

La blockchain comme modalité de sécurisation de la prise de décision collective par votes.

Sous l'aimable direction de Stéphane Dalbera, Atopos.

Ce qu'il y a d'intéressant à propos de la cryptographie, c'est qu'on peut commencer à créer des modèles institutionnels qui ne reposent plus sur la faillibilité de l'autorité humaine mais qui sont strictement basés sur le code, les mathématiques et le cryptage. On peut commencer à construire une réalité institutionnelle où les freins et contrepoids sont protégés par des promesses fermes, des constructions mathématiques fondamentales qui sont simplement impossibles à briser en raison des propriétés inhérentes au fonctionnement des informations.

[Santiago Siri, Democracy Earth Foundation](#)

Nombre d'observateurs s'accordent pour considérer que nous entrons dans une période de crise de confiance vis-à-vis des services offerts par internet.

Failles de sécurités, atteintes à la vie privée, manipulations de l'opinion, cybercriminalité, cyberguerre, etc. sont aujourd'hui des enjeux largement médiatisés hors des cercles d'initiés.

Le temps de la croyance aveugle dans les bienfaits de la révolution internet et des fantasmes semble révolu.

Cette crise de confiance n'est pas propre au secteur numérique, elle se diffuse dans toutes les strates de nos sociétés. Elle se manifeste dans le champ politique, dans le champ médiatique si bien que l'ère dans laquelle nous vivons porte désormais le nom d'ère post-vérité (*post-factual era*).

Cette crise a déjà de nombreuses conséquences dans le champ politique ainsi que dans le champ économique où la confiance est la clé de voûte de l'investissement et de l'adhésion.

L'opinion publique, les législateurs et les acteurs de l'industrie commencent à prendre la pleine mesure des chantiers qui s'annoncent pour sortir d'une période que l'on considérera bientôt, peut-être, comme celle du Far West.

Le travail de reconstruction de la confiance, qui commence seulement à s'effriter, sera dans les années à venir un des secteurs offrant les plus forts potentiels de croissance et d'innovation.

C'est dans ce cadre que nous comptons ici nous intéresser à l'impact que pourrait avoir une technologie largement médiatisée car au coeur des cryptomonnaies: la blockchain.

Si cette approche est apparue dans la mouvance du BitCoin, il s'agit avant tout d'une approche décentralisée de sécurisation de contrat ayant de très vastes potentiels d'usages.

Des services sécurisés et décentralisés de vote offrent un large champ de création de nouveaux modes d'interaction autour d'un des enjeux majeurs de toute société structurée: la prise de décision.

Dans ce travail nous analyserons les perspectives ouvertes par l'usage de la blockchain comme outil de sécurisation de la prise de décision collectives. À travers les impératifs réclamés par ces processus de décision, nous tenterons d'évaluer la capacité de la blockchain à y répondre.

Nous tenterons également d'évaluer le coût de l'utilisation de la blockchain pour les prises de décisions collective en portant une attention particulière aux critères environnementaux.

Enfin, nous illustrerons notre propos à l'aide de réalisations en cours ou de preuves de concept et émettrons des pistes prospectives.

Table des matières

Introduction

Résumé

Remerciements

Définitions

- Blockchain
- Modalité de sécurisation
- Prise de décision collective
- Vote

A. Du besoin d'outils sécurisés de prise de décision collective et de leur potentiel impact

- 1. Les origines de la crise de confiance
- 2. Une aspiration à la transparence
- 3. Du statut de la preuve au vote
- 4. Les domaines d'enjeux

B. De la blockchain comme potentiel cœur de ce changement

- 1. Qu'est-ce que la blockchain?
- 2. Qu'est-ce que les smart-contracts?
- 3. Preuve de Travail vs Preuve de l'Enjeu
- 4. Blockchain privée vs Blockchain publique
- 5. Gestion de l'identification et confidentialité
- 6. Quid de la sécurité de la blockchain?
- 7. Quid de ses impacts énergétiques?
- 8. Vers une normalisation?
- 9. Les limites de la blockchain

C. Scénarios d'usages

- 1. Gouvernance des entreprises
- 2. Management collaboratif de projet
- 3. Démocratie participative
- 4. Vie associative et gestion des collectivités.

Conclusion

Sources et glossaire

Résumé

Nos sociétés font face à une crise de la confiance, les entreprises, institutions, associations et autres acteurs du champ public en subissent déjà les conséquences.

Ces effets délétères sont multiples, allant du scandale économique avec les pertes financières que cela implique, au désintérêt du grand public pour une cause, ou, plus généralement, pour la participation citoyenne.

Ces institutions sont observées de près et elles doivent se prémunir en agissant avec plus de transparence et de consultation du public.

Le vote est la forme reine de la participation ; bien qu'il représente la forme la plus embryonnaire de la démocratie, il reste la solution la plus simple à mettre en oeuvre à grande échelle.

La blockchain apparaît comme une solution potentielle à ces problématiques, lorsqu'elle encadre ce processus de participation.

La blockchain est un registre distribué dans lequel les informations sont stockées sous forme de blocs et dont la validation est soumise à différentes méthodes cryptographiques et de consensus. Elle offre des garanties en matière de sécurité et ses limites sont identifiées.

Si de nombreuses expériences et preuve de concept démontrent l'intérêt du grand public pour ces questions, les pistes prospectives sont encore plus nombreuse et la blockchain pourrait être le moteur de ce changement. Ces expérimentations permettent d'envisager des entreprises impliquant le consommateur, des associations décentralisées dont les actions sont soumise au vote permanent de leurs soutiens ou bien encore des institutions publiques pilotées en temps réel par les citoyens.

De nombreux défis et problèmes rendent la blockchain inutilisable raisonnablement en l'état à grande échelle, en particulier le défi énergétique.

Les pistes pour répondre à ce défi environnemental sont la mise en place de blockchains implémentant la preuve de l'enjeu (technique de validation des blocs moins couteuse énergétiquement) et les différentes formes de normalisation.

Remerciements

La réalisation de ce mémoire a été possible grâce au concours de plusieurs personnes à qui je voudrais témoigner toute ma reconnaissance.

Je tenais tout d'abord adresser toute ma gratitude au directeur de ce mémoire, Monsieur Stéphane Dalbera, pour sa patience, sa disponibilité et surtout ses judicieux conseils, qui ont contribué à alimenter ma réflexion.

Je voudrais exprimer une reconnaissance toute particulière envers Virgile Deville, dont les conseils et critiques ont guidé mes réflexions.

Définitions

1. La blockchain
2. Modalité de sécurisation
3. Prise de décision collective
4. Vote

Définition: blockchain

Une (ou un) blockchain, ou chaîne de blocs est une technologie de stockage et de transmission d'informations sans organe de contrôle.

Techniquement, il s'agit d'une base de données distribuée dont les informations envoyées par les utilisateurs et les liens internes à la base sont vérifiés et groupés à intervalles de temps réguliers en blocs, l'ensemble étant sécurisé par cryptographie, et formant ainsi une chaîne.

Par extension, une chaîne de blocs est une base de données distribuée qui gère une liste d'enregistrements protégés contre la falsification ou la modification par les nœuds de stockage.



Une blockchain est donc un registre distribué et sécurisé de toutes les transactions effectuées depuis le démarrage du système réparti.

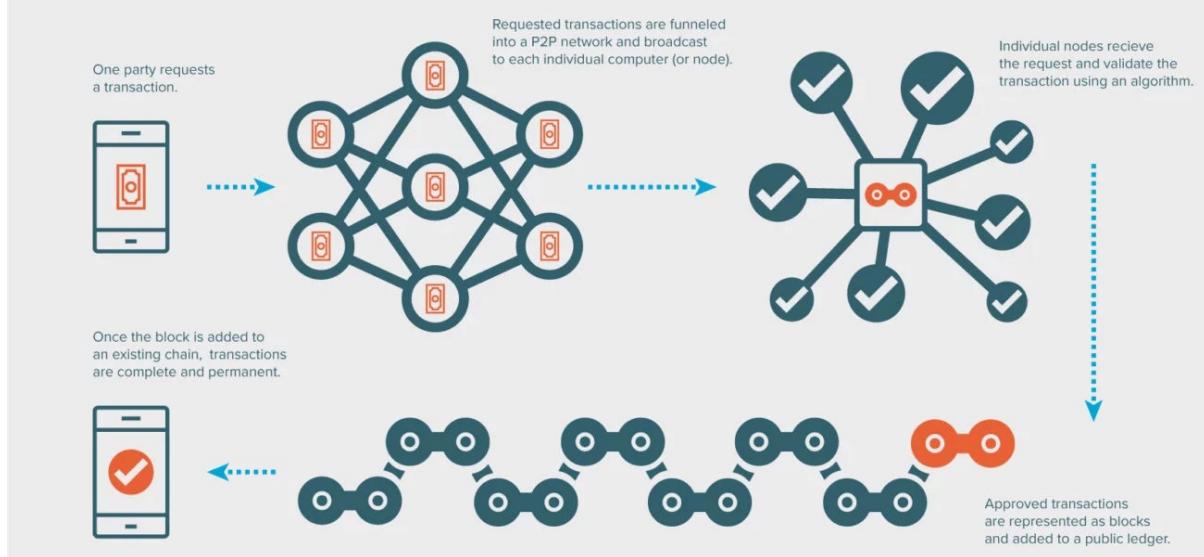
Il existe des blockchains publiques, ouvertes à tous, et des blockchains privées dont l'accès et l'utilisation sont limités à un certain nombre d'acteurs.

Une blockchain publique peut donc être assimilée à un grand livre comptable public, anonyme et infalsifiable.

Il faut s'imaginer «un très grand cahier, que tout le monde peut lire librement et gratuitement, sur lequel tout le monde peut écrire, mais qui est impossible à effacer et indestructible.»

Jean-Paul Delahaye, *Les blockchains, clefs d'un nouveau monde*

HOW DOES BLOCKCHAIN WORK?



Définition: modalité de sécurisation

Nous entendons les modalités de sécurisation comme les différentes méthodes et moyens déployés dans le but de sécuriser.

L'action de sécurisation est engagée par l'application de techniques de sécurité au sens informatique.

La sécurité des systèmes d'information (SSI) ou plus simplement sécurité informatique, est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires à la mise en place de moyens visant à empêcher l'utilisation non-autorisée, le mauvais usage, la modification ou le détournement du système d'information.

La sécurité est un enjeu majeur pour les entreprises ainsi que pour l'ensemble des acteurs qui l'entourent.

- Sa finalité sur le long terme est de maintenir la confiance des utilisateurs et des clients.
- Sa finalité sur le moyen terme est la cohérence de l'ensemble du système d'information.

«Le système d'information représente un patrimoine essentiel de l'organisation, qu'il convient de protéger. La sécurité informatique consiste à garantir que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu.»

JF Pillou, Tout sur les systèmes d'information

La sécurité des systèmes d'information vise les objectifs suivants:

Objectif	Explication
La disponibilité	Le système doit fonctionner sans faille durant les plages d'utilisation prévues et garantir l'accès aux services et ressources installées avec le temps de réponse attendu.
L'intégrité	Les données doivent être celles que l'on attend, et ne doivent pas être altérées de façon fortuite, illicite ou malveillante. En clair, les éléments considérés doivent être exacts et complets.
La confidentialité	Seules les personnes autorisées peuvent avoir accès aux informations qui leur sont destinées. Tout accès indésirable doit être empêché.
La traçabilité (ou «preuve»)	Il faut garantir que les accès et tentatives d'accès aux éléments considérés sont tracés et que ces traces sont conservées et exploitables.
L'authentification	L'identification des utilisateurs est fondamentale pour gérer les accès aux espaces de travail pertinents et maintenir la confiance dans les relations d'échange.
La non-répudiation et l'imputation	Aucun utilisateur ne doit pouvoir contester les opérations qu'il a réalisées dans le cadre de ses actions autorisées et aucun tiers ne doit pouvoir s'attribuer les actions d'un autre utilisateur. Une fois les objectifs de la sécurisation déterminés, les risques pesant sur chacun de ces éléments peuvent être estimés en fonction des menaces.

Le niveau global de sécurité des systèmes d'information est défini par le niveau de sécurité du maillon le plus faible. Les précautions et contre-mesures doivent être envisagées en fonction des vulnérabilités propres au contexte auquel le système d'information est censé apporter service et appui.

Il faut pour cela estimer:

- La gravité des conséquences au cas où les risques se réaliseraient.
- La vraisemblance des risques (ou leur potentialité), ou encore leur probabilité d'occurrence).

Définition: prise de décision collective

La prise de décision collective est une situation où des individus sont rassemblés en un groupe pour résoudre des problèmes.

Selon l'idée de synergie, les décisions prises collectivement ont tendance à être plus efficaces que les décisions prises individuellement. Cependant, il existe des situations dans lesquelles les décisions prises en groupe aboutissent à un mauvais jugement.

En psychologie sociale, la prise de décision collective peut être définie comme:

«une convergence d'interactions cognitives et visuelles, planifiées ou opportunistes, où des personnes acceptent de se rassembler pour un objectif commun, dans une période de temps définie, [...] dans le but de prendre des décisions»

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

La prise de décision collective est un domaine d'étude vaste auquel plusieurs disciplines s'intéressent, comme les sciences sociales, les sciences politiques, l'informatique ; on s'y intéresse également en marketing et en management, chacun de ces champs d'étude ayant son point de vue sur la question.

Du point de vue de la psychologie sociale plus spécifiquement, des applications et des conséquences théoriques sont nombreuses et variées dans différents domaines comme la gestion d'équipe, les situations de jurys, la politique, etc. Il existe différents types de décisions collectives chacune ayant des modalités et des processus psychologiques bien spécifiques, tels que la polarisation, la pensée de groupe et l'[effet de la connaissance commune](#).

Définition: vote

Le vote (du latin *votum* signifiant «vœu») désigne une méthode permettant à un groupe une prise de décision commune.

Les organisations formelles ou informelles, de toute nature (économiques, politiques, associatives, etc.), ont recours à cette pratique. La pratique du vote vise à donner une légitimité à la décision en montrant qu'elle ne vient pas d'un individu isolé. Avant que le vote proprement dit n'ait lieu, il est fréquent qu'un temps de discussion ou de débat soit ménagé pour permettre à chacun des votants d'exposer ou de prendre connaissance des arguments, afin de motiver au mieux sa décision.

Le vote est généralement encadré par un processus électoral aussi dénommé «scrutin» ou «élection».

Les enjeux du vote:

Principe	Explication
Décidabilité	Le but premier est généralement de pouvoir décider d'une position, qu'il s'agisse d'une position consistant à prendre une décision, ou d'une position consistant à ne pas prendre de décision; c'est notamment le cas d'un référendum.
Unicité du vote	Généralement on souhaite l'unicité du vote: pour permettre à chacun d'être justement représenté, il ne faut pas permettre à un électeur de voter plusieurs fois, c'est-à-dire d'être sur représenté.
Représentativité	Certains systèmes de propriété (propriété au sens légal) conduisent à ce que les voix de chaque électeur soient pondérées par une quote-part de participation.
Secret et transparence	Suivant le scrutin, on peut souhaiter que le vote soit secret, afin de prévenir la corruption du vote, ou bien au contraire public, afin de contraindre à un positionnement assumé.
Vérifiabilité	Afin de lever tout doute sur la légitimité du scrutin, lorsqu'un enjeu existe, on souhaite que le scrutin soit vérifiable, c'est-à-dire que l'on puisse démontrer aux yeux de tous l'absence de triche. On souhaite alors s'assurer que les personnes et matériels impliqués dans l'organisation ne soient pas détournés aux profits d'intérêts spécifiques.
Attractivité	Certaines organisations commerciales promeuvent des votes dans le but inavoué de susciter la participation à une action qui sans le dire est un acte d'achat. C'est notamment le cas des votes visant à l'achat par «numéros de services à valeur ajoutée» également connues sous l'appellation de communication téléphonique surtaxée.
Non-participation	Pour éviter qu'une décision ne soit prise par défaut ou pour pallier certains aléas, il est de coutume de permettre la non-participation, par exemple au travers de l'abstention, ou du vote nul ou blanc.
Quorum et majorité	Pour donner une légitimité accrue à la prise de décision, la méthode de vote peut être corrélée à un système de quorum et/ou de majorité qualifiée.
Rapidité	Dans un vote où l'on attend un résultat positif, il est d'usage de demander d'abord qui est contre et ensuite qui s'abstient. Les personnes qui ne se prononcent pas sont alors supposées en faveur de la décision. Ceci présente une double avantage: cela évite de devoir compter les nombreux pour, tout en maximisant leur nombre.

Modes d'expression:

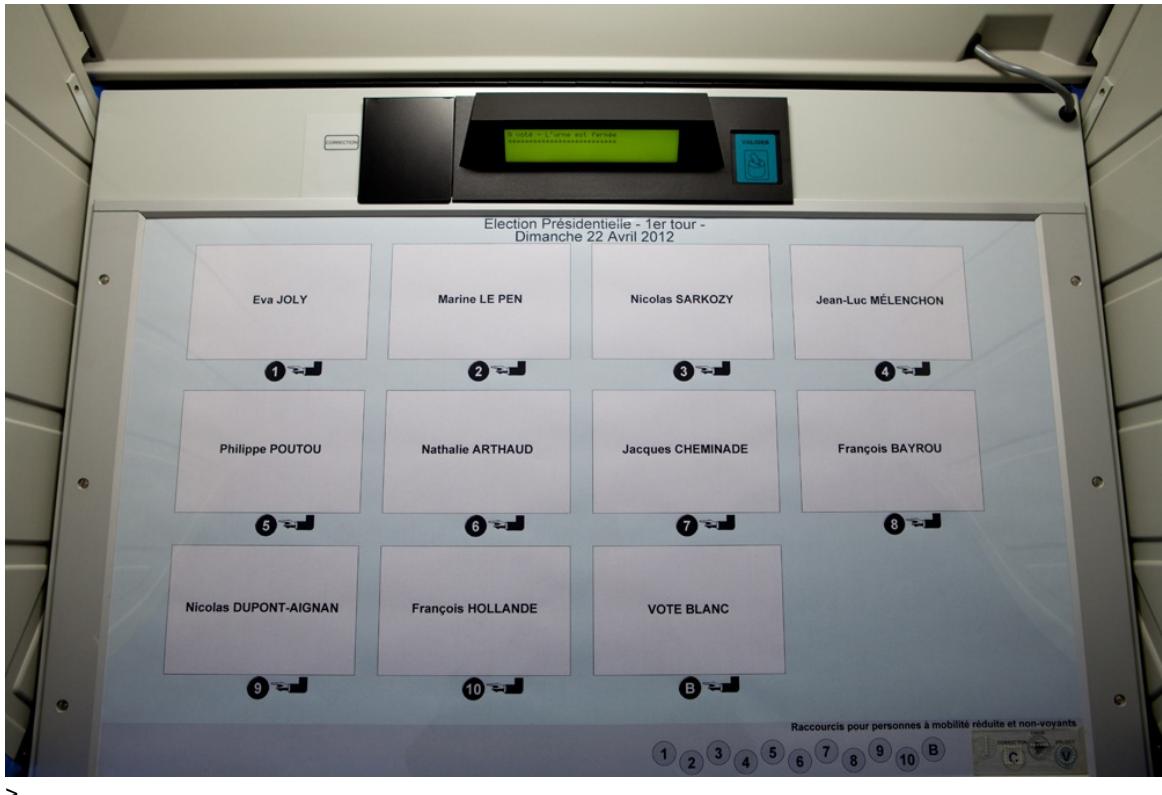
- Vote à bulletin secret: Le vote à bulletin secret, aussi appelé scrutin secret, consiste à donner son avis sur plusieurs propositions, de manière anonyme.
- Vote à main levée: Le vote à main levée consiste à lever sa main pour donner son avis entre plusieurs propositions. Il permet une prise de décision rapide, car le dépouillement est quasi immédiat. Mais cela oblige à ce que tous les votants soient présents en même temps. La procédure peut commencer par le vote par acclamation, où on estime le volume sonore de chaque option comme à l'assemblée spartiate ou lors de la conclusion de primaires présidentielles aux États-Unis.



>

Vote à main levée, source Assemblée Nationale Française

- Vote public: Le vote public, aussi appelé vote à l'appel nominal, consiste à appeler tour à tour chacun des membres d'une assemblée à exprimer son vote publiquement. Celui-ci est alors consigné dans le registre des délibérations et il est ensuite possible de publier le vote de chacun des participants au scrutin.
- Vote par correspondance: il consiste à envoyer à l'avance son bulletin de vote par voie postale ; un numéro d'identification permet de garantir qu'une personne ne vote qu'une fois, tout en maintenant le secret du vote.
- Vote par procuration: Le vote par procuration permet au mandant de désigner un mandataire qui ira voter à sa place.
- Vote de remplacement: Le vote de remplacement permet à ceux qui votent pour des candidats ou des listes n'ayant pas d'élus faute d'avoir atteint le quorum de prévoir le report de leur voix sur un autre candidat.
- Vote électronique: Le vote électronique est un système de vote automatisé, notamment des scrutins, à l'aide de systèmes informatiques. Ce terme générique relève en vérité de plusieurs situations concrètes. Par exemple, il peut correspondre à l'informatisation du processus de vote permettant de voter à distance, c'est-à-dire de voter de chez soi, ou de n'importe où dans le monde et ainsi éviter de se déplacer dans des bureaux de vote.



>

Une machine à voter électronique Française, source Mairie de Saint-Pol-sur-Mer.

- Vote par clé: Il consiste à voter à l'aide d'une clé physique sur un pupitre dédié.
-

Le cas particulier du vote par Internet n'en est pas un.

Le vote par internet, qui s'inscrit dans le mode d'action du vote électronique à longtemps été décrié au motif que son principal inconvénient serait l'absence d'isoloir (rien ne garantirait que le citoyen soit seul devant l'ordinateur au moment où il vote, ni ne permet de le vérifier). Néanmoins cette assurance est également absente lors du vote public, par correspondance, à main levée. Il est également impossible de s'assurer que la volonté du mandant ait bien été respectée dans le cadre d'un vote par procuration.

A. Du besoin d'outils sécurisés de prise de décision collective et de leur potentiel impact

1. Les origines de la crise de confiance
2. Une aspiration à la transparence
3. Du statut de la preuve au vote
4. Pour la res publica
4. Les domaines d'enjeux

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.

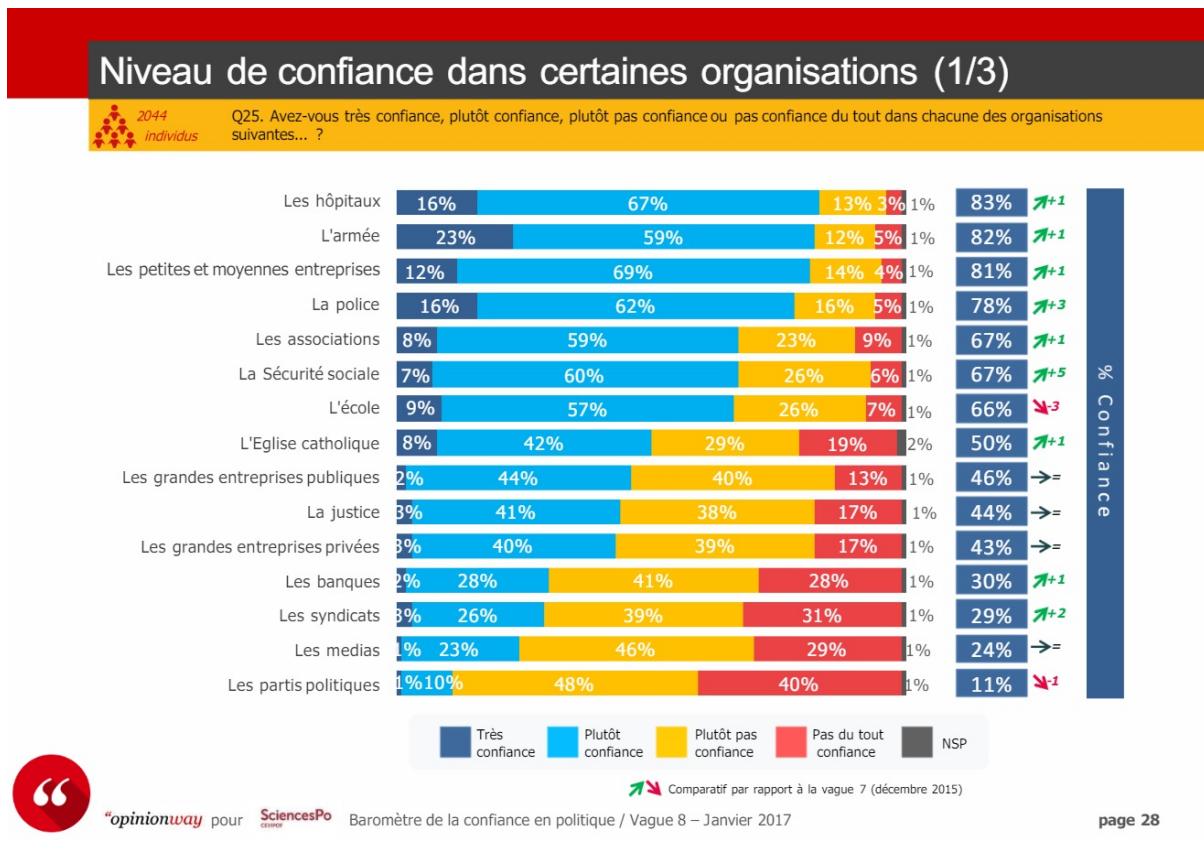
Le postmodernisme n'a pas créé les fondations de l'ère «post-vérité».

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 apparaît 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 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 pattes blanches».

Les entreprises engagées dans des actions de communications doivent prendre conscience qu'elles sont hyper-scrutées et qu'elles doivent engager des 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, dual. 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 utilisé.

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 métacontôle .

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.

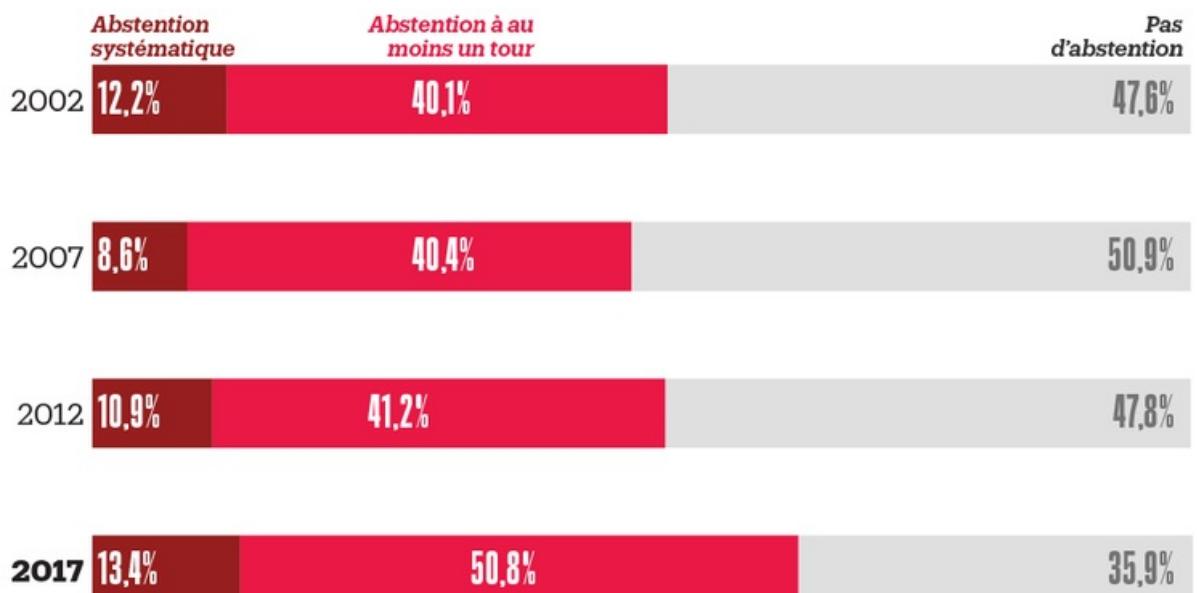
Le vote dans la sphère publique invite à s'interroger sur la représentativité en matière de prise de décision, de disponibilité physique des votants, de la transparence du processus démocratique, de l'intégrité et de la traçabilité.

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:

La progression de l'abstention au fil des élections

Participation électoral aux élections présidentielles et législatives depuis 2002, en % des personnes interrogées



Source : enquêtes Insee auprès d'environ 40 000 personnes Note : en raison des arrondis, les totaux peuvent ne pas être égaux à 100
>

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 délégué est dans la capacité de dépasser ou d'outrepasser les choix préalables du ou des délégués.
- 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 publique. 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 à 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. De la blockchain comme potentiel cœur de ce changement

Les entreprises, institutions et associations traversent une crise de la confiance. Elles sont désormais scrutées, analysées et le moindre faux-pas peut avoir des conséquences coûteuses. Si la participation par le biais du vote est un premier pas facile vers la réconciliation, il n'est pas pour autant suffisant. En effet, le grand public réclame désormais des processus fiables et transparents, afin de permettre un contrôle par le plus grand nombre. La blockchain apparaît comme une opportunité de redonner confiance et comme moteur de réengagement auprès de ces organisations.

1. Qu'est-ce que la blockchain ?
2. Qu'est-ce que les smart-contracts ?
3. Preuve de Travail vs Preuve de l'Enjeu
4. Blockchain privée vs Blockchain publique
5. Gestion de l'identification et confidentialité
6. Quid de la sécurité de la blockchain ?
7. Quid de ses impacts énergétiques ?
8. Vers une normalisation ?
9. Les limites de la blockchain

Qu'est-ce que la blockchain ?

Le terme blockchain désigne à la fois le système et la technologie sous-jacente à ce système.

La blockchain est connue majoritairement du grand public comme étant la technologie utilisée par le bitcoin.

Inventé en 2008, le Bitcoin est à l'origine un prototype destiné à démontrer la possibilité de créer une crypto-monnaie dont le mécanisme repose sur un registre distribué et réparti entre de multiples nœuds d'un réseau.

De part leur nature intrinsèquement [open-source](#), les algorithmes de chiffrement sont un argument de plus au regard de la confiance en ce système.

Si le Bitcoin a bénéficié d'une telle exposition médiatique, c'est qu'il s'agit d'une monnaie limitée en volume qui sort du référentiel courant. Mais surtout, il s'agit d'une monnaie qui remet en question le rôle des institutions bancaires et des états en tant que [tiers de confiance](#) et en tant qu'entité légitimes à émettre et à réguler la monnaie.

Les trois piliers de la blockchain

La blockchain est basée sur trois piliers: deux sont technologiques, à savoir la cryptographie asymétrique et les systèmes distribués, et le troisième est sociologique.

1. La cryptographie,

Elle repose sur le concept de clé. Il existe deux types de clés: les symétriques et les asymétriques.

Les premières sont connues depuis l'antiquité et les secondes ont vu le jour dans les années 1970.

La seconde est essentielle à la technologie blockchain car elle permet de s'assurer de l'authenticité de l'expéditeur du message. L'expéditeur utilise sa clé privée pour coder un message que le destinataire peut décoder avec la clé publique de l'expéditeur. La méthode du chiffrement symétrique a l'avantage d'être peu coûteuse en puissance de calcul, et de demeurer très sûre. Malheureusement elle présente des limites:

L'inconvénient est que pour chiffrer un message de n bits, il faut au préalable avoir échangé une clé de n bits avec le destinataire du message, et cela par une voie absolument sûre, sinon chiffrer devient inutile.

[Claude Shannon, Communication theory of secrecy system](#)

À cette méthode on préférera le chiffrement asymétrique qui permet de contourner l'obstacle de la clé commune aux parties prenantes. En effet, dans le cadre du chiffrement asymétrique, deux clés sont présentes: la privée et la publique. La clé qui est choisie privée n'est jamais transmise à personne alors que la clé qui est choisie publique est transmissible sans restriction.

Cette technique permet:

- Le chiffrement

L'un des rôles de la clé publique est de permettre le chiffrement. C'est donc cette clé qu'utilisera un premier sujet pour envoyer des messages chiffrés à un second. L'autre clé — l'information secrète — sert à déchiffrer. Ainsi, le second sujet, et lui seul, peut prendre connaissance des messages du premier sujet.

La connaissance d'une clé ne permet pas de déduire l'autre clé.

- L'Authentification de l'origine

L'utilisation par l'un des sujets de sa clé privée sur le condensat d'un message permettra à ce dernier de vérifier que le message provient bien de l'interlocuteur attendu et de prévenir l'usurpation: il appliquera la clé publique que son interlocuteur lui a fournie sur le condensat (condensat chiffré avec la clé privée de l'autre sujet) et retrouve donc le condensat original du message.

Il lui suffira donc de comparer le condensat ainsi obtenu et le condensat réel du message pour savoir si son interlocuteur est bien celui qu'il prétend. C'est sur ce mécanisme notamment que fonctionne la signature numérique.

2. La distribution

Internet se trouve être l'une des plus belles preuves de système distribué, nul besoin d'un opérateur de télécommunication unique pour que toute personne, où qu'elle se trouve dans le monde, puisse se connecter aux Internets.

3. Le consensus distribué

Pour comprendre le concept de consensus distribué, l'exemple d'une opération de lutte contre des narco-trafiquants nous apparaît le plus indiqué.

Imaginons une ville en lutte contre le crime, tout particulièrement un cartel puissant. Dans le cadre d'une opération de lutte contre le trafic de drogue, toutes les forces de police de la région sont réunies pour anéantir les criminels.

Les différentes organisations de police doivent toutes attaquer ensemble pour profiter de l'effet de surprise. Le cas contraire elles seraient submergées et les trafiquants risqueraient de profiter de la confusion pour s'enfuir.

Ils doivent donc se coordonner quant à la date et l'heure de l'attaque, et, ne pouvant pas se rencontrer tous, ils déléguent à certains le rôle de messager afin de limiter les allers et venues.

Malheureusement dans une ville aussi corrompue, on ne peut se fier à personne et certains policiers sont en réalité des criminels sous-couverture dont l'objectif est de déjouer l'attaque.

Par exemple, l'un d'entre eux peut dire à la moitié des forces de polices qu'il faut attaquer à telle date et à telle heure, et à l'autre moitié qu'il faut se retirer, désorganisation qui ne leur permettra pas de bénéficier de l'effet de surprise et de la supériorité numérique.

La grande nouveauté apportée par la blockchain est de proposer un système qui permet de se défaire de cette autorité hiérarchique.

En substance, chaque force de police ne peut envoyer qu'un seul ordre à la fois, associé à un horodatage.

Mais, surtout, les ordres sont aggrégés les uns aux autres, puis chiffrés, formant une chaîne stockée dans un «grand livre de transactions», lequel est redistribué à toutes les services de polices en présence.

Une chaîne est ainsi formée, contenant un [hash](#) de tous les ordres précédents.

Ainsi, si un messager reçoit l'information «La perquisition aura lieu demain à 16h00», et qu'il décide de ne la répercuter qu'à la moitié des autres et d'envoyer un horaire différent à l'autre moitié, il changera la valeur de ce [hash](#).

Les autres messagers partageant l'information avec tous les services de police en présence, il sera possible de déterminer les chaînes incohérentes et d'identifier les corrompus simplement en comparant la valeur des hashs.

Ceci implique bien entendu que le nombre de messagers honnêtes soit supérieur au nombre de corrompus.

Les différentes méthodes de consensus:

Type de consensus	Description	Avantages	Inconvénients	Type de blockchain
-------------------	-------------	-----------	---------------	--------------------

1. Qu'est-ce que la blockchain ?

Preuve de travail (PoW)	Les ordinateurs des mineurs sont mis à disposition pour résoudre un problème mathématique compliqué. Le 1er qui trouve une solution gagne la récompense du prochain bloc de la chaîne.	Sécurisé, éprouvé et robuste.	Très consommateur d'électricité et de matériel informatique.	Publique
Preuve de l'enjeu (PoS)	Les validateurs de transactions doivent mettre en gage la possession de cryptomonnaie pour recevoir une récompense. Si un nœud est malveillant, il peut perdre sa mise en gage au profit des validateurs honnêtes.	Peu consommateur en ressources énergétiques.	Peu testé à grande échelle.	Publique
Système tolérant les défaillances (PBFT)	Consensus dont la liste des validateurs est connue au départ et peut tolérer jusqu'à 1/3 de nœuds compromis (déconnectés ou malveillants).	Consensus de groupe rapide et performant. Pas de fork ou de réorganisation de chaîne.		Privée
Preuve d'autorité	Consensus dont la liste des validateurs est connue au départ et qui valide à tour de rôle un bloc. Ce type de consensus peut tolérer jusqu'à 49% de nœuds malveillants ou déconnectés.	Consensus de groupe rapide.		Privée

Qu'est-ce que les smart contracts?

Principe

La blockchain Ethereum dispose d'une capacité singulière vis-à-vis des autres blockchains. Elle peut être programmée à l'aide d'un langage spécifique: [Solidity](#). C'est un langage de programmation «complet» ([turing-complete](#)), c'est-à-dire qu'il permet d'exécuter l'ensemble des fonctions utilisés pour développer une application moderne.

Cela permet de programmer des engagements sur la blockchain Ethereum. Ceux-ci peuvent être simples, comme engager une transaction ou plus complexes, car constitués de plusieurs actions en série ou parallèle.

Lorsque les conditions d'exécution de ces engagements sont réunies, ces contrats s'exécutent automatiquement sur la blockchain, en tenant compte de l'ensemble des conditions et des limitations programmées à l'origine.

Un contrat de prestation de service entre deux entités peut aisément se modéliser sous la forme d'un [smart-contract](#).

La première souhaite rémunérer la seconde en paiement de la prestation, ce contrat est formalisé dans la blockchain Ethereum par la création d'un engagement de type [smart-contract](#). La somme correspondante est alors mise en gage sur la blockchain. Lorsque la prestation est réalisée, l'engagement vérifie automatiquement que les conditions fixées ont bien été remplies et le cas échéant, verse la somme gagée. En cas de manquement aux stipulations du contrat, la partie gageante se voit restituer la somme.

Les transactions effectuées sont publiques, il s'agit du principe de publicité. La bonne exécution du contrat peut ainsi être vérifiée, n'importe quelle partie qui dispose du code source du contrat peut vérifier que le contrat a bien été enregistré.

La blockchain prodigue une sécurité élevée, l'une de ses limites est la vulnérabilité à l'attaque des 51%. Voir [sécurité de la blockchain](#).

Les données qui sont enregistrées dans la blockchain y sont enregistrées de manière immuable: l'historique est conservé depuis l'origine. Un engagement est irrémédiablement enregistré dans la blockchain.

Mettre hors ligne une blockchain nécessiterait d'arrêter simultanément tous les nœuds de celle-ci, ce qui est virtuellement. C'est donc un système que l'on peut considérer comme fiable.

En résumé les smart-contrats permettent d'engager des accords entre deux parties sans que l'une ne puisse entraver son exécution, mais également des applications décentralisées.

Limites

Se pose alors la question de la validation des conditions d'exécutions. En effet, puisqu'elle interagit avec le monde physique, le [smart-contract](#) doit parfois disposer de capacités matérielles. Pour cela deux possibilités:

- Condition d'exécution interne: Lorsque les conditions d'exécution ne nécessitent pas une interaction physique avec l'environnement, les conditions sont inscrites dans la blockchain. Le contrat est exécuté dès que les conditions sont remplies et que la date d'exécution est atteinte.
- Condition d'exécution externe: Lorsque les conditions d'exécution sont extérieures à la blockchain comme la réalisation d'une prestation, survenance d'un événement... etc. Dès lors, le recours à un [tiers de confiance](#), appelé «oracle» est nécessaire. Il lui est délégué l'observation des ces événements étrangers et l'écriture des

conditions dans la blockchain.

La principale limitation inhérente à la technologie blockchain est la lenteur du réseau, contrepartie de sa sécurité.

Dans le cadre du vote:

Exemple avec l'utilisation d'un service d'oracle:

Le recours à un service d'oracle nécessite un nombre important de participants. Chaque protagoniste vote pour le résultat qu'il juge exact et le résultat est confié au consensus. On peut citer en la matière le projet Oraclize. Dans le cadre du vote cela sous-entend de confier un nombre de propositions au consensus qui détermine les éléments valides.

Une proposition est dans ce cas de figure un [smart-contract](#) classique dont les conditions fixent le cadre d'application. Une fois ces conditions validées, le contrat voit son exécution programmée.

Ce système présente une limite et nécessite une vigilance particulière. En effet l'interruption du contrat (et donc de l'exécution de la proposition) est en pratique impossible, sauf si cette condition d'interruption a été prévue dès l'origine.

Preuve de travail vs preuve de l'enjeu

Nous avons vu précédemment qu'une blockchain est un registre distribué chiffré et répliqué dans tous les nœuds du réseau, qui contient les chaînes d'ordres permettant, grâce à l'obtention d'un consensus, de gérer la confiance sans institution externe.

Concernant la preuve de travail:

De l'anglais [proof-of-work](#). Abrégé PoW.

Nous avons vu précédemment que la chaîne est constituée d'un ensemble de blocs de données contenant des informations ainsi qu'un horodatage. À chaque transaction, ces blocs sont intégrés à la chaîne.

Afin de garantir son intégrité, cette chaîne est chiffrée et doit être certifiée.

Pour certifier la transaction, de puissants ordinateurs constitués de nœuds en réseau réalisent des calculs cryptographiques.

Le travail global de certification se nomme «preuve de travail» (proof of work).

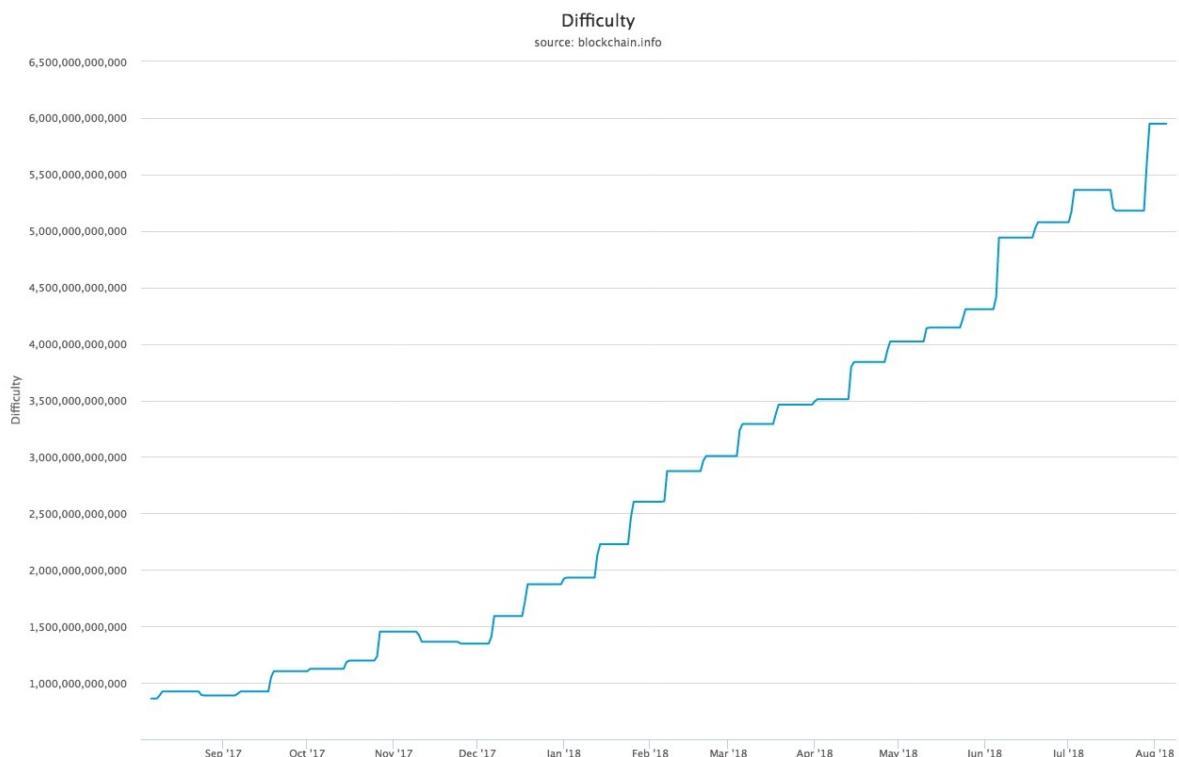
On appelle les machines (ou institutions) qui effectuent ce travail de certification des «mineurs» de l'anglais [mining](#).

L'objet cryptographique créé par le [mineur](#) est la preuve du temps passé à la certification, il constitue la preuve de travail.

Il est essentiel de garantir la nature réelle du travail des parties prenantes afin de préserver le consensus.

Fruit d'une invention d'[Adam Back, inventeur du protocole Hashcash](#), elle évite un clonage facile qui aurait pour conséquences de pouvoir contrôler la blockchain de manière rétroactive.

Le mécanisme est même plus sophistiqué : à intervalles de temps réguliers, la difficulté augmente.



Graphique illustrant la mesure relative de la difficulté à trouver un nouveau bloc. La difficulté est ajustée périodiquement en fonction de la puissance de hachage déployée par le réseau de mineurs.

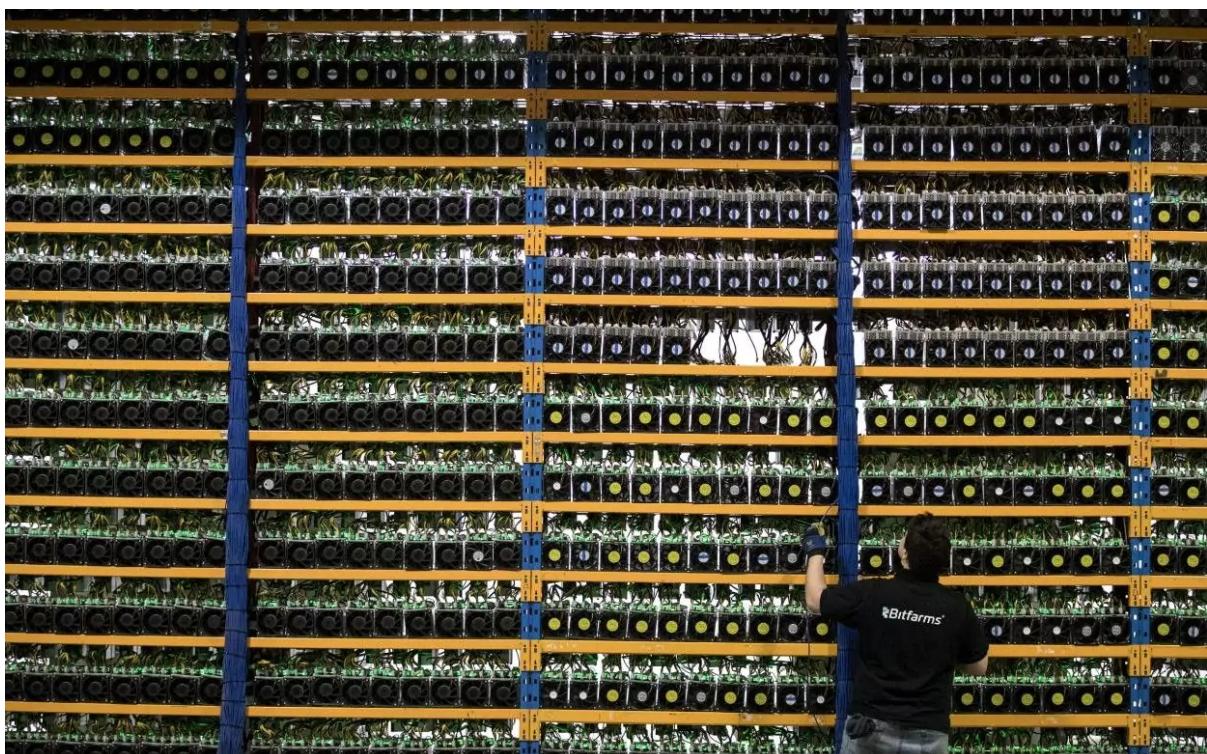
Source: blockchain.com

La mise en concurrence est la méthode utilisée pour motiver à la certification, ainsi le premier **mineur** à valider un nouveau bloc sera récompensé.

Concernant le bitcoin, la tâche de certification était à l'origine accessible par les particuliers grâce à l'utilisation des cartes graphiques, dont la puissance pour le type de calcul nécessaire à la certification était supérieure.

Depuis, des mineurs spécifiques sont apparus pour réaliser la preuve de travail et les cartes graphiques grand-public sont délaissés car non compétitives.

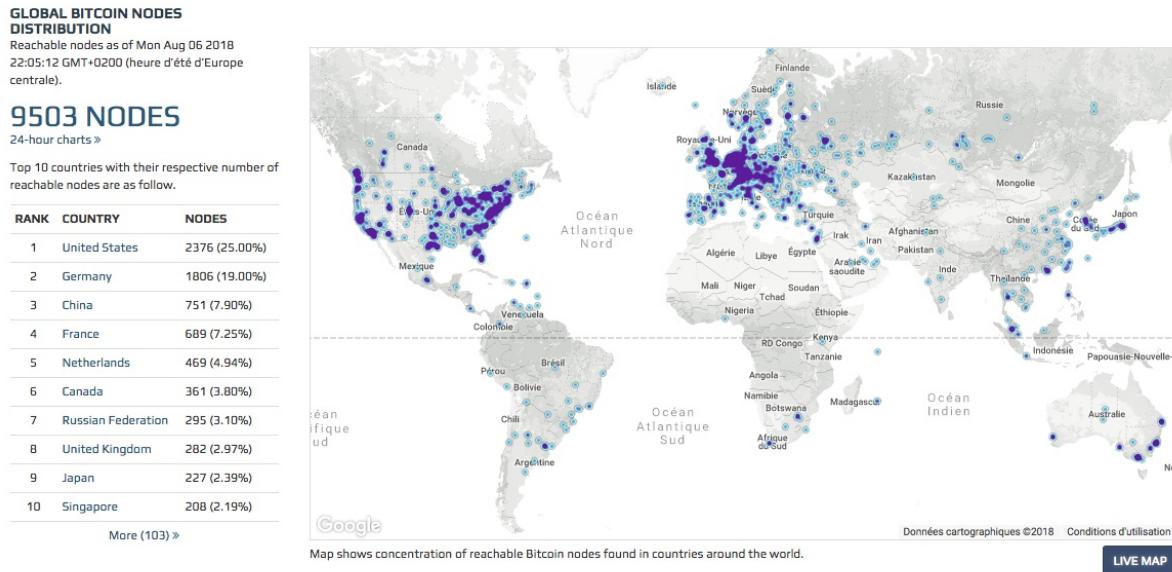
Car plus la taille des chaînes augmente, plus la puissance de calcul doit augmenter. Cette relation d'interdépendance a chassé les particuliers de la course à la certification et ce sont désormais des institutions qui ont pris le relais.



La ferme de calcul bitfarms

Source: bitfarms.io

En août 2018, il y avait 9 503 nœuds de traitement de la blockchain Bitcoin dans le monde.



Global bitcoin nodes distribution

Source: bitnodes.earn.com

Les services de [mining](#) sont disponibles dans le cloud à travers le [cloud-mining](#), ce qui reste néanmoins un modèle plus orienté vers les entreprises ou les grandes organisations que vers les particuliers.

Concernant la preuve de l'Enjeu:

De l'anglais [proof-of-stake](#). Abrégé PoS.

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

La preuve de l'enjeu est un algorithme différent de la preuve de travail permettant d'obtenir un consensus distribué.

Dans les crypto-monnaies basées sur les preuves d'enjeux, le créateur du bloc suivant est choisi par divers critères (ex. : combinaisons de sélection aléatoire, richesse ou âge). Ces critères dépendent de l'enjeu économique d'un validateur dans le réseau.

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).

Dans les chaînes de blocs publiques basées sur les preuves d'enjeux (par exemple, l'implémentation prochaine de Casper d'[Ethereum](#)), 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 de sa mise).

Les avantages significatifs de la méthode par la preuve de l'enjeu comprennent la sécurité, la réduction des risques de centralisation et l'efficacité énergétique.

Il existe deux types d'algorithmes de preuve par l'enjeu:

- Preuve en chaîne de l'enjeu:

Dans la preuve basée sur la chaîne, l'algorithme choisit un validateur au hasard pendant chaque tranche de temps (Ex: toutes les dix secondes), et assigne à ce validateur le droit de créer un bloc unique, et ce bloc doit pointer vers un bloc précédent (normalement le bloc se situant à la fin de la chaîne la plus longue). Ainsi on observe dans le temps une croissance en une chaîne unique.

- Preuve de l'enjeu de type Byzantine-Fault-Tolerant (BFT): Dans la preuve de mise de type BFT, l'attribution se fait au hasard et le validateur se voit doté du droit de proposer des blocs. L'accord sur les blocs canoniques se fait à travers un consensus à plusieurs tours où chaque validateur vote pour un bloc spécifique. À la fin de ce processus, un accord est conclu entre tous les validateurs sur l'appartenance d'un bloc à la chaîne ou son rejet.

Avantages de la preuve de l'enjeu par rapport à la preuve de travail:

La preuve de l'enjeu apporte un avantage indéniable par rapport à la preuve de travail : la quantité d'électricité nécessaire pour sécuriser une chaîne de blocs est réduite.

Le coût du mécanisme de Bitcoin et d'[Ethereum](#) est estimé à plus d'un millions de dollars en électricité et en matériel informatique par jour. Le sujet est donc crucial pour le développement futur de la blockchain.

(Voir [Quid de ses impacts énergétiques](#))

Une plus faible consommation en matière première implique un besoin moindre de motivation, et donc un coût par transaction plus faible et une meilleure participation du réseau.

Cela ouvre la porte à une meilleure régulation des dérives qui peuvent toucher la blockchain comme le phénomène du [mineur égoïste](#) ou les activités des cartels qui tentent de centraliser la blockchain.

La preuve de l'enjeu introduit une réduction des risques de centralisation. Le fait de sélectionner aléatoirement un validateur limite l'intérêt de développer de grandes infrastructures et permet à de petits acteurs de subsister.

Un avantage annexe à l'utilisation d'une validation par preuve de l'enjeu est l'augmentation du coût d'une «attaque des 51%» de manière spectaculaire par rapport à la méthode de la preuve de travail. Ainsi la sécurité de la blockchain est renforcée.

«C'est comme si votre ferme ASIC brûlait si vous participiez à une attaque des 51%».

Vlad Zamfir, [Ethereum](#) Foundation researcher

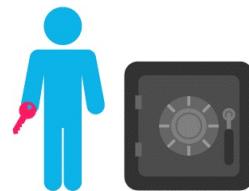
Infographie comparative des deux méthodes:



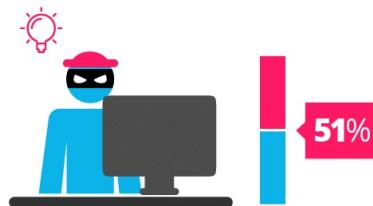
Proof of Work vs Proof of Stake



proof of work is a requirement to define an expensive computer calculation, also called mining



Proof of stake, the creator of a new block is chosen in a deterministic way, depending on its wealth, also defined as stake.



A reward is given to the first miner who solves each blocks problem.



The PoS system there is no block reward, so, the miners take the transaction fees.



Network miners compete to be the first to find a solution for the mathematical problem



Proof of Stake currencies can be several thousand times more cost effective.

La méthode de validation par preuve de l'enjeu offre des avantages indéniables sur les méthodes actuellement utilisées, meilleure sécurité, moindre consommation, plus grande décentralisation. Malheureusement les méthodes de validation alternatives sont encore au stade de développement. Les différents problèmes de taille et de fréquence d'ajout des blocks, de finalité du minage et de la concentration des capacités de minages sont autant de challenges que les développeurs devront résoudre afin que ces méthodes puissent être considérées comme des alternatives viables.

Blockchain privée vs blockchain publique

	Blockchain publique	Blockchain privée
 Usage	Gérer des traces simples (hash). Au-delà est moins pertinent compte tenu de son coût de manipulation des données et de ses limites dans la gestion de la confidentialité.	Gérer des échanges plus riches que de simples traces. L'absence de frais de transaction permet une taille des données stockées plus importante. La gestion des droits d'accès et de la confidentialité peut être davantage maîtrisée.
 Sécurité	Plus il y a d'utilisateurs, plus la sécurité est garantie. Généralement, le consensus est garanti par la preuve de travail.	Seuls les nœuds validateurs sont autorisés à valider une transaction. Un consensus de n% (par ex 2/3) des membres validateurs est requis.
 Confidentialité	Les données transitent de manière transparente. Sauf divulgation, les détenteurs des adresses sont anonymes.	Seuls les acteurs autorisés ont accès aux transactions.
 Scalabilité	Entre 3 et 7 transactions par seconde mais une transaction peut contenir plusieurs milliers de hash .	1 000 transactions par seconde, voire plus.
 Accessibilité	«Permissionless»: comme internet, accessible à tous.	Accès aux membres du consortium uniquement.

Comparatif blockchain privée et publique

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

Gestion de l'identification et confidentialité

Sur la blockchain Bitcoin et Ethereum (avant 2017), l'identification d'un utilisateur peut être découverte. Elle n'assure donc pas l'impératif de confidentialité requis pour un vote à bulletin secret.

En effet, la nature de la chaîne de blocs publique signifie que chaque transaction qui a lieu sera publiée et liée à une publication d'une clé cryptographique publique. Cette clé est chiffrée pour qu'une personne qui regarderait l'historique de la chaîne de blocs ne soit en mesure d'identifier l'identification réelle de l'individu derrière cette clé.

Cet anonymat pourrait être préservé si cette clé publique était utilisée une seule fois. Mais si cette clé est utilisée plusieurs fois, il est possible de déterminer qu'un même individu se cache derrière cette clé publique.

Public key/Private key on a bitcoin transaction

B = Bitcoin

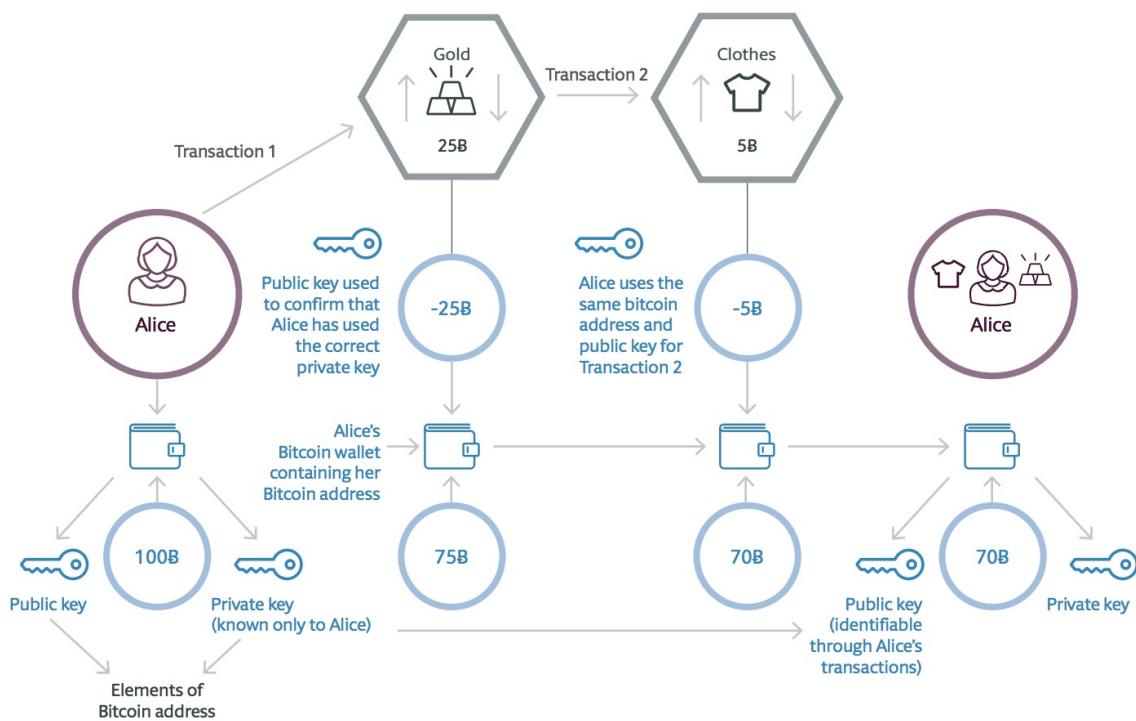


Schéma démontrant la possibilité de relier un utilisateur à de multiples transactions sur la blockchain Bitcoin

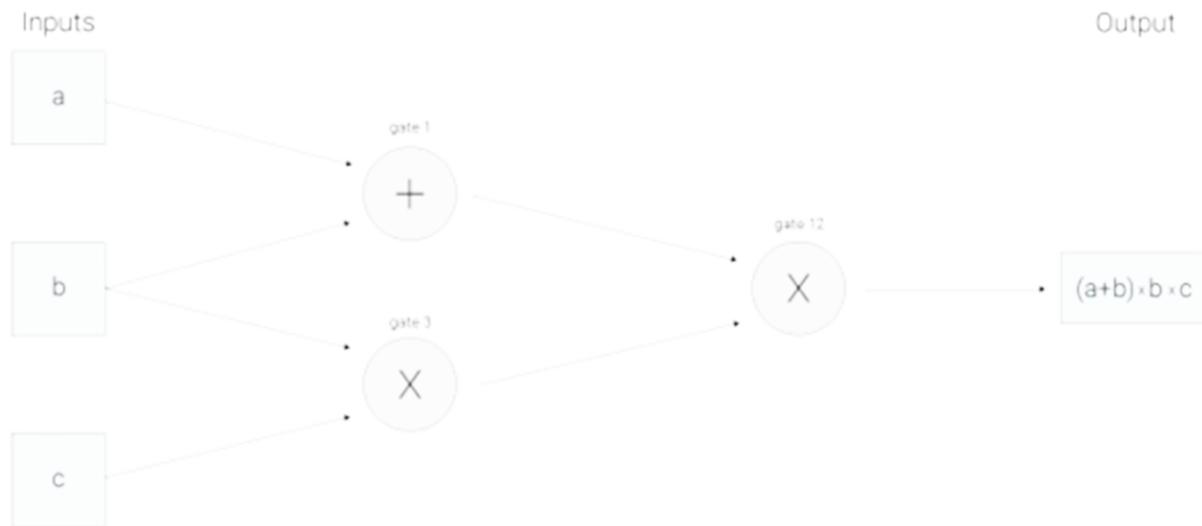
Bien entendu, l'objectif de la clé publique est de distinguer un utilisateur d'un autre sur le réseau pour s'assurer que la transaction est attribuée au bon auteur.

Une solution à ce problème est d'utiliser la méthode de preuve à divulgation nulle de connaissance (Zero knowledge proof ou ZKP).

La forme la plus répandue à l'heure actuelle est zk-SNARKs (zero-knowledge Succinct Non-Interactive ARgument of Knowledge), présente nativement sur Ethereum depuis la mise à jour Metropolis (Byzantium Fork) le 12 octobre 2017 et présente depuis l'origine sur Zcash. On trouve également une autre forme de ZKP sur la blockchain Monero, qui implémente un système de signature de cercle: Monero Ring Confidential Transactions (RingCT).

Afin d'avoir une «vie privée sans connaissance» dans Zcash, la fonction déterminant la validité d'une transaction selon les règles consensuelles du réseau doit retourner la réponse sur la validité ou non de la transaction, sans révéler aucune information des calculs effectués sur cette dernière. Cela se fait en codant certaines des règles de consensus du réseau dans zk-SNARKs.

À un niveau élevé, les zk-SNARKs fonctionnent en transformant d'abord ce que vous voulez prouver en une forme équivalente sur la connaissance d'une solution à certaines équations algébriques.



Démonstration du circuit arithmétique pour calculer $(a+b)(bc)$ à l'aide de zk-SNARKS

Source: [Zcash à propos de zk-SNARKS](#)

En regardant un tel circuit, on peut considérer les valeurs d'entrée a, b, c comme «se déplaçant» de gauche à droite sur les fils vers le fil de sortie. L'étape suivante consiste à construire ce qu'on appelle un système de contraintes de rang 1, ou R1CS (Rank 1 Constraint System), pour vérifier que les valeurs se déplacent «correctement». Dans cet exemple, le R1CS confirmera, par exemple, que la valeur qui sort de la porte de multiplication où b et c sont entrés est $b*c$.

Dans cette représentation R1CS, le vérificateur doit vérifier de nombreuses contraintes - une pour presque tous les fils du circuit. Cette méthode utilise une représentation du circuit appelée Programme arithmétique quadratique (QAP). La seule contrainte qui doit être vérifiée est maintenant entre les polynômes plutôt qu'entre les nombres. Les polynômes peuvent être assez grands, mais ce n'est pas grave, car lorsqu'une identité ne tient pas entre les polynômes, elle ne tiendra pas à la plupart des points. Par conséquent, il suffit de vérifier que les deux polynômes correspondent à un point choisi au hasard afin de vérifier correctement la preuve avec une probabilité élevée.

Concrètement, cela signifie qu'il est possible d'obtenir une transaction sans partager d'informations.

Pour mieux comprendre le fonctionnement en pratique de zk-SNARKS, observons un exemple de «comment Alice peut transférer de l'argent d'un de ses comptes bancaires à un autre, sans fournir à Bob de la banque Acme des informations pour garantir son identité».

Nous devrons pour ce scénario disposer de quatre entités:

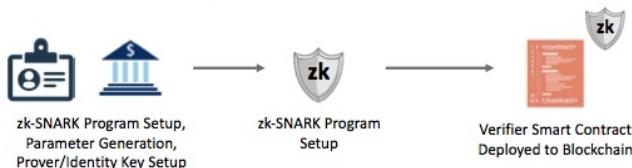
- Alice—un individu qui désire prouver son identité sans la transmettre
- Acme Bank—[Tiers de confiance](#) pour les attestations de compte bancaire, et un [tiers de confiance](#) pour l'installation de zk-SNARK.
- Bob—Représentant du centre d'appels d'Acme Bank
- Solution d'identité autosouveraine - Fournisseur de données d'identité numérique à Acme Bank App, et un [tiers de confiance](#) pour l'installation de zk-SNARK.

Alice calls Bob using Prior Authentication Feature (zk-SNARK)

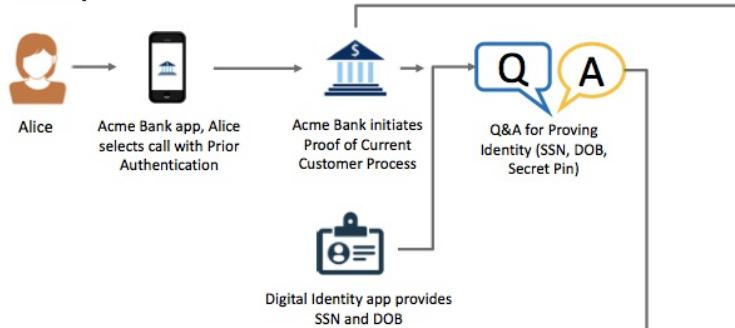
1 Create a smart contract enabled blockchain



2 Setup a zk-SNARK program and verifier smart contracts



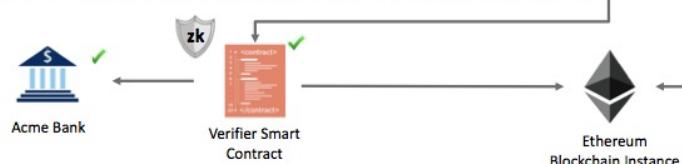
3 Alice opens Acme Bank app and logs in, Acme Bank proves Alice's account status, and Alice answers questions to authenticate her identity



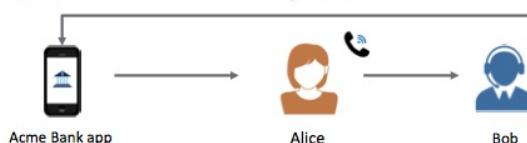
4 Proof created and sent to smart contract for verification. Acme Bank sends Proof of Current Customer transaction to blockchain



5 Smart contract verifies zero-knowledge proof sent from Alice's phone, Acme reads updated contract and sees proof accepted



6 Alice calls Acme Bank without needing to confirm her identity to Bob, and then initiates the money transfer



Pour réaliser cette opération d'authentification, le recours à une tierce partie «ACME BANK» est nécessaire : celle-ci va authentifier Alice grâce à une application tierce et retourner la valeur vraie si Alice est bien la personne qu'elle prétend être.

L'intérêt de ce système est que ni la Banque, ni Bob ne disposent des informations d'identification d'Alice, de même que la tierce partie n'a aucune idée de la nature de l'opération entre la Banque et Alice. Il y a donc un parfait cloisonnement entre les opérations effectuées et l'authentification.

Quid de la sécurité de la blockchain ?

Les garanties de la blockchain en matière de sécurité:

Il n'existe pas de technologie sûre dans la mesure où la sécurité et la sureté sont un idéal, pas un absolu. Mais il est possible de s'approcher de cet idéal, on peut d'ailleurs considérer que la blockchain répond à ces impératifs dans la mesure où elle assure les points suivants:

- La disponibilité: Les données étant distribuées et décentralisées, elles sont disponibles tant qu'un nœud est en mesure de transmettre le registre.
- L'intégrité: le mécanisme de consensus est conçu pour permettre aux informations d'être intégrées et conservées sans que celles-ci ne soient altérées. Le pré-requis à cette disposition est qu'un nombre suffisant de nœud soit connecté au réseau et que les conditions permettant une attaque des 51% ne soient pas atteintes.
- La confidentialité: La confidentialité est un point complexe concernant la blockchain puisque les données sont disponibles publiquement pour garantir la transparence.

Néanmoins cette confidentialité peut être rendue possible par l'implémentation d'un système de [preuve à divulgation nulle de connaissance](#). Les protocoles sans connaissance permettent le transfert de ressources à travers un réseau distribué, peer-to-peer blockchain, en toute confidentialité. Dans les transactions régulières en chaîne de blocs, lorsqu'un actif est envoyé d'une partie à l'autre, les détails de cette transaction sont visibles pour toutes les autres parties du réseau. En revanche, dans une transaction sans connaissance, les autres parties ne savent pas qu'une transaction valable a eu lieu, mais aucune information sur l'émetteur, le destinataire, la catégorie d'immobilisations et la quantité n'est divulguée. [Voir Gestion de l'identification et confidentialité](#)

- La traçabilité: Parce qu'elle est basée sur un empilement de blocs cryptographique, la blockchain permet d'enregistrer l'intégralité des transactions et de remonter au bloc zéro, assurant la meilleure des traçabilités.
- L'authentification: Pour s'assurer de la bonne identité d'une transaction, l'émetteur signe celle-ci à l'aide de sa clé privée qui «tant qu'elle n'est pas connue assure la véracité de la transaction».
- La non-répudiation et l'imputation: Par le biais de la validation basée sur le consensus, la blockchain permet nativement la non-répudiation des données. Quant à l'imputation, chaque [mineur](#) certifiant une transaction est authentifié sur le réseau, il est donc possible d'identifier un [mineur fautif](#) et de le disqualifier.

Les menaces qui pèsent sur la blockchain en matière de sécurité:

Selon Patricia Egger et Dusko Karaklajic dans *La sécurité du blockchain*, des menaces pèsent sur l'écosystème naissant en raison de l'immaturité et la complexité de la technologie.

En effet, les nombreux algorithmes de consensus disponibles, les types de blockchain et protocoles cryptographiques complexes sous-jacents rendent la technologie difficile à appréhender.

L'absence de normes et de réglementations sur la technologie du blockchain constitue également un risque. Ces vides juridiques sont un terreau fertile au piratage et à la manipulation frauduleuse rendent la technologie encore peu crédible pour des usages sérieux.

Le risque le plus important demeure la croyance dans la sécurisation absolue autour de la blockchain bien qu'elle repose sur des mécanismes cryptographie fiables et éprouvés. Cette sécurisation ne sera jamais complète par nature: les protocoles cryptographiques ont leurs limites et la sécurité globale intègre également les éléments

périphériques, le risque humain est ainsi toujours présent. En ce dernier point, la blockchain apporte une nouvelle manière de traiter certaines données mais n'affranchit pas des démarches classiques en matière de sécurité des systèmes d'informations.

En outre la blockchain est sensible à des attaques particulières, comme l'attaque de type Goldfinger.

Attaque des 51% ou attaque Goldfinger

Une attaque des 51% cible les blockchains basée sur la preuve de travail et preuve de l'enjeu.

Le but de cette attaque est d'empêcher les validations des transactions et de paralyser le réseau, ou de manipuler l'historique pour valider deux fois une transaction sans pour autant que la dépense ne soit effective.

La validation des blockchains se fait grâce aux minages.

Afin de se garantir une rémunération dans le cadre d'une blockchain fonctionnant sous la méthode de la preuve de travail, les mineurs se constituent en groupe (ou pools), de façon à disposer d'une puissance supérieure et de mutualiser les coûts. Ils partagent alors les efforts ainsi que les gains.

Mais le danger d'un groupe disposant d'une puissance trop importante est qu'il peut réaliser une attaque des 51%.

En effet l'un des principes fondateurs de la blockchain est que le calcul est distribué entre tous les nœuds où le calcul est validé par la méthode de consensus. Ainsi si un seul individu introduit une erreur de calcul volontairement ou falacieusement, les autres mineurs vont automatiquement disqualifier son travail et son bloc va demeurer orphelin et ne sera jamais intégré. Ainsi seul, il ne peut pas nuire.

Lorsqu'un groupe de **mineur** dispose d'au moins 51% des capacités de calcul, il devient possible en théorie, d'outrepasser le mécanisme de consensus et donc d'imposer des blocs fallacieux qui seront ajoutés au registre officiel. Dès lors si un groupe devient trop puissant, il est en capacité de définir quelles informations sont légitimes au sein d'une blockchain.

L'exemple de la 'double dépense'

En imaginant qu'un groupe dispose de plus de 51% de la puissance totale, il peut alors procéder à une manipulation frauduleuse du registre appelée le *hack de la double dépense*.

Ce hack consiste à effectuer des transactions entre deux comptes. Il effectue un débit du premier compte vers le second, et disposant de la puissance nécessaire pour manipuler la blockchain, efface la transaction. Pour ce faire il suffit de ne pas inclure la transaction dans les blocs minés, et attendre qu'une blockchain plus longue que la blockchain courante vienne la remplacer.

Une fois la transaction effacée du registre distribué, le second compte apparaît comme n'ayant jamais été débité tant que le second a bien reçu la somme. Il s'agit d'une création de monnaie ex-nihilo des unités de crypto-monnaie.

Une telle opération entraînera rapidement la chute du cours de la cryptomonnaie. Le groupe menant des activités frauduleuses devra alors rapidement convertir ses actifs dans une monnaie courante comme l'euro ou le dollar, ce qui accélérera la chute du cours.

L'opération est facilitée par le biais de moyens automatisés.

Cette attaque est inenvisageable sur des blockchains bien installée comme le Bitcoin, en raison du coût que représente une telle opération, du moins une telle approche est inaccessible pour une entreprise privée, mais pas d'un État voyou, qui dispose des budgets nécessaires et peut avoir comme motivation de perturber une blockchain concurrente ou occasionnant un trouble.

À l'inverse, sur des blockchains ayant une faible capacité de minage (récente ou de petite taille), cette attaque est facilement envisageable.

Dans ce dernier cas, une puissance de calcul faible, dont pourrait disposer une organisation lambda suffirait à réaliser l'attaque.

Les blockchains récemment créées sont donc dans une position d'extrême vulnérabilité.

Les objectifs d'une attaque des 51%

- Fraude des registres et disparition des transactions:

Dans le cadre d'une blockchain privée, par exemple permettant l'implémentation du vote ou permettant la traçabilité alimentaire, cela permettrait de falsifier les informations.

Dans le cas d'une cryptomonnaie, cela permet la double dépense, qui permet à la fois de s'enrichir et de déstabiliser le cours de la monnaie.

- Rompre le lien de confiance:

Les blockchains de par leur fonctionnement décentralisé posent des problématiques de gouvernance et sont perçues comme une menace par certains états ou institutions. C'est pourquoi perturber le fonctionnement de ces blockchains permet d'aliéner le lien de confiance des utilisateurs envers la blockchain.

Résilience des blockchains à l'attaque

Le système des crypto-monnaies est conçu pour être résilient aux attaques des 51%, lorsqu'une telle attaque est constatée. Un patch peut être déployé et limite les dégâts causés par l'attaque.

Coûts estimés d'une attaque au 51%

Les coûts pour réaliser une attaque des 51% varie en fonction de l'échelle de la blockchain visée.

Concernant le Bitcoin diverses estimations ont été réalisées par Jean-Paul Delahaye dans L'attaque Goldfinger d'une blockchain.

À l'aide de ses calculs, on peut estimer le coût en mai 2017 à 878 millions de dollars.

En comparaison le budget de l'État Français est de 400 milliards d'euros par an, celui d'une agence gouvernementale comme la NSA est de 45 milliards de dollars.

L'attaque est donc inaccessible à une institution lambda.

Stratégie du mineur égoïste

L'exemple du mineur égoïste est explicité dans Les risques des blockchains, par Laurent Dehouck, Maître de conférences en sciences de gestion, ENS Rennes et Audrey Thomas, ENSAM.

Lorsqu'une transaction a lieu, le **mineur** qui découvre la solution en premier dispose d'un bloc Be.

Ce bloc est censé être communiqué aux autres nœuds afin d'être intégré dans la blockchain.

Mais ce **mineur**, malhonnête, peut garder ce bloc secret et travailler de suite à la validation du bloc suivant.

Dès l'instant qu'un autre **mineur** «honnête» valide un bloc Bh, il souhaite le diffuser aux autres nœuds.

Le **mineur** malhonnête va alors diffuser son bloc Be. Le réseau se retrouve ainsi en présence de deux blocs validés presque en même temps et temporairement conservés sur la blockchain.

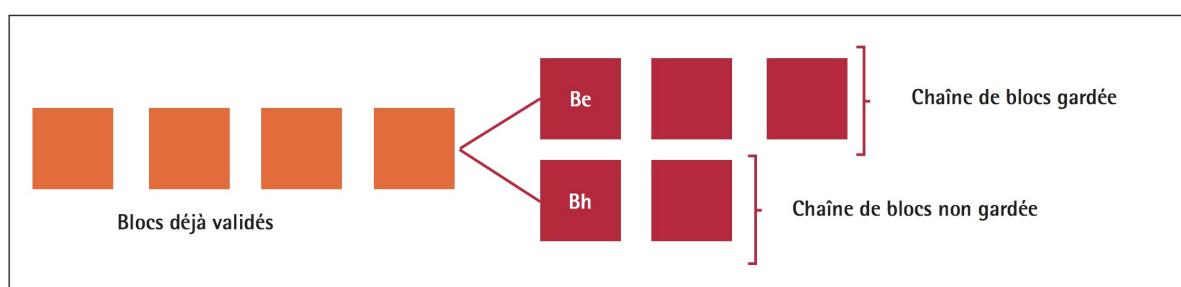
Certains nœuds du réseau auront connaissance du bloc Be et d'autres auront connaissances du bloc Bh.

Des nouveaux blocs vont alors s'ajouter à la suite de Be et Bh.

Pour le **mineur** malhonnête, l'avantage demeure dans l'acte de ne pas divulguer le bloc Be. Cela lui donne un avantage stratégique vis-à-vis du reste des utilisateurs du réseau pour la recherche de la solution suivante, car chaque bloc validé est relié aux blocs précédents.

La création simultanée de deux blocs provoque ce qu'on appelle une «bifurcation», dès lors la chaîne contenant sera conservée car la chaîne contenant le bloc Be sera plus longue.

Le **mineur** malhonnête disqualifie ses concurrents en les faisant travailler à perte, leurs rendements s'effondrant rapidement.



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

Ce genre de stratégie invite à repenser la question de la normalisation de la blockchain et les techniques de consensus pour se prémunir contre ces pratiques délétères.

Quid de ses impacts énergétiques ?

Selon un [rapport de l'Office parlementaire d'évaluation des choix scientifiques](#), la consommation du Bitcoin est d'au moins 24 TWh/an, soit la production totale annuelle de 3 réacteurs nucléaires du Palier CP0 et CPY (soit les plus anciens en France) dont la production avoisine les 8 TWh.

Celle des blockchains publiques (dont fait partie le Bitcoin) serait comprise 46,5 TWh/an et 200TWh/an selon les estimations.

En comparaison, la consommation énergétique annuelle de la France est de 530 TWh/an. La blockchain représenterait donc entre 8,68% et 37,74% des dépenses énergétiques Françaises si les fermes de minages étaient implantées sur le sol Français en exclusivité. Or, 60 % des fermes de minages sont situées en Chine dont la production énergétique provient majoritairement du charbon. Il y a là une problématique écologique majeure qui porte un préjudice considérable au développement de la technologie blockchain.

Par ailleurs, Bitcoin opère aujourd'hui environ 80 transactions par minute, quand Visa et Mastercard en exécutent respectivement près de 100 000. Ce coût énergétique est donc faramineux lorsqu'il est comparé à d'autres alternatives centralisées. Cette comparaison est d'autant plus choquante lorsque la majorité des ressources sont gaspillées durant le processus de vérification de blocs non-valides.

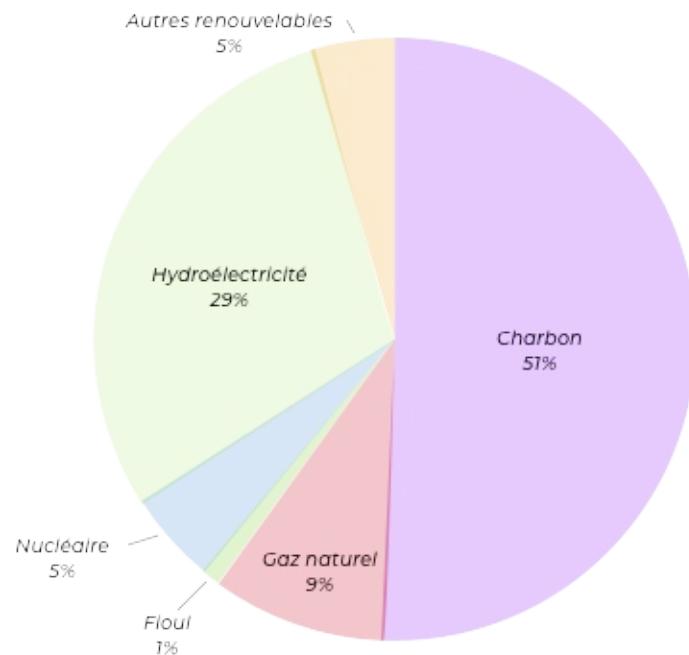
Ces chiffres sont à manipuler avec prudence car l'estimation de la consommation énergétique des blockchains n'est pas fiable, le matériel évoluant en permanence et les mineurs se gardant bien de communiquer sur leur consommation électrique.

En Islande, Genesis [Mining](#) indiquait en 2015 dans Business Insider, qu'elle constituait l'une des entreprises les plus énergivores de l'île, avec une dépense d'électricité de l'ordre de 60 dollars par bitcoin «extrait». Soit au cours actuel du bitcoin, une rémunération de 6243,99 dollars par bitcoin extrait.



Le mix énergétique de la production du Bitcoin révèle une utilisation massive des énergies fossiles. Mais également d'Hydroélectrique, renouvelable.

Mix d'énergies primaires à la production énergétique consommée par le minage



| Source: Energie Sia Partners

Vers une normalisation ?

10% du PIB mondial en 2025 proviendra d'activités utilisant la blockchain.

Ravi Jhawar, le responsable du projet au sein du GIE de l'Anec

Une régulation par la normalisation

Le Luxembourg, par le biais de l'Ilnas, participe à la création d'une norme technique internationale pour encadrer la blockchain.

Dans un [livre blanc](#), l'organisation espère initier une démarche et s'imposer comme un acteur de la régulation à travers une norme ISO.

L'objectif est d'encadrer la gouvernance des blockchains afin de peser dans les enjeux économiques et écologiques qui la concernent.

Cette normalisation se confronte à la volonté d'indépendance et de décentralisation, base fondatrice des technologies blockchains.

Néanmoins la mise en place d'une norme peut impliquer une meilleure régulation énergétique en imposant par exemple l'origine renouvelable de l'électricité nécessaire au fonctionnement de la technologie.

La standardisation pour lutter contre la consommation et l'obsolescence des moyens de productions.

Le terrain de réduction de la consommation énergétique de la blockchain se dessine lorsque l'on évoque la standardisation ou la normalisation.

Il s'agit de la standardisation des algorithmes et celui du matériel polyvalent.

Ces deux directions d'optimisation ne sont en fait qu'une seule et même voie: un standard algorithmique signifie un matériel dédié adapté, et donc une optimisation plus importante car les investissements de Recherche & Développement seraient focalisés sur un seul type de matériel.

Les blockchains fonctionnant sur la méthode de preuve de travail ont en commun l'utilisation d'un algorithme de hachage. Celui de Bitcoin est nommé Hashcash.

En recherchant un algorithme plus économique pour remplir cette fonction, la blockchain pourrait voir son coût écologique se réduire et se présenter comme une alternative viable à grande échelle.

Afin de miner, les individus ou institutions mettent à disposition du matériel pour réaliser des calculs.

Sur certaines blockchains, comme bitcoin, il est inutile et non-rentable de s'essayer à la chose avec du matériel classique.

Ce mode de calcul est réservé à des blockchains plus récentes ou bénéficiant de moins d'engouement.

Les mineurs professionnels ont recours à du matériel performant, qui exclut les mineurs amateurs de la course à la rémunération, dans le cadre de la preuve de travail seulement. Ceux-ci sont en effet bien trop lents pour valider les transactions face à ces sprinteurs.

Le minage est divisé entre deux technologies, les puces dédiées: FPGA / ASICS et les puces généralistes CPU / GPU.

Explication des acronymes:

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

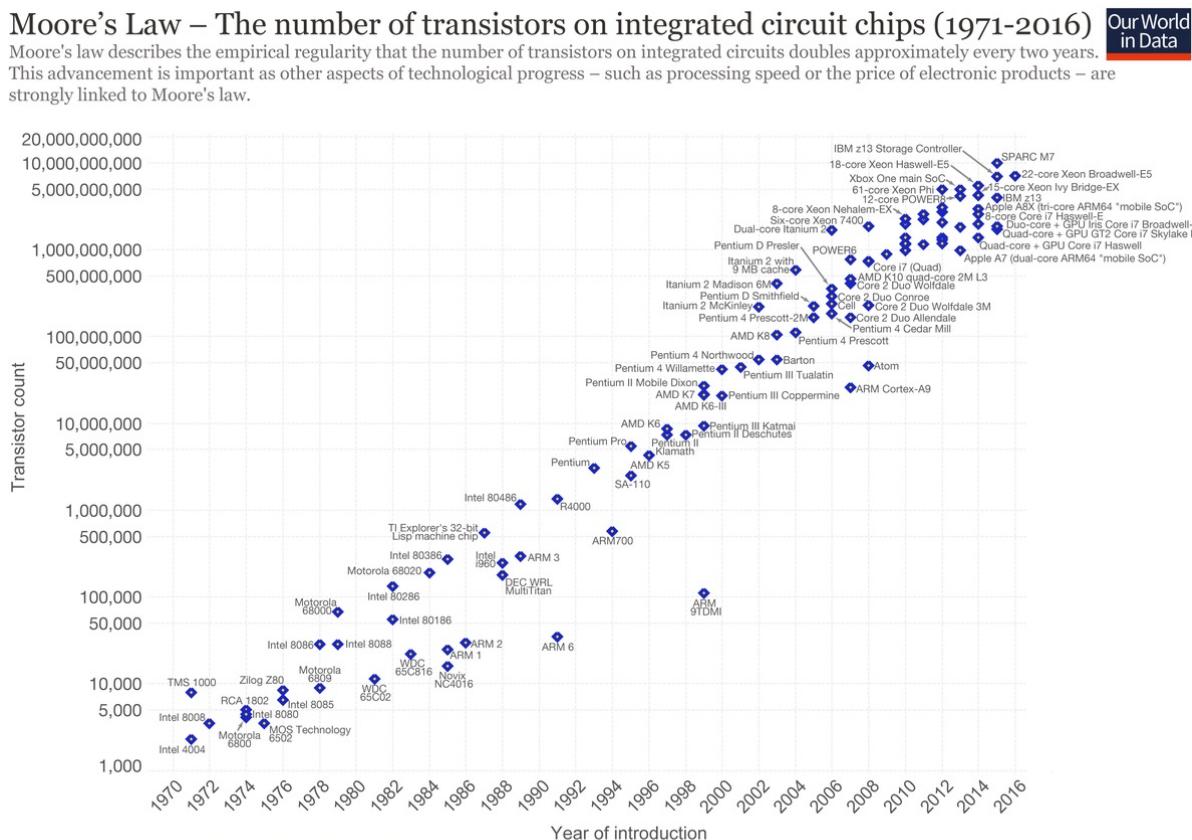
Les premières ne sont utilisées que dans le calcul cryptographique dans le cadre de la blockchain, les secondes trouvent une utilisation dans les opérations courantes.

Les mineurs ASICS ET FPGA sont majoritairement utilisées dans le calcul SHA256 (Bitcoin), tandis que les CPU / GPU sont plutôt utilisés sur des cryptomonnaies plus récentes.

Afin de maintenir la complexité de calcul au sein d'une blockchain, la difficulté doit augmenter au fil des avancées technologiques.

Lorsqu'on observe les capacités des puces de calculs, on constate une augmentation significative de leur puissance. Ainsi, réaliser un calcul cryptographique considéré comme complexe dans les années 80 prend quelques secondes avec un téléphone portable actuel.

Ce schéma présente l'augmentation de la puissance de calcul des puces CPU.



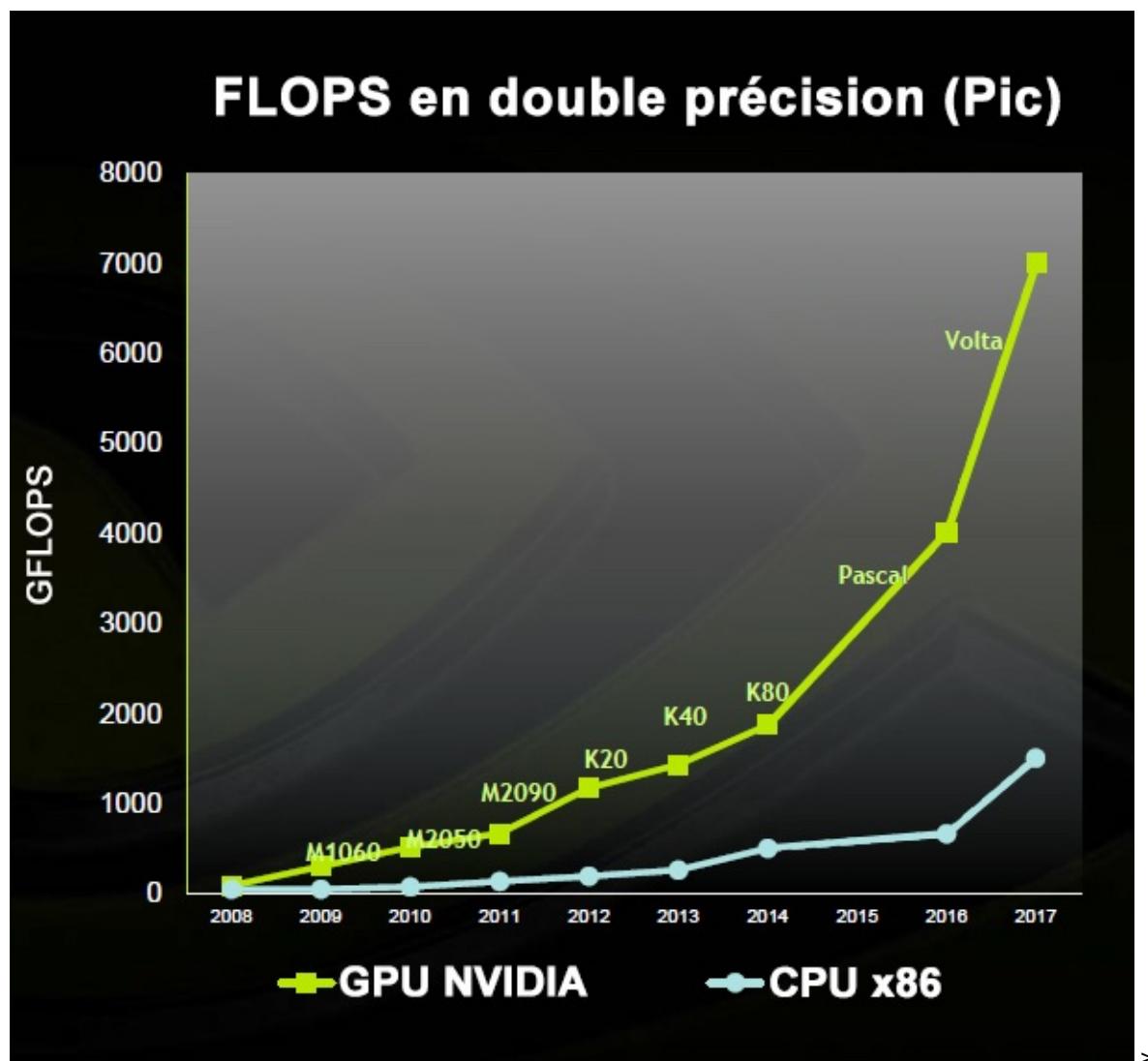
Data source: Wikipedia (https://en.wikipedia.org/wiki/Transistor_count)
The data visualization is available at OurWorldInData.org. There you find more visualizations and research on this topic.

Licensed under CC-BY-SA by the author Max Roser.

3

Evolution de la puissance de calcul des ordinateurs et de la complexité du matériel informatique selon les conjectures de Moore

Lorsque l'on compare l'augmentation de la puissance de calcul des GPUs par rapport aux CPUs, on imagine aisément le bond de complexité que les algorithmes ont subis.



Comparaison entre le nombre d'opérations en virgule flottante par seconde (FLOPS) des CPUs (architecture X86) et les GPUs NVIDIA

Sur cette dernière illustration, nous pouvons constater que la puissance de calcul des GPUs sur certaines opérations est spéctaculairement plus importante que les CPUs, or, dans le cadre de la blockchain, les mineurs ASICS ET FPGA sont bien plus performants que les GPUs.

D'autres contraintes reposent également sur le choix du matériel, c'est ainsi que certains algorithmes nécessitant une importante utilisation de la mémoire rendaient les mineurs ASICS peu compétitif car les composants mémoires sont particulièrement couteux.

Mais 2017 a marqué un tournant dans l'utilisation de ces cartes avec une amélioration substantielle de ces modules mémoires. La solution pour maintenir la complexité fut de modifier les algorithmes, rendant le matériel obsolète car les fonctions d'un [mineur](#) ASICS sont gravées à même le silicium. On parle alors de fonctions câblées.

Ces fonctions câblées se retrouvent dans d'autres architectures de puces, comme les GPUs.

Un coût économique et écologique important pour garantir la sécurité et la scalabilité de ces blockchains.

Pour comprendre pourquoi les puces sont rendues obsolètes, il faut intégrer que la différence entre un CPU et un ASIC (ou entre un CPU et un GPU) réside dans le fait que le CPU est une puce programmable, et doté d'une grande polyvalence dans son utilisation au prix néanmoins d'une performance moindre.

Un GPU ou un ASIC est une puce spécialisée, dont les performances sont excellentes dans l'accomplissement des tâches pour lesquels elle est programmée, mais qui sont plus réduites en nombre que pour un CPU.

Par exemple, pour un GPU spécialisé dans la représentation graphique, l'affichage d'un maillage 3D texturé à 60-100 frames par seconde.

Cette performance permet d'obtenir des meilleures performances en termes de calcul brut sur ces tâches précises, mais également une consommation électrique plus faible.

Cette amélioration de performance est rendue possible par le fait de graver directement dans le silicium de la puce les fonctions nécessaires à la translation, rotation etc. On appelle cela «câbler» les fonctions.

Pour un [mineur](#) ASIC, cette spécialisation se traduira dans une performance inégalable dans la résolution d'un algorithme de chiffrement par exemple. Mais il n'est pas possible d'utiliser un ASIC spécialisé dans le calcul de hashs SHA256 pour du KECCAK et inversement.

Dans ces tendances, une solution intermédiaire a vu le jour et exploite le meilleur des deux mondes: le FPGA.

Le FPGA.

Les FPGA (Field-Programmable Gate Array) sont des circuits intégrés en silicium reprogrammables.

Reprogrammer un FPGA consiste à redéfinir le circuit intégré lui-même pour implémenter la fonctionnalité souhaitée, au lieu d'exécuter une application logicielle.

On peut voir le FPGA comme une puce qui simule au plus bas niveau une puce spécialisée.

Les FPGA sont particulièrement utilisés pour simuler un [mineur](#) ASIC dans la phase de préproduction afin de tester le modèle et ajuster les schémas logiques. Lorsque le fonctionnement est jugé suffisant, le schéma est alors figé pour produire un [mineur](#) ASIC.

Les mineurs FPGA offrent des performances légèrement moindres que les mineurs ASICS. On note aussi que la logique de programmation d'un fpga nécessite des compétences poussées et peu répandues.

Malgré ces désavantages, des cartes FPGA aux capacités de calcul titaniques sont en train de se développer pour répondre aux besoins du machine-learning et du deep-learning.

Ces cartes permettent d'envisager une continuité d'utilisation future malgré les bifurcations (forks) et les évolutions des algorithmes, ce qui permet de limiter les coûts et de limiter l'impact écologique dû à l'obsolescence du matériel.

La normalisation par le câblage de fonctions

Pour comprendre comment des cartes dédiées à la blockchain pourraient voir le jour, il faut revenir en arrière dans l'histoire de l'informatique. À l'origine seuls les CPUs effectuaient des calculs attenant à la 3D. Puis vinrent les GPU, dont les fonctions câblées permettaient des performances plus grandes. Il est tout à fait envisageable de câbler les fonctions nécessaires aux algorithmes implantés dans la blockchain, à la manière des Physics Processing Unit qui implétaient une carte supplémentaire pour la gestion de la physique et qui sont depuis intégrés aux cartes graphiques Nvidia.

À l'heure actuelle, les blockchains sont optimisées en fonction du matériel disponible, elles s'adaptent à du matériel qui n'est que peu optimisé pour cet usage. Cette optimisation pourrait s'effectuer à l'aide du câblage de fonctions, mais pour cela il faut que les constructeurs puissent anticiper l'avenir de la blockchain pour prévoir les gains à long terme.

Aujourd'hui, celles-ci évoluent vite et de nombreuses implémentations sont divergeantes, autant de contraintes qui repoussent l'étape d'optimisation matérielle.

Cette étape pourrait être facilitée par la normalisation des blockchains.

Les limites de la blockchain

Il y a des passes périlleuses dans toute révolution technologique. Certaines personnes dans l'industrie des blockchains ont souligné que la chaîne de blocs s'est hypertrophiée, alors qu'en réalité, la technologie a ses limites et est inappropriée pour de nombreuses interactions numériques. Mais grâce à la recherche et au développement, aux succès et aux échecs, aux essais et aux erreurs, nous savons quels sont les problèmes et les limites actuelles des blockchains.

Complexité

La technologie blockchain implique un vocabulaire entièrement nouveau. Il a rendu la cryptographie plus courante, mais l'industrie hautement spécialisée fait appel à un vocabulaire spécifique (certains diront jargon). Heureusement, plusieurs efforts sont déployés pour fournir des glossaires et des index complets et faciles à comprendre.

Taille du réseau

Les chaînes de blocage (comme tous les systèmes distribués) ne résistent pas tant aux mauvais acteurs qu'elles sont «antifragiles», c'est-à-dire qu'elles résistent aux attaques et se renforcent. Cela nécessite toutefois un vaste réseau d'utilisateurs. Si une chaîne de blocs n'est pas un réseau robuste avec une grille de nœuds largement distribués, il devient plus difficile d'en tirer pleinement profit. Il y a une discussion et un débat sur la question de savoir s'il s'agit d'une faille fatale pour certains projets de la chaîne de blocs autorisés.

Coûts de transaction et vitesse du réseau

Bitcoin a actuellement des coûts de transaction notables après avoir été présenté comme «presque gratuit» pendant les premières années de son existence. À la fin de 2016, il ne peut traiter qu'environ sept transactions par seconde et chaque transaction coûte environ 0,20 \$ et ne peut stocker que 80 octets de données. Il y a aussi l'aspect politiquement sensible de l'utilisation de la chaîne de blocs bitcoin, non pas pour les transactions, mais comme une réserve d'informations. C'est la question du «gonflement», souvent mal perçue parce qu'elle oblige les mineurs à retraiter et à réenregistrer perpétuellement l'information.

Erreur humaine

Si une chaîne de blocs est utilisée comme base de données, l'information qui y entre doit être de haute qualité. Les données stockées sur une chaîne de blocs ne sont pas intrinsèquement fiables, de sorte que les événements doivent d'abord être enregistrés avec précision. L'expression «poubelle à l'entrée, poubelle à la sortie» est vraie dans un système d'enregistrement en chaîne de blocs, tout comme dans une base de données centralisée.

Un défaut de sécurité inévitable

Il y a une faille de sécurité notable dans bitcoin et d'autres chaînes de blocage: si plus de la moitié des ordinateurs servant de nœuds pour entretenir le réseau mentent, le mensonge deviendra la vérité. C'est ce qu'on appelle une «attaque à 51 %» et Satoshi Nakamoto l'a souligné lorsqu'il a lancé Bitcoin.

(Voir [Quid de la sécurité de la blockchain](#))

Pour cette raison, les gisements miniers de bitcoin sont surveillés de près par la communauté, s'assurant ainsi que personne n'obtient sans le savoir une telle influence du réseau.

Politique

Parce que les protocoles de la chaîne de blocs offrent la possibilité de numériser les modèles de gouvernance, et parce que les mineurs forment essentiellement un autre type de modèle de gouvernance incitative, il y a eu de nombreuses possibilités de désaccords publics entre les différents secteurs communautaires. Ces désaccords sont une caractéristique notable de l'industrie de la chaîne de blocs et s'expriment le plus clairement autour de la question ou de l'événement de « bifurquer » une chaîne de blocs, un processus qui implique la mise à jour du protocole de la chaîne de blocs lorsqu'une majorité des utilisateurs d'une chaîne de blocs l'ont acceptée. Ces débats peuvent être très techniques et parfois passionnantes, mais ils sont instructifs pour ceux qui s'intéressent au mélange de démocratie, de consensus et de nouvelles possibilités d'expérimentation de la gouvernance que la technologie de la chaîne de blocage ouvre.

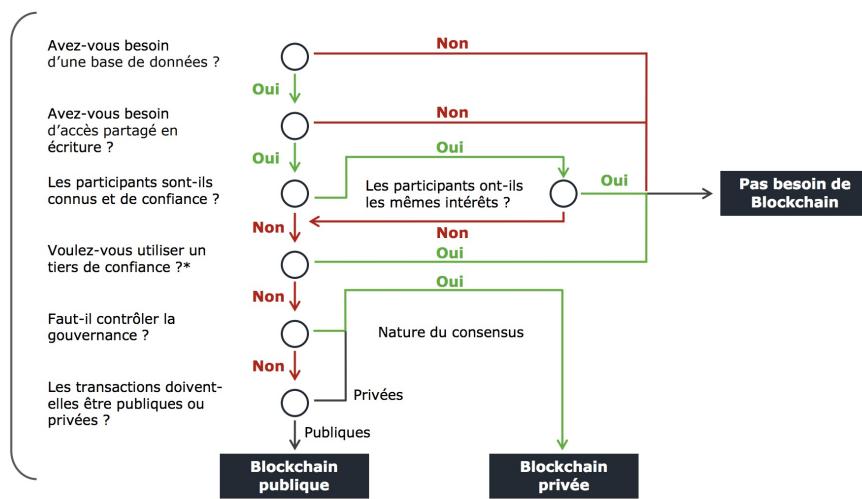
Dans quel cas se doter d'une blockchain ?

Un organigramme d'aide à la décision sur la mise en place d'une blockchain est proposé par *Julien Maldonato et Rémi Foul* dans *La Blockchain, panorama des technologies existantes*.

Les types de Blockchain

Comment construire une stratégie Blockchain?

Avez-vous besoin d'une Blockchain ?



Tiers de confiance traditionnel déjà existant. Excluant les Oracles qui jouent le rôle de confiance au sein d'une Blockchain.

© 2017 Deloitte SAS

La Blockchain - Panorama des technologies existantes 3

Avez-vous besoin d'une blockchain ?

Julien Maldonato et Rémi Foul, La Blockchain, panorama des technologies existantes

Concernant la question de la prise de décision collective par le vote, ces limites montrent que la blockchain ne sera pas la réponse providentielle et invite à mesurer l'opportunité comparativement d'autres méthodes éprouvées.

C. Scénarios d'usages

La blockchain est donc un registre distribué dans lequel les informations sont stockées sous forme de blocs et dont la validation est soumise à différentes méthodes cryptographiques et de consensus. Les deux utilisations principales de la blockchain sont les transactions financières et les contrats-intelligents ([smart-contract](#)). Ces derniers permettent de corrélérer une prise de décision collective, basée sur le vote pour exécuter des actions prédéfinies. L'utilisation de la blockchain pose la question légitime de la consommation énergétique et de l'impact environnemental, nous avons ainsi abordé l'opportunité de la normalisation comme réponse potentielle à ce questionnement. La technologie blockchain n'est pas la réponse universelle, elle présente des limites et ne sera à préconiser que dans des cas précis.

1. Gouvernance des entreprises
2. Management collaboratif de projet
3. Démocratie participative
4. Vie associative et gestion des collectivités.

Gouvernance des entreprises

La blockchain propose un modèle de gouvernance des entreprises avec preuves, traçabilité et transparence.

DAO

Une DAO (Decentralized Autonomous Organization) est une organisation décentralisée. Les règles la régissant sont inscrites dans une 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, auditabile par chacun.

Stephan Tual, TheDAO

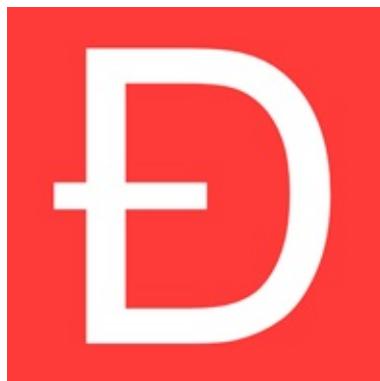
Les DAOs utilisent la technologie des smart-contracts (voir [smart-contract](#)) pour fonctionner.

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 auditabile 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

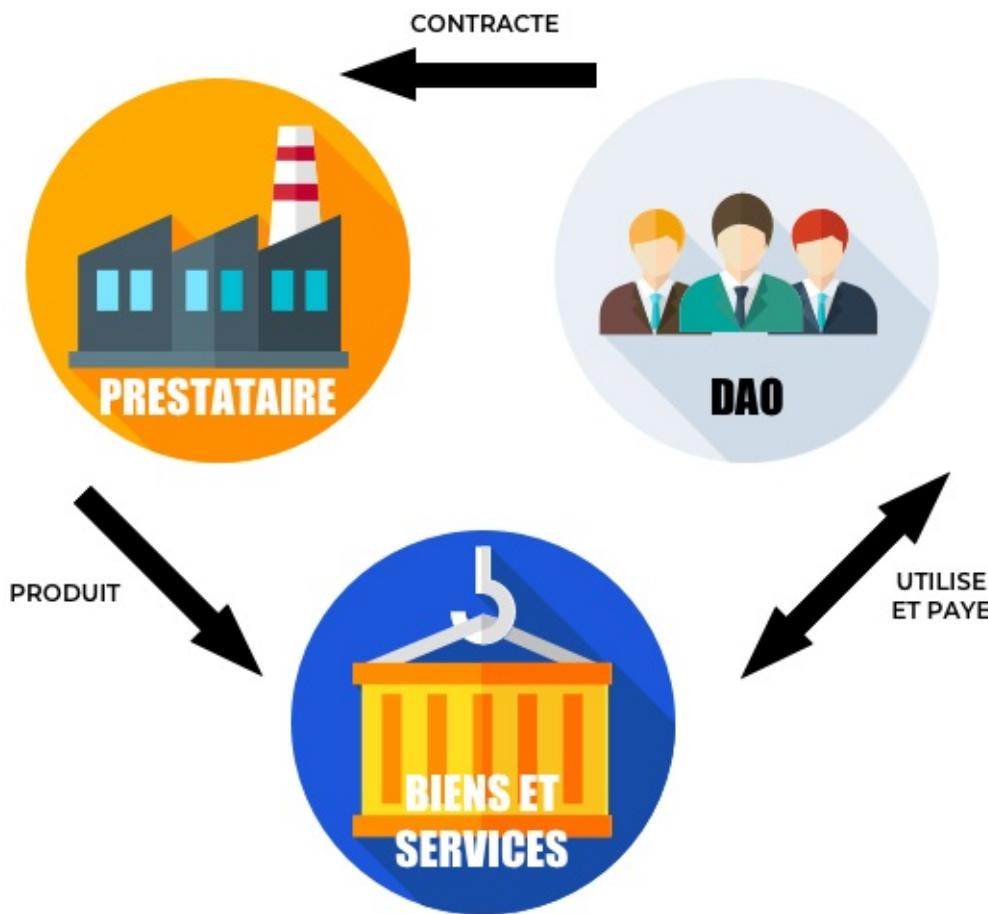


Le projet TheDAO est à l'initiative de la start-up slock.it et est l'exemple le plus remarquable de ce genre d'organisation. C'est avant tout une réalisation expérimentale concrète, illustrant la faisabilité d'un tel système ([POC](#)).

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'appuie pour fonctionner sur la blockchain Ethereum.

Les trois actions possibles à l'intérieur de TheDAO étaient 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 rappeler que lors de sa crowdfund, 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.

Management collaboratif de projet

La blockchain offre une nouvelle promesse: celle de baser sans risque sa confiance sur l'humain. Celle d'ouvrir son entreprise à l'extérieur, sans craindre d'ingérence, de faire participer ses salariés à la décision avec des règles accessibles et vérifiables par toutes et par tous.

Mais surtout elle ouvre la porte à la consultation mixte, en interne en provenance des salariés et en externe en provenance du grand public. Cette ouverture duale pourrait se faire en recourant à des services centralisés mais la blockchain offre des avantages substantiels.

Gestion interne: un management tourné vers le salarié

La blockchain permet de résoudre un grand nombre de problèmes des entreprises [holocratique](#) qui est un système d'organisation de la gouvernance, fondé sur la mise en œuvre formalisée de l'intelligence collective. De part son fonctionnement décentralisé, ces entreprises se prêtent particulièrement à ce type de structures qui ont besoin de systèmes numériques pour faire communiquer leurs salariés et permettre la prise de décision collective. En fournissant un système traçable et intégré, la blockchain permettrait de résoudre la problématique d'éclatement géographique tout en maintenant un niveau de connaissance partagée sur les processus actifs.

De plus, le fonctionnement de la blockchain par le biais des smart-contracts permet d'inscrire des principes de fonctionnement consultable par tous et modifiable uniquement par le consensus. Ainsi il n'est pas impossible d'imaginer une organisation disposant de strates de gestion intermédiaire réduites voire inexistantes, et remplacées par des smart-contracts.

Gestion externe: l'intégration du grand public dans les décisions managériales

Cette nouvelle forme de gestion de l'entreprise pourrait permettre des formes d'hybridation entre les entreprises telles que nous les connaissons et les DAOs. En permettant l'encadrement clair et anticipé du grand public dans la prise de décision collective, la blockchain invite à repenser les interactions avec le client et laisse présager une nouvelle forme d'engagement autour d'un produit ou d'une marque.

Démocratie participative

Ici sont réunis conjointement les concepts de démocratie participative mais également de démocratie représentative.

- La «démocratie délégative» est une forme de démocratie où le pouvoir de vote est confié à un délégué plutôt qu'à un représentant. On peut considérer ce système comme une synthèse entre la démocratie directe et la démocratie représentative.
- La «démocratie participative» qui évoque l'idée d'une implication et d'une participation des citoyens dans le débat public mais aussi dans la prise de décisions politiques. Ce terme, très à la mode, désigne bien souvent des réalités extrêmement variées.

Premières expérimentations

- L'Open Vote Network

Dans A Smart Contract for Boardroom Voting with Maximum Voter Privacy, Patrick McCorry, Siamak F. Shahandashti and Feng Hao présentent la première mise en œuvre d'un système décentralisé et auto-comptabilisateur de vote par Internet avec un maximum de confidentialité de l'électeur en utilisant la blockchain.

Le scrutin abordé dans cet exemple est à «bulletin découvert» et est adapté aux élections du conseil d'administration. Il est écrit comme un «smart-contract» pour Ethereum.

Contrairement à de précédentes expérimentations sur les protocoles de vote électronique, les chercheurs ont réussi à mettre en œuvre un système qui ne s'appuie sur aucune autorité de confiance pour calculer le décompte ou pour protéger la vie privée de l'électeur.

L'Open Vote Network est un réseau de vote autonome et chaque électeur est maître de la confidentialité de son vote.

Avec une telle implémentation, ce vote ne pourrait être compromis que par une collusion totale impliquant tous les autres votants.

Le protocole de vote est garanti par le mécanisme de consensus qui sécurise également la blockchain Ethereum.

La mise en œuvre de ce réseau a été effectuée sur le réseau de test social d'Ethereum pour démontrer sa faisabilité et a montré que sa mise en œuvre peut être possible avec un minimum de configuration pour les élections et à un coût de 0,73 \$ par électeur.

Le coût peut être considéré comme raisonnable dans la mesure où ce vote assure une protection maximale de la vie privée de l'électeur et est vérifiable publiquement.

C'est la première mise en œuvre d'un protocole décentralisé de vote par Internet fonctionnant sur un système de vote par Internet.

Il utilise la chaîne de blocs d'Ethereum non seulement comme un tableau d'affichage public, mais plus important encore, en tant que plate-forme de calcul par consensus qui fait respecter les règles de l'exécution correcte du protocole de vote.

Bien que le nombre de sujets testés puisse sembler dérisoire, il s'agit d'une première initiative qui ne demande qu'à être poursuivie à plus grande échelle. Dans le cadre de travaux futurs, les chercheurs ont déclaré qu'ils étudieront la faisabilité de l'exploitation à une échelle nationale.

Le point soulevé par cette étude est que si un telle perspective est rendue possible, elle nécessitera presque certainement une chaîne de blocs dédiée.

Par exemple, cela peut être une chaîne de blocs de type [Ethereum](#) qui ne stocke que le contrat de vote électronique.

La nouvelle chaîne de blocs peut avoir une taille de bloc plus grande pour stocker plus de transactions sur la chaîne et peut être maintenue d'une manière centralisée similaire à [RSCoin](#).

- **La première élection basée sur la blockchain s'est déroulée en Sierra Leone**

"La Sierra Leone souhaite créer un climat de confiance avec les électeurs dans une élection controversée, en particulier en examinant comment l'élection sera perçue publiquement après les élections. En utilisant la chaîne de blocage comme moyen d'enregistrer de manière immuable les bulletins de vote et les résultats, le pays espère créer une légitimité autour de l'élection et réduire les retombées des partis d'opposition ", a-t-il dit.

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

Le 7 mars 2018 s'est déroulé un vote basé sur la blockchain en Sierra Leone enregistrant 70% de participation sur une blockchain.

La technologie Agora, créée par Leonardo Gammar, stocke anonymement les votes dans un registre immuable, offrant ainsi un accès instantané aux résultats des élections.

Les votes/bulletins anonymes sont enregistrés sur la chaîne de blocage d'Agora, qui sera accessible au public pour que toute partie intéressée puisse les examiner, les compter et les valider. C'est la première fois qu'une élection gouvernementale utilise la technologie blockchain.«

[Leonardo Gammar, Agora](#)

Cette expérience trouve son origine dans un grand mouvement d'aspiration à la transparence et de lutte contre la corruption qui s'élève en Sierra Leone, particulièrement dans le cadre des élections, dont les résultats sont souvent controversés.

Cette expérimentation permettra de tester les retombées en matière de perception d'intégrité dans le cadre de l'élection. Ainsi les citoyens et les parties prenantes espèrent créer une légitimité autour de l'élection et réduire les retombées des partis d'opposition

Bien qu'il ne s'agisse que d'une preuve de concept ([POC](#)), il ne s'agit pas d'un registre électoral complet, mais plutôt d'une pluralité de votes en quantité acceptable.

Il est fascinant de voir la technologie mise en œuvre en Sierra Leone, un pays d'environ 7,4 millions d'habitants.

L'objectif ultime est de réduire les coûts du vote en supprimant les bulletins de vote en papier et en réduisant la corruption dans le processus de vote.

Cette première expérimentation démontre la faisabilité de l'opération dans un pays de plusieurs millions d'habitants où la corruption et la criminalité sont élevées.

Son créateur prend en exemple le retour en arrière de nombreux pays sur le vote électronique pour avancer le caractère incontournable des blockchains dans les processus de prise de décision par le vote, arguant qu'il n'existe pas d'autres systèmes de vote de bout en bout vérifiable et totalement transparent pour cet avenir.

Toutefois, il s'agit de remettre cette expérience en perspective, car une élection dans un pays n'est pas encore un mouvement massif. Cependant, Gammar et son équipe ont annoncé leur intention d'étendre leur produit à d'autres pays africains et, au reste du monde.

- **Le projet DEMOCRACY EARTH**



Logo de la Democracy Earth Foundation

Democracy Earth Foundation (DEF) est une fondation américaine à but non lucratif qui construit une plateforme de gouvernance orientée «[démocratie liquide](#)» basée sur une blockchain open source.

La DEF a publié la version 1.0 Alpha de la plate-forme de gouvernance, Sovereign, en mai 2017 et son livre blanc, [The Social Smart Contract](#), en septembre 2017. La fondation a piloté, lors du référendum pour la paix en Colombie, un vote symbolique parmi la diaspora d'environ 6 millions de Colombiens expatriés. Le projet pilote a permis aux gens de voter séparément sur différentes parties du référendum et de déléguer leur vote à des représentants, les résultats du vote symbolique révélant des nuances importantes dans les préférences des électeurs qui n'ont pas été prises en compte lors du référendum. Le projet pilote montre activement comment la démocratie participative réduit la polarisation, l'impuissance et l'apathie des électeurs.

L'implémentation du vote dans le projet DEF

Le jeton de vote vise à être une norme pour la démocratie numérique capable d'interagir avec d'autres jetons, en établissant un langage commun pour la gouvernance des organisations basées sur la chaîne de blocs. Dans le contexte des démocraties liquides, une gamme d'opérations de vote est permise:

- Vote direct: un utilisateur a le droit d'utiliser ses jetons pour voter directement sur des questions comme dans une démocratie directe.
- Délégation de base: un utilisateur peut déléguer des votes à un représentant. Tant que ce dernier a accès à ces jetons, il peut les utiliser pour voter au nom du premier.
- Délégation limitée sur des sujets: Un utilisateur peut déléguer des votes à un autre à la condition spécifiée qu'il ne peut utiliser ces jetons que sur des questions portant une étiquette spécifique. Si la délégation précise que les votes délégués ne peuvent être utilisés que pour les décisions du sujet «environnement», alors le représentant ne pourra pas les utiliser ailleurs. Ce potentiel de représentation peut être utilisé pour déléguer un vote à un expert de tel ou tel sujet.
- Délégation transitoire: Si un utilisateur a reçu des votes d'un autre, il peut alors les déléguer à un troisième. Cela génère une chaîne de délégations qui aide à responsabiliser des acteurs spécifiques au sein d'une communauté. Ce caractère est désactivable par le premier utilisateur s'il le souhaite.
- Vote prépondérant: Un utilisateur peut supprimer le résultat du vote de son représentant s'il a changé d'avis, ainsi il peut exercer un contrôle a posteriori de son opinion déléguée.
- Vote public: Souvent appelée la règle d'or des démocraties liquides, toute personne qui délégue a le droit de savoir comment son délégué a voté sur une question donnée avec son vote. De la même manière que les votes des membres du Congrès sont publics, sur les démocraties liquides, les délégués en compétition sur un sujet

donné sont incités à se bâtir une réputation publique en se basant sur leurs résultats de vote afin d'attirer plus de délégations.

- Vote secret: Une méthode capable de garantir des transactions de vote non traçables à l'électeur. C'est indispensable dans le contexte d'élections publiques organisées au sein de larges populations qui présentent un risque élevé de coercition. Même si le secret parfait sur la transaction de vote est atteint, les utilisateurs peuvent toujours être identifiés grâce aux empreintes digitales avec les méta-données exposées. Pour cette raison, la recherche sur l'intégration avec des blockchains conçues pour les transactions anonymes ayant fait leurs preuves est encouragée. La DEF poursuit d'ailleurs ses recherches sur l'intégration des votes secrets avec les blockchains suivantes:
 - Ethereum: utilise des contrats pré-compilés pour l'addition et la multiplication scalaire sur la courbe elliptique alt_bn128, pour les contrôles d'appariement, qui permettent les zk-SNARKs.
 - ZCash: implémente des transactions sécurisées en utilisant des preuves à divulgation nulle de connaissance
 - Monero: utilise des signatures en cercle avec des adresses furtives.

Les frais de transaction nécessaire à la validation du vote peuvent être soit subventionnés par l'organisme d'exécution, soit payés directement par les électeurs.

DEF utilise un système de preuve à connaissance nulle pour garantir l'identité du votant sans pour autant les inscrire publiquement dans la blockchain. Il s'agit d'une avancée majeure dans le processus de vote à l'aide de cette technologie. Ainsi, le problème de la confidentialité dans le cadre du scrutin à bulletin secret trouve un premier élément de réponse.

Vie associative et gestion des collectivités.

La participation du grand public dans la gouvernance des associations

Les associations ont tout à gagner à implémenter des systèmes de vote basés sur la blockchain afin de permettre à leurs membres d'intervenir dans le processus de décision. Cela permettrait de résoudre le problème de l'éclatement géographique des membres en maintenant conjointement un niveau élevé de sécurité et de traçabilité.

L'ensemble de ces points répondants à l'impératif de transparence que le grand public réclame.

Gestion des collectivités: le citoyen comme acteur du service public

La blockchain permet d'envisager un nouveau niveau d'intégration du citoyen dans la gestion des collectivités. Au-delà de la participation par le biais du vote, cela invite à repenser les modalités d'actions du service public.

De nombreuses expérimentations ont d'ailleurs lieu sous l'impulsion de [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.

Suite à cette annonce, on distingue différents cas d'usage notamment au niveau du secteur de la commande publique qui se prête particulièrement aux dynamiques offertes par les smart-contracts et l'automatisation des contrats. On distingue également une nouvelle opportunité concernant la transmission de documents.

Mais le cas d'usage le plus ambitieux concerne le portage du droit administratif sous forme de code. L'objectif est de pouvoir confronter la situation individuelle d'un administré aux règles applicables.

L'ambition à terme est de d'envisager une expérimentation d'une collectivité sous forme de DAO.

Conclusion

La blockchain est un outil qui laisse présager une révolution et fait la promesse d'un monde décentralisé, ouvert et collaboratif.

Les raisons de l'engouement autour de cette technologie sont à chercher dans les crises successives que nos sociétés post-industrielles rencontrent, crise du savoir, de la confiance, défiance légitime ou excessive envers les institutions étatiques. Les réponses et interrogations nouvelles que la blockchain apporte permettront d'envisager un futur différent autour de ces problèmes et en particulier autour de la question du vote, et plus largement de la participation.

Si de multiples expériences et preuves de concept soutiennent l'intérêt de ces questions, les pistes prospectives sont encore plus nombreuse et nous croyons que la blockchain sera une des technologies qui vont bouleverser les usages et les systèmes en place. Ces expérimentations permettent d'envisager des entreprises impliquant le consommateur, des associations décentralisées dont les actions sont soumises au vote permanent de leurs soutiens ou bien encore des institutions publiques pilotées en temps réel par les citoyens.

Cette révolution n'est pas exempte de points de friction, en particulier autour des questions environnementales que la blockchain devra résoudre. Il faudra également repenser les algorithmes afin de les rendre plus viables aux échelles souhaitées.

Il faut considérer la blockchain comme elle est aujourd'hui, à son stade embryonnaire, et ne pas perdre de vue les nombreux défis et succès que cette technologie présage.

Santiago Siri, Democracy Earth Foundation

Créateur de la Democracy 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: [Ethereum 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 déléguants.

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.