Table des matières

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

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 … sont aujourd'hui des enjeux largement médiatisés hors des cercles d'initiés.

Le temps de la croyance aveugle dans les bienfait de la révolutions 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 la l'ère dans laquelle nous vivons porte désormais le nom d'ère post-vérité (post-factual era).

Cette crise de confiance a déjà de nombreuses conséquences dans le champ politique mais également dans le champ économque où la confiance est la clé de voute de l'investissement et de l'adhésion à une marque ou à un produit

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 considèrera 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 cœur des cryptomonnaie : 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.

Nous explorerons ici les perspectives ouvertes par l'usage de la blockchain comme outils de sécurisation de la prise de décision collective aussi bien dans le cadre public que privé.

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

Ce travail est en cours et de nombreuses sections ne sont pas dans leur état définitif

Table des matières

- Vote

Du besoin d’outils sécurisés de prise de décision collective et de leur potentiel impact

- Les origines de la crise de confiance
- Une aspiration à la transparence
- Du statut de la preuve au vote
- Pour la res publica
- Pour la gouvernance des entreprises
- Pour les modes de management basé sur le consensus
- Pour le cercle privé

De la blockchain comme potentiel cœur de ce changement

- Qu'est ce que la blockchain ?
- Preuve de Travail vs Preuve de l’Enjeu
- Quid de la sécurité de la blockchain ?
- Quid de ses impacts énergétiques ?
- Vers une normalisation ?
- Les limites de la blockchain

Scénarios d’usages

- Gouvernance des entreprises
- Management collaboratif de projet
- Démocratie participative
- Vie associative et gestion des collectives.

Conclusion

Glossaire

Annexes

Définitions

La blockchain

Modalité de sécurisation

Prise de décision collective

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.

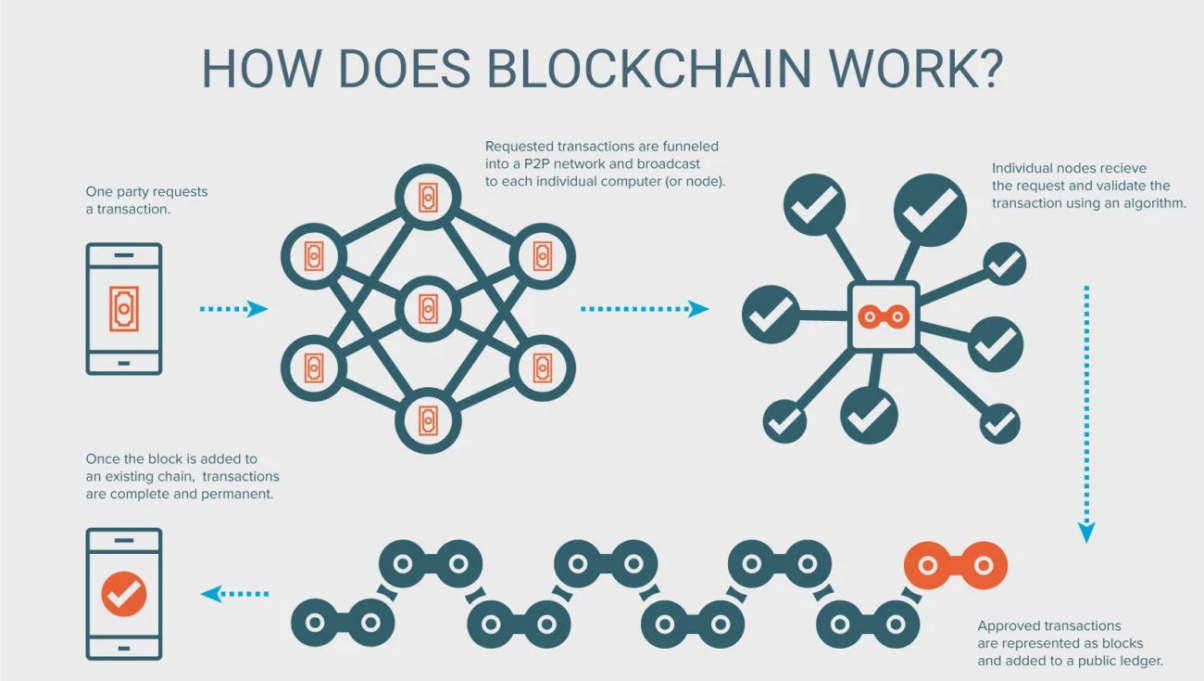
Par extension, une chaîne de blocs est une base de données distribuée qui gère une liste d'enregistrements protégés contre la falsification ou la modification par les nœuds de stockage.

Une blockchain est donc unregistre distribué et sécurisé de toutes les transactions effectuées depuis le démarragedu système réparti.

Il existe des blockchains publiques, ouvertes à tous, et des blockchains privéesdont l'accès et l'utilisation sont limitées 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?
One party requests a transaction.
Requested transactions are funneled into a P2P network and broadcast to each individual computer (or node).
Individual nodes recieve the request and validate the transaction using an algorithm.
Approved transactions are represented as blocks and added to a public ledger.
Once the block is added to an existing chain, transactions are complete and permanent.

Définition : modalité de sécurisation

Nous entendons les modalité de sécurisation comme les différents 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 :

- 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 ») : garantie 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 plusefficaces 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 recherche de la prise de décision collective.

Du point de vue de la psychologie sociale plus spécifiquement, des applications et des conséquences théoriques sont nombreux et variés 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 à la prise de décision collective, tels que la polarisation, la pensée de groupe et le Common Knowledge Effect.

Définition : vote

Le vote (terme dérivé de l'anglais vote, provenant du latin votum signifiant « vœu ») désigne une méthode permettant à un groupe une prise de décision commune.

Les organisations formelles ou informelles ont recours à cette pratique, de toute nature (économiques, politiques, associatives, etc.). 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 ».

Enjeux :

- 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 tous doutes 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 triches. 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 sou 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 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.
- Vote par clé : Il consiste à voter à l'aide d'une clef 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). Nénamoins 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 étét respectée dans le cadre d'un vote par procuration.

Du besoin d’outils sécurisés de prise de décision collective et de leur potentiel impact

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, TheConversation*

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 réussie 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 un âme, une conscience et une morale.

Au tournant du siècle, le gouvernement se préoccupait déjà moins de « la vérité » que de 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 creusée par le détournement malhonnete d'un certain nombre de concept évoqué par le post-modernisme alliés aux révélations de scandales politique, économique et écologique au cours de ces cinquantes dernières années.

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

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

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

Il serait vain de tenter de lister toutes les manifestations de cette crise de confiance ni même ses origines qui sont sujettes à controverses. Nénamoins, il convient de constater que celle-ci existe indubitablement et que son existence impose de repenser profondément le rapport au monde que les entreprises, les états en intégrant ses nouveaux impératifs de transparence.

Une aspiration à la transparence

Pour répondre à cette problématique, une solution semble apparaitre : "montrer pattes blanche".

Il s'agit d'intégrer qu'il n'existe pas de présomption d'inonnence ni de culpabilité, mais un soupçon préalable dont les organisations communicantes doivent s'affranchir.

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 entitées émetrices de messages envers le public.

Pour accompagner cette réfection de la confiance, des outils technologiques ont vu le jour plateforme participative, management holocratique, consultation publique.

Ces nouveaux outils sont par exemple devenus un pré-requis au développement d'un projet urbain dans le cadre de 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 conçu de manière ouverte (Open Source) mais également respecter des principe de sécurité par conception (security by design) et de protection de la vie privée (privacy by design).

Nous avons choisi ici de nous concentrer sur la blockchain en raison de l'engouement du grand public pour cette technologie et de la perspectuve qu'elle représente de mettre en pratique les préceptes explicités plus haut.

Du statut de la preuve au vote

Si la transparence nécessite d'apporter la preuve de sa bonne foi, la preuve mértite 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 (exemple document contractuel, attestation) qui démontre, établit, prouve la vérité ou la réalité d'une situation de fait ou de droit : La preuve d'un crime. La preuve est également une opération par laquelle on contrôle l'exactitude d'un calcul ou la justesse de la solution d'un problème.

C'est bien cette double nature qui nous intéresse ici au regard de la question du vote.

Le vote et la preuve

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

Preuve entourant le processus :

- Fiabilité
- Traçabilité

Ce processus doit être réfutable, c'est à dire qu'il doit présenter des éléments tangibles et objectifs permettant sa potentielle disqualification ou non.

Si le processus ne présente des critères de réfutabilité potenitelles, il est jugé corrompu à priori.

Preuve entourant le vote :

- Authenticité
- Intégrité
- Confidentialité

Pour la res publica

L'administration du bien public en toute transparence est une préoccupation majeure de ces dernières années.

Elle se pose à deux niveau, le premier concerne la prise de décision et implique la concertation publique.

La seconde implique la gestion continue du bien et sa gouvernance.

Les biens public sont mutliples et les propositions le concernant peuvent provenir des citoyens mais également des institutions.

La question de l'identitée

Puisque le vote nécessite l'authentification du sujet de façon à éviter la fraude, la question de l'identitée est cruciale. La blockchain invite à repenser le rôle des insitutions en tant que tiers de confiance

Pour la gouvernance des entreprises

Pour les modes de management basé sur le consensus

Pour le cercle privé

De la blockchain comme potentiel cœur de ce changement

La blockchain c’est quoi exactement ?

Quid de la sécurité de la blockchain ?

Quid de ses impacts énergétiques ?

Vers une normalisation ?

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 utlisée par le bitcoin.

Inventée en 2008, le bitcoin est à l'origine un prototype pour montrer qu'il était possible de faire reposer une crypto-monnaie dont le mécanisme repose sur un registre distribué et réparti entre de multiples noeuds d'un réseau.

De part leur nature intrinséquement open-source, les algorithmes de chiffrages sont un argument de plus au regard de la confiance en ce système.

De fait, le bitcoin est la première manifestation de l'obsolescence d'une banque en l'occurrence en tant que tiers de confiance.

Les trois pilliers de la blockchain

Celle-ci 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 symmétriques et les assymmétriques.

Les premières sont connues depuis l'antiquité et les secondes ont vues 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 clef privée pour coder un message que le destinataire peut décoder avec la clef publique de l'expéditeur.

Si la méthode du chiffrement symétrique à l'avantage d'être peu coûteuse en puissance de calcul, et de demeurer très sûre.

> 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

A 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 clef qui est choisie privée n'est jamais transmise à personne alors que la clef qui est choisie publique est transmissible sans restrictions.

Cette technique permet:

Le Chiffrement

L'un des rôles de la clef publique est de permettre le chiffrement.c'est donc cette clef qu'utilisera un premier sujet pour envoyer des messages chiffrés à un second. L'autre clef — 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 clef ne permet pas de déduire l'autre.

L'Authentification de l'origine

L'utilisation par l'un des sujet de sa clef privée sur le condensat d'un message, permettra à ce dernier de vérifier que le message provient bien de l'interlocuteur attendu et qu'il n'y a pas cas d'usurpation:

il appliquera la clef publique que son interlocuteur lui a fourni sur le condensat (condensat chiffré avec la clef 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'ellese 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 apparait le plus indiqué.

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

Les différents organisations de police doivent toutes attaquerensemble pour profiter de l'effet de surprise. Le cas contraire ils seraient submergés 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 délèguent 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 lamoitié des forces de polices qu'il faut attaquer à telle date et à telle heure, et à l'autremoitié qu'il faut se retirer, désunion qui ne leur permettra pas de bénéficier de l'effet de surprise et de la supériorité numérique.

Dans le cadre d'une opération de police, la garantie de la coordination provient du supérieur hierarchique qui tient lieu de tiers de confiance.

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 policene peut envoyer qu'un seul ordre à la fois, associé à un horodatage.

Mais, surtout, lesordres sont agglomérés les uns aux autres, puis chiffrés, formant une chaînestockée dans un « grand livre de transactions », lequel est redistribué à tousles services de polices en présence.

Une chaine 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'informations avec tous les services de police en présence, il sera possible de déterminer les chaines 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.

Preuve de travail vs preuve de l'enjeu

Une blockchain est donc un registre distribué chiffré,et répliqué dans tous les noeuds du réseau, qui contient les chaînesd'ordre 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 précedemment que la chaîne est constituée d'un ensemble de blocs de données contenant des informations ainsi qu'un horodatage. A chaque transaction, ces blocs sont intégrés à la chaîne.

Afin de garantir son intégrité, cette chaîne est chiffré et doit êtrecertifiée.

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

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

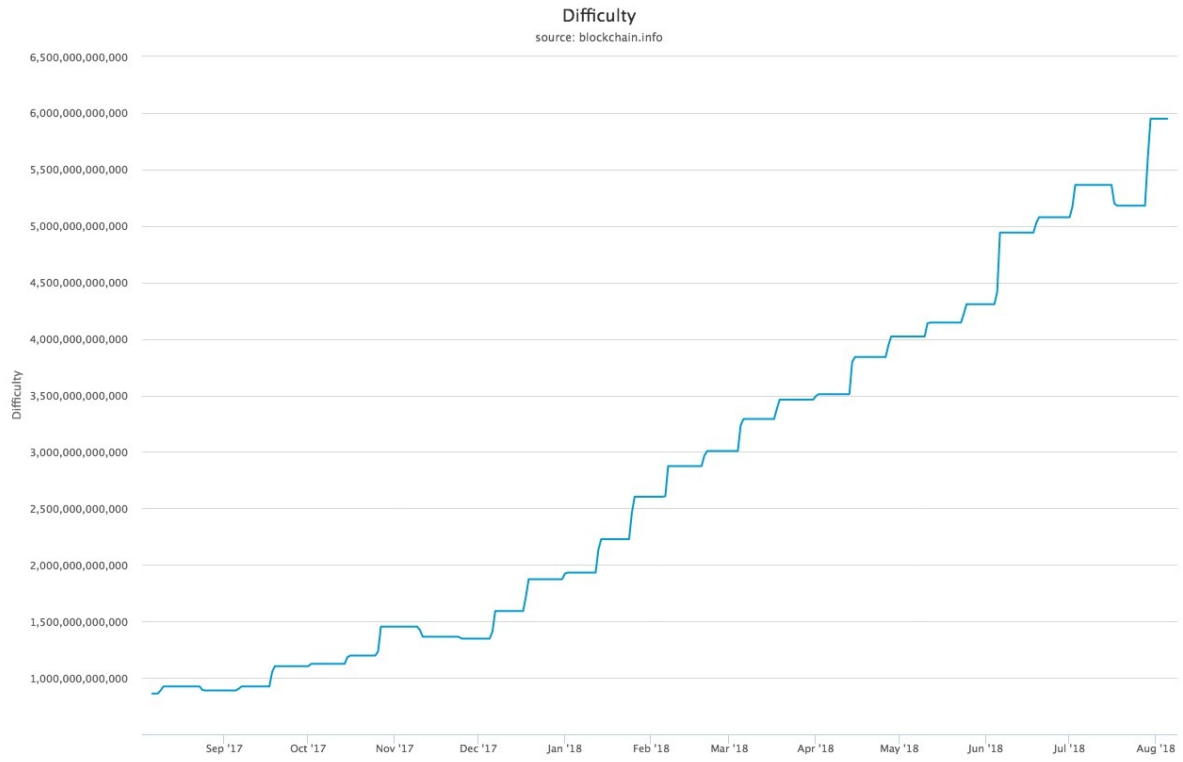
On appelle les machines (ou institutions) quieffectuent ce travail de certification des « mineurs » de l'anglais mining.

L'objet cryptographique crée 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 unclonage facile qui aurait pour conséquences de pouvoir controller la blockchain de manière rétroactive.

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



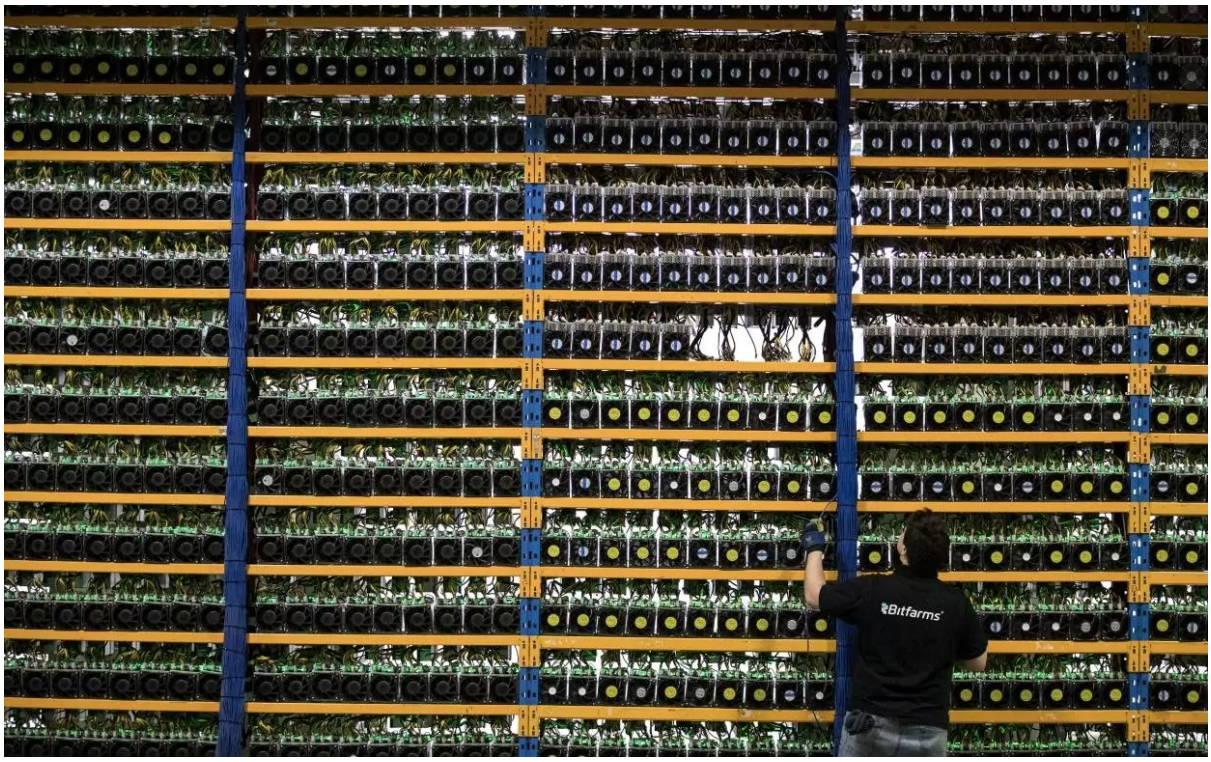
> Mesure relative de la difficulté de trouver un nouveau bloc. La difficulté est ajustée périodiquement en fonction de la puissance de hachage déployée par le réseau de mineurs.
>
> Source: blockchain.com

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 cetification est supérieure.

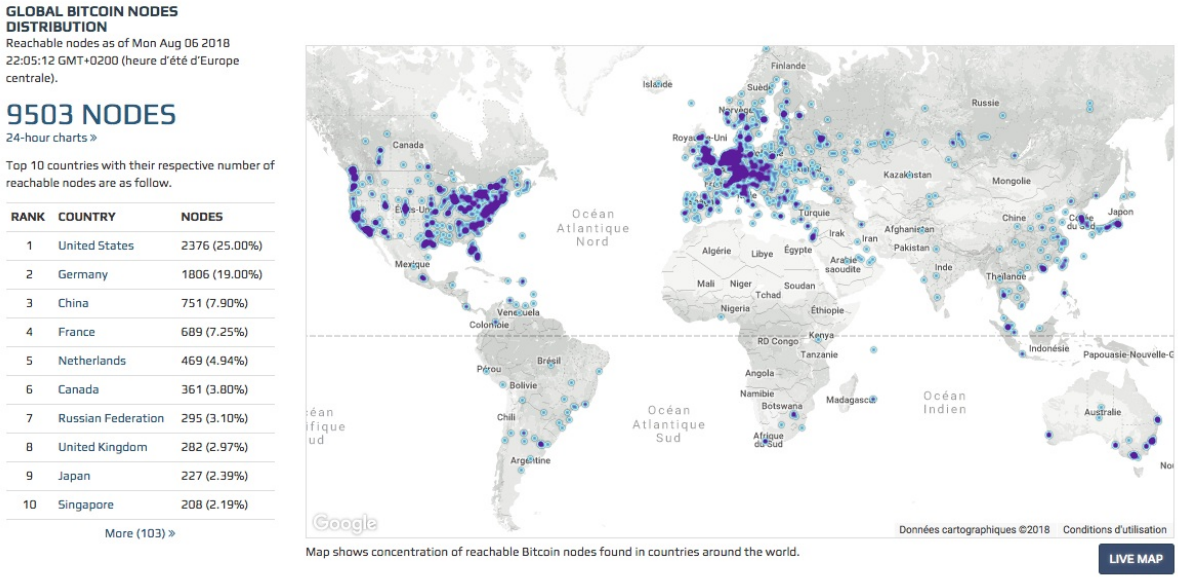
Depuis des mineurs spécifiques sont apparus pour réaliser la preuve de travail et les cartes graphiques grand-public sont délaissés car non compétitive.

Car plus la taille des chaînes augmente, plus la puissance de calcul doit augmenter. Cette relation d'interpendance a chassé les particuliers de la course à la certification et se 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 noeuds 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 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 différant de la PoW permettant d'obtenir un consensus distribué.

Dans les crypto-monnaies basées sur les PoS, le créateur du bloc suivant est choisi par diverses combinaisons de sélection aléatoire et de richesse ou d'âge (c'est-à-dire l'enjeu).

La preuve de l'enjeu (PoS) est une catégorie d'algorithmes de consensus pour les chaînes de blocs publics qui 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 (i.e. l'exploitation minière). Dans les chaînes de blocs publics basées sur les PdS (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 du PDS comprennent la sécurité, la réduction des risques de centralisation et l'efficacité énergétique.

En général, un algorithme de preuve de mise ressemble à ce qui suit. La chaîne de blocs garde la trace d'un ensemble de validateurs, et toute personne qui détient la cryptocurrency de base de la chaîne de blocs (dans le cas d'Ethereum, ether) peut devenir un validateur en envoyant un type spécial de transaction qui enferme son éther dans un dépôt. Le processus de création et d'acceptation de nouveaux blocs se fait alors par le biais d'un algorithme de consensus auquel tous les validateurs actuels peuvent participer.

Il existe de nombreux types d'algorithmes de consensus et de nombreuses façons d'attribuer des récompenses aux validateurs qui participent à l'algorithme de consensus, de sorte qu'il existe de nombreuses "saveurs" de preuve de l'enjeu. D'un point de vue algorithmique, il existe deux types principaux : la preuve en chaîne de l'enjeu et la preuve de l'enjeu de type BFT.

Dans la preuve de mise basée sur la chaîne, l'algorithme choisit un validateur au hasard pendant chaque tranche de temps (par exemple, chaque période de 10 secondes peut être une tranche de temps), et assigne à ce validateur le droit de créer un bloc unique, et ce bloc doit pointer vers un bloc précédent (normalement le bloc à la fin de la chaîne la plus longue précédemment), et ainsi, au fil du temps, la plupart des blocs convergent vers une chaîne unique en croissance constante.

Dans la preuve de mise de type BFT, les validateurs se voient attribuer au hasard le droit de proposer des blocs, mais s'accorder sur quel bloc est canonique se fait à travers un processus à plusieurs tours où chaque validateur envoie un "vote" pour un bloc spécifique pendant chaque tour, et à la fin du processus, tous les validateurs (honnêtes et en ligne) s'accordent en permanence sur le fait qu'un bloc donné fait ou non partie de la chaîne.

Notez que les blocs peuvent encore être enchaînés ensemble ; la principale différence est que le consensus sur un bloc peut se situer à l'intérieur d'un bloc et ne dépend pas de la longueur ou de la taille de la chaîne qui suit.

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

Quels sont les avantages de la preuve de l'enjeu par rapport à la preuve du travail ?

Il n'est pas nécessaire de consommer de grandes quantités d'électricité pour sécuriser une chaîne de blocs (par exemple, on estime que Bitcoin et Ethereum brûlent plus d'un million de dollars d'électricité et de matériel informatique par jour dans le cadre de leur mécanisme de consensus)

En raison de la faible consommation d'électricité, il n'est pas nécessaire d'émettre autant de nouvelles pièces afin de motiver les participants à continuer à participer au réseau. Il peut même théoriquement être possible d'avoir une émission nette négative, où une partie des frais de transaction est "brûlée" et où l'offre diminue au fil du temps. La preuve de l'enjeu ouvre la porte à un plus large éventail de techniques qui utilisent la conception de mécanismes de la théorie des jeux afin de mieux décourager les cartels centralisés de se former et, s'ils se forment, d'agir d'une manière nuisible au réseau (p. ex. comme l'exploitation minière égoïste dans la preuve du travail).

Réduction des risques de centralisation, car les économies d'échelle sont beaucoup moins problématiques. 10 millions de pièces vous rapporteront exactement 10 fois plus que 1 million de pièces, sans gains disproportionnés supplémentaires parce qu'au niveau supérieur, vous pouvez vous permettre d'acheter de meilleurs équipements de production de masse, ce qui est un avantage pour la preuve du travail.

Capacité d'utiliser des pénalités économiques pour rendre les différentes formes d'attaques de 51% beaucoup plus coûteuses à réaliser que la preuve du travail - pour paraphraser Vlad Zamfir, "c'est comme si votre ferme ASIC brûlait si vous participiez à une attaque de 51%".

Quid de la sécurité de la blockchain ?

Quid de ses impacts énergétiques ?

Vers une normalisation ?

Les limites de la blockchain

Scénarios d’usages

Gouvernance des entreprises

Management collaboratif de projet

Démocratie participative

Vie associative et gestion des collectives.

Gouvernance des entreprises

DAO

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

Management collaboratif de projet

Démocratie participative

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

- La "démocratie représentative" (aussi appelée "démocratie délégative" et "aristocratie élective") dans laquelle le citoyen délègue son pouvoir à des représentants qui incarnent la volonté générale. Les représentants votent la loi. On parle également de démocratie liquide
- La "démocratie participative" qui évoque l'idée d'une implication et d'une participation des citoyens dans le débat public mais aussi 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 d'intimité de l'électeur en utilisant la Blockchain.

Le réseau de vote ouvert est adapté aux élections du conseil d'administration. Et est écrit comme un "smart-contract" pour Ethereum.

Contrairement à de précédentes experimentations 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 protection, du point de vue de la vie privée de son vote.

Avec un telle implémentation son vote ne pourrait être violé que par une collusion totale impliquant tous les autres votants.

L'exécution du protocole est exécutée 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 est 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 deu suet testé puisse sembler dérisoire, il s'agit d'une première initiativequi ne demande qu'à être poursuivie à plus grande échelle.Dans le cadre de travaux futurs, Les chercheurs ont déclarés 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

> John Biggs, TechCrunch

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

La technologie Agora, crée 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

Un mouvement d'aspiration à la transparence et de lutte contre la corruption s'élève en Sierra Leone. Ses citoyens aspirent à un climat de confiance dans le cadre des élections, habituellement controversé.

Cette experimentation permettra de tester les retombées en matière de perception d'intégrité dans le cadre de l'élection. Ainsi les citoyens et les parties prenangtes 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, un POC Il ne s'agit pas d'un registre électoral complet, mais plutôt d'une pluralité de votes en quantitée 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 experimentation 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 price de décision par le vote, arguant qu'il n'existe pas d'autres sytème de vote de bout en bout vérifiable et totalement transparente pour cet avenir.

Toutefois il s'agit de remttre 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.

Vie associative et gestion des collectives.

Conclusion

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, TheConversation

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

Vérité et politique, Hannah Arendt

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

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 programmé sans aucune possibilité de temps d'arrêt, de censure, de fraude ou d'interférence de tiers. Source : Ethreum project

RSCOIN

RSCoin, une crypto monnaie 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 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 de données centralisé.

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

mining

proof-of-work

proof-of-stake

John Biggs, TechCrunch

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

Leonardo Gammar, Agora

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