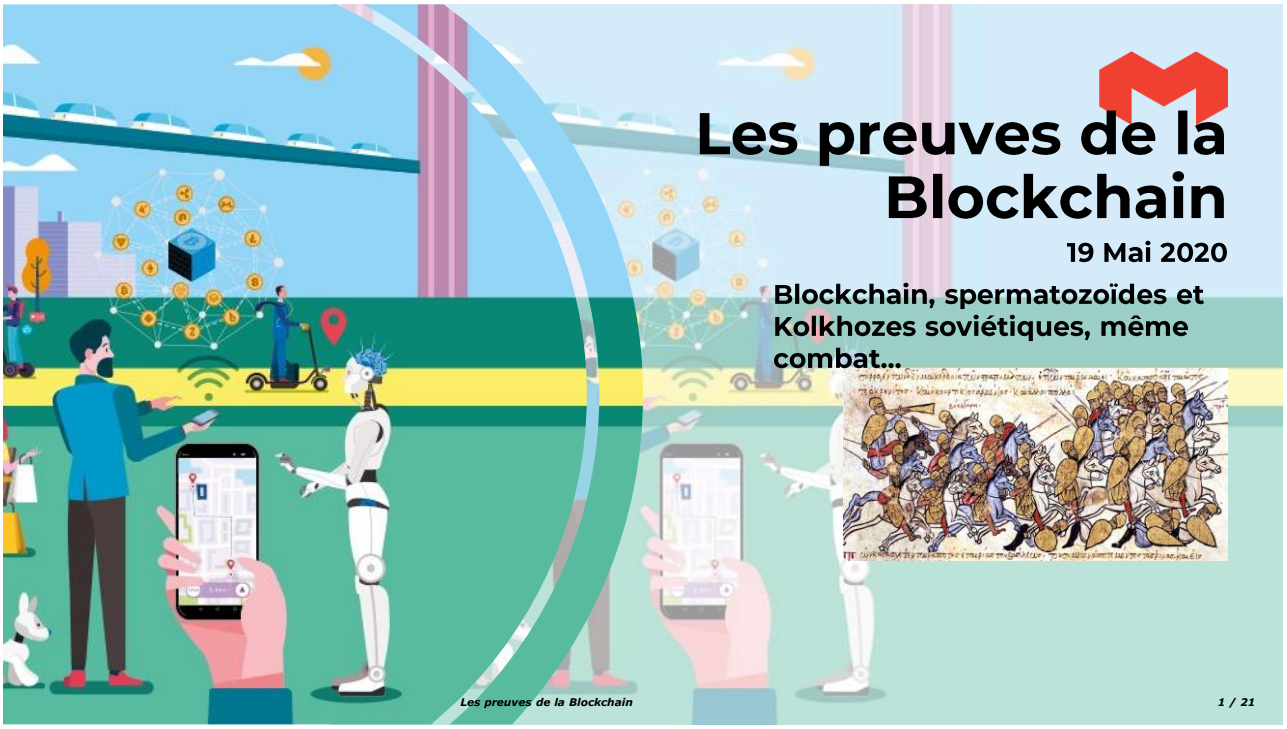


Les preuves de la Blockchain

19 Mai 2020

Blockchain, spermatozoïdes et Kolkhozes soviétiques, même combat…

Sommaire

L'apport de preuves de la Blockchain

- Concept global de Blockchain : une architecture
- Chaînes, blocs et transactions
- La mise à jour d'une vérité unique
- Les grandes familles de preuves d'autorité
- Les bases mathématiques
- Théorème de CAP, impossibilité « FLP » et limites à la tolérance aux failles
- Preuve de travail (PoW) des Bitcoin
- Preuves d'enjeux (PoS) d'Ethereum
- Comparaison et autres techniques
- Pourquoi faut-il s'intéresser de près à ce monde nouveau

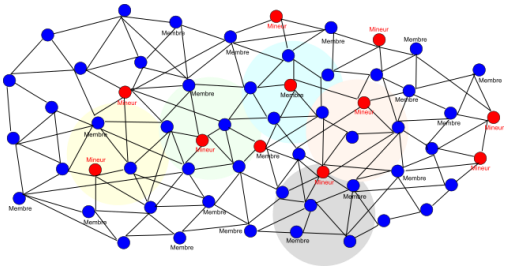
La Blockchain, le kolkhoze du TI
(comparaison purement sémantique…)

- Le Kolkhoze est une contraction de коллективное хозяйство, qui veut dire "économie collective"… on s'en serait douté…
- Appropriation par les acteurs de la gestion et du développement de ressources mises en commun
- Une blockchain n'est rien d'autre que l'implémentation dans le TI du concept
- La vérité n'appartient plus à une entité centrale, mais à toute la communauté
- Une blockchain peut être privée ou publique
- En 2020, les exemples de blockchain publiques commencent à se développer, mais ce sont les instances privées qui ont le vent en poupe
- Il ne faut pas être trop pressé, les grands principes mettent du temps
- La blockchain est une architecture à cinq paliers déclinable à l'infini
- La seule question à se poser est de savoir si la décentralisation de la vérité et son partage présentent un intérêt…

100 ans plus tard, le concept de kolkhoze trouve une étonnante "mise à jour" avec la blockchain…

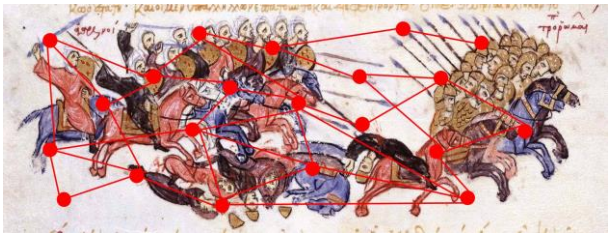
Ce qu'il faut savoir de la Blockchain

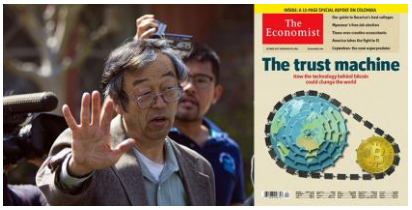
- La Blockchain s'applique à une communauté d'utilisateurs, dite « pair à pair », réunis dans un même réseau, sans qu'il y ait de hiérarchie entre eux.
- Les acteurs qu'ils soient simples usagers ou mineurs (forgeurs), sont connectés à un nombre réduit d'autres acteurs.
- Un acteur A est connecté à un acteur B, qui lui-même est connecté à un acteur C… et il ne faut que quelques secondes pour qu'un événement traverse tout le réseau.
- Les membres de la Blockchain sont propriétaires d'une « vérité » partagée par la communauté, que personne ne pourra contester.
- Ils effectuent des transactions, des opérations élémentaires, qui regroupées dans des blocs, seront envoyées et partagées par les autres membres.



Critères	Blockchain publique	Blockchain privée
Nouveaux membres	N'importe qui	Membres autorisés
Créateur des transactions	N'importe qui	Membres autorisés
Vitesse des transactions	Faible	Haute
Coût des transactions	Elevé	Faible
Consensus	PoW, PoS, dPoS	PBFT, PoA (Autorité)
Confiance	Aucune confiance n'est exigée entre les membres	Confiance nécessaire entre noeuds
Identité	Anonyme ou Pseudonyme	Identités connues
Ressource concernée	Native Blockchain (monnaie…)	N'importe laquelle

La métaphore des généraux byzantins



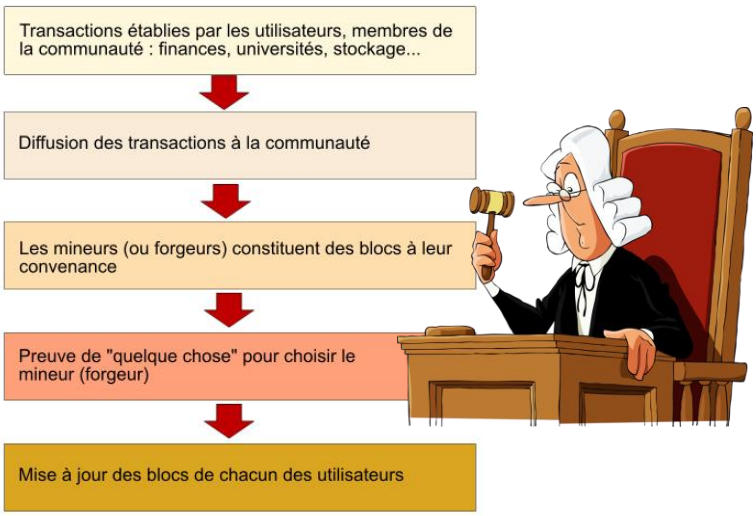


Satoshi Nakamoto

- Un problème bien connu en mathématiques, qui consiste à s'assurer qu'un ensemble de nœuds constituant un ensemble, serait capable de gérer les défaillances et malveillances et garantir la fiabilité du système, si une part minoritaire mais non négligeable des nœuds venaient à sortir du « droit chemin ».
- Le processus de la Blockchain est un algorithme de mise à jour des chaînes de blocs des participants, chaque bloc témoignant de la réalité des transactions, par un système de minage (Bitcoin).
- La Blockchain est donc un ensemble de blocs, qui sont ajoutés par minage au fur et à mesure des transactions, identique pour l'ensemble des acteurs.
- Les mineurs fournissent la puissance de calcul nécessaire, pour effectuer les mises à jour dans le réseau.
- C'est la mise à jour d'une grosse base de données répliquée (pas décentralisée).

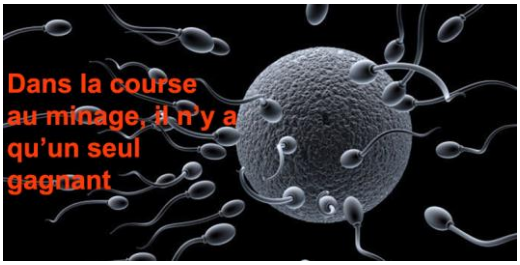
Les cinq phases de la Blockchain

- Chacun peut développer sa propre architecture en implémentant des versions privées de l'ossature Blockchain : une technique spécifique de recherche de consensus, un minage particulier fondé sur le théorème de CAP…



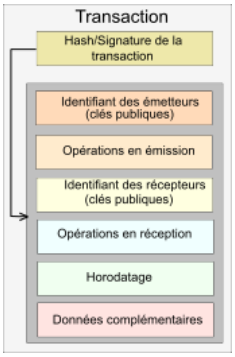
La mise à jour d'une vérité unique : le minage

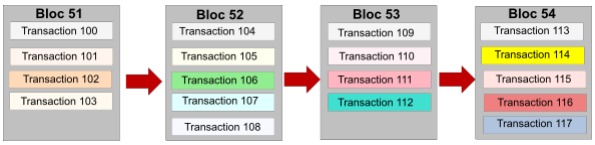
- Le minage est un algorithme, dont la finalité est de mettre à jour LA vérité portée par chacun des participants, un portefeuille de titres, les opérations boursières d'une place de marché, le cadastre d'un pays, un portefeuille de monnaies cryptographiques, des preuves de possession immobilières, etc.
- Le principe veut qu'il n'y ait qu'une seule vérité partagée par tout le monde et qu'il n'y ait qu'un seul intervenant pour faire la mise à jour de cette vérité, à un instant donné.
- Le minage est issu de la mise en concurrence des candidats à la mise à jour, qui seront rémunérés pour cela.
- C'est la manière dont ces lauréats sont choisis qui constitue le cœur des procédures de preuves (recherche de consensus).
- Les candidats au minage vont apporter la preuve, d'abord qu'ils sont éligibles à la mise à jour et que la chaîne de blocs qu'ils proposent, celle qui viendra se superposer aux chaînes existantes de chacun des participants, est la plus pertinente.
- **C'est comme les spermatozoïdes. Il y a beaucoup de candidats au départ à la fonction reproduction, mais il n'y en a qu'un seul de retenu, qui l'emporte sur des critères spécifiques.**



Chaînes, blocs et transactions
(ex de Bitcoin)

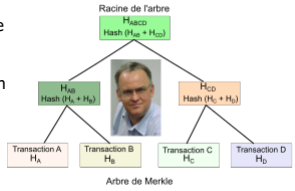
- Une transaction regroupe une ou plusieurs opérations élémentaires, avec nature et identité de l'opérateur.
- On ne désigne pas les émetteurs et récepteurs par leur nom, mais par leur clé publique, attribuée quand ils se sont intégrés à la communauté. En fait, le hash de ces clés, calculé par l'algorithme SHA-256.
- Chaque transaction est horodatée et peut comporter des informations complémentaires.
- La transaction est signée électroniquement : l'auteur chiffre le hash de l'ensemble de la transaction, avec sa clé privée, y compris les différentes opérations qui la constitue.
- Le fait de signer la transaction permet de garantir son intégrité.
- Les transactions peuvent se contenter d'un simple hash plutôt qu'une signature électronique complète.



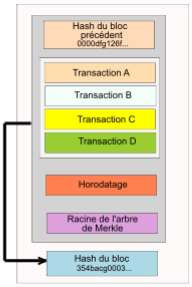


Le format des blocs
(Bitcoin)

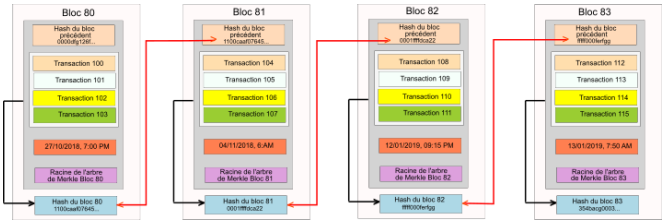
- Chaque bloc est structuré de manière identique. Il comporte un numéro séquentiel, le hash du bloc précédent, auquel il est lié, la liste d'un certain nombre de transactions que le mineur aura reçues, un horodatage, mais aussi un **arbre de Merkle** (la racine de cet arbre.
- Si quelqu'un modifie une transaction appartenant à un bloc, l'arbre de Merkle qu'il contient deviendra faux, puisque la transaction « corrigée » n'aura plus le même hash et par transitivité génèrera une racine d'arbre différente.
- Chaque bloc possède un numéro qui l'identifie à l'intérieur de la chaîne.
- Il comporte aussi le hash du bloc précédent (32 bytes d'identification), qui lui sert de lien avec les autres blocs.
- Les autres éléments sont un horodatage, son propre hash, obtenu avec l'algorithme SHA-256 et la racine de l'arbre de Merkle qui caractérise les transactions du bloc. A noter que le hash du bloc porte sur l'ensemble du bloc, y compris le hash du bloc précédent et celui de la racine de l'arbre de Merkle.



Arbre de Merkle

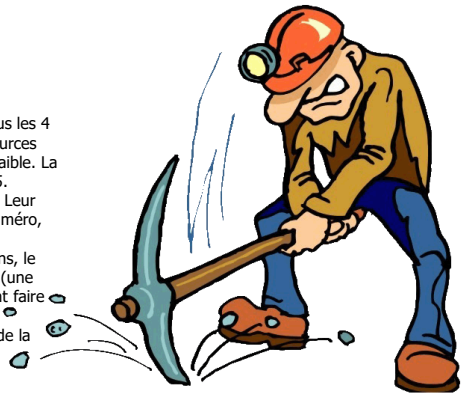


Structure de bloc

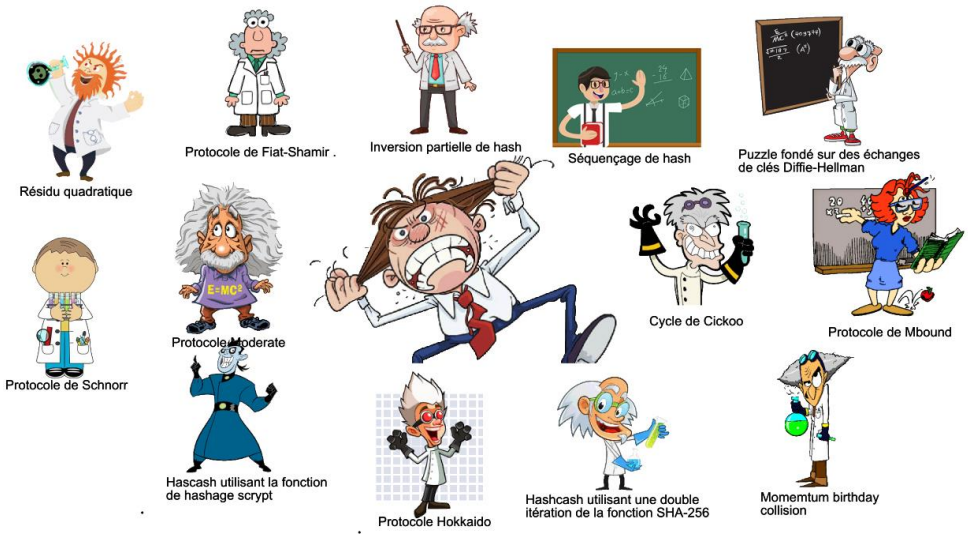


La technique du minage
(bitcoin)

- Quand une transaction est finalisée, elle est diffusée dans le réseau.
- Parmi les nœuds qui reçoivent l'information, certains jouent un rôle particulier, les **mineurs.**
- Ils disposent de leurs propres ressources machines, dont ils vont se servir et sont rémunérés en conséquence, la rémunération étant cependant divisée par deux tous les 4 ans, soit environ tous les 210 000 blocs, car elle est calculée en fonction des ressources globales des mineurs. Plus ces ressources sont élevées, plus la rémunération est faible. La récompense d'origine était de 50 BTC, de 12,5 BTC en 2019 et elle tombera à 6,25.
- Les mineurs reçoivent donc comme les autres, un certain nombre de transactions. Leur travail étant de les valider et de les constituer en blocs, chaque bloc portant un numéro, avec un certain nombre de transactions insérées.
- A partir de leur mempool, les mineurs choisissent un certain nombre de transactions, le plus souvent en privilégiant celles dont la « valeur marchande » est la plus élevée (une « fee registration » est affectée à chacune d'elles), distinction que sait parfaitement faire l'application de preuve de travail, dans chacun des noeuds clients.
- Le travail de minage consistera à ajouter ce bloc, qui viendra se placer au-dessus de la chaîne existante, partagée par tous les membres.

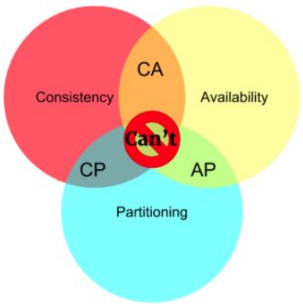


Les bases mathématiques



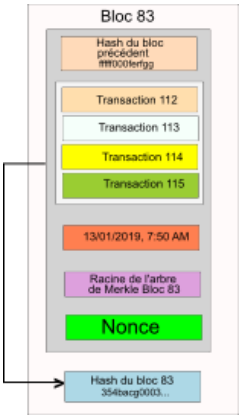
Théorème de Cap, impossibilité FLP, tolérance

- **Théorème de CAP : i**l est impossible pour un système de calcul distribué de garantir strictement et en même temps, les trois contraintes de :
  - **Cohérence**
  - **Disponibilité**
  - **Tolérance au partitionnement**
- **Impossibilité FLP**, du nom des auteurs de l'article fondateur en 1985 (Fischer, Lynch et Patterson) : dans un réseau asynchrone, pour lequel il ne peut y avoir de latence imposée, il n'est pas possible d'atteindre le consensus dans un intervalle de temps donné, si l'un des nœuds (ou plus) est "en panne » ou malhonnête" (généraux félons du modèle byzantin).
- **Limites à la tolérance aux fautes :** indiquent le pourcentage de défaillance de nœuds, que le réseau peut supporter : 1/3 par exemple, avec un modèle partiellement synchrone, donc contraint par une latence donnée, mais que l'on ne connaît pas et sans tolérance avec un modèle asynchrone, sans contrainte de latence.



La preuve de travail ou PoW
(Bitcoin)

- Dès lors qu'il a constitué un bloc, le mineur va tenter d'en faire le nouveau dernier bloc vérité de la chaîne, enregistré chez tous les participants. Et de bénéficier de la rémunération qui l'accompagne.
- Satoshi Nakamoto avait imaginé le principe de la « preuve de travail », pour résoudre ce problème.
- L'idée était de proposer un « challenge » à tous les candidats mineurs, sachant qu'il n'y aura qu'un seul gagnant, que les mineurs vont tenter de résoudre.
- Ce challenge revient à demander aux mineurs d'ajouter un nombre à leur bloc, dit le « nonce » (« number only used once ») de 4 octets et de recalculer le hash du bloc, celui-ci devant répondre, cette fois, à une contrainte, dite de complexité.
- Cette complexité consiste à imposer une condition au hash à calculer, qui devra commencer par exemple par 10 fois le chiffre « 0 » : **0000000000ffec23…** Ce qui revient à exiger que le hash calculé soit inférieur à une certaine valeur. On dira alors que la complexité est de 10. On pourra aussi choisir un autre nombre de "0".
- On ne peut pas prévoir la structure du hash à partir d'un document à « hasher ».
- Les mineurs doivent tester toutes les valeurs du nonce, jusqu'à ce que cela fonctionne. Comme un nonce de 32 bits peut être un nombre entier parmi 4 294 967 296…
- Ce n'est qu'après désignation du « vainqueur » que le bloc sera transmis au reste de la communauté (20 sec en moyenne), avec mise à jour des mempools.
- Tout dépend de la capacité informatique du mineur.
- Mathématiquement, deux mineurs distincts peuvent trouver la clé en même temps ou à peu près. Dans ce cas, Bitcoin prendra le bloc le plus long, celui qui comporte le plus de transactions, le ou les autres, appelés les « oncles », tombant dans l'oubli.



Inconvénients de la preuve de travail

- Une consommation électrique effarante, déjà estimée à 3 GW pour la seule Chine en 2014 et évaluée en 2019 à l'équivalent de la consommation d'un pays comme l'Irlande.
- Power Compare estime que le Bitcoin à lui seul consomme plus d'électricité qu'une vingtaine de pays en Europe et 159 à l'échelle mondiale (2018).
- Si une organisation dispose d'une puissance de calcul supérieure à 51 % de la totalité de la puissance de minage, elle sera forcément gagnante et rémunérée en tant que telle.
- Les bénéficiaires des paiements ont tendance à se débarrasser rapidement de leurs montants cryptographiques, car il s'agit d'une monnaie, ce qui fait mécaniquement baisser sa valeur marchande.
- Son principal inconvénient est d'avoir été le premier à être implémenté, ce qui a permis à ses détracteurs de débusquer ses zones d'ombre et de proposer des solutions plus pertinentes.

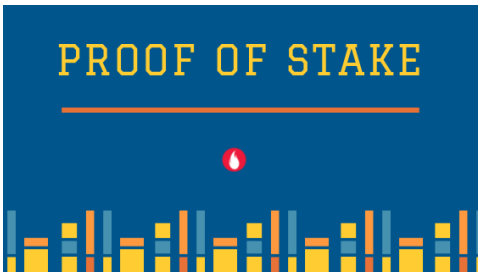
Les preuves d'enjeux

- La preuve d'enjeu (« Proof of Stake »), ou preuve de participation a été imaginée par Sunny King et Scoot Nadal en 2012, une réponse à la PoW.
- Il n'y a, à un moment donné qu'un seul mineur, le **validateur**, susceptible de proposer une chaîne de blocs.
- La fonction de minage telle qu'elle a été conçue, n'attribue l'opération qu'à l'un des (nombreux) mineurs, les forgeurs.
- Chacun des mineurs candidats doit être propriétaire d'un certain volume de monnaies cryptographiques et la probabilité pour qu'un candidat mineur soit désigné, est proportionnelle au nombre de « cryptos » qu'il aura dans son portefeuille et… qu'il aura mis en dépôt dans l'organisation (d'où l'enjeu).

Vitalik Buterin

Les preuves d'enjeux

- De nombreuses preuves d'enjeux se sont succédées dans le temps, depuis les Peercoin.
- Certaines d'entre elles ne se contentent pas du montant en cryptos, mais tiennent compte aussi de l'âge du dépôt et d'autres paramètres.
- Au départ, la fonction « validation » était attribuée à un intervenant différent, toutes les secondes.
- Dans d'autres algorithmes, il n'y a pas de sélection, remplacée par une procédure pour mettre tous les validateurs d'accord, sur le prochain bloc de mise à jour.
- Quelle que soit la méthode choisie pour retenir ou non un validateur, toutes les « Proof of stake » se caractérisent par le fait que les candidats doivent déposer un montant de monnaie cryptographique et le bloquer.
- Le gros avantage par rapport à la preuve de travail, est donc que le process consomme beaucoup moins d'énergie puisqu'il n'y a qu'un seul validateur/consommateur en activité à un instant donné.
- Mais il a un gros défaut : « nothing at stake » ou « rien à perdre ».
- La solution pour éviter le blocage est de pénaliser les validateurs s'ils minent plusieurs blocs simultanément, sanction qui peut aller jusqu'à confisquer leur mise.



Les preuves d'enjeux

- Peercoin a été la première monnaie cryptographique à utiliser la preuve d'enjeu, en 2013.
- Peercoin exploite un mécanisme hybride de PoW et PoS, le validateur étant sélectionné à la fois sur le montant de son enjeu et sur la date de son dépôt.
- NXT remonte également à 2013 : il a été le premier à ne pas appliquer un algorithme de preuve mixte, comme l'a fait Peercoin.
- NXT est à la fois une crypto-monnaie et un système de paiement décentralisé.
- NEM (« New Economic Movement ») fait partie de la même mouvance, une « hard fork » de NXT, au départ, mais revue depuis de A à Z. Elle exploite désormais une « preuve de réputation » de manière à minimiser le seul critère de possession des cryptos.
- Ce qui va dans le sens « humaniste » de cette organisation américaine, qui tente de restructurer l'économie sur des bases plus saines, dans laquelle l'être humain, plus que l'argent, doit jouer le premier rôle.
- Ethereum, créé par Vitalik Buterin, fonctionne encore pour quelques mois sur une PoW. Mais celle-ci sera prochainement remplacée par Casper, une preuve d'enjeu issue de l'adaptation d'un algorithme, qui à l'origine cherchait à réduire l'intervalle de temps entre les blocs d'une PoW.
- D'autres méthodes telles que Dash et PIVX, qui mettent en scène des nœuds maîtres (on n'est plus dans un mode égal-à-égal) utilisent aussi une preuve d'enjeu.

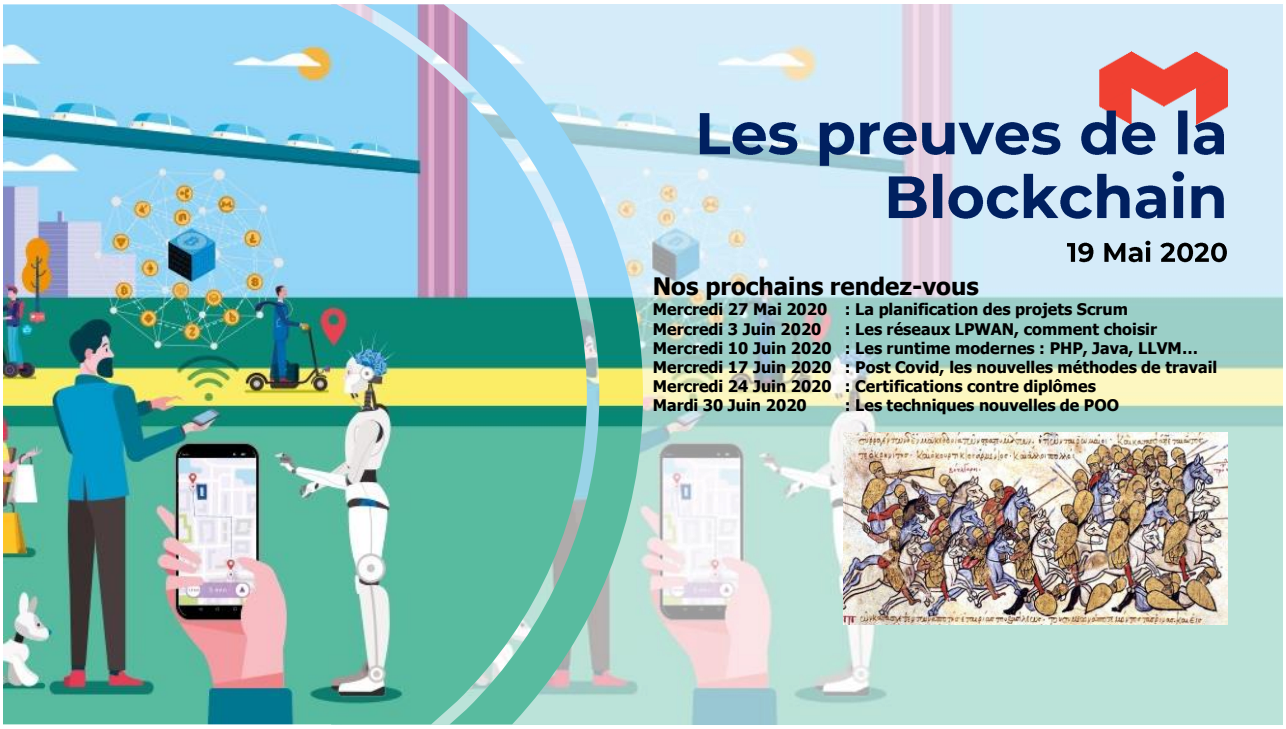
Comparison PoW et PoS

La preuve d'enjeu déléguée

- Unicité ponctuelle du validateur
- La preuve d'enjeu déléguée (« Delegated Proof of Stake, DPoS), est fondée sur un mécanisme d'élection en temps réel et de réputation, les candidats à la validation votant pour désigner des délégués, la valeur de leur vote étant proportionnelle au montant de tokens ou cryptos qu'ils ont déposés.
- Ce sont les délégués qui vont valider les blocs et seront rémunérés en conséquence.
- Plusieurs systèmes se réclament de la preuve déléguée, avec des appellations qui varient, des témoins, des « slot-leaders », des producteurs de blocs, des nœuds de consensus, etc.
- Le travail des délégués n'est pas neutre. Ils doivent s'assurer que leur nœud est toujours actif, récupérer les transactions qui circulent sur le réseau (comme tout mineur ou forgeur), valider les transactions, etc.
- Il faut donc les motiver, grâce à des récompenses mensuelles, qui se réduisent avec le temps.
- Les exemples les plus connus de PoS déléguée sont les réseaux BitShares, Steemit, Ark, Lisk, EOS et Cardano.

Les grandes familles de preuves d'autorité

- Il existe plus de trente méthodes de recherche de preuves (consensus), qui toutes consistent à désigner les validateurs chargés du minage ou forgeage.
- Certaines sont rapides, d'autres économiques, voire démocratiques ou peu consommatrices en énergie, d'autres encore favorisent les « possédants ».
- On ne peut pas toutes les couvrir, d'autant qu'elles n'ont pas nécessairement la même pérennité, ni les mêmes contraintes. Tout dépend de la finalité de la communauté : monnaie cryptographique ou tout autre usage de la Blockchain.
- Dans les mois à venir, avec l'explosion des applications de la Blockchain, le minage (forgeage) et les algorithmes de preuves vont se multiplier, qui vont jouer le même rôle qu'un langage et une API pour la programmation.



Les preuves de la Blockchain

19 Mai 2020

Nos prochains rendez-vous

Mercredi 27 Mai 2020 : La planification des projets Scrum
Mercredi 3 Juin 2020 : Les réseaux LPWAN, comment choisir
Mercredi 10 Juin 2020 : Les runtime modernes : PHP, Java, LLVM...
Mercredi 17 Juin 2020 : Post Covid, les nouvelles méthodes de travail
Mercredi 24 Juin 2020 : Certifications contre diplômes
Mardi 30 Juin 2020 : Les techniques nouvelles de POO