acme Bank app
Alice
Bob

To perform this authentication operation, it is necessary to use a third party "ACME BANK": this third party will authenticate Alice using a third party application and return the true value if Alice is the person she claims to be.

> The advantage of this system is that neither the Bank nor Bob has Alice's identifying information, nor does the third party have any idea of the nature of the transaction between the Bank and Alice. There is therefore a perfect separation between the operations performed and authentication.

# What about the blockchain security?

## The blockchain's security guarantees:

There is no safe technology as safety and security are an ideal, not an absolute. But it is possible to approach this ideal, and we can consider that the blockchain meets these requirements insofar as it ensures the following points:

- Availability: As data is distributed and decentralized, it is available as long as a node is able to transmit the register.
- Integrity: the consensus mechanism is designed to allow information to be integrated and retained without altering it. The prerequisite for this provision is that a sufficient number of nodes are connected to the network and that the conditions for a 51% attack are not met.
- Confidentiality: Confidentiality is a complex issue regarding the blockchain since the data are publicly available to ensure transparency.

  Nevertheless, this confidentiality can be made possible by the implementation of a system of proof with zero disclosure of knowledge. Knowledgeless protocols allow the transfer of resources through a distributed network, peer-to-peer blockchain, in complete confidentiality. In regular block chain transactions, when an asset is sent from one party to another, the details of that transaction are visible to all other parties in the network. In an unconscious transaction, however, the other parties do not know that a valid transaction has occurred, but no information on the sender, recipient, asset class and quantity is disclosed. Voir Gestion de l'identification et confidentialité
- Traceability: Because it is based on a stack of cryptographic blocks, the blockchain makes it possible to record all transactions and go back to block zero, ensuring the best traceability.
- Authentication: To ensure the correct identity of a transaction, the issuer signs it with his private key, which "until it is known, ensures the veracity of the transaction".
- Non-repudiation and imputation: Through consensus-based validation, the blockchain natively allows data non-repudiation. As for imputation, each minor certifying a transaction is authenticated on the network, so it is possible to identify and disqualify an offending minor.

## Security threats threatening the blockchain:

According to Patricia Egger and Dusko Karaklajic in The Security of the Blockchain, threats to the emerging ecosystem are posed by the immaturity and complexity of the technology.

Indeed, the many consensus algorithms available, the blockchain types and the underlying complex cryptographic protocols make the technology difficult to understand.

The lack of standards and regulations on blockchain technology is also a risk. These legal loopholes are fertile ground for piracy and fraudulent manipulation, making technology still unreliable for serious use.

The most important risk remains the belief in absolute security around the blockchain although it is based on reliable and proven cryptographic mechanisms. This security will never be complete by nature: cryptographic protocols have their limits and global security also integrates peripheral elements, so the human risk is always present. In this last point, the blockchain provides a new way of processing certain data but does not free us from the traditional approaches to information system security.

In addition, the blockchain is sensitive to particular attacks, such as the Golfinger attack.

## 51% attack or Goldfinger attack

A 51% attack targets blockchains based on proof of work and proof of stake.

The purpose of this attack is to prevent transaction validations and paralyze the network, or to manipulate the history to validate a transaction twice without the expense being effective.

The validation of blockchains is done through mining.

In order to guarantee themselves remuneration within the framework of a blockchain operating under the proof of work method, miners are formed in groups (or pools), in order to have more power and to pool costs. They then share the effort and the gains.

But the danger of a group with too much power is that it can make a 51% attack.

Indeed, one of the founding principles of the blockchain is that the calculation is distributed among all the nodes where the calculation is validated by the consensus method. Thus if a single individual introduces a miscalculation voluntarily or falsifiedly, the other miners will automatically disqualify his work and his block will remain orphaned and will never be integrated. Thus alone, he cannot harm.

> When a group of minors has at least 51% of the calculation capacities, it becomes possible in theory to bypass the consensus mechanism and thus to impose fallacious blocks that will be added to the official register. So if a group becomes too powerful, it is able to define what information is legitimate within a blockchain.

'Double spending' example.

Assuming that a group has more than 51% of the total power, it can then fraudulently manipulate the registry called the double expense hack.

This hack consists of making transactions between two accounts. He debits from the first account to the second, and with the power to manipulate the blockchain, erases the transaction. To do this, do not include the transaction in the mined blocks, and wait until a blockchain longer than the current blockchain replaces it.

Once the transaction has been deleted from the distributed registry, the second account appears as never having been debited as long as the second account has received the sum. It is a creation of ex-nihilo currency of crypto-currency units.

Such an operation will quickly lead to a drop in the price of cryptomonnaise. The group carrying out fraudulent activities will then have to quickly convert its assets into a current currency such as the euro or the dollar, which will accelerate the fall in the price.

The operation is facilitated by automated means.

This attack is unthinkable on well-established blockchains such as Bitcoin, because of the cost of such an operation, at least such an approach is inaccessible to a private company, but not to a rogue state, which has the necessary budgets and may have as its motivation to disrupt a competing blockchain or causing disorder.

On the other hand, on blockchains with a low mining capacity (recent or small), this attack is easily possible.

In the latter case, a low computing power, which could be available to an average organization, would be sufficient to carry out the attack.

> The newly created blockchains are therefore in an extremely vulnerable position.

51% attack objectives

- Fraudulent records and disappearance of transactions:

  In the context of a private blockchain, for example allowing the implementation of the vote or allowing food traceability, this would make it possible to falsify the information.

  In the case of a cryptomonnaise, this allows for double spending, which both enriches and destabilizes the exchange rate.

- Breaking the bond of trust:

  Because of their decentralized operation, blockchains pose governance problems and are perceived as a threat by certain states or institutions. This is why disrupting the operation of these blockchains can alienate the trust of users towards the blockchain.

Resilience of blockchains to attack

The cryptocurrency system is designed to be resilient to 51% attacks, when such an attack is detected. A patch can be deployed and limits the damage caused by the attack.

Estimated costs of a 51% attack

The costs to carry out a 51% attack vary according to the scale of the blockchain targeted.

*Concerning Bitcoin, various estimates were made by Jean-Paul Delahaye in L'attaque Goldfinger d'une blockchain.*

Based on his calculations, the cost in May 2017 can be estimated at 878 million dollars.

In comparison, the budget of the French State is 400 billion euros per year, that of a government agency such as the NSA is 45 billion dollars.

The attack is therefore inaccessible to a normal institution.

## Selfish miner strategy

*The example of the selfish minor is explained in Les risques des blockchains, by Laurent Dehouck, Senior Lecturer in Management Sciences, ENS Rennes and Audrey Thomas, ENSAM.*

When a transaction takes place, the minor who discovers the solution first has a Be block.

This block is supposed to be communicated to the other nodes in order to be integrated into the blockchain.

But this dishonest minor can keep this block secret and work immediately on the validation of the next block.

As soon as another "honest" miner validates a Bh block, he wants to broadcast it to the other nodes.

The dishonest minor will then broadcast his Be block. The network is thus in the presence of two blocks validated almost at the same time and temporarily stored on the blockchain.

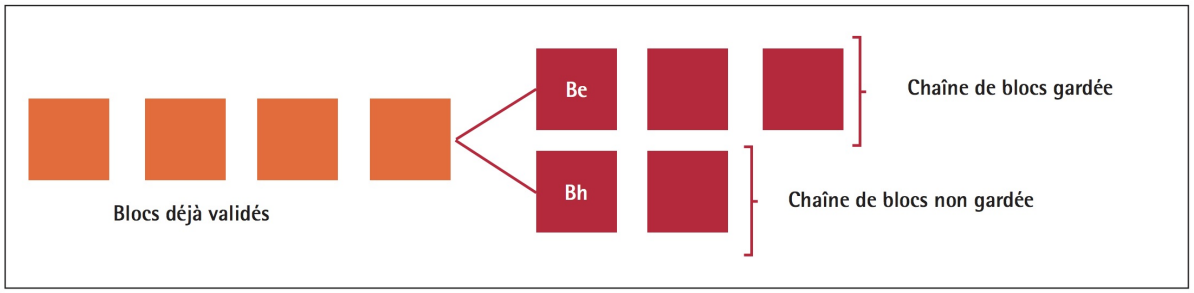
Some nodes in the network will be aware of the Be block and others will be aware of the Bh block.

New blocks will then be added following Be and Bh.

For the dishonest minor, the advantage remains in the act of not disclosing the Be block. This gives it a strategic advantage over the rest of the network users in the search for the next solution, because each validated block is linked to the previous blocks.

The simultaneous creation of two blocks causes what is called a "bifurcation", so the containing chain will be preserved because the chain containing the Be block will be longer.

The dishonest miner disqualifies his competitors by making them work at a loss, their yields quickly collapsing.




Source : d'après J. Göbel *et al.*, « Bitcoin Blockchain Dynamics: The Selfish-Mine Strategy in the Presence of Propagation Delay », *Performance Evaluation*, n° 104, 2016, p. 23-41.

Illustration d'une bifurcation

This type of strategy invites us to rethink the question of blockchain standardization and consensus techniques to protect against these harmful practices.

# What about its energy impacts?

Selon un rapport de l'Office parlementaire d'évaluation des choix scientifiques, Bitcoin consumption is at least 24 TWh/year, i.e. the total annual production of 3 CP0 and CPY nuclear reactors (the oldest in France) with a production of around 8 TWh.

The cost of public blockchains (including Bitcoin) is estimated to be 46.5 TWh/year and 200 TWh/year.

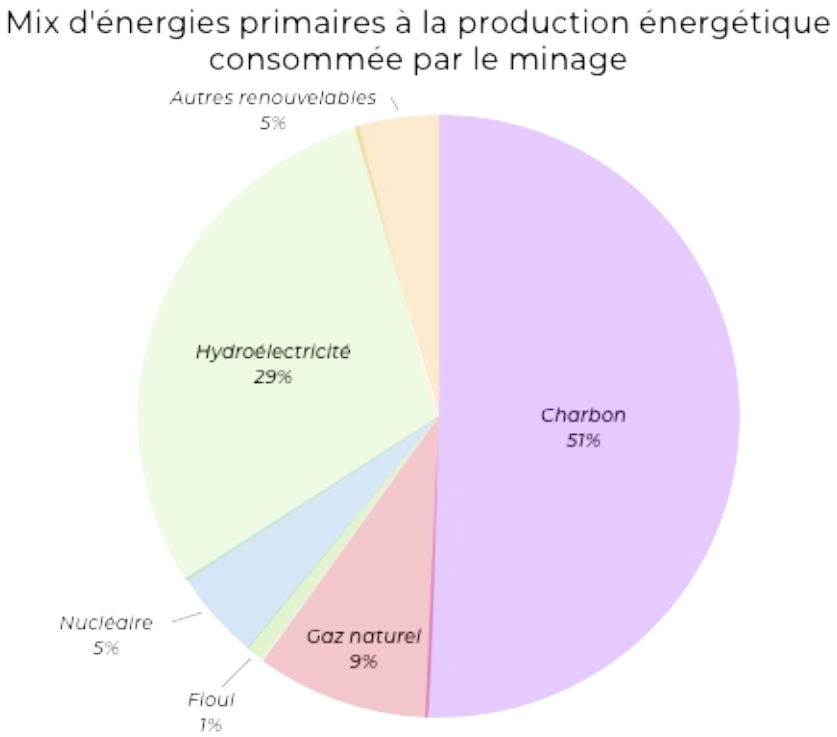
In comparison, France's annual energy consumption is 530 TWh/year. The blockchain would therefore represent between 8.68% and 37.74% of French energy expenditure if mining farms were exclusively located on French soil. However, 60% of mining farms are located in China, where most of the energy production comes from coal. This is a major ecological problem that is causing considerable damage to the development of Blockchain technology.

In addition, Bitcoin currently operates about 80 transactions per minute, while Visa and Mastercard execute nearly 100,000 transactions per minute. This energy cost is therefore staggering when compared to other centralized alternatives. This comparison is all the more shocking when the majority of resources are wasted during the process of checking invalid blocks.

These figures should be handled with caution because the estimate of the energy consumption of blockchains is not reliable, as the equipment is constantly evolving and miners are careful not to communicate their electricity consumption.

In Iceland, Genesis Mining reported in Business Insider in 2015 that it was one of the most energy-intensive companies on the island, with an electricity expenditure of around $60 per "extracted" bitcoin. That is, at the current Bitcoin price, a remuneration of $6243.99 per Bitcoin extracted.

The energy mix of Bitcoin production reveals a massive use of fossil fuels. But also Hydroelectric, renewable.




Source: Energie Sia Partners

# Towards standardization?

> 10% of the world's GDP in 2025 will come from activities using the blockchain.
>
> Ravi Jhawar, project manager within the Anec GIE (economic interest group)

## Regulation through standardization

Luxembourg, through the Ilnas, is participating in the creation of an international technical standard to regulate the blockchain.

Dans un livre blanc, the organization hopes to initiate a process and establish itself as a regulatory actor through an ISO standard.

The objective is to provide a framework for blockchain governance in order to influence the economic and ecological issues that concern it.

This standardization is confronted with the desire for independence and decentralization, the founding foundation of Blockchain technologies.

Nevertheless, the implementation of a standard may imply better energy regulation by imposing, for example, the renewable origin of the electricity needed for the technology to operate.

## Standardization to fight against consumption and obsolescence of means of production.

The field for reducing the blockchain's energy consumption can be seen when we talk about standardization or normalization.

These are the standardization of algorithms and the standardization of multi-purpose hardware.

These two optimization directions are in fact only one and the same way: an algorithmic standard means an adapted dedicated hardware, and therefore a more important optimization because the Research & Development investments would be focused on a single type of hardware.

The blockchains running on the work proof method have in common the use of a hash algorithm. The one in Bitcoin is called Hashcash.

By seeking a more economical algorithm to perform this function, the blockchain could see its ecological cost reduced and present itself as a viable alternative on a large scale.

In order to undermine, individuals or institutions provide equipment to perform calculations.

On some blockchains, such as Bitcoin, it is useless and unprofitable to try it with conventional equipment.

This method of calculation is reserved for more recent blockchains or those with less enthusiasm.

Professional miners use high-performance equipment, which excludes amateur miners from the pay race, as part of proof of work only. They are indeed far too slow to validate the transactions against these sprinters.

Mining is divided into two technologies, dedicated chips: FPGA / ASICS and generalist chips CPU / GPU.

Acronyms explanation:

| Acronyme | Explication |
| --- | --- |
| | |

| | |
|---|---|
| CPU | *Central processing unit* ( Unité centrale de traitement ) |
| GPU | *Graphics Processing Unit* ( Processeur graphique ) |
| ASICS | *Application Specific Integrated Circuit* ( Circuit intégré spécifique à l'application ) |
| FPGA | *Field-Programmable Gate Array* ( Réseau de portes programmables in situ ) |

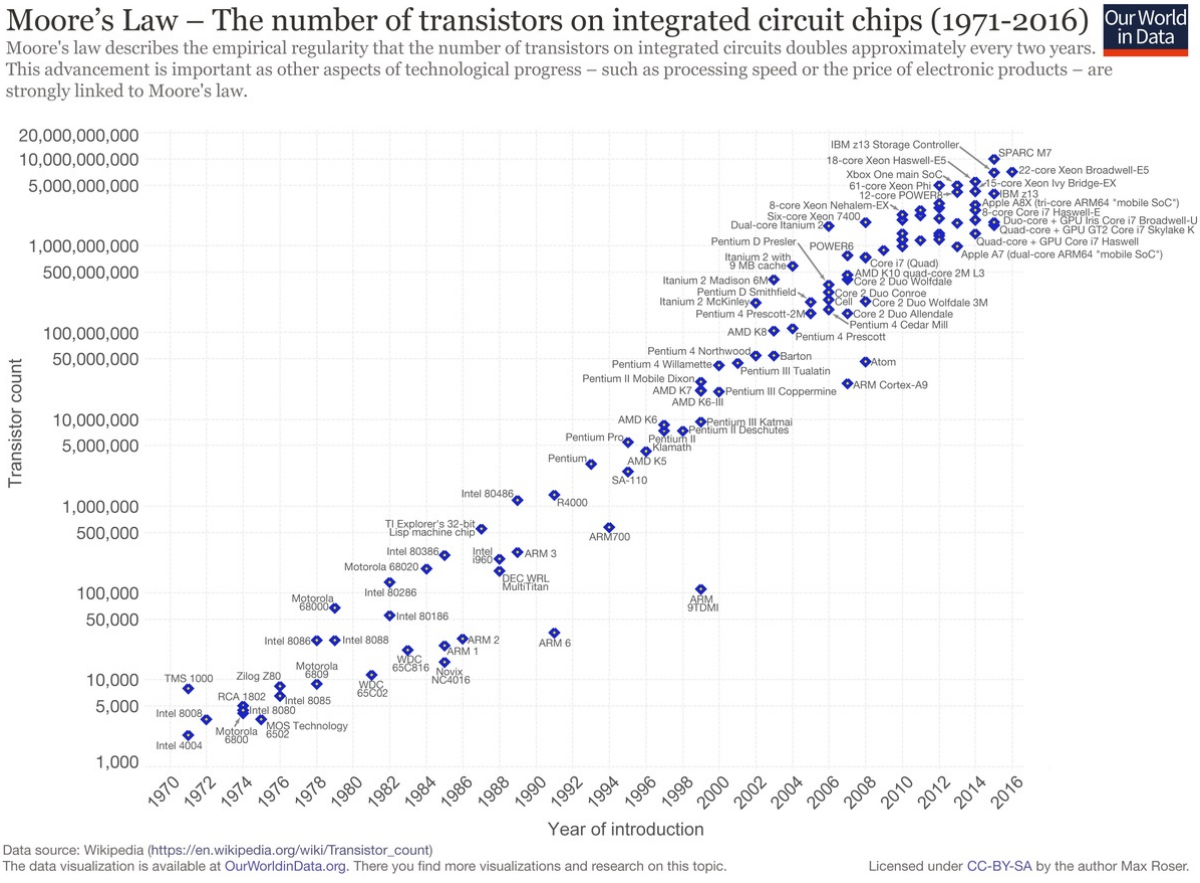
The former are only used in cryptographic calculation as part of the blockchain, the latter are used in everyday operations.

ASICS AND FPGA miners are mainly used in the SHA256 (Bitcoin) calculation, while CPU / GPU are used on more recent cryptometers.

In order to maintain the complexity of calculation within a blockchain, the difficulty must increase as technology advances.

When we look at the capabilities of computation chips, we see a significant increase in their power. Thus, performing a cryptographic calculation considered complex in the 1980s takes a few seconds with a current mobile phone.

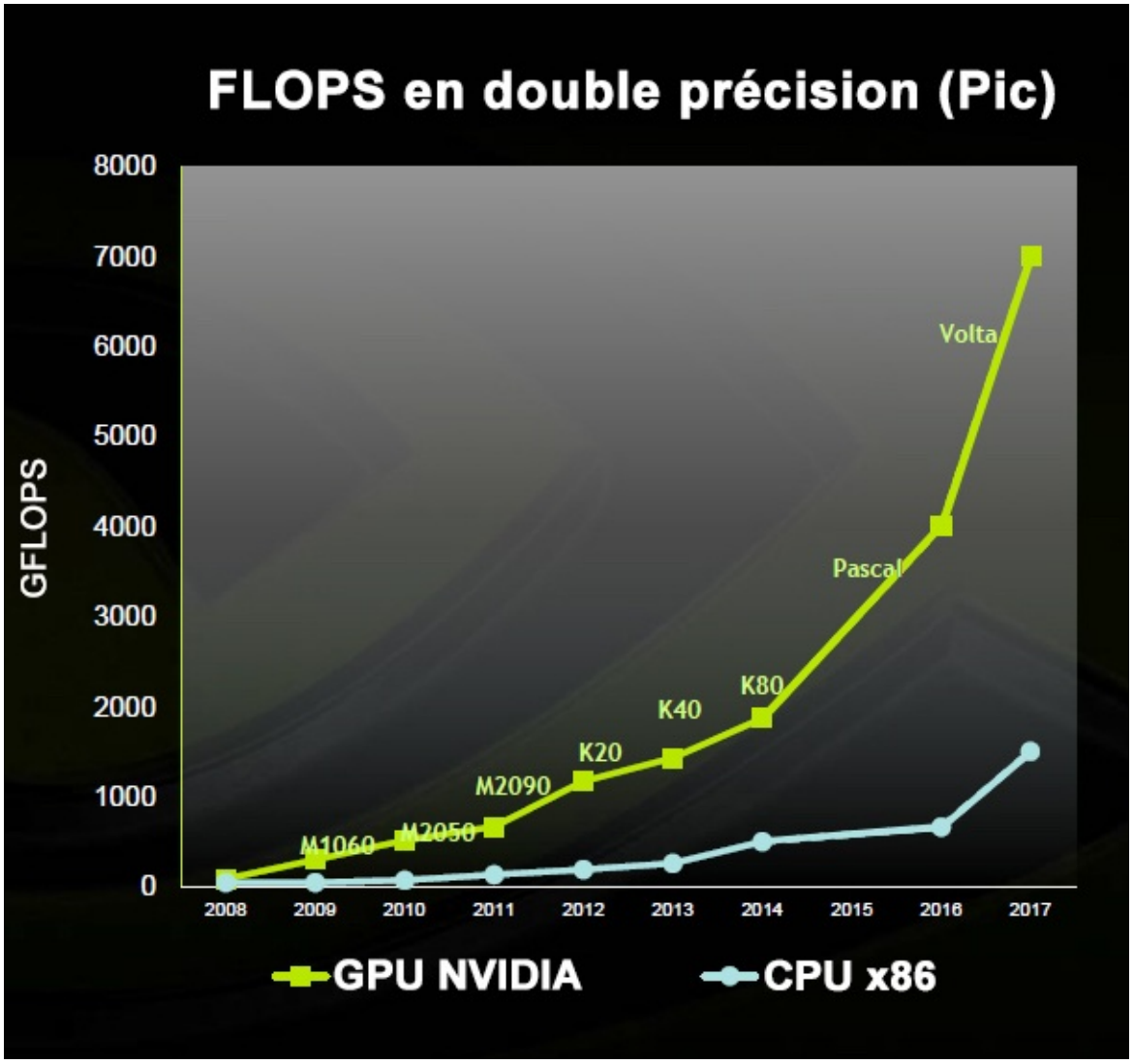
This diagram shows the increase in computing power of CPU chips.




>

> Evolution of computer computing power and hardware complexity according to Moore's assumptions

When we compare the increase in computing power of GPUs compared to CPUs, we can easily imagine the increase in complexity that algorithms have undergone.



>

> Comparison between the number of floating point operations per second (FLOPS) of CPUs (X86 architecture) and NVIDIA GPUs

On the latter illustration, we can see that the computing power of GPUs on some transactions is spectacularly higher than CPUs, yet, in the context of the blockchain, ASICS AND FPGA miners are much more efficient than GPUs.

Other constraints are also based on the choice of hardware, which is why some algorithms requiring a large amount of memory use made ASICS minors uncompetitive because memory components are particularly expensive.

But 2017 marked a turning point in the use of these cards with a substantial improvement in these memory modules. The solution to maintain complexity was to modify the algorithms, making the hardware obsolete because the functions of an ASICS miner are engraved on the silicon. This is referred to as wired functions.

These wired functions are found in other chip architectures, such as GPUs.

An important economic and ecological cost to guarantee the safety and scalability of these blockchains.

To understand why chips are rendered obsolete, it must be understood that the difference between a CPU and an ASIC (or between a CPU and a GPU) lies in the fact that the CPU is a programmable chip, and has great versatility in its use at the price of lower performance.

A GPU or ASIC is a specialized chip, whose performance is excellent in performing the tasks for which it is programmed, but which are fewer in number than for a CPU.

For example, for a GPU specialized in graphic representation, the display of a textured 3D mesh at 60-100 frames per second.

This performance allows for better gross calculation performance on these precise tasks, but also lower power consumption.

This improvement in performance is made possible by engraving directly into the silicon of the chip the functions necessary for translation, rotation, etc. This is called "wiring" the functions.

For an ASIC minor, this specialization will result in an unbeatable performance in the resolution of an encryption algorithm for example. But it is not possible to use an ASIC specialized in the calculation of SHA256 hashes for KECCAK and vice versa.

In these trends, an intermediate solution has emerged that exploits the best of both worlds: the FPGA.

## FPGA.

FPGAs (Field-Programmable Gate Arrays) are reprogrammable silicon integrated circuits.

Reprogramming an FPGA is about redefining the integrated circuit itself to implement the desired functionality, rather than running a software application.

The FPGA can be seen as a chip that simulates a specialized chip at the lowest level.

FPGAs are particularly used to simulate an ASIC miner in the pre-production phase to test the model and adjust logical schemas. When the operation is considered sufficient, the schematic is then frozen to produce an ASIC minor.

FPGA miners offer slightly lower performance than ASICS miners. It is also noted that the programming logic of an fpga requires advanced and uncommon skills.

Despite these disadvantages, FPGA boards with titanic computing capabilities are being developed to meet the needs of machine learning and deep learning.

These cards make it possible to envisage a continuity of future use despite forks and changes in algorithms, which makes it possible to limit costs and limit the ecological impact due to the obsolescence of the equipment.

Standardization through the cabling of functions

To understand how cards dedicated to the blockchain could emerge, it is necessary to go back in time in the history of computing. Originally, only CPUs performed calculations related to 3D. Then came the GPUs, whose wired functions allowed for greater performance. It is quite possible to cable the functions necessary for the algorithms implemented in the blockchain, in the same way as the Physics Processing Unit, which implemented an additional card for physics management and which are now integrated into Nvidia graphics cards.

> At present, blockchains are optimized according to the available equipment, they adapt to equipment that is only slightly optimized for this use. This optimization could be done using function cabling, but for this to happen, manufacturers must be able to anticipate the future of the blockchain in order to predict long-term gains.
>
> Today, these are evolving rapidly and many implementations are diverging, all of which push back the hardware optimization step.
>
> This step could be facilitated by the standardization of blockchains.

# Blockchain limits

There are perilous passes in any technological revolution. Some in the blockchain industry have pointed out that the block chain has become oversized, when in reality, the technology has its limitations and is inappropriate for many digital interactions. But through research and development, successes and failures, trial and error, we know what the current problems and limitations of blockchains are.

## Complexity

Blockchain technology involves an entirely new vocabulary. It has made cryptography more common, but highly specialized industry uses a specific vocabulary (some would say jargon). Fortunately, several efforts are being made to provide comprehensive and easy-to-understand glossaries and indexes.

## Taille du réseau

Blocking chains (like all distributed systems) are not so much resistant to the wrong actors as they are "antifragile", i.e. they resist attacks and become stronger. However, this requires a large network of users. If a block chain is not a robust network with a grid of widely distributed nodes, it becomes more difficult to take full advantage of it. There is a discussion and debate on whether this is a fatal flaw for some projects in the chain of authorized blocks.

## Transaction costs and network speed

Bitcoin currently has significant transaction costs after being presented as "almost free" in the early years of its existence. By the end of 2016, it can only process about seven transactions per second and each transaction costs about $0.20 and can only store 80 bytes of data. There is also the politically sensitive aspect of using the bitcoin block chain, not for transactions, but as a store of information. This is the issue of "swelling", often misunderstood because it forces minors to constantly reprocess and re-register information.

## Human error

If a block string is used as a database, the information entered must be of high quality. The data stored on a block chain is not inherently reliable, so events must first be accurately recorded. The expression "garbage can at the entrance, garbage can at the exit" is true in a chain block recording system, just like in a centralized database.

## An unavoidable safety defect

There is a significant security gap in bitcoin and other blocking chains: if more than half of the computers used as nodes to maintain the network lie, the lie will become the truth. This is called a "51% attack" and Satoshi Nakamoto pointed this out when he launched Bitcoin.

(Voir Quid de la sécurité de la blockchain)

For this reason, bitcoin mining deposits are closely monitored by the community, ensuring that no one unknowingly obtains such influence from the network.

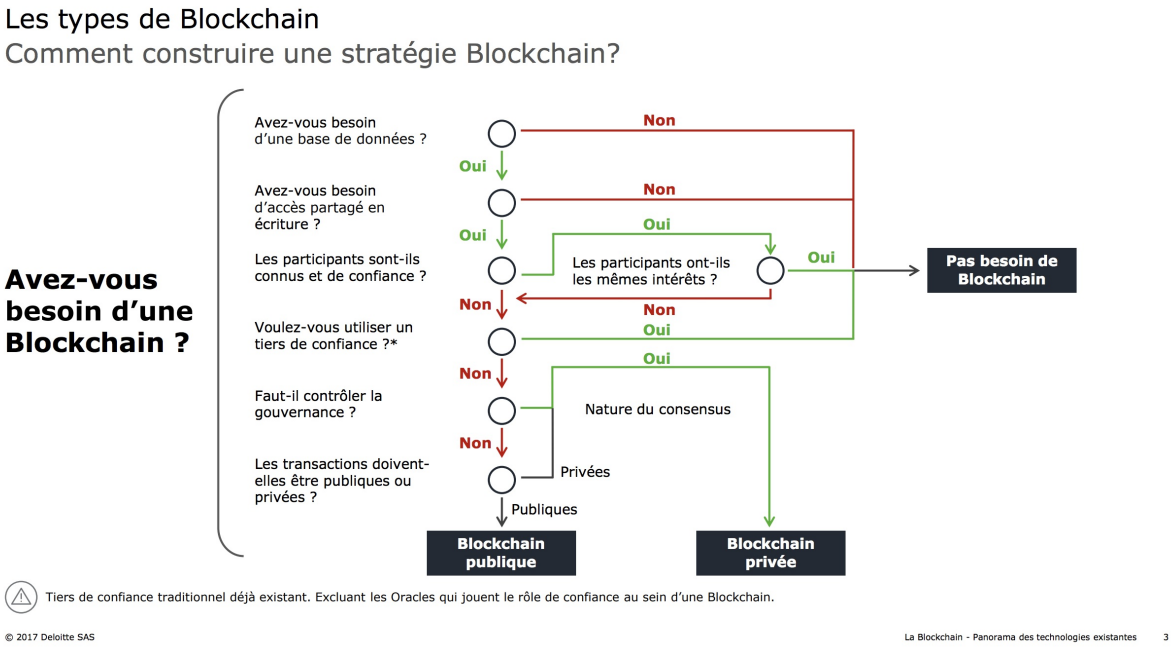
## Politics

Because the protocols of the block chain offer the possibility of digitizing governance models, and because miners are essentially another type of incentive governance model, there have been many opportunities for public disagreements between different community sectors. These disagreements are a notable feature of the block chain industry and are

most clearly expressed around the issue or event of "forking" a block chain, a process that involves updating the block chain protocol when a majority of users of a block chain have accepted it. These debates can be very technical and sometimes exciting, but they are instructive for those interested in the mix of democracy, consensus and new opportunities for experimentation with governance that blocking chain technology opens up.

## In which case should you equip yourself with a blockchain?

A flowchart to assist in the decision to set up a blockchain is proposed by *Julien Maldonato et Rémi Foult in La Blockchain, panorama des technologies existantes*.




> Avez-vous besoin d'une blockchain ?
>
> Julien Maldonato et Rémi Foult, La Blockchain, panorama des technologies existantes

Regarding the question of collective decision-making through voting, these limitations show that blockchain will not be the providential answer and invite to measure the opportunity comparatively of other proven methods.

# C. Use cases

The blockchain is therefore a distributed registry in which information is stored in blocks and validated by different cryptographic and consensus methods. The two main uses of the blockchain are financial transactions and smart-contracting. The latter allow to correlate a collective decision making, based on the vote to execute predefined actions. The use of blockchain raises the legitimate question of energy consumption and environmental impact, so we have addressed the opportunity of standardization as a potential answer to this question. Blockchain technology is not the universal answer, it has limitations and will only be recommended in specific cases.

## 1. Gouvernance des entreprises

## 2. Management collaboratif de projet

## 3. Démocratie participative

## 4. Vie associative et gestion des collectivitées.

# Gouvernance des entreprises

La blockchain propose un modèle de gouvernance des entreprises avec preuves, traçabilité et transparence. Certaines organisations s'appuient déjà sur cette technologie, c'est le cas des DAOs.

## DAO

Une DAO (Decentralized Autonomous Organization) est une organisation décentralisée s'appuyant sur la blockchain pour fonctionner. Les membres font l'acquisition de jetons (tokens) pour participer à des votes sur diverses décisions qui s'incarneront sous la forme de smart-contracts. Les règles la régissant sont inscrites au préalable dans cette même blockchain.

Cela rejoint le principe de loi par le code (law by code).

L'intérêt de cette méthode est de disposer d'une preuve immuable.

> C'est une forme d'organisation incorruptible qui appartient aux personnes qui ont aidé à la créer et à la financer, et dont les règles sont publiques. Il n'y a donc pas besoin de faire confiance à qui que ce soit, car tout est dans le code, auditable par chacun.
>
> Stephan Tual, TheDAO

Les DAOs utilisent la technologie des smart-contracts (voir smart-contract) pour fonctionner.

## Quels sont les éléments apportés par une DAO?

Selon Simon de la Rouviere, blockchain Consensys: il existe trois éléments fondamentaux apportés par une DAO. Le premier est que la DAO est inarrêtable, elle ne peut ni être fermée ni stoppée. Le second est que l'entité est forcée de faire acte de transparence et l'intégrité de ses données sont préservée, ainsi un individu ne peut prétendre à la manipuler ou la contrôler. Le dernier, et non pas des moindres, est le caractère auditable à l'échelle supranationale. En effet, lors du contrôle d'une entité, les auditeurs s'appuient soit sur des organes de contrôle du pays de résidence, soit sur des auditeurs indépendants. Parfois il est impossible d'effectuer ces contrôles librement ou sans crainte d'une fraude.

La DAO apparaît comme une organisation ouverte, globale, indépendante de toute juridiction et protégée d'une partie des fraudes qui agitent les organisations classiques grâce à l'application de la Loi par le code.

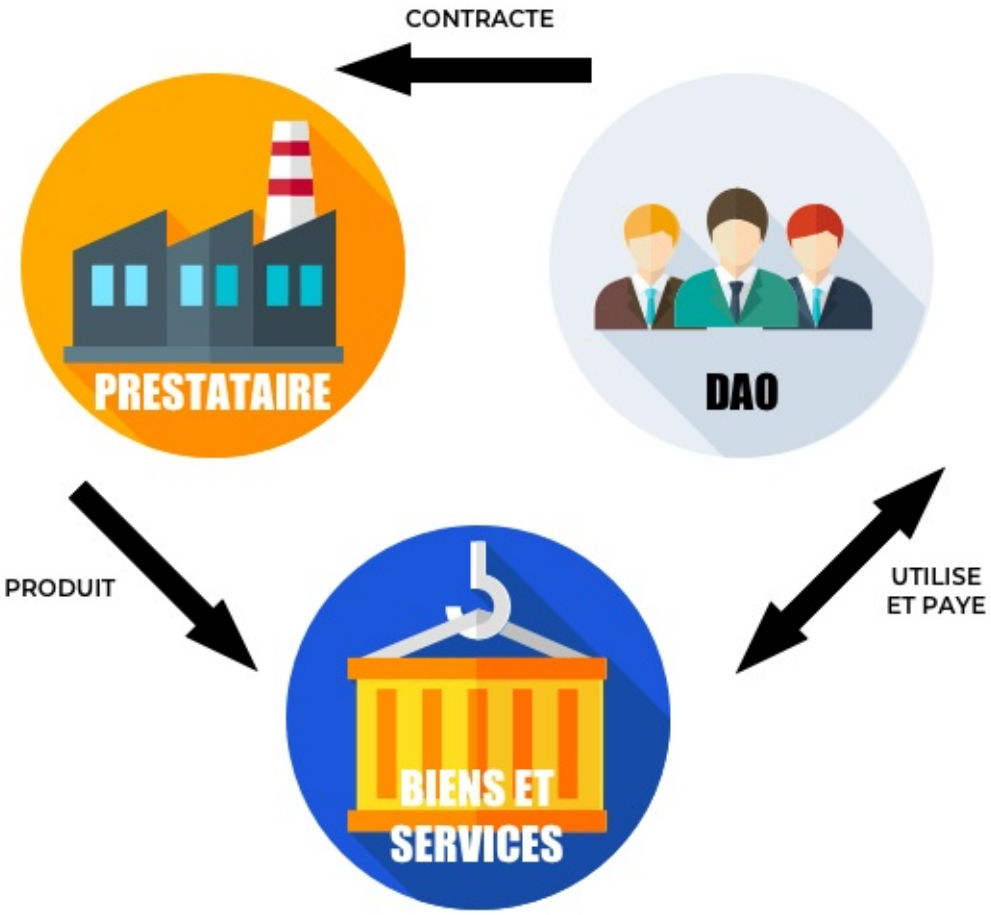
## TheDAO

Le projet TheDAO est à l'initiative de la start-up slock.it et est l'exemple le plus remarquable de ce genre d'organisation. C'est avant tout une réalisation expérimentale concrète, illustrant la faisabilité d'un tel système ( POC ).

Le type d'organisation DAO n'est pas adapté à la totalité des situations, mais elle répond concrètement à une situation où la confiance n'est pas nécessaire puisque le fonctionnement de l'organisation est garanti. TheDAO s'appuit pour fonctionner sur la blockchain Ethereum.

Les trois actions possibles à l'intérieur de TheDAO était premièrement l'évaluations des projects, deuxièmement la décision collective et troisièmement la distribution des risques et rémunérations relatives.

Ce projet se situait à la frontière du crowdfunding, de la fondation et du fonds d'investissement.




> Un schéma d'illustration d'une DAO

TheDao et le vote

Afin de participer au vote sur la plateforme TheDAO, il fallait au préalable avoir fait l'acquisition de jetons (tokens) et en faire l'échange contre un vote.

Il s'agit donc d'une transaction conventionnelle.

Le votant se verra alors retribué si sa proposition est financée.

Fin du projet

En juin 2016, TheDAO a vu son développement arrêté suite à une attaque de grande ampleur. Cela n'aura donc été qu'une courte expérimentation qui a permis la mise en lumière des axes d'améliorations pour le développement de ce type d'organisation.

On peut imaginer aisément que disposer d'une blockchain pour enregistrer les actions de son entreprise deviendra aussi indispensable qu'un expert comptable pour les marchés financiers.

> Afin de remettre en perspective cet échec et d'illustrer l'engouement du public pour la technologie blockchain, il est de bon ton de rappeller que lors de sa crowdsale, la mise en vente publique de token, TheDAO était la plus grosse campagne de crowdfunding de tous les temps avec une levée de plus de 160 millions de dollars en seulement un mois.

## La co-gouvernance de l'entreprise: piste prospective

La blockchain est une opportunité pour les entreprises à plusieurs titres. Elle offre à la fois la perspective de transparence que le grand public réclame, mais solutionne également l'implication des consommateurs au sein de la gouvernance de produits et de services.

Cette participation peut s'envisager à deux échelons: au niveau de la gouvernance du produit ou du service, ou bien de l'entreprise.

La co-gouvernance ou co-conception d'un produit ou d'un service pour une entreprise permettrait de maximiser l'implication du client, et donc de concevoir un outil adapté à la majorité d'entre eux. Cette co-gestion n'implique pas de laisser à la foule la totalité des décisions, bien au contraire. Il est possible grâce à la blockchain de repenser la place du client et de fixer la participation en toute transparence, avec des règles préalablement bien définies.

La co-gérance de l'entreprise permet d'impliquer le consommateur à un échelon supérieur, en participant aux décisions stratégiques de l'entreprise. Une telle participation ne force pas l'entreprises à remettre au grand public les pleines commandes, il appartiendra à chaque entité de définir la zone d'influence souhaitée, cette définition pourra même être confiée au vote.

Ainsi l'implication du grand public est maximale et pourra être génératrice d'une adhésion plus grande.

> La forme potentielle de cet outil pourrait être à mi-chemin entre les plateformes de crowdfunding actuelles et une DAO. L'innovation vis-à-vis des plateformes actuelles serait la transparence des processus et le contrôle fin des conséquences de la prise de décision collaborative.

# Collaborative project management

The blockchain offers a new promise: that of basing one's trust on the human without risk. That of opening up your company to the outside world, without fear of interference, of involving your employees in the decision making process with rules that are accessible and verifiable by everyone.

But above all, it opens the door to mixed consultation, internally from employees and externally from the general public. This dual opening could be achieved by using centralized services, but the blockchain offers substantial advantages.

## Internal management: employee-oriented management

The blockchain solves a large number of problems of holacratic enterprises which is a system of governance organization, based on the formalized implementation of collective intelligence. Because of its decentralized operation, these companies are particularly suited to this type of structure, which requires digital systems to communicate with their employees and enable collective decision-making. By providing a traceable and integrated system, the blockchain would solve the geographical fragmentation problem while maintaining a shared level of knowledge about active processes.

In addition, the operation of the blockchain through smart-contracts makes it possible to record operating principles that can be consulted by everyone and modified only by consensus. Thus, it is not impossible to imagine an organization with reduced or non-existent middle management layers replaced by smart-contracts.

## External management: the integration of the general public into managerial decisions

This new form of business management could allow forms of hybridization between companies as we know them and DAOs. By allowing the general public to be clearly and proactively guided in collective decision-making, the blockchain invites us to rethink interactions with the customer and heralds a new form of commitment around a product or brand.

# Participatory democracy

These are a combination of the concepts of participatory democracy and representative democracy.

- "Delegated democracy" (liquid democracy) is a form of democracy where voting power is entrusted to a delegate rather than a representative. This system can be considered as a synthesis between direct democracy and representative democracy.
- "Participatory democracy" which evokes the idea of citizen involvement and participation in public debate but also in political decision-making. This term, which is very much in vogue, often refers to extremely varied realities.

# First experiments

- L'Open Vote Network

**In A Smart Contract for Boardroom Voting with Maximum Voter Privacy, Patrick McCorry, Siamak F. Shahandashti and Feng Hao present the first implementation of a decentralized and self-accounting Internet voting system with maximum voter confidentiality using the blockchain.

**The voting in this example is "open ballot" and is suitable for board elections. It is written as a "smart-contract" for Ethereum.

Unlike previous experiments on electronic voting protocols, the researchers were able to implement a system that does not rely on any trusted authority to calculate the count or to protect the voter's privacy.

The Open Vote Network is an autonomous voting network and each voter is responsible for the confidentiality of his or her vote.

With such an implementation, this vote could only be compromised by total collusion involving all other voters.

The voting protocol is guaranteed by the consensus mechanism that also secures the Ethereum blockchain.

The implementation of this network was carried out on Ethereum's social test network to demonstrate its feasibility and has shown that its implementation can be possible with a minimum of configuration for elections and at a cost of $0.73 per voter.

The cost can be considered reasonable as long as this vote ensures maximum protection of the elector's privacy and is publicly verifiable.

This is the first implementation of a decentralized Internet voting protocol based on an Internet voting system.

It uses the Ethereum block chain not only as a public bulletin board, but more importantly, as a consensus calculation platform that enforces the rules for the correct execution of the voting protocol.

Although the number of subjects tested may seem trivial, this is a first initiative that needs to be pursued on a larger scale. In future work, the researchers have stated that they will study the feasibility of exploitation on a national scale.

The point raised by this study is that if such a perspective is made possible, it will almost certainly require a dedicated block chain.

For example, it may be a chain of Ethereum-type blocks that only stores the electronic voting contract.

The new block chain can have a larger block size to store more transactions on the chain and can be maintained in a centralized manner similar to RSCoin.

- The first blockchain-based election took place in Sierra Leone

> "Sierra Leone wishes to build trust with voters in a controversial election, in particular by examining how the election will be perceived publicly after the elections. By using the blocking chain as a means of immutably recording ballots and results, the country hopes to create legitimacy around the election and reduce the impact of opposition parties," he said.
>
> Leonardo Gammar in "Sierra Leone just held the first blockchain-based elections."

On March 7, 2018, a blockchain-based vote was held in Sierra Leone with a 70% participation in one blockchain.

Agora technology, created by Leonardo Gammar, anonymously stores votes in an unchanging register, providing instant access to election results.

> Anonymous votes/bulletins are recorded on Agora's blocking chain, which will be accessible to the public for any interested party to review, count and validate. This is the first time a government election has used blockchain technology.
>
> Leonardo Gammar, Agora

This experience stems from a major movement towards transparency and anti-corruption in Sierra Leone, particularly in the context of elections, the results of which are often controversial.

This experiment will test the impact on the perception of integrity in the context of the election. In this way, citizens and stakeholders hope to create legitimacy around the election and reduce the impact of opposition parties.

Although this is only a proof of concept (POC), it is not a complete electoral register, but rather a plurality of votes in acceptable quantities.

It is fascinating to see the technology being implemented in Sierra Leone, a country of about 7.4 million people.

The ultimate objective is to reduce the costs of voting by eliminating paper ballots and reducing corruption in the voting process.

This first experiment demonstrates the feasibility of the operation in a country of several million inhabitants where corruption and crime are high.

Its creator takes as an example the backtracking of many countries on electronic voting to advance the inevitability of blockchains in voting decision-making processes, arguing that there are no other verifiable and fully transparent end-to-end voting systems for this future.

However, it is a question of putting this experience into perspective, because an election in a country is not yet a massive movement. However, Gammar and his team have announced their intention to expand their product to other African countries and the rest of the world.

- DEMOCRACY EARTH project


> Democracy Earth Foundation logo

Democracy Earth Foundation (DEF) is a US non-profit foundation that builds a "liquid democracy" oriented governance platform based on an open source blockchain.

The DEF published version 1.0 Alpha of the governance platform, Sovereign, in May 2017 and its white paper, The Social Smart Contract, in September 2017. During the referendum for peace in Colombia, the foundation conducted a symbolic vote among the diaspora of approximately 6 million Colombian expatriates. The pilot project allowed people to vote separately on different parts of the referendum and to delegate their vote to representatives, with the results of the symbolic vote revealing important nuances in voters' preferences that were not taken into account during the referendum. The pilot project actively shows how participatory democracy reduces polarization, powerlessness and voter apathy.

## The implementation of the vote in the DEF project

The voting token aims to be a standard for digital democracy capable of interacting with other tokens, by establishing a common language for the governance of organizations based on the block chain. In the context of liquid democracies, a range of voting operations is permitted:

- Direct voting: a user has the right to use his or her tokens to vote directly on issues such as in a direct democracy.
- Basic delegation: a user can delegate votes to a representative. As long as the latter has access to these tokens, he can use them to vote on behalf of the former.
- Limited delegation on topics: A user may delegate votes to another on the specified condition that he/she may only use these tokens on issues bearing a specific label. If the delegation specifies that delegated votes can only be used for decisions on the subject of "environment", then the representative may not use them elsewhere. This potential for representation can be used to delegate a vote to an expert on a particular subject.
- Transitional delegation: If a user has received votes from another user, they can then delegate them to a third. This generates a chain of delegations that helps to empower specific actors within a community. This character can be disabled by the first user if he/she wishes.
- Overriding vote: A user may delete the result of his representative's vote if he has changed his mind, so that he can exercise ex post control of his delegated opinion.
- Public voting: Often referred to as the golden rule of liquid democracies, anyone who delegates has the right to know how his or her delegate voted on a given issue with his or her vote. In the same way that the votes of Congress members are public, on liquid democracies, delegates competing on a given subject are encouraged to build a public reputation based on their voting results in order to attract more delegations.

- Secret vote: A method capable of guaranteeing voting transactions that are not traceable to the voter. This is essential in the context of public elections held among large populations at high risk of coercion. Even if the perfect secrecy over the voting transaction is achieved, users can still be identified through fingerprints with the exposed metadata. For this reason, research on integration with blockchains designed for proven anonymous transactions is encouraged. The DEF is continuing its research on the integration of secret votes with the following blockchains:
    - Ethereum: uses pre-compiled contracts for addition and scalar multiplication on the elliptic curve alt_bn128, for matching controls, which allow zk-SNARKs.
    - ZCash: implements secure transactions using zero disclosure evidence of knowledge
    - Monero: use circle signatures with stealth addresses.

The transaction costs necessary for the validation of the vote may either be subsidised by the implementing body or paid directly by the voters.

DEF uses a zero knowledge proof system to guarantee the identity of the voter without publicly registering them in the blockchain. This is a major step forward in the voting process using this technology. Thus, the problem of confidentiality in the context of the secret ballot finds a first element of answer.

# Associative life and community management.

## Public participation in the governance of associations

Associations have everything to gain by implementing blockchain-based voting systems to allow their members to participate in the decision-making process. This would solve the problem of geographical fragmentation of members by jointly maintaining a high level of security and traceability.

All these points respond to the need for transparency that the general public demands.

## Local authority management: the citizen as an actor in the public service

The blockchain makes it possible to envisage a new level of integration of the citizen into the management of communities. Beyond participation through voting, this invites us to rethink the modalities of public service actions.

Many experiments are also taking place under the impetus of Mounir Mahjoubi, Secretary of State for Digital Technology, during a debate organized on July 20 at the University of Paris Dauphine on digital justice and legal technologies.

Following this announcement, we can distinguish different cases of use, particularly in the public procurement sector, which is particularly suited to the dynamics offered by smart-contracts and contract automation. There is also a new opportunity for the transmission of documents.

But the most ambitious use case concerns the porting of administrative law into code form. The objective is to be able to compare the individual situation of a constituent with the applicable rules.

> The long-term ambition is to consider an experiment of a community in the form of a DAO.

# Conclusion

The blockchain is a tool that heralds a revolution and promises a decentralized, open and collaborative world.

The reasons for the craze for this technology are to be found in the successive crises that our post-industrial societies are facing, a crisis of knowledge, trust, legitimate or excessive mistrust of state institutions. The new answers and questions that the blockchain brings will make it possible to envisage a different future around these problems and in particular around the question of voting, and more broadly participation.

While many experiments and proofs of concept support the interest of these questions, the prospective leads are even more numerous and we believe that the blockchain will be one of the technologies that will revolutionize the uses and systems in place. These experiments make it possible to consider companies involving the consumer, decentralized associations whose shares are subject to permanent voting by their supporters or public institutions managed in real time by citizens.

This revolution is not without its friction points, especially around the environmental issues that the blockchain will have to resolve. It will also be necessary to rethink the algorithms in order to make them more viable at the desired scales.

We must consider the blockchain as it is today, in its embryonic stage, and not lose sight of the many challenges and successes that this technology promises.

## Santiago Siri, Democraty Earth Foundation

Créateur de la Democraty Earth Foundation Source: Meet the Man With a Radical Plan for Blockchain Voting - Wired

## JF Pillou, Tout sur les systèmes d'information

Titre: Tout sur les systèmes d'information Auteur: JF Pillo Source: Edition Dunod

## Abdelkader Adla, Aide à la Facilitation pour une prise de Décision Collective: Proposition d'un Modèle et d'un Outil

Titre: Abdelkader Adla Auteur: Aide à la Facilitation pour une prise de Décision Collective: Proposition d'un Modèle et d'un Outil Source: Université Paul Sabatier - Toulouse III

## smart-contract

Définition: Le smart contract est un acte de notarisation par la blockchain

## Andrew Calcutt, The Conversation

Titre: Comment la gauche libérale a inventé la «post-vérité» Auteur: Andrew Calcutt Source: The Conversation

## Vérité et politique, Hannah Arendt

Titre: Vérité et politique, La Crise de la culture Auteur: Hannah Arendt Source: Wikipédia

## A Smart Contract for Boardroom Voting with Maximum Voter Privacy, Patrick McCorry, Siamak F. Shahandashti and Feng Hao

Titre: A Smart Contract for Boardroom Voting with Maximum Voter Privacy Auteurs: Patrick McCorry, Siamak F. Shahandashti and Feng Hao Source: School of Computing Science, Newcastle University UK

## Ethereum

Définition: Ethereum est une plate-forme décentralisée qui gère des contrats intelligents (smart-contract): des applications qui fonctionnent exactement comme programmée sans aucune possibilité de temps d'arrêt, de censure, de fraude ou d'interférence de tiers. Source: Ethreum project

## RSCOIN

RSCoin, une cryptomonnaie contrôlée par la Banque d'Angleterre dans le but de renforcer l'économie du pays et le commerce mondial, combine les avantages de la technologie du registre distribué avec le contrôle des monnaies traditionnelles, gérées de manière centralisée. Source: Rscoin project

## registre distribué

Un registre distribué (aussi appelé registre partagé ; en anglais, distributed ledger ou shared ledger) est un registre simultanément enregistré et synchronisé sur un réseau d'ordinateurs, qui évolue par l'addition de nouvelles informations préalablement validées par l'entièreté du réseau et destinées à ne jamais être modifiées ou supprimées. Un registre distribué n'a ni administrateur central ni stockage centralisé de données.

## re publica

Composé de res et de publicus, souvent traduit mot-à-mot par «chose publique» quoique «bien public» soit plus idiomatique.

## tiers de confiance

Un tiers de confiance est un organisme dont le but est de garantir l'authenticité d'une chose.

## open-source

La désignation open source, ou «code source ouvert», s'applique aux logiciels (et s'étend maintenant aux œuvres de l'esprit) dont la licence respecte des critères précisément établis par l'Open Source Initiative, c'est-à-dire les possibilités de libre redistribution, d'accès au code source et de création de travaux dérivés. Mis à la disposition du grand public, ce code source est généralement le résultat d'une collaboration entre programmeurs.

## Claude Shannon, Communication theory of secrecy system

Titre: Communication theory of secrecy system Auteur: Claude Shannon Source: Bell Systems Technical Journal

## hash

On nomme fonction de hachage, de l'anglais hash function, une fonction particulière qui, à partir d'une donnée fournie en entrée, calcule une empreinte servant à identifier rapidement, bien qu'incomplètement, la donnée initiale.

## Jean-Paul Delahaye, Les blockchains, clefs d’un nouveau monde

Titre: Les blockchains, clefs d’un nouveau monde Auteur: Jean-Paul Delahaye Source: Pour la Science - n° 449

## Adam Back, Inventeur du protocole Hashcash

Hashcash est un système de preuve du travail utilisé pour limiter les spams et les attaques par déni de service. Il a été proposé en 1997 par Adam Back.

## mining

Miner des cryptomonnaies signifie réaliser des calculs cryptographiques pour vérifier la chaîne de blocs. On désigne par la présente à la fois la machine, la pratique, et la personne ou l'institution effectuant l'opération.

## proof-of-work

En preuve de travail (PoW), l'algorithme récompense les participants qui résolvent des puzzles cryptographiques afin de valider les transactions et de créer de nouveaux blocs (c.-à-d. l'exploitation minière).

## proof-of-stake

Dans les blockchains publiques basées sur la preuve de mise en jeu (par exemple, l'implémentation prochaine d'Ethereum Casper), un ensemble de validateurs se relaient pour proposer et voter sur le bloc suivant, et le poids du vote de chaque validateur dépend de la taille de son dépôt (c'est-à-dire la mise en jeu).

## Leonardo Gammar dans «La Sierra Leone vient d'organiser les premières élections basées sur une blockchain.»

Titre: Sierra Leone just ran the first blockchain-based election Auteur: John Biggs Source: Techcrunch

## Leonardo Gammar, Agora

Agora est une entreprise qui s'engage à développer des élections sûres et transparentes dans le monde entier. site Agora

## Usman W. Chohan, Proof-of-Stake Algorithmic Methods: A Comparative Summary

Titre: Proof-of-Stake Algorithmic Methods: A Comparative Summary Auteur: Usman W. Chohan Source: SSRN

## Loi par le code

Titre: Code Is Law Auteur: LAWRENCE LESSIG Source: Harvard Magazine

## Simon de la Rouviere, blockchain Consensys

ConsenSys est un studio de production d'entreprise qui construit des applications décentralisées et divers outils de développement et d'utilisation finale pour les écosystèmes de la chaîne de blocs, principalement centrés sur Ethereum. site blockchain Consensys

## POC

Une preuve de concept (de l'anglais: proof of concept, POC) ou démonstration de faisabilité, est une réalisation expérimentale concrète et préliminaire, courte ou incomplète, illustrant une certaine méthode ou idée afin d'en démontrer la faisabilité.

## Art. L.225-36-1 C. com.

Equilibre des pouvoirs et fonctionnement des organes dirigeants. Art. L.225-36-1 C. com.

## Solidity

Solidity est un langage de programmation orienté contrat pour la rédaction de contrats intelligents. Il est utilisé pour la mise en œuvre de contrats intelligents sur différentes plates-formes de la chaîne de blocs. Il a été développé par Gavin Wood, Christian Reitwiessner, Alex Beregszaszi, Liana Husikyan, Yoichi Hirai et plusieurs anciens collaborateurs d'Ethereum pour permettre la rédaction de contrats intelligents sur des plateformes à chaînes multiples comme Ethereum.

## turing-complete

Un système complet de Turing signifie un système dans lequel un programme peut être écrit et qui trouvera une réponse à un problème donné.

## Vlad Zamfir, Ethereum Foundation researcher

Vlad Zamfir est chercheur à la Fondation Ethereum. Source: ethereum wiki

## Jean-Paul Delahaye dans L’attaque Goldfinger d’une blockchain

Titre: L’attaque Goldfinger d’une blockchain Auteur: Jean-Paul Delahaye Source: scilogs

## Patricia Egger et Dusko Karaklajic dans La sécurité du blockchain:

Titre: La sécurité du blockchain, protéger le Grand livre distribué Auteur: Patricia Egger et Dusko Karaklajic Source: Deloitte

## Julien Maldonato et Rémi Foult dans La Blockchain, panorama des technologies existantes.

Titre: La Blockchain, panorama des technologies existantes. Auteur: Julien Maldonato et Rémi Foult Source: Deloitte

## Rapport d'étude d'impact du projet de loi relatif à la croissance et la transformation des entreprises

Titre: ÉTUDE D'IMPACT PROJET DE LOI relatif à la croissance et la transformation des entreprises source: Assemblée Nationale

## Projet de loi PACTE article 62, alinéa II

Titre: PROJET DE LOI relatif à la croissance et la transformation des entreprises, source: Assemblée Nationale

## crowdfunding

Le financement participatif désigne l'ensemble des outils et méthodes de transactions financières qui font appel à un grand nombre de personnes afin de financer un projet.

## Mounir Mahjoubi, secrétaire d'État au numérique lors d'un débat organisé le 20 juillet à l'Université Paris Dauphine sur la justice numérique et les legaltechs

Titre: Expérimentation de la blockchain dans les collectivités: quelles possibilités ? La Gazette des communes

## preuve à divulgation nulle de connaissance

Un protocole de connaissance zéro est une méthode par laquelle une partie (le prouveur) peut prouver à une autre partie (le vérificateur) que quelque chose est vrai, sans révéler aucune information en dehors du fait que cette déclaration spécifique est vraie.

## Les risques des blockchains, par Laurent Dehouck, Maître de conférences en sciences de gestion, ENS Rennes et Audrey Thomas, ENSAM

Titre: Les risques des blockchains. Auteur: Laurent Dehouck, Maître de conférences en sciences de gestion, ENS Rennes et Audrey Thomas, ENSAM Source: reseau-canope

## The Social Smart Contract

Titre: The Social Smart Contract Source: Whitepaper

## démocratie liquide

La démocratie liquide, aussi appelée démocratie délégative, est une forme de gouvernement démocratique où le pouvoir de vote est confié à un délégué plutôt qu'à un représentant. Le déléguataire est soumis au contrôle des délégants.

## La signature de cercle

La signature de cercle est un procédé cryptographique permettant à une personne de signer électroniquement de façon anonyme un message ou un document au nom d'un « cercle ». Les membres de ce cercle sont choisis par l'auteur de la signature et ne sont pas nécessairement informés de leur implication dans la création de la signature électronique. La seule contrainte est qu'ils doivent tous avoir une clé cryptographique publique.

## Zcash à propos de zk-SNARKS

Source: site zcash

## holacratique

L'holacratie est un système d'organisation de la gouvernance, fondé sur la mise en œuvre formalisée de l'intelligence collective. Opérationnellement, elle permet de disséminer les mécanismes de prise de décision au travers d'une organisation fractale d'équipes auto-organisées.

## effet de la connaissance commune

De Common Knowledge Effect, L'effet des connaissances communes décrit l'impact sur la prise de décision du groupe, d'une information connue de tous avant la discussion a une influence plus forte sur les décisions que l'information non partagée par tous. L'effet de notoriété publique démontre qu'un facteur non pertinent - le nombre de membres qui connaissent un élément d'information particulier - peut influencer les décisions du groupe. Si un élément d'information non partagé est crucial pour prendre une décision correcte, le résultat peut être une mauvaise décision.
Source: SAGE

## mineur

un mineur est un individu vérifiant les transactions et opérations effectuées par les utilisateurs sur le réseau. Il les inscrit ensuite sur la blockchain (registre public). La vérification des transactions requiert de la puissance de calcul. Dans la mesure où le code informatique de la blockchain est open-source, devenir mineur est ouvert à tous.

## conjectures de Moore

Les conjectures de Moore sont des lois empiriques qui ont trait à l'évolution de la puissance de calcul des ordinateurs et de la complexité du matériel informatique.