Lutte des cryptomonnaies : travail ou enjeu
Les arguments en faveur de la « Preuve d'enjeu »

***Lundi de la cybersécurité,* 16 janvier 2023**

Jean-Paul Delahaye
Université de Lille, **UMR CNRS 9189, CRISTAL**
Centre de recherche en informatique signal et automatique de Lille

« Preuve de travail » = « Proof of work » = POW et

« Preuve d'enjeu » = « Proof of stake » = POS

Des défenseurs du Bitcoin soutiennent que la POW est meilleure et indispensable.

Mon point de vue est diamétralement opposé :

La POS possède de multiples avantages sur la POW qui n'est qu'une option choisie par Nakamoto pour s'opposer aux « attaques Sybil », que la POS freine tout aussi bien.

Attention !

• Je parlerai de la « **preuve de travail** » et de la « **preuve d'enjeu** » dans le contexte d'un réseau pair-à-pair de cryptoactifs où une protocole permet de désigner un validateur pour ajouter une nouvelle page à un registre distribué fonctionnant en chaîne de blocs ouverte.

• Au sens général la **preuve de travail** est un moyen forçant à faire un calcul prenant du temps.

• Invention : Cynthia Dwork et Moni Naor, 1992.

Méthode pour lutter contre le **spam** et les **attaques par dénis de service**.

Cyntia Dwork, Moni Naor. Pricing via Processing or Combating Junk Mail, Crypto '92, pp. 139–147, 1992.

• Le système **Hashcash** de **Adam Back** en 1997 (pour les attaques par dénis de service) utilise des fonctions à sens unique pour définir les problèmes soumis.

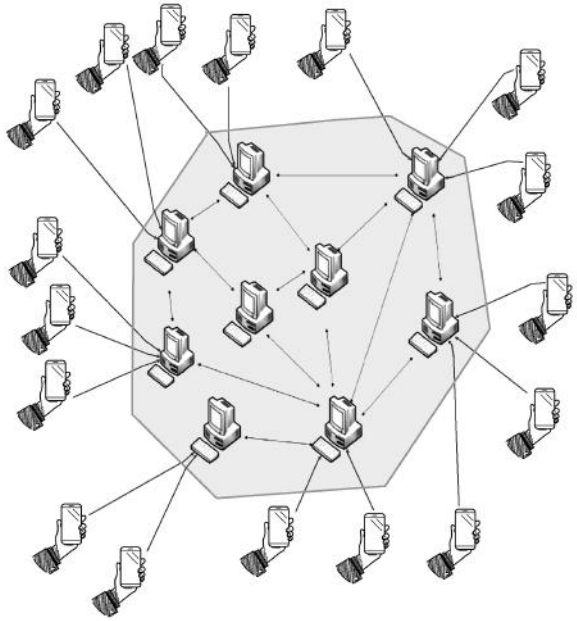
Idée : lancer *k* dés, jusqu'à ce que tous les dés tombent sur le "6".
Lancer *k* dés = calculer une fonction de hachage en regardant les premiers chiffres

A Au cœur du problème : "les attaques Sybil".

« POS, POW et POA sont des mécanismes anti-Sybil » (https://www.ethereum-france.com/)

L'argument principal en faveur de la POS : analyse des protocoles POW et POS.
Conclusion : « **La POW est une POS qui confisque les mises** »

Explications.
Considérons un **réseau pair-à-pair** faisant fonctionner un cryptoactif par le biais
d'un registre (une « blockchain ») détenu par chacun des validateurs du réseau.



Modèle économique

Pour qu'il y ait des validateurs, le protocole prévoit une « ***incitation*** ».

Incitation : création de nouvelles unités de la cryptomonnaie et/ou des commissions.

L'attribution de l'incitation doit s'opérer selon un procédé « équitable ».

Problème délicat quand le réseau accepte **l'anonymat des validateurs.**

Attaque Sybil : un acteur peut multiplier les pseudo-identités.

Principe général de la lutte contre les attaque Sybil :

- L'attribution se fait à chaque période de fonctionnement à **un validateur choisi "au hasard".**
- On donne des chances de gagner aux validateurs en **proportion de leur "engagement"**.
- Il faut une méthode qui annule les avantages obtenus en multipliant des pseudo-identités.
- La POW et POS sont efficaces pour contrer les attaques Sybil.

Avantage du POW sur le POS :

c'est un peu plus facile de concevoir un bon modèle de POW que de POS

POW

• Avec la POW la probabilité d'être choisi pour recevoir l'incitation est
proportionnelle à la capacité du validateur à mener un certain type de calcul.

Le travail de calcul se nomme le « **minage** ». Machines : « **rigs de minage** ».

Coûts : achat des machines + achat d'électricité + fonctionnement.

Le livre blanc de Nakamoto de 2008 ("Bitcoin: A Peer-to-Peer Electronic Cash System") est clair, même si le terme « attaque Sybil » n'est pas utilisé :

« The proof-of-work solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. »

« La preuve de travail résout le problème de la détermination de la représentation dans la prise de décision à la majorité. Si la majorité était basée sur le principe "une adresse IP, un vote", elle pourrait être détournée par **quiconque serait capable d'allouer de nombreuses adresses IP**. »

POS

- Avec la POS la probabilité d'être choisi pour recevoir l'incitation est

proportionnelle à la somme que le validateur engage en la mettant sous séquestre.

Récupération des sommes engagées.

Coûts : immobilisation des mises déposées et risque de confiscation ("slashing").

Le POS a été introduit dans le cadre d'une cryptomonnaie dans Peercoin en 2012.
En fait c'est *QuantumMechanic* (c'est un speudo) qui a proposé l'idée du POS dans un cadre des cryptomonnaie en 2011 :

https://bitcointalk.org/index.php?topic=27787.0

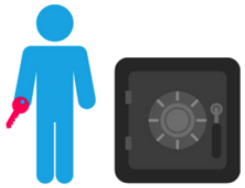
• Dans les deux cas, POW ou POS, un validateur **engage des ressources**.
• S'il multiplie ses pseudo-identités cela ne lui sert à rien.
• La POW et la POS rendent inopérantes les attaques Sybil.

• **Le problème a été perçu par Nakamoto : c'est pour cela qu'il y a une POW dans Bitcoin !**

Preuve de travail

La probabilité de gagner l'incitation est propotionnelle à sa capacité à mener de gros calculs

Preuve d'enjeu



La probabilité de gagner l'incitation est proportionnelle à l'argent qu'on a déposé.

POW : Bitcoin, Litecoin, Dogecoin, Monero, Ethereum Classic, Bitcoin Cash, Bitcoin Gold, Zcash, Dash, ...

POS : Ethereum, Cardano, Polkadot, Solana, Tezos, BNB, Avalanche, Cosmos, Toncoin, Algorand, EOS, ...

Avec la POW l'engagement d'un validateur est perdu. Avec la POS il est récupéré.

« La POS est une POW dans laquelle un validateur récupère son engagement. »

« La POW est une POS qui confisque les mises ! »

• Les validateurs d'une POW ne reçoivent qu'un partie de ce qui est "payé" (directement ou indirectement) par les utilisateurs.

• Le fonctionnement d'une POW est inutilement coûteux.

Handicap économique d'un réseau POW vis-à-vis d'un réseau POS

Ne pas confondre :

« Travail de validation »

et

« Travail pour augmenter la probabilité d'être choisi pour la prochaine page et recevoir l'incitation »

Travail de validation :

- garder et mettre à jour une copie du registre (fichier blockchain).
- faire circuler les transactions et les pages.
- contrôler qu'elles sont conformes aux règles de fonctionnement.
- avoir la capacité de proposer une nouvelle page (gérer une mempool, composer la page, etc.)

Quelle est la dépense électrique de la validation en général ?

Consommation des N ordinateurs (des validateurs) de puissance moyenne allumés en continu.
et connectés à internet.

Pour le Bitcoin N = 15 000. (https://bitnodes.io/ 10-1-2023)

Coût électrique validation Bitcoin = 15 000 ordinateurs de puissance moyenne 200 W.

Coût de la preuve de travail = 2,4 millions de rigs de minage de 3000 W environ.

160 fois plus de machines, chacune au moins 10 fois plus énergivore donc

1600 fois plus d'électricité dépensée par le minage que par la validation

2,4 millions de machines de 3000 W

2 400 000 × 3000 × 24 × 365 Wh/an = 63 TWh/an

= 8 réacteurs nucléaires

Les 63 TWh de mon calcul sont conformes aux autres calculs.

l'Université de Cambridge (https://ccaf.io/cbeci/index) :
Cambridge Bitcoin Electricity Comsumption Index
50,39 TWh/an (10-1-2023)

Digiconomist (https://digiconomist.net/bitcoin-energy-consumption) :
72,62 TWh/an (10-1-2023)

C'est un calcul minimum. La réalité sensiblement plus importante.

La dépense d'électricité dans un réseau POW (comme celui du Bitcoin)
n'est pas due au travail demandé par la validation,
mais provient principalement du **minage** destiné à désigner lequel des validateurs
doit recevoir l'incitation toutes les 10 minutes et composer la nouvelle page

Lorsque cette désignation se fait sans dépense électrique,
(c'est le cas pour un réseau POS),
on a un réseau beaucoup moins énergivore.

Exemple : de l'ordre de 1600 fois plus économe
si Bitcoin passait au POS.

Pour Ethereum passé le 15 septembre 2022 à la preuve d'enjeu l'économie a été évaluée à :

- au moins 99%

https://geeko.lesoir.be/2022/09/16/ethereum-la-consommation-energetique-a-diminue-de-99/

https://www.developpez.com/actu/315223/L-Ethereum-consommera-au-moins-99-pourcent-d-energie-en-moins-a-l-issue-du-projet-The-Merge-qui-constitue-la-transition-d-Ethereum-de-Proof-of-Work-a-Proof-of-Stake/

- au moins 99,84%

« The Ethereum network likely reduced its power demand by 99.84% to 9.9996% as a result of this change.

(Alex De Vries, Cryptocurrencies on the road to sustainability: Ethereum paving the way for Bitcoin,

https://www.cell.com/patterns/fulltext/S2666-3899(22)00265-3)

- 99,95 %

https://blog.ethereum.org/2021/05/18/country-power-no-more

D'insensible en 2009 la POW du Bitcoin est devenu un concours fou !

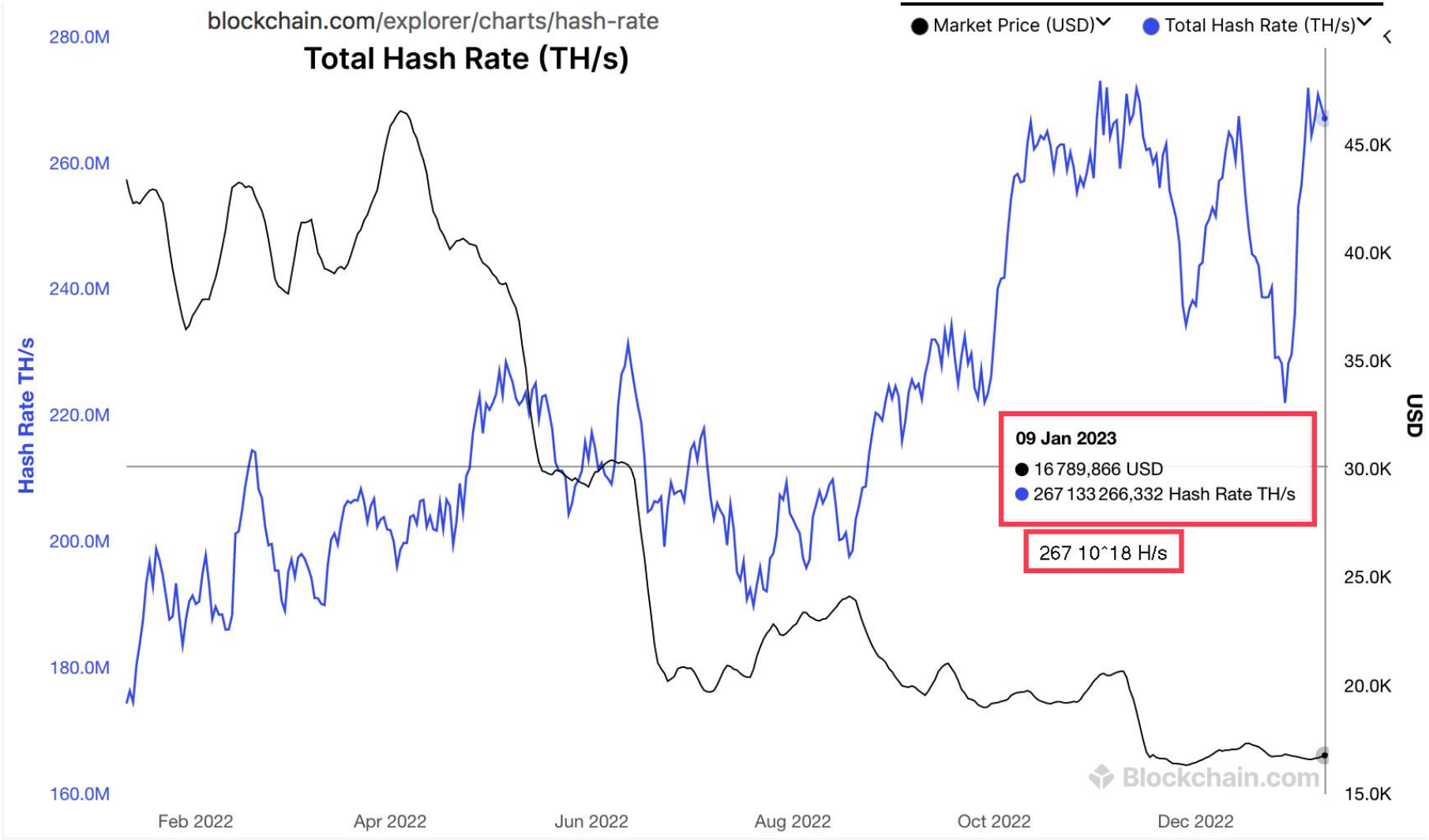
Evolution du hashrate du Bitcoin : passage par les puissances de 10

Juillet 2010 : $\mathbf{10^9}$ hash/s	octobre 2010 : $\mathbf{10^{10}}$ hash/s	Décembre 2010 : $\mathbf{10^{11}}$ hash/s
mai 2011 : $\mathbf{10^{12}}$ hash/s	Juillet 2011 : $\mathbf{10^{13}}$ hash/s	Juin 2013 : $\mathbf{10^{14}}$ hash/s
Septembre 2013 : $\mathbf{10^{15}}$ hash/s	Décembre 2013 : $\mathbf{10^{16}}$ hash/s	Juin 2014 : $\mathbf{10^{17}}$ hash/s
Février 2016 : $\mathbf{10^{18}}$ hash/s	Novembre 2017 : $\mathbf{10^{19}}$ hash/s	Janvier 2020 : $\mathbf{10^{20}}$ hash/s

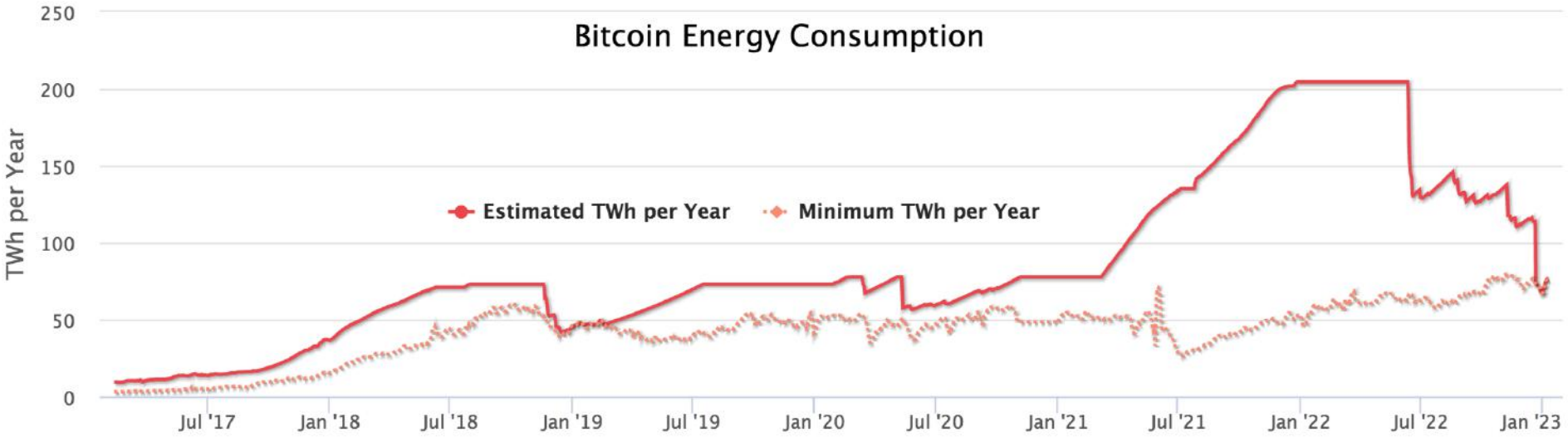
Janvier 2023 : $\mathbf{2{,}6.10^{20}}$ hash/s

8.10^9 d'humains sur terre. Pour chacun, à chaque seconde, on calcule 32 milliards de hash !

2.10^{16} fourmis sur terre. Pour chaque fourmi, à chaque seconde, on calcule 13 000 hash !


blockchain.com/explorer/charts/hash-rate
Total Hash Rate (TH/s)
Market Price (USD)
Total Hash Rate (TH/s)
Hash Rate TH/s
USD
280.0M
260.0M
240.0M
220.0M
200.0M
180.0M
160.0M
45.0K
40.0K
35.0K
30.0K
25.0K
20.0K
15.0K
Feb 2022
Apr 2022
Jun 2022
Aug 2022
Oct 2022
Dec 2022
09 Jan 2023
16 789,866 USD
267 133 266,332 Hash Rate TH/s
267 10^18 H/s
Blockchain.com

Digiconomist :



Pourquoi baisse de la courbe rouge ?

Les rigs les moins efficaces ont été arrêtés récemment car devenu non rentable à cause de la baisse des cours du bitcoin.

Plus les cours du bitcoin son bas, moins le réseau consomme !

D'où viennent les 2,4 millions de rigs ?

Antminer s19 Pro est parmi les meilleur avec 110 Th/s pour 3250 W

https://www.softwaretestinghelp.com/bitcoin-mining-hardware/#1_Antminer_S19_Pro

Hashrate du réseau = 267.10^{18} hash/s (10-1-2023)

https://www.blockchain.com/charts/hash-rate

Donc : $(267.10^{18}) / (110.10^{12}) = 2427272$ = **2,4 millions de machines**

qui dépensent 2400000*3250 W = 7800000000 W = $7{,}8*10^{9}$ W

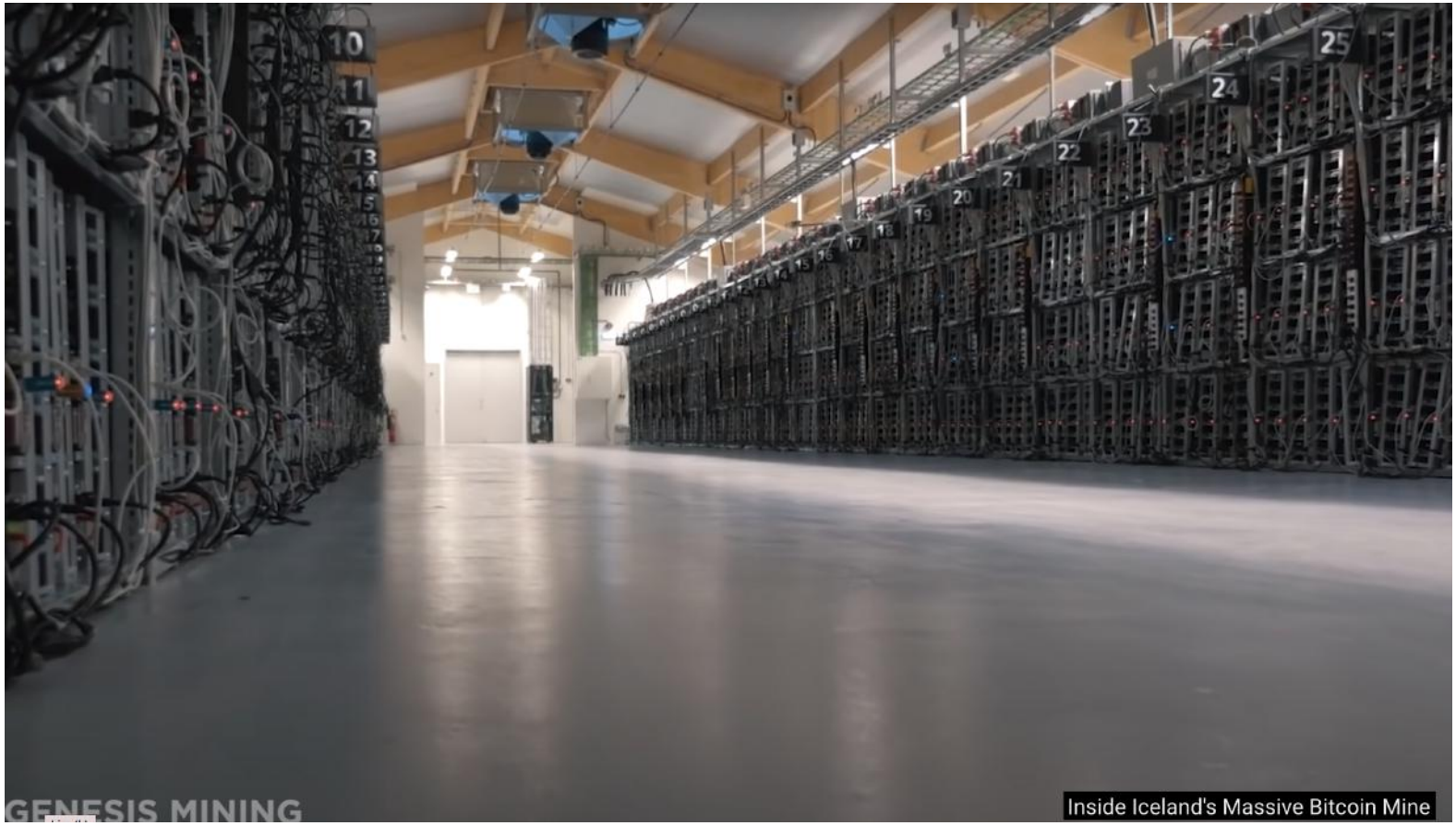
ce qui donne $(7.8*10^{9})*(24*365)$ Wh/an = $6.8*10^{12}$ Wh/an = **68 TWh/an**

(63 TWh/an si on utilise 3000 W au lieu de 3250)


OCCASION
ANTMINER S19 PRO 110TH/S
4 083.60 €


+12V GND
ANTMINER
ANTMINER

Époque du bricolage amateur !

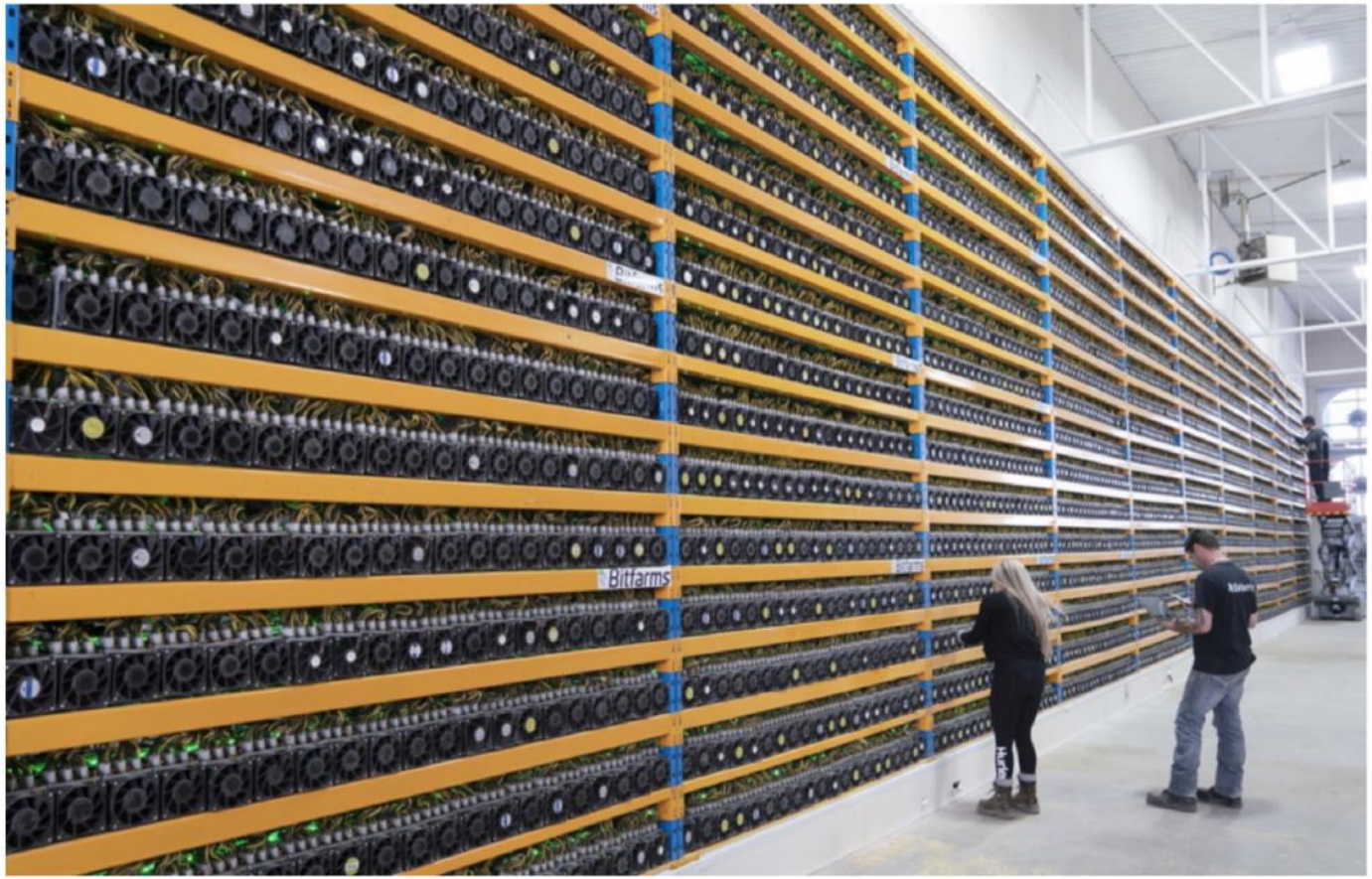


Genesis, Islande.

Bitmain, Chine.

Bitfury, Amsterdam.

Stronghold Digital Mining (SDIG), based in the United States,



Mine de Bitcoins. Bitfarm Canada

CryptoUniverse, Russie.

Hyperblock, Canada

Riot Blockchain, Castel Rock USA. (50% de ce que produit un réacteur nucléaire)

La Chine a interdit le minage, il y a deux ans.

Le Kosovo aussi.

L'état de New York aux États-Unis a interdit le minage avec des énergies fossiles, en novembre 2022.

L'Europe hésite.

B Arguments contre la POW, liés aux conséquences techniques, sociales et économiques

B1 La POW incite aux vols d'électricité (pas la POS !)

Un exemple parmi des centaines. **En décembre 2022 dernier en Thaïlande**.

L'Autorité provinciale de l'électricité (PEA) a constaté que de l'électricité était volée via des câbles branchés directement sur les lignes de transport d'électricité.

Le vol durait depuis neuf mois.

Pertes d'environ 1 million de bahts (27 071 euros).

https://toutelathailande.fr/news/augmentation-des-vols-delectricite-par-des-fermes-a-bitcoin-en-thailande/

B2 La POW incite au vol de puissance de calcul (*cryptojacking*) (pas la POS !)

Rapport (Mars 2022) **Atlas VPN** et **Trend Micro**, (sociétés spécialisées en sécurité informatique),

• Les malwares pour le **cryptojacking** : 150 00 cyberattaques détectées au cours de l'année 2021.

https://www.phonandroid.com/bitcoins-le-cryptojacking-est-devenu-la-technique-preferee-des-pirates-en-2021.html

B3 La POW contribue à la pénurie de composants électroniques. (pas la POS !)

Publication dans une revue scientifique :

Alex De Vries : Bitcoin's growing e-waste problem, Resources, Conservation and Recycling, V 175, Dec 2021.

« Les déchets électroniques de Bitcoin représentent **30,7 millions de kg par an**, comparable aux déchets des équipements informatiques et de télécommunication des Pays-Bas. »

B4 La POW est un frein instantané à la montée des cours. (pas la POS !)

• Les mineurs pour amortir leurs investissements et le coût de l'électricité vendent leurs jetons.

• En 2022, on estime que tout ce que les mineurs de bitcoins ont gagnés a été vendu.

(ce qui n'a pas empêché la faillite de Core Scientific)

B5 La POW est un frein sur le long terme à la montée des cours. (pas la POS !).

Si on ne prend pas en compte les halvings :

La dépense électrique du minage est en gros proportionnelle

au coût du minage,

qui est proportionnel (ou au moins directement lié) aux revenus des mineurs,

qui sont proportionnels aux cours du Bitcoin

L'électricité du minage = entre 10% et 20% de la production électrique en France.

Imagine-t-on que cela devienne 100% 200% !!!

B6 La POW tend à masquer la multitude des risques.

Partout on lit que **plus le minage est important plus le Bitcoin est sécurisé.**

C'est oublier que toutes sortes de dangers qui guettent un réseau blockchain ne sont pas du tout concerné par le minage quel que soit sont niveau :

- **Bug** :

- 15 août 2010. Un hacker de créer 184 milliards de faux bitcoins. Réaction rapide des validateurs.

- Bug CVE-2018-17144 découvert en 2018. Corrigé *in extremis*. Possible chute du réseau.

- **Attaque des primitives** : fonction de hachage SHA256, protocole de signatures des transactions (ECDSA avec secp256k1). Il y a, à moyen terme, un risque **quantique**.

- **Attaques diverses.**

B7 Attaquer un réseau POW est moins risqué qu'attaquer un réseau POS.

- On ne peut pas confisquer les machines de l'attaquant d'un réseau POW !

- La confiscation des sommes déposées dans le cas du POS est très dissuasive !

C Arguments basés sur les conséquences économiques et environnementales de la POW

C1 La POW produit inévitablement de la pollution.

C2 Réprobation morale : handicap compétitif pour la POW face à la POS.

C3 Ponction sur les réseaux pouvant créer des pannes électriques graves.

C4 Trouble environnemental immédiat (bruit, chaleur).

C5 Impact général sur les prix de l'électricité.

C6 Handicap réglementaire potentiel : risque d'interdiction élevé pour la POW

C7 Frein à la décentralisation.

D Arguments factuels montrant que la POS sécurise bien une blockchain publique

D1 Résistance avérée de la POS : Cardano, Polkadot, etc.

D2 Les nouvelles blockchains n'utilisent jamais la POW.

D3 Ethereum passé en POS le 15 septembre 2022 et tout va bien !

E Les faux arguments en faveur de la POW

E1 Argument :

« Il est normal que la sécurisation ait un coût.

L'absence d'un tel coût important pour la sécurisation des réseaux POS montrent qu'ils sont moins bien protégés que les réseaux POW ».

La magie de la consommation d'électricité : « il faut souffrir pour être belle ! »

E2 Argument :

« La POW est utile de manière générale aux centrales de production électriques.

Acheter l'électricité qu'elles surproduisent leur apporte un soutien financier.

Le développement du minage favorise le développement en général des centrales électriques, et particulièrement de celles qui fonctionnent avec des énergies renouvelables dont la production est intermittente. ».

Réponse à Argument "POW favorable aux énergies renouvelables"

Acheter l'énergie sur-produite encourage à en sur-produire encore plus ce qui engendre de plus en plus de dégâts environnementaux.

Réponse à Argument "POW favorable aux énergies renouvelables"

On peut faire autre chose de l'énergie produite non utilisée immédiatement.

- **A -** **La faire circuler** en développant les réseaux électriques.
- **B -** La stoker en produisant de l'**hydrogène vert** par électrolyse
  Pour les éoliennes en mer : Lhyfe au large du Croisic. https://fr.lhyfe.com/
- **C -** Produire de l'**hydrogène et du méthane de synthèse**.
  Projet Jupiter1000 https://www.jupiter1000.eu
- **D -** STEP en montagne. Utiliser des "STEP" **Station de transfert d'énergie par pompage**
  On monte l'eau quand trop d'électricité est produite, on la descend pour la récupérer.
- **E -** STEP à l'eau de mer : en cours de développement.
- **F -** Batteries (station massive, ou voitures).
- **G -** CAES (Compressed Air Energy Storage), stockage par air comprimé.
- **H -** Le stockage d'énergie par volant d'inertie.

Est-ce que l'électricité utilisée est de l'énergie renouvelable ?

Bitcoin Mining Concil (11-1-2023)

Association de mineurs qui représente 45% du minage dans le monde.

Pour les membres 67,8 % d'énergie renouvelable.

Pour tout le minage 59,7 % d'énergie renouvelable

https://bitcoinminingcouncil.com/bitcoin-mining-council-survey-confirms-year-on-year-improvements-in-sustainable-power-mix-and-technological-efficiency-in-q3-2022/

Ce sont les données d'une association de lobbying pro-minage.

Même en acceptant leurs données :

Il y a donc 40,3 % d'énergies non renouvelables.

Donc aujourd'hui une dépense colossale d'énergies non renouvelables !!!

N'oublions jamais que toute production d'énergie est polluante.
Les énergies renouvelables le sont moins que les autres mais le sont.

Données du GIEC :

La production d'un KWh d'électricité produit

11 g de CO_2 pour l'éolien,
12 g pour le nucléaire,
24 g pour l'hydro-électricité,
de 40 g à 48 g pour le photovoltaïque,
230 g pour la biomasse,
490 g pour le gaz naturel,
820 g pour le charbon.

Rapport : British Columbia Hydro (BC Hydro) Décembre 2022

(Compagnie de production et distribution électrique en Colombie-Britannique.)

Crypto conundrum:

Why cryptocurrency mining could challenge B.C.'s clean transition.

« L'extraction de crypto-monnaies consomme des quantités massives d'électricité pour faire fonctionner et refroidir des séries d'ordinateurs puissants 24h sur 24, 7 jours sur 7, 365 jours sur 365, tout en créant très peu d'emplois dans l'économie locale.

L'énergie rendue disponible par BC Hydro pourrait être mise à mal par les opérations de minage de crypto-monnaies.

Cela pourrait signifier **moins d'énergie pour des évolutions vertes** comme l'électrification ou la production d'hydrogène.

Cela pourrait aussi signifier des **tarifs d'électricité plus élevés** pour les habitants de la Colombie Britannique »

Campagne Greenpeace

https://cleanupbitcoin.com/manifesto

https://cleanupbitcoin.com/

« Change The Code: Not The Climate »

Campagne pour pousser Bitcoin à modifier son code lancée par :

l'Environmental Working Group, Greenpeace USA.

Le POS une des 10 percées technologiques de 2022, pour le MIT

MIT Technology Review's list of the 10 biggest technology breakthroughs in 2022.

1. Moving away from passwords
2. Coronavirus variant tracking
3. A long-lasting grid battery
4. Artificial intelligence for protein folding
5. GlaxoSmithKline's malaria vaccine
6. Proof of stake
7. COVID-19 antiviral pills
8. Practical fusion reactors
9. Synthetic data for training AI
10. The world's largest carbon removal factory in Iceland

Conclusion

Ceux qui défendent l'intérêt général
et non les intérêts particuliers des surproducteurs d'électricité,
des mineurs ou des détenteurs de cryptoactifs POW
doivent lutter farouchement contre la POW qui est une folie.

Remarque. On n'a pas traité des rançongiciels (ransomware) qui ont conduit parfois à réclamer l'interdiction générale de toutes les cryptoactifs car avec les rançongiciels c'est l'anonymat possible des utilisateurs qui est en cause et pas la POW.

Riot Blockchain, Castel Rock USA

Le hachage et les preuves de travail

• **Une fonction de hachage cryptographique** est une fonction ***h*** qui à toute suite de symboles **S** (un fichier) associe une autre suite de symboles (plus courte)

$$h(S) = R, \text{ vérifiant :}$$

— il est impossible en pratique pour une valeur possible **R** de trouver un **S** tel que :

$$h(S) = R.$$

— les valeurs ***h*(S)** produites par quelqu'un qui essaie diverses valeurs pour **S**, sont aussi imprévisibles que si elles étaient tirées au hasard.

— en particulier changer un symbole de **S** change totalement ***h*(S))**

• Disposant de ***h*** on définit un *travail* impossible à faire rapidement :

Travail de niveau *k* : Trouver **S** tel que ***h*(S)** commence par ***k*** fois '0'.

Plus ***k*** est grand, plus il faut essayer de nombreux **S**
avant d'en trouver un **S** convenable.

Ceux qui prétendent avoir trouvé **S** ont fourni un travail
qui est d'autant plus important que ***k*** est grand.

• C'est comme si on demandait à quelqu'un de :

lancer deux dés jusqu'à obtenir un double 6

(en moyenne, il doit les lancer 36 fois pour réussir).

• On vérifie facilement que les **S** prétendument trouvés sont bons et en calculant ***h*(S)** qui doit être un résultat avec ***k*** '0' en tête.

Un seul calcul de ***h*** vérifie que les calculs faits pour trouver S ont bien aboutis.

Trouver S est long, vérifier S est rapide

L'idée de ces ***preuves de travail*** a été proposée pour lutter contre le spam :

- si chaque ordinateur qui veut accéder à ma boîte de messages doit prouver qu'il a effectué un certain travail, il devient impossible d'envoyer de milliers de spam.

Pour Bitcoin, le validateur qui propose une page calcule le hash de l'en-tête de la page.

Cet en-tête contient un nombre appelé le **nonce**.

Le validateur fait varier le nonce jusqu'à ce que le hash H vérifie la propriété

$$H < D$$

où D est la difficulté réévaluée toutes les 2016 pages (14 jours) pour que le temps moyen qu'un validateur du réseau trouve le nonce qui fera gagner sa page soit 10 minutes.

Est-ce que Wei Dai avec B-money a inventé la POS ?

Non, dans le cas de Wei Dai B-Money, on ne peut pas parler de POS, car il ne s'agit pas de choisir un validateur pour lui attribuer l'incitation dans un réseau pair-à-pair mais au contraire d'un droit que les validateurs payent pour valider.

Il n'y a d'ailleurs **pas de distribution de l'incitation puisqu'il n'y a pas d'incitation**.

Comme le protocole ne comporte pas de distribution d'incitation et qu'il n'est pas mentionné que les sommes à déposer sont proportionnelles à quoi que ce soit, on ne peut pas parler de POS.

Celui qui prétend que c'est du POS, doit remonter encore plus loin quand on pratiquait des systèmes de vote censitaire (où plus vous avez d'argent plus votre vote compte).

Il n'y a que deux attitudes cohérentes :

- ou bien (a) le POS et le POW sont de vielles inventions et le POW est sans doute première ;
- ou bien (b) la POW et la POS doivent être considérées comme liées à un registre distribué sur une réseau P2P, ce que Bitcoin a inventé, et alors la POS est venue après la POW avec **Peercoin en 2012**.

• En fait... c'est *QuantumMechanic* (c'est un speudo) qui propose l'idée du POS en 2011 :
https://bitcointalk.org/index.php?topic=27787.0

• Concernant l'idée que Nakamoto connaissait la POS grâce à Wei Day et ne l'a pas choisie :
Ludovic Lars explique et justifie qu'en fait Nakamoto n'avait pas lu le papier de Wi Day.
https://journalducoin.com/analyses/b-money-wei-dai-prefiguration-conceptuelle-de-bitcoin/

Wei Day B-money-2 Des détails !

https://learn.saylor.org/mod/book/view.php?id=30735&chapterid=6705

Il n'y a pas de chaînes de blocs mais seulement des "validateurs" appelés "**server**" qui doivent garder et mettre à jour un cahier de compte.

Ils peuvent être sollicités par ceux qui font des transactions (appelés « **regular user** ») quand ils veulent contrôler qu'il n'y pas de doubles dépenses : ils interrogent plusieurs "**servers**" et font confiance à la transaction reçue si les réponses sont compatibles.

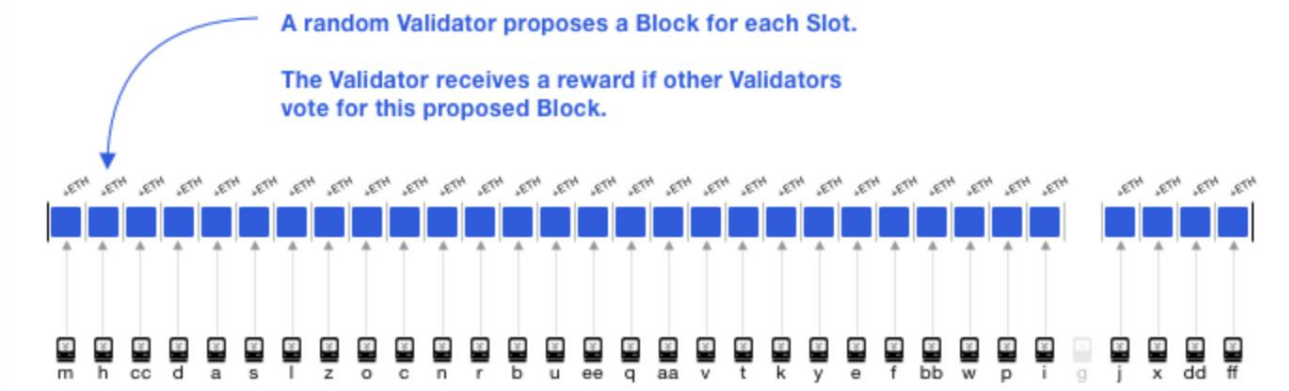
Pour être "**server**" il faut déposer une somme, mais il n'est rien précisé sur cette somme. Il n'est pas dit que cette somme ne doit pas être la même pour tout le monde.

Dans le système, il n'y a pas d'incitation, et surtout il n'est pas dit que la probabilité d'avoir une récompense (il n'y en a pas !!!) est proportionnelle à la somme engagée.

The Merge Ethereum

15 septembre 2023

The Merge : changer un moteur d'avion de 170 milliards de $ en vol !!!



Pour être **validator** il faut engager **32 Ethers**.

12 secondes par (slot) block. **32 slots (= 6,4 minutes) = Une epoch**

Vocabulaire : validator, slot, epoch, committee, proposer, proposed, justified, finalised, checkpoint, supermajority, etc. etc.

Les **epoch** sont des groupes de 32 **slots**.

128 validators sont choisis au hasard pour former chaque **committee** d'un **slot.**

Un **slot** peut être vide. Pour chaque **slot** un **proposer** est choisi au hasard.

Le **proposer** produit le **block**, les **validators** donnent leur accord.

Un **block** passent par trois étapes : **proposé, justifié, finalisé**.

Il faut à la fin d'une **epoch** que les 2/3 des **validators** l'acceptent.

L'aléa est engendré par la balise aléatoire RANDAO.

À chaque instant, il y a un ensemble de **validators** actifs.

Un validateur ne peut être que dans un seul **committee** d'une **epoch**.

Il est possible qu'un **validator** soit le **proposer** d'un slot en même temps qu'un des 32 **validators** du slot.

À chaque **epoch** les **validators** sont répartis au hasard par RANDAO
sur les slots, et regroupés en **committee**.
Un algorithme fixe le nombre de **committee** par **slot** de façon à avoir 128 **validators** par **committee**. Un **checkpoint** est un bloc dans une **epoch**.

Quand une **epoch** se termine si son **checkpoint** a obtenu une **supermajority** des 2/3 le **checkpoint** est **finalisé.**

Les Eth engagés sont bloqués jusqu'à la mise à jour **Shanghai** dans quelques mois.

Plus de 11% des ethers existants ont été engagés.

La récompense moyenne pour un engagement de 32 ethers (dépend du nombre total de validateurs) avec l'accroissement du nombre de validateurs le rendement est passé de 15% à 4,44%

Riot Blockchain, Castel Rock USA