Bitcoin

Alexis Direr

18 juin 2023

Plan de la leçon

Genèse

Le 31 octobre 2008, un développeur anonyme Satoshi Nakamato décrit sur mailing list le fonctionnement de Bitcoin :

"I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party. (...) The main properties : Double-spending is prevented with a peer-to-peer network. No mint or other trusted parties. Participants can be anonymous. New coins are made from Hashcash style proof-of-work. The proof-of-work for new coin generation also powers the network to prevent double-spending."

source

Bitcoin: A Peer-to-Peer Electronic Cash System

Bitcoin est “un système de paiement électronique basé sur une preuve cryptographique plutôt que sur la confiance, permettant à deux parties désireuses d’effectuer des transactions directement l’une avec l’autre sans avoir besoin d’un tiers de confiance.”

source

3 janvier 2009 : le bloc 0 est codé.

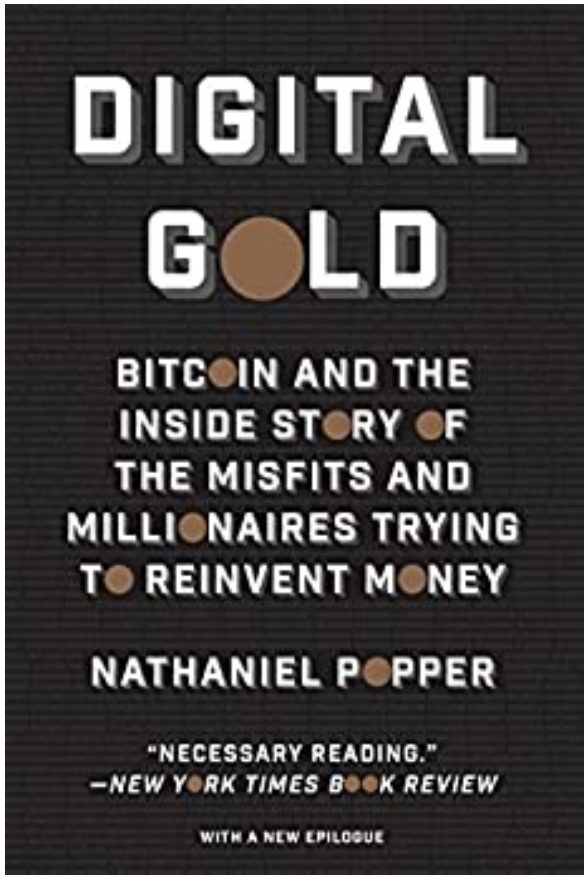
9 janvier 2009 : le premier bloc est miné.

12 janvier 2009 : la première transaction a lieu.

$\longrightarrow$ naissance des cryptomonnaies à l'origine d'un éco-système foisonnant et d'une industrie pesant des milliers de milliards de dollars

source : 1

Histoire de Bitcoin :



source : 1

Les visages multiples de Bitcoin

Une technologie entachée d'inefficacités :

▷ dépenses massive d'énergie (preuve de travail)

▷ scalabilité limitée (7 transactions par seconde)

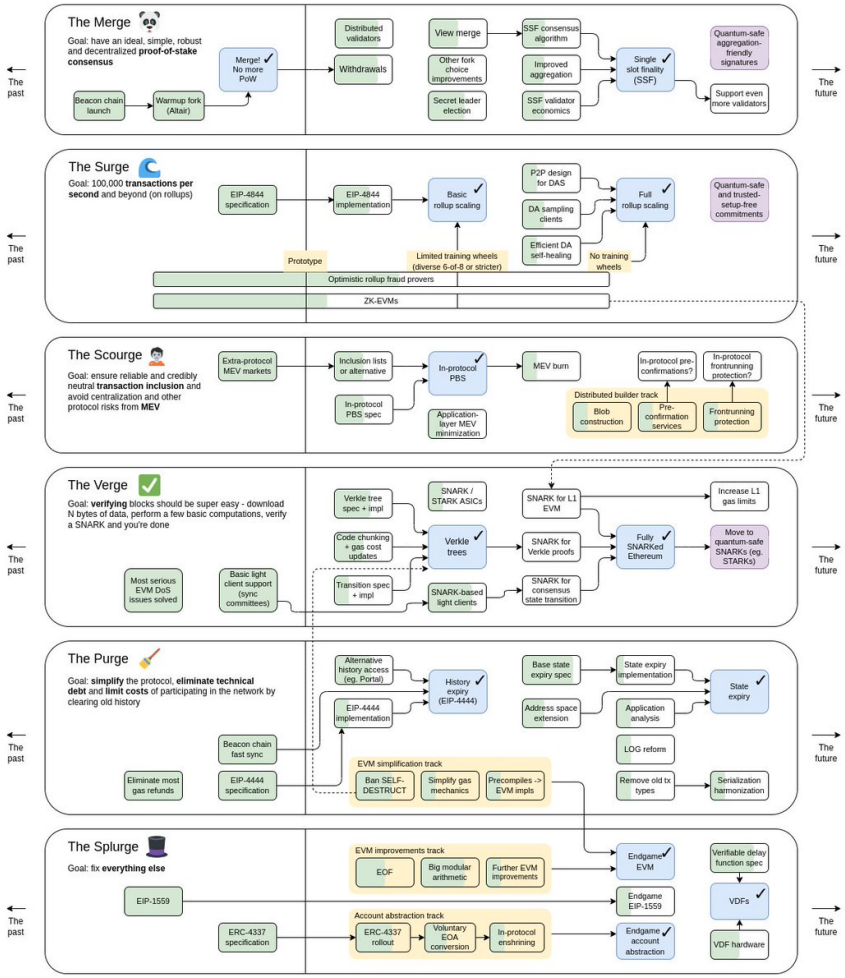
Une technologie minimale :

▷ peu d'améliorations depuis sa création

▷ pas de smart contracts

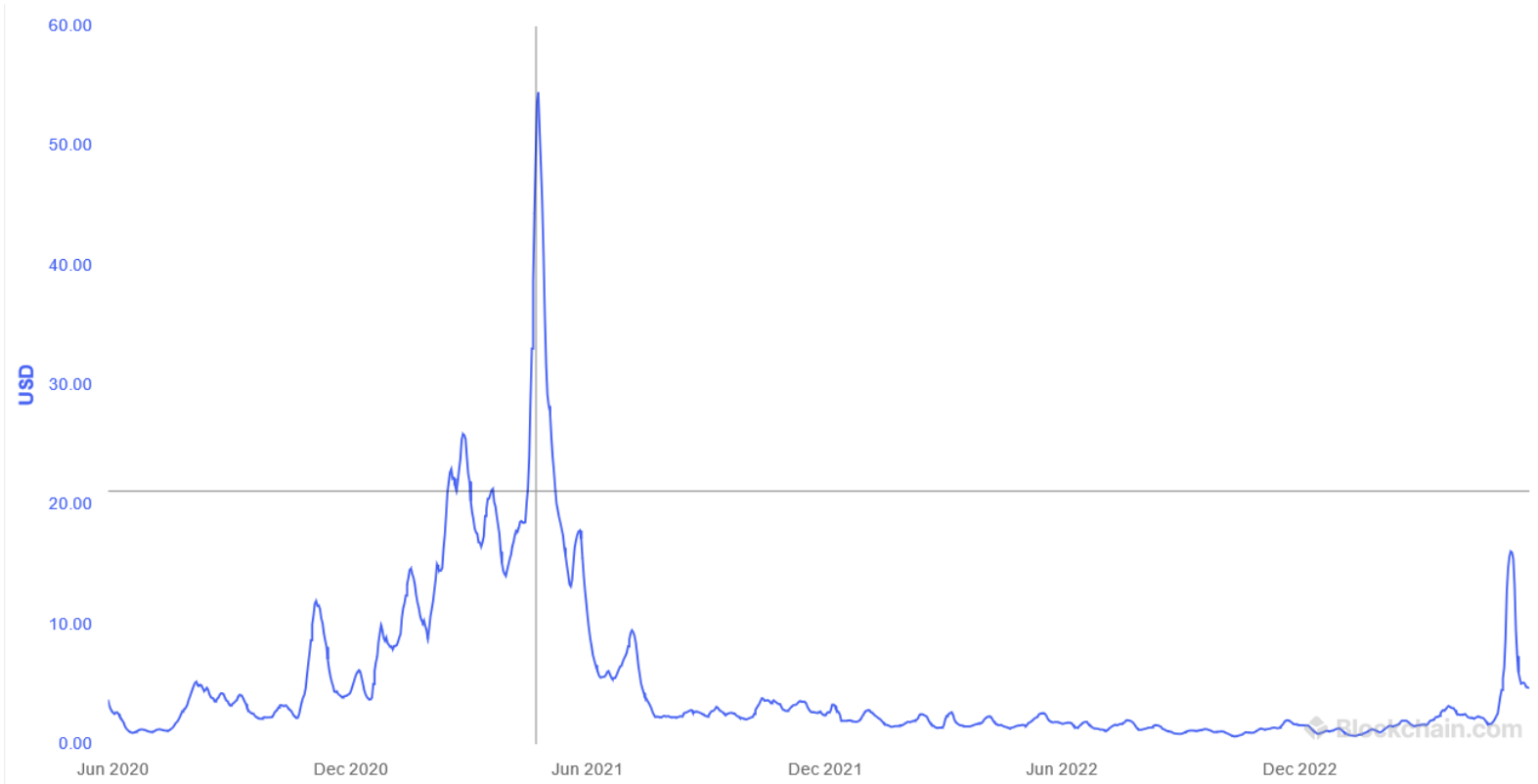
▷ *roadmap* limitée (ossification du protocole)

La *roadmap* d'Ethereum (pour comparaison)



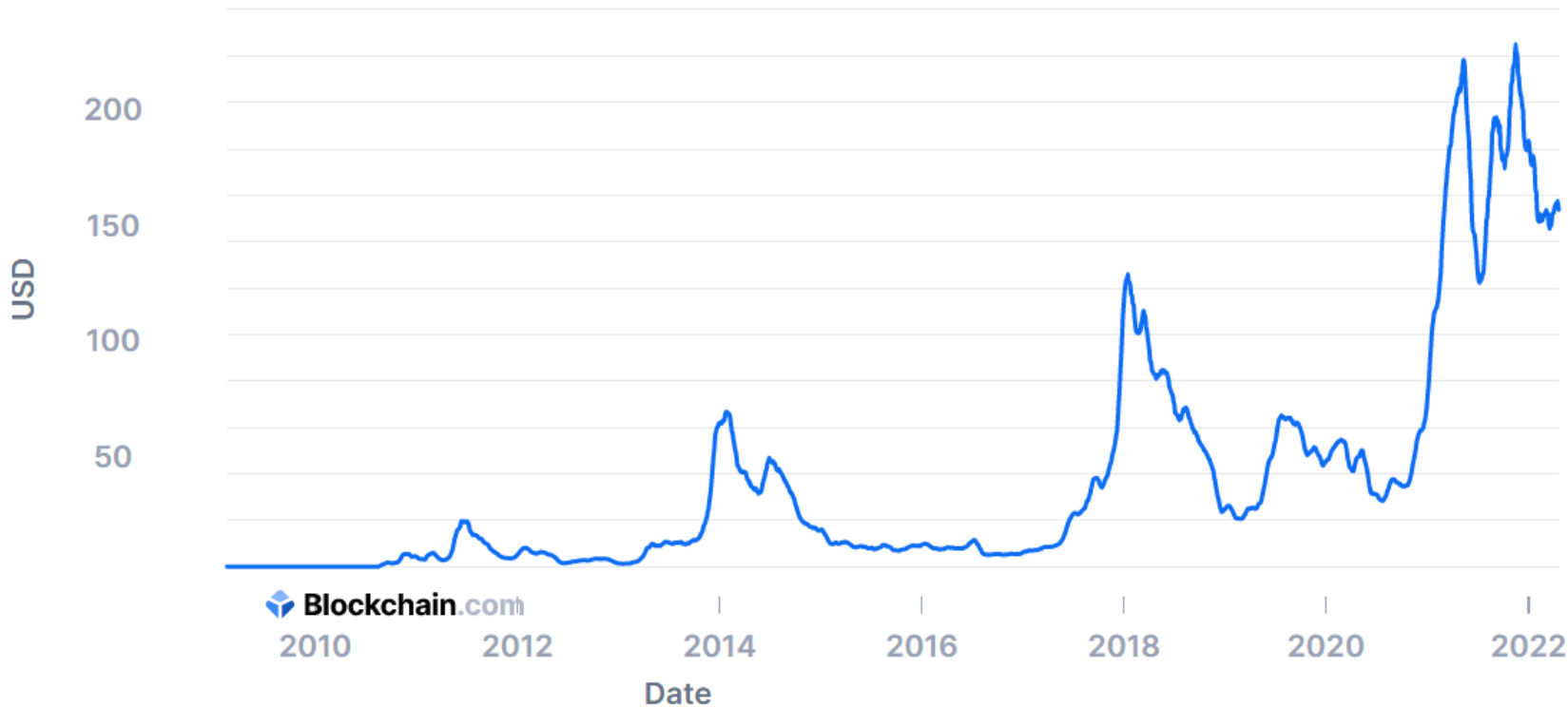
source : 1

Frais de transaction explicites : quelques dollars



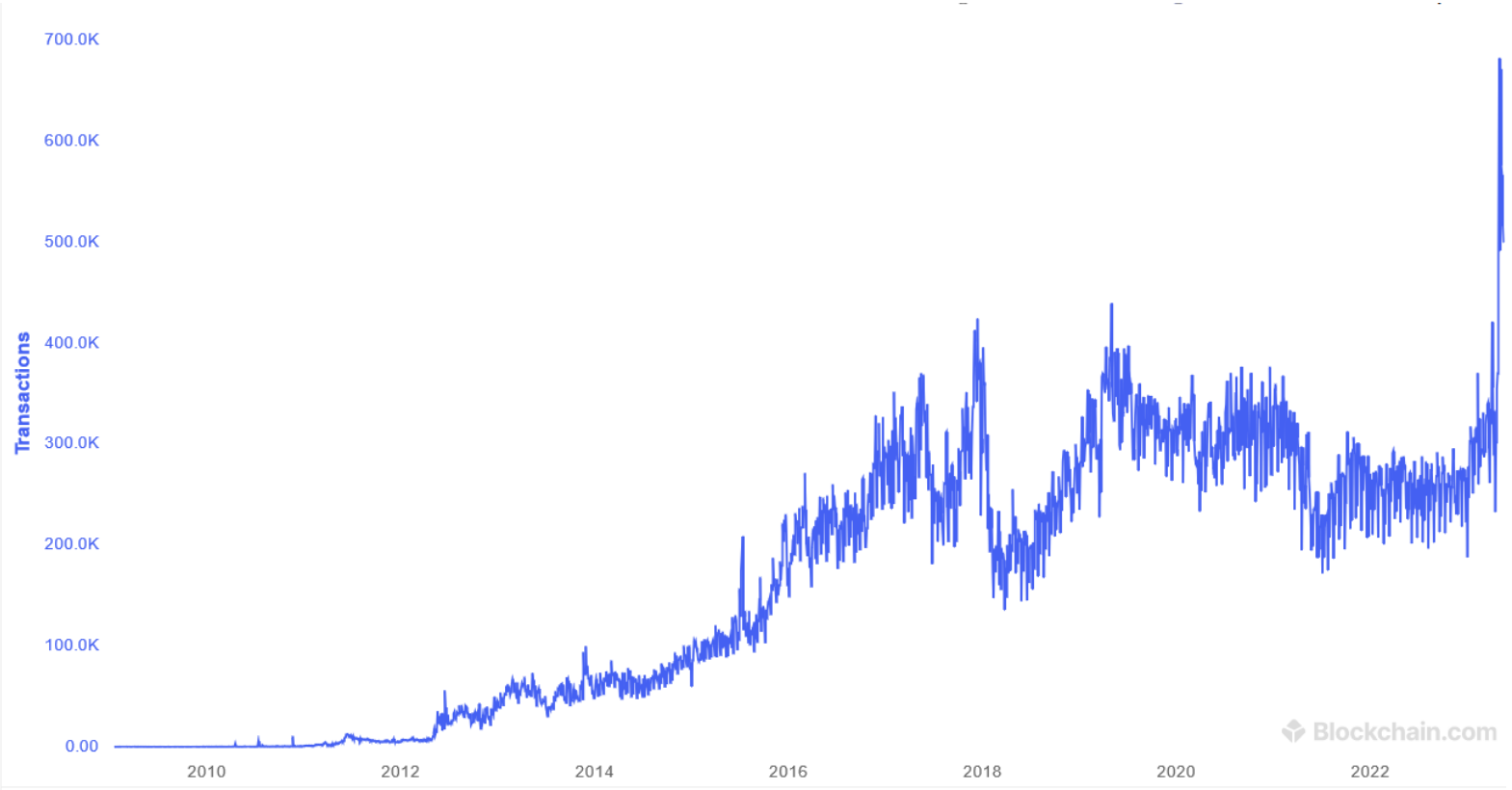
Moyenne sur 7 jours (source)

Coût complet par transaction (incluant la création monétaire)



Moyenne sur 30 jours (source)

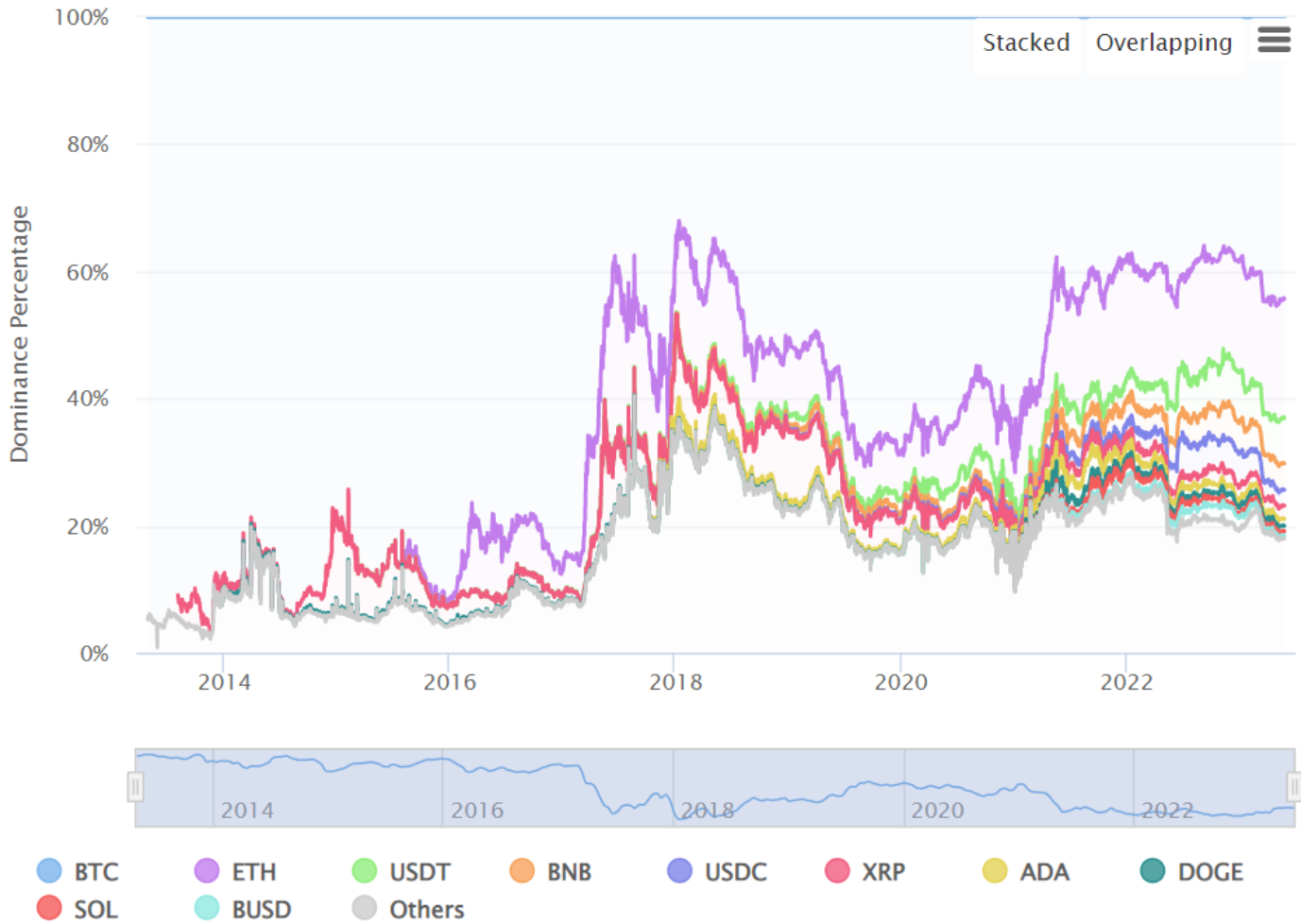
Usage : entre 200 000 et 400 000 transactions par jour (3-4 tps)



source

vu le 23/05/2023

Popularité de Bitcoin (40 % de la capitalisation totale des cryptoactifs)



source vu le 27/05/2023

Comment expliquer la domination de Bitcoin ?

Des messages qui passent :

- Absence d'intermédiaire (être sa propre banque)
- Nombre maximal de pièces capé (21 millions)
- Or digital
- Décentralisation et protection contre la préemption et la censure (sécurité cryptographique)

source

Décentralisation d'une blockchain : nombre de participants vérifiant la validité des blocs

Hasu
@hasufl

Let's make one thing clear:

You defend against malicious protocol changes by having a culture of users validating the blockchain

Not by having PoW or PoS

1:41 PM · Mar 30, 2021 · Twitter for iPad

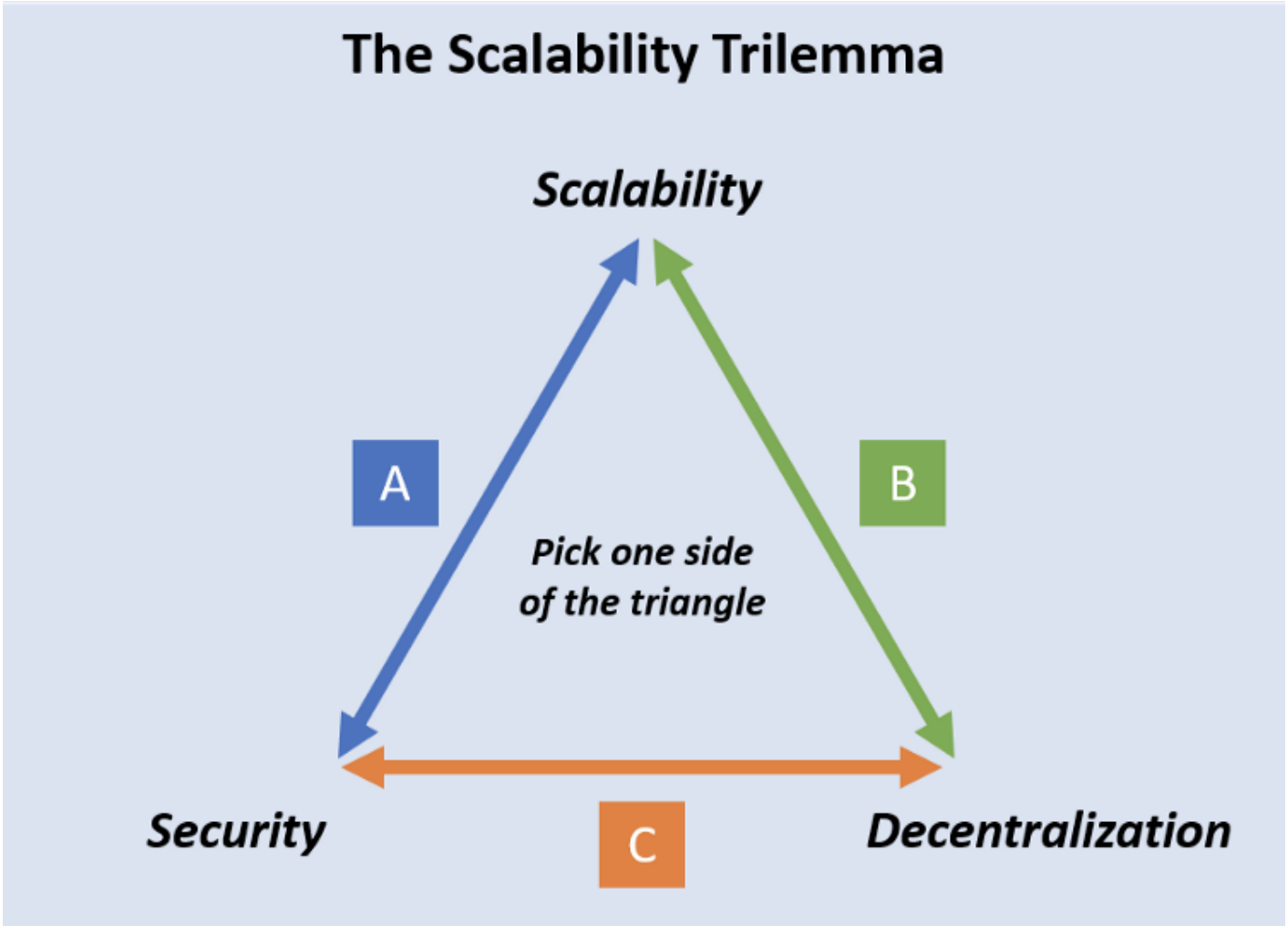
34 Retweets **6** Quote Tweets **295** Likes

source

Une blockchain optimisée pour la décentralisation : facilité d'exécution d'un noeud

"*Features, not bugs*" :

- scalabilité limitée (rejet d'un accroissement de la taille des blocs)
- gouvernance minimisée (BIP)
- pas de smart contracts
- pas de dépendances externes (oracles, stablecoins, ...)
- preuve de travail (contesté)


The Scalability Trilemma
Scalability
A
B
Pick one side
of the triangle
Security
C
Decentralization

Une communauté forte

▷ militante, exclusive et parfois maximaliste (*no second best*, déni du changement climatique, anti-establishment, ...)

source

Une culture de memes

source

Une défiance vis à vis du système monétaire et bancaire mondial

THE TIMES

DIEU ET MON DROIT

Max 5C, min -5C | Saturday January 3 2009 timesonline.co.uk No 69523 | £1.50

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

Francis Elliott Deputy Political Editor
Gary Duncan Economics Editor

Alistair Darling has been forced to consider a second bailout for banks as the lending drought worsens.

The Chancellor will decide within weeks whether to pump billions more into the economy as evidence mounts that the £37billion part-nationalisation last year has failed to keep credit flowing. Options include cash injections, offiering banks cheaper state guarantees to raise money privately or buying up "toxic assets", The Times has learnt.

The Bank of England revealed yesterday that, despite intense pressure, the banks curbed lending in the final quarter of last year and plan even tighter restrictions in the coming months. Its findings will alarm the Treasury.

The Bank is expected to take yet more aggressive action this week by cutting the base rate from its current level of 2 per cent. Doing so would reduce the cost of borrowing but have little effect on the availability of loans.

Whitehall sources said that ministers planned to "keep the banks on the boil" but accepted that they need more help to restore lending levels. Formally, the Treasury plans to focus on state-backed gurantees to encourage private finance, but a number of interventions are on the table, including further injections of taxpayers' cash.

Under one option, a "bad bank" would be created to dispose of bad debts. The Treasury would take bad loans off the hands of troubled banks, perhaps swapping them for government bonds. The toxic assets, blamed for poisoning the financial system, would be parked in a state vehicle or "bad bank" that would manage them and attempt to dispose of them while "detoxifying" the mainstream banking system.

The idea would mirror the initial proposal by Henry Paulson, the US Treasury Secretary, to underpin the American banking system by buying

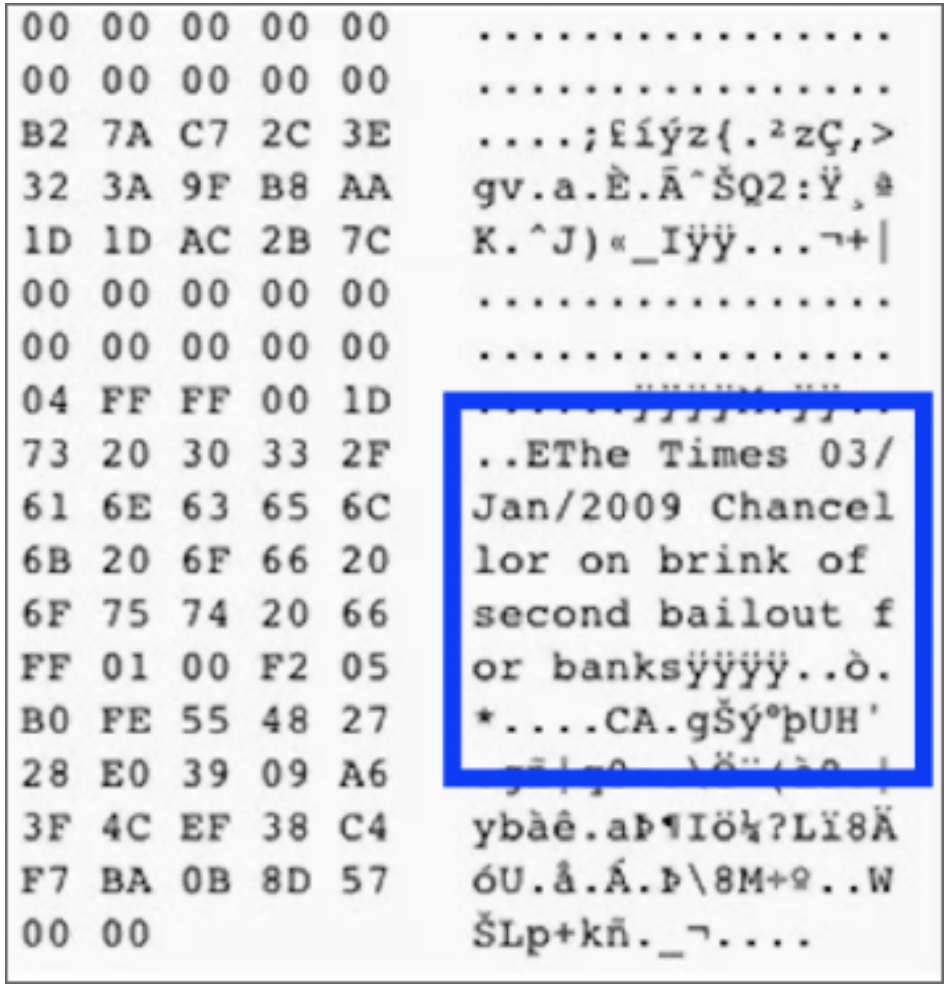
Continued on page 6, col 1
Leading article, page 2

99p

Pub chain cuts the price of a pint from £1.69 to 1989 levels

Business, page 47

source


00 00 00 00 00 .....
00 00 00 00 00 .....
B2 7A C7 2C 3E ....;£íýz{.²zÇ,>
32 3A 9F B8 AA gv.a.È.Ã^ŠQ2:Ÿ¸ª
1D 1D AC 2B 7C K.^J)«_Iÿÿ...¬+|
00 00 00 00 00 .....
00 00 00 00 00 .....
04 FF FF 00 1D .....
73 20 30 33 2F ..EThe Times 03/
61 6E 63 65 6C Jan/2009 Chancel
6B 20 6F 66 20 lor on brink of
6F 75 74 20 66 second bailout f
FF 01 00 F2 05 or banksÿÿÿÿÿ..ò.
B0 FE 55 48 27 *....CA.gŠý°þUH'
28 E0 39 09 A6
3F 4C EF 38 C4 ybàê.aÞ¶Iö¼?Lï8Ä
F7 BA 0B 8D 57 óU.å.Á.Þ\8M+º..W
00 00 ŠLp+kñ._¬....

Raisons économiques

▷ Effets de réseau : l'utilité d'une technique ou d'un produit s'accroît avec le nombre de ses utilisateurs.

Exemples d'effets de réseaux :

- L'anglais
- Logiciels et applications (Windows, Python, ...)
- Les réseaux sociaux (Facebook, Twitter, ...), ...

source

Implication des effets de réseau

▷ *First mover advantage*

▷ *Winner takes all*

▷ Masse critique (*cold start problem**)

▷ Tension possible entre les coûts de congestion et les effets de réseau

Effet Lindy

▷ théorie selon laquelle l'espérance de vie d'une technologie ou d'une idée, est proportionnelle à leur âge actuel.

Plus une technique a survécu longtemps et est utilisé, plus elle est résistante à l'obsolescence ou à la concurrence.

Exemples :

- Les livres imprimés
- La langue anglaise
- Les jeux de société traditionnels (échecs, dames, dominos, ...)

Source

Comment fonctionne Bitcoin ?

- ▷ Les noeuds du réseau
- ▷ Les blocs et le problème de la double dépense
- ▷ Les attaques sybils et la preuve de travail
- ▷ Sécurité et immuabilité des transactions
  - ⟶ attaques à 51 %
  - ⟶ soft forks et hard forks
  - ⟶ modèle de l'oignon

Les noeuds du réseau

Bitcoin, un réseau de noeuds : environ 15 000 ordinateurs indépendants connectés les uns aux autres.

Chaque noeud valide indépendamment toutes les transactions en attente et met à jour son propre registre avec les blocs validés de transactions confirmées.

Les noeuds communiquent entre eux selon le mécanisme de la rumeur (*gossip*). Les noeuds partagent leurs infos avec un ensemble aléatoire de noeuds, qui peuvent ensuite les diffuser eux-mêmes.

$\rightarrow$ Diffusion quasi-instantanée (visualisation)

Les noeuds exécutent une application dédiée (principalement Bitcoin Core), qui contient les fonctionnalités permettant de participer au réseau :

▷ se connecter à d'autres participants du réseaux

▷ créer et envoyer des transactions sur le réseau

▷ recevoir de nouvelles transactions et les valider (l'adresse émettrice a-t-elle suffisamment de bitcoins ? La signature est-elle valide ?)

▷ recevoir de nouveaux blocs et les valider

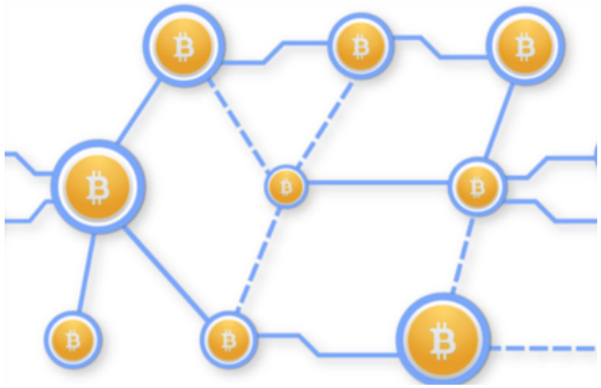
▷ relayer les transactions et les blocs validés aux autres noeuds du réseau

▷ stocker une copie à jour de la blockchain

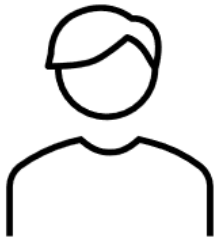
Les mineurs

Noeuds spécialisés qui regroupent les transactions valides **en blocs**, les minent et distribuent ces blocs aux noeuds du réseau.

Les transactions non encore intégrées dans un bloc restent en attente dans le *memory pool* (ou *mempool*), dupliquées dans tous les noeuds du réseau, avant d'être ajoutées dans un bloc par un mineur.



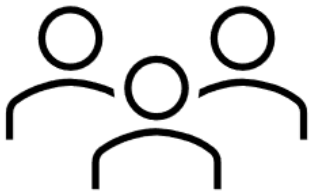
1. Envoie une transaction
+ signature aux noeuds



Bob

2. Valident la transaction

Memory pool



Mineurs

3. Confirment la transaction
En l'incluant dans un bloc

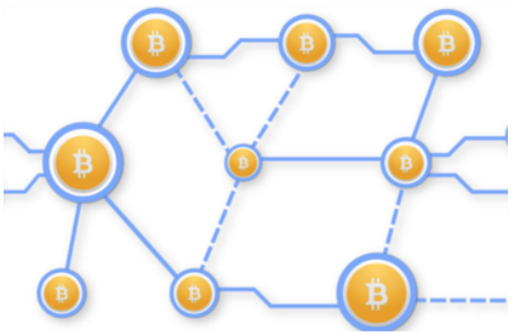
Visualisation du Mempool

Les transactions classées par frais d'inclusion dans un bloc : mempool.observer

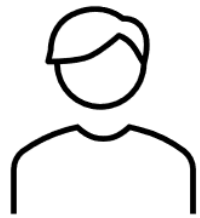
Visualisation des blocs passées et à venir : mempool.space

Des blocs comme des bus, les transactions comme des passagers : txstreet.com

Les transactions valides sont signées avec la clé privée



3. Envoie le message + la signature aux noeuds du réseau



Bob

4. Les nœuds déchiffrent le message avec la clé publique XYZ = adresse XYZ

5. Si valide, transferent les 10 bitcoins de XYZ vers ABC

1. "J'autorise l'envoi de 10 bitcoins de l'adresse XYZ vers l'adresse ABC"

2. Chiffre le message avec la clé privée XYZ = signature

Bob abandonne le contrôle de ses 10 bitcoins au détenteur de l'adresse privée associée à l'adresse publique ABC.

Pourquoi des blocs ?

▷ Le problème de la double dépense

Avec la signature numérique, Bob ne peut transférer à son profit les bitcoins détenus par Alice, protégés par sa clé privée.

Mais imaginons qu'Alice transfère les *mêmes bitcoins* à Bob et Charlie au *même moment*.

Certains noeuds pourraient valider Alice $\Longrightarrow$ Bob

D'autres noeuds pourraient valider Alice $\Longrightarrow$ Charlie

Le problème de la double dépense

(...) pour avoir connaissance de toutes les transactions (...) sans un tiers de confiance, (...) nous avons besoin d'un système pour que les participants se mettent d'accord sur un historique unique de l'ordre dans lequel elles ont été reçues. – Satoshi Nakamoto (white paper)

Comment régler un désaccord dans un réseau décentralisé ?

Solution : une transaction valide n'est pas automatiquement finalisée. Elle doit au préalable être intégrée dans un *bloc* de transactions.

Comme un seul bloc ne peut être validé à la fois, que ce bloc est proposé par un seul mineur, lequel vérifie la cohérence des transactions contenues, un bloc ne peut contenir les deux transactions d'Alice.

$\longrightarrow$ moyen par lequel les participants du réseau s'accordent sur un "historique unique des transactions".

$\longrightarrow$ centralisation temporaire du réseau

Comment sélectionner le noeud qui propose le bloc ?

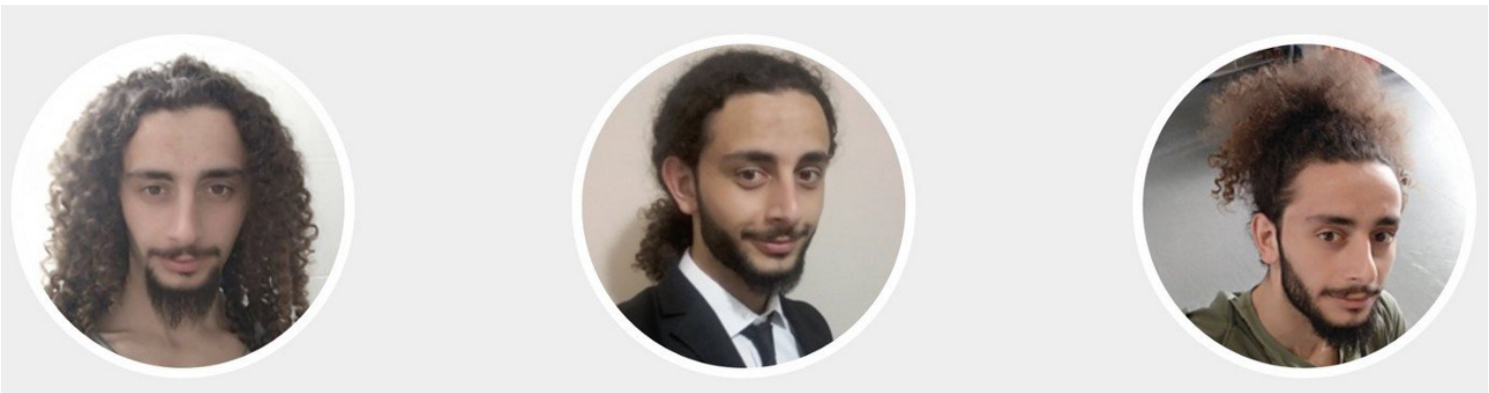
▷ personne ne peut *désigner* le noeud (point de centralité)

▷ ne doit pas être connu à l'avance (vecteur d'attaque du réseau)

▷ si tiré au sort, s'expose aux attaques sybils

Attaque sybil

En sécurité informatique, l'attaque Sybil est un détournement des règles fondé sur la création de multiples identités dans un réseau pair à pair.



Dans le cas de Bitcoin, un attaquant pourrait multiplier les noeuds sous son contrôle et émettre une majorité des blocs qu'il ferait valider par le réseau.

La preuve de travail

▷ Prévention des attaques sybils : la transaction finalisée est celle confirmée par le mineur qui a gagné un concours de devinette mathématique fondée sur le hashage (brouillage) du bloc miné.

Propriétés d'un message hashé :

1) Un même message obtient toujours le même hash

2) On ne peut pas remonter au message à partir de son hash

3) Deux messages différents ne peuvent avoir le même hash

→ Illustration : andersbrownworth.com

La recette du minage :

1) former un bloc valide en piochant des transactions dans le *mempool*

2) ajouter une transaction ex nihilo envoyant un montant défini de btc à l'adresse de son choix (transaction *coinbase*)

3) ajouter au bloc le hash du bloc précédent

4) deviner un nombre (*nonce* : *number only used once*)

5) hasher le bloc complet (hash du bloc précédent + nouvelles transactions + nonce)

6) si le hash commence par 0000000000000000000, c'est gagné !

7) sinon recommencer à l'étape 4) avec un autre nonce ...

→ Illustration : andersbrownworth

Une fois la solution trouvée :

▷ Le mineur diffuse le bloc sur le réseau.

▷ Les autres noeuds vérifient que le bloc est valide, puis l'ajoutent à leur copie de la blockchain et diffusent le bloc aux autres noeuds.

▷ Dès que les mineurs reçoivent un bloc valide, ils cessent de miner le bloc précédent et essaient de miner un nouveau bloc par-dessus le bloc miné qui vient d'être reçu.

Un nouveau concours de devinettes commence.

Pourquoi rechercher un hash ?

▷ seule la force brute permet de trouver le bon hash ⟶ plus de puissance = plus de coûts

▷ difficile à trouver, facile à vérifier par les autres noeuds du réseau

▷ prévient les attaques sybils :

- multiplier les comptes est inutile puisque seule compte la puissance de hash qu'une même entité peut installer
- démultiplier la puissance de hash est très coûteux

Autres intérêts de la preuve de travail fondée sur le hashage

▷ Le temps moyen de résolution est calculable (Loi des grands nombres)

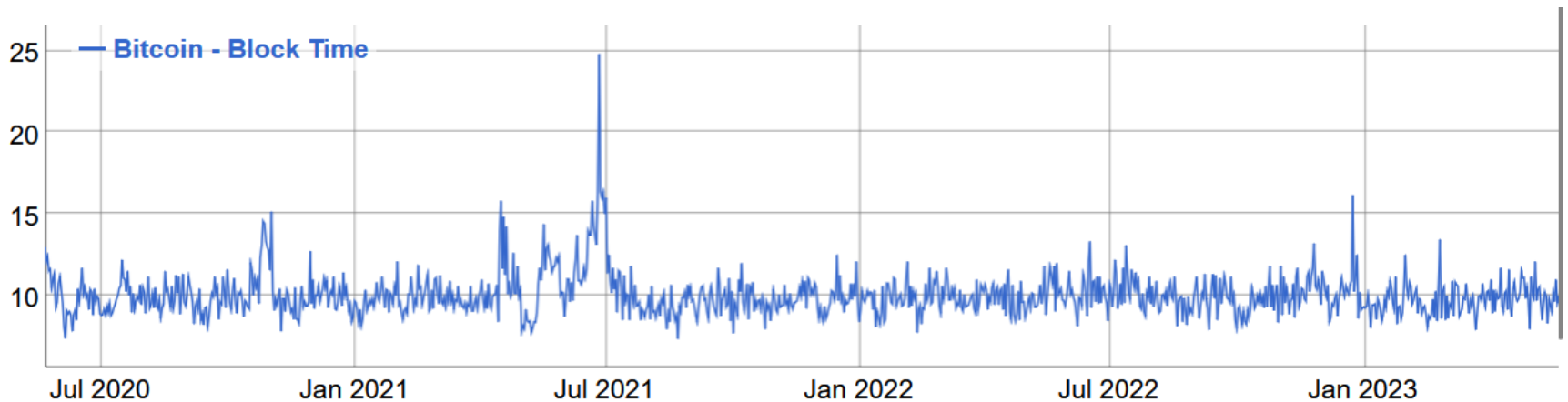
▷ Le niveau de difficulté est modulable : si le délai moyen ente deux blocs est

- inférieur à 10 minutes → ajouter des zéros
- supérieur à 10 minutes → retirer des zéros

Pourquoi 10 minutes ?

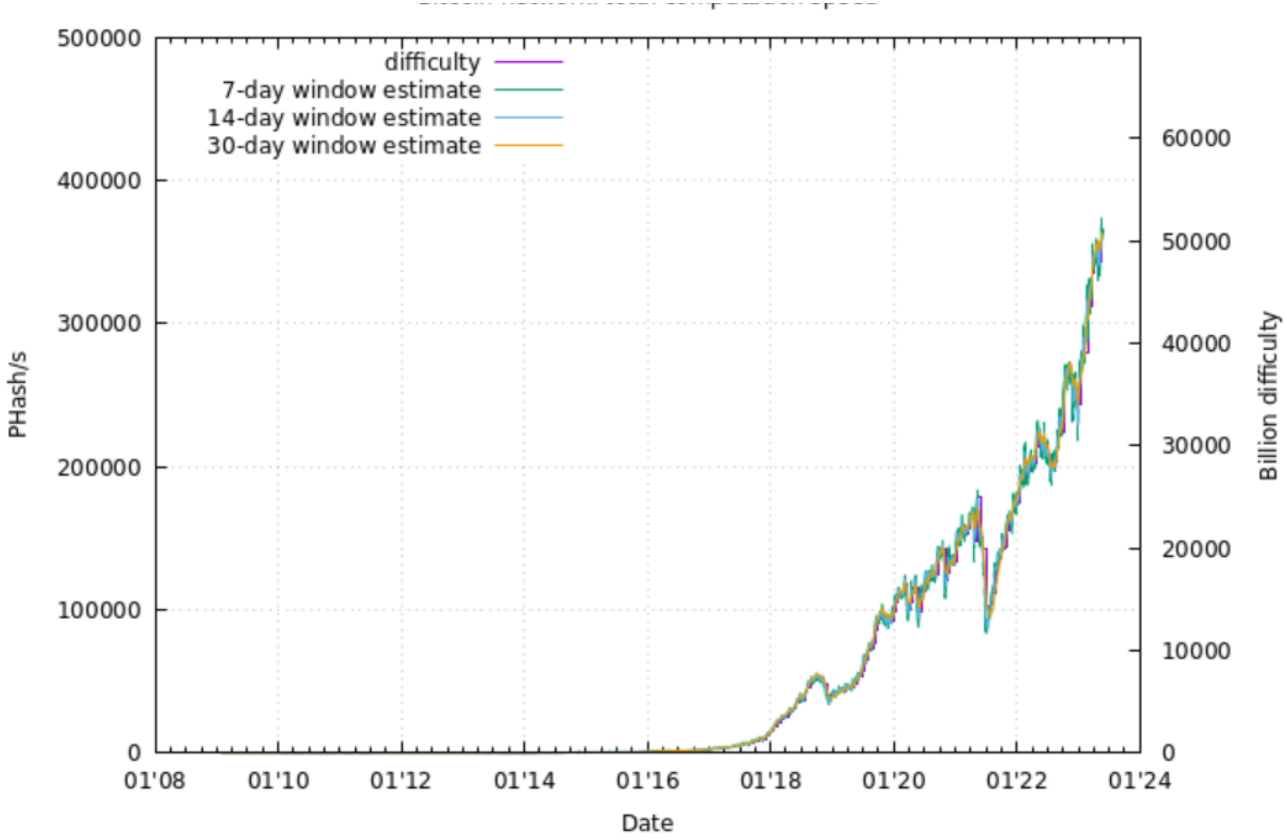
La difficulté (le nombre de zéros) est ajustée environ tous les 2016 blocs ($\approx$ deux semaine).

Temps moyen entre deux blocs



source

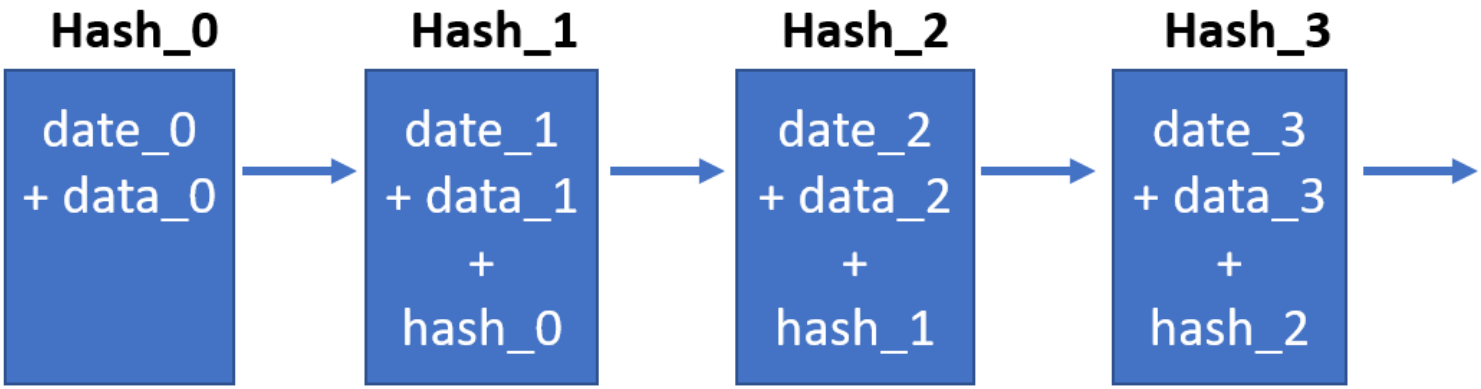
Nombre de hashs/s



400 000 Phashs = 400 millions de milliards de hashs

1, 2

Pourquoi ajouter au bloc miné le hash du bloc précédent ?



▷ réécrire un bloc nécessite de rehasher tous les blocs suivants

▷ plus un bloc est ancien dans la chaîne, plus les transactions qu'il contient sont sécurisées.

cf. Harber et Stornetta, leçon introductive

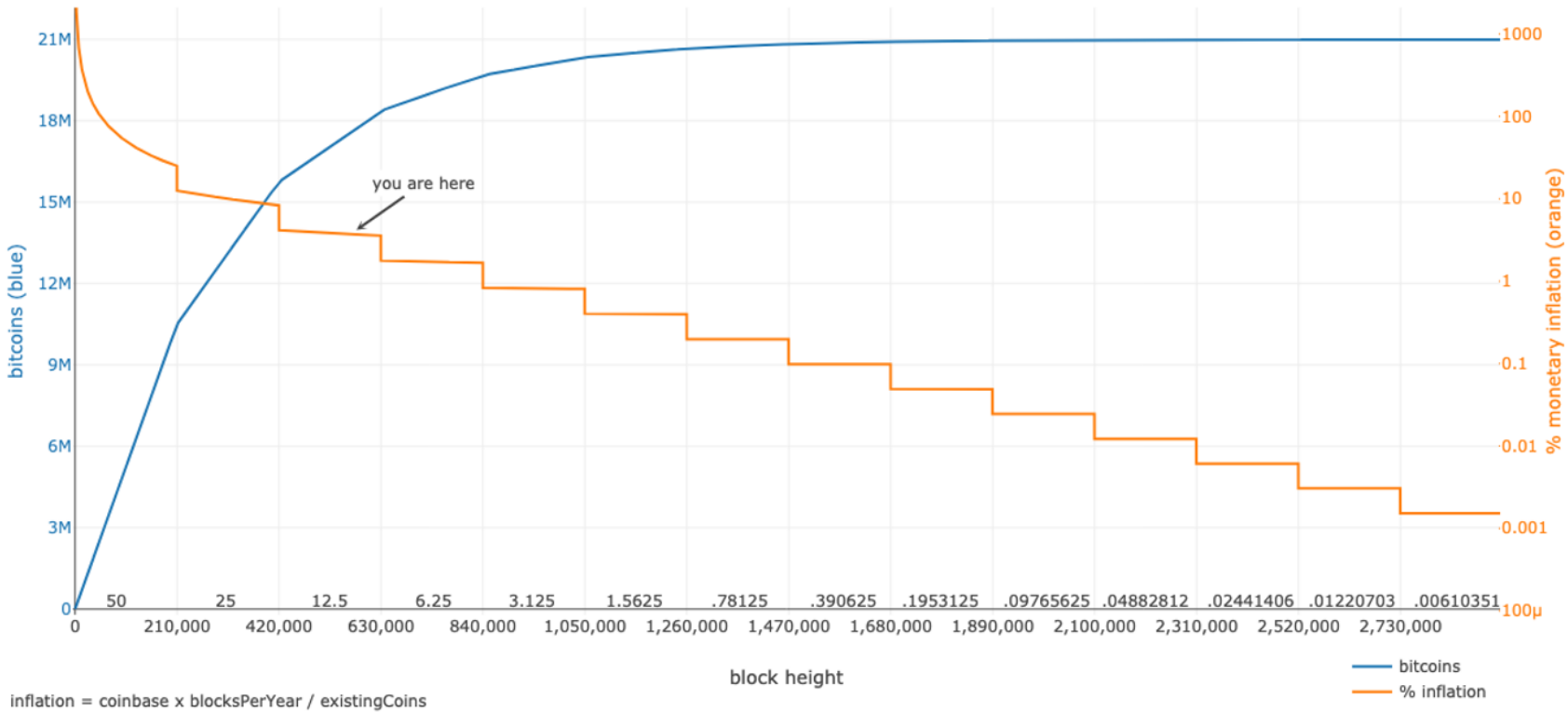
Récompenses du minage

▷ création de nouveaux bitcoins + frais de transaction

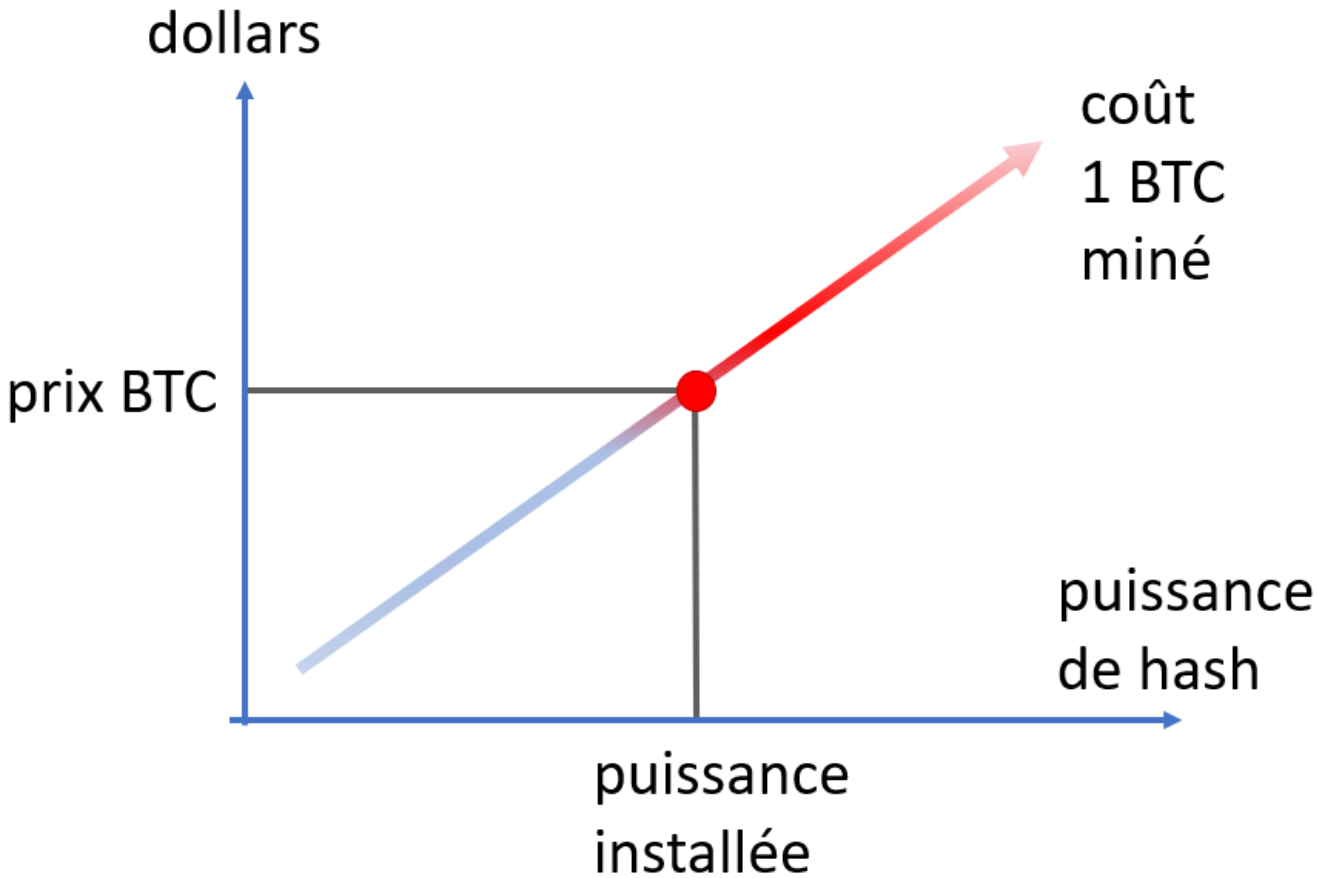
Pour chaque bloc miné, les mineurs obtiennent ou obtenaient :

- 2009-2012 : 50 btc
- 2012-2016 : 25 btc
- 2016-2020 : 12,5 btc
- depuis mai 2020 : 6,25 btc (environ 190,000 $)
- vers avril 2024 : 3,125 btc

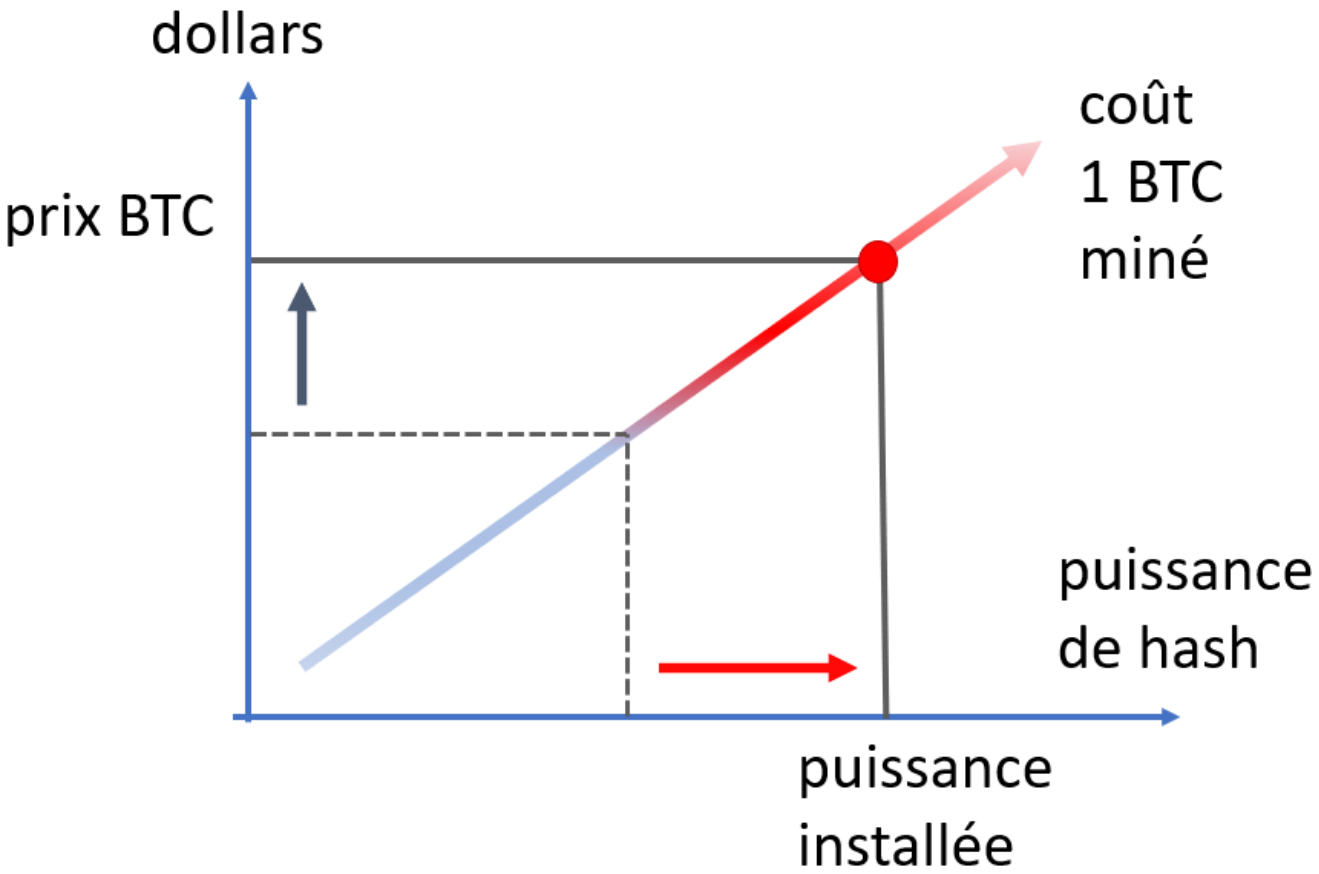
L'offre de bitcoins est borné à 21 millions



Comment est déterminé la puissance de hash totale maximale ?



La puissance de hash déployée augmente avec le prix du bitcoin



Sécurité d'une blockchain

- ▷ immuabilité des transactions
  - ⟶ règle de Nakamoto de la chaîne la plus longue
- ▷ résistance aux attaques
  - ⟶ les forks
  - ⟶ quelle protections contre les attaques à 51 % ?
  - ⟶ le modèle de l'oignon

Immuabilité des transactions

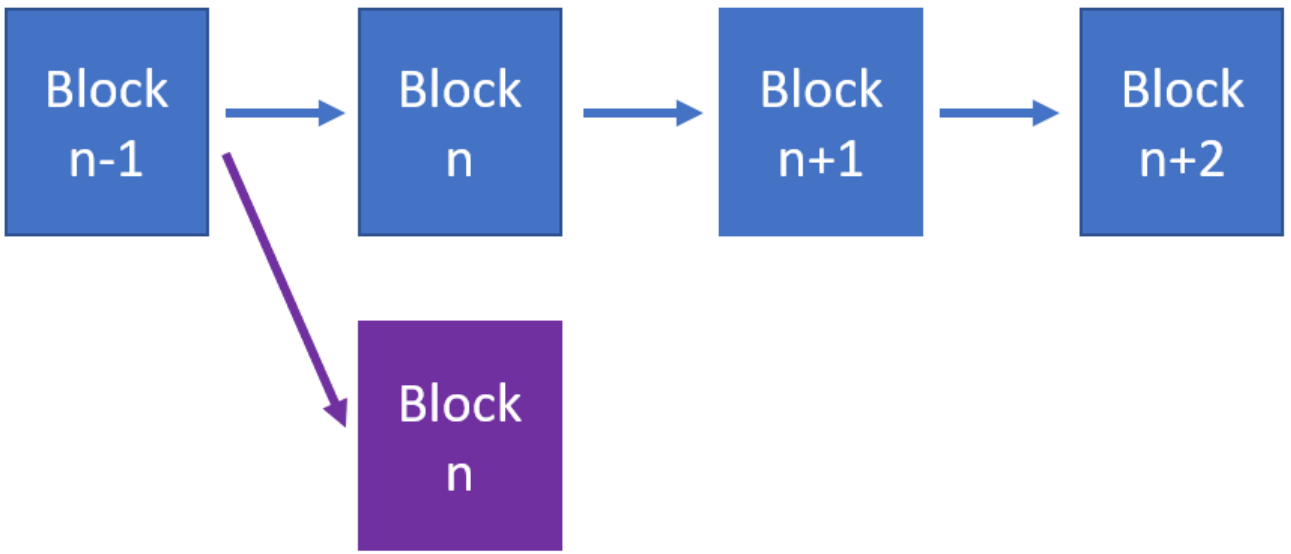
Peut-on réécrire l'histoire des transactions ? A partir de quand une transaction est-elle finalisée ?

▷ pour empêcher la double dépense les transactions sont ajoutées au registre bloc après bloc.

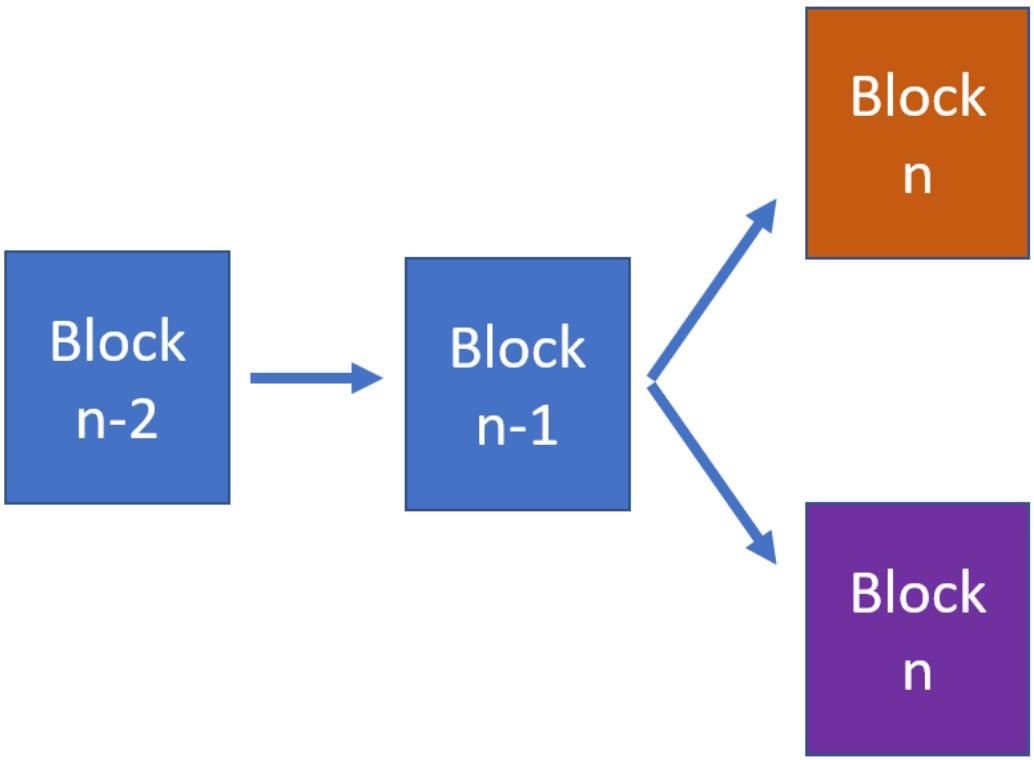
Que se passe-t-il si :

- un mineur remine un bloc passé et le diffuse dans le réseau ? (*quel intérêt ?*)
- deux mineurs minent et diffusent simultanément un bloc de même niveau ?

▷ Un mineur crée une branche dans l'historique des blocs : un *fork*.

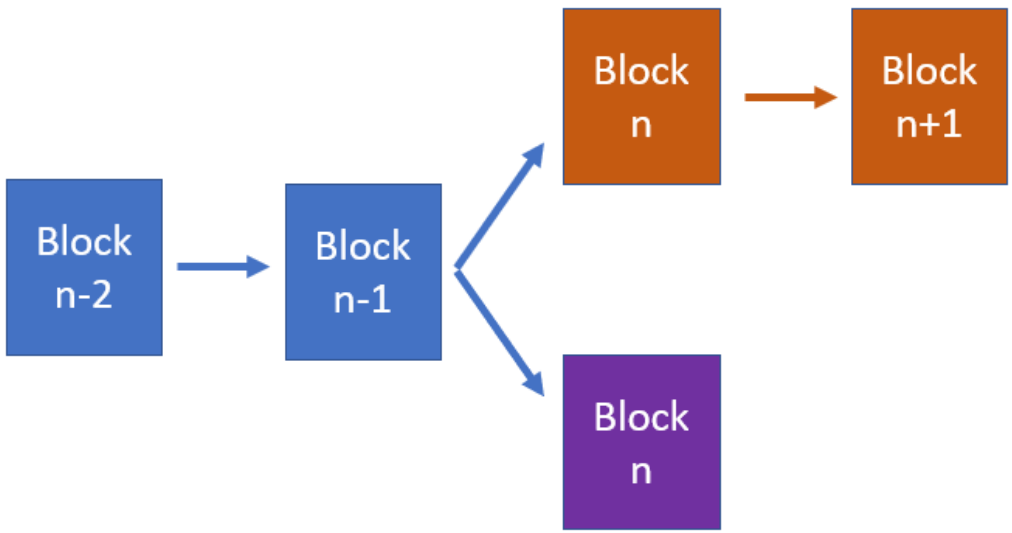


Deux mineurs minent et diffusent simultanément un bloc valide :



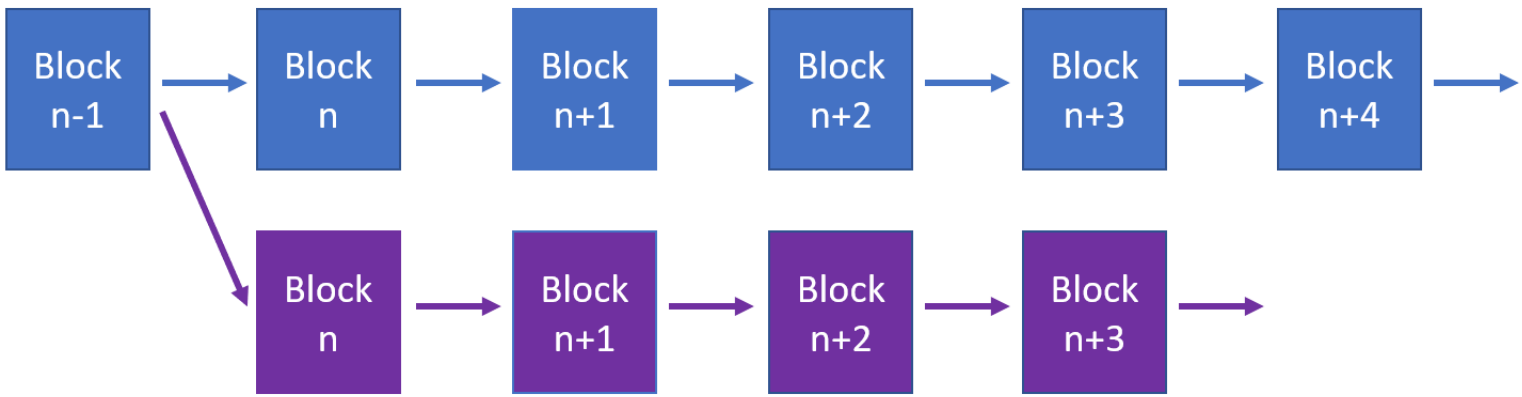
La règle de la chaîne la plus longue

Si deux blocs minés différents parviennent à un noeud du réseau, le bloc valide est le dernier miné appartenant à la chaîne la plus longue.



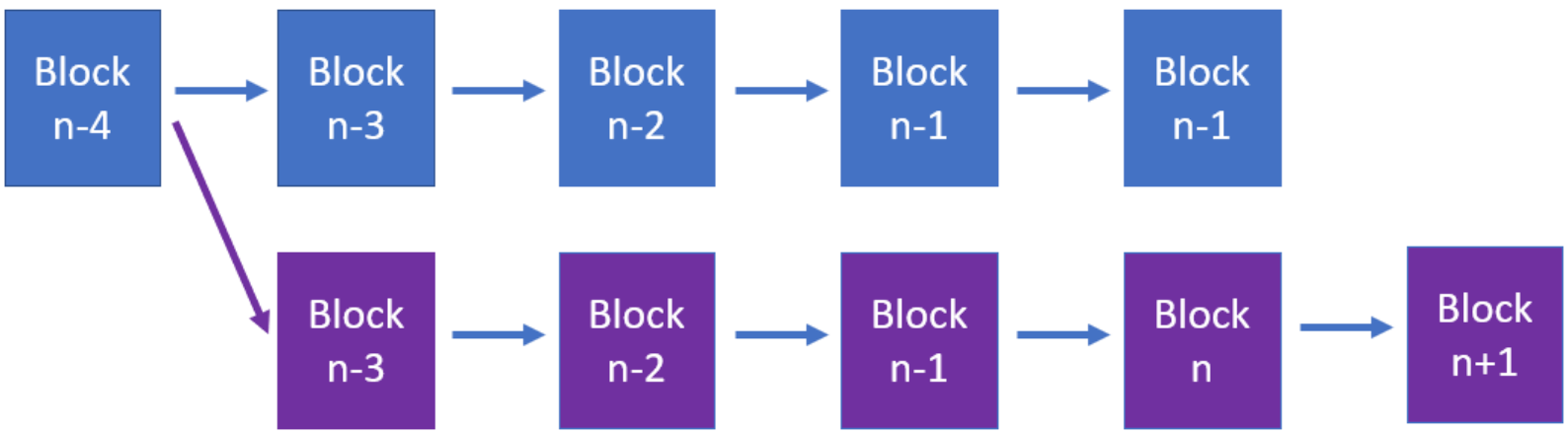
$\longrightarrow$ garantit que la majorité du réseau s'accorde sur une unique version de l'histoire.

$\longrightarrow$ décourage les acteurs malveillants de tenter de créer une chaîne alternative



$\longrightarrow$ course poursuite entre les mineurs : dépasser la chaîne principale nécessite de disposer d'au minimum 51 % de la puissance de hash totale du réseau.

L'attaquant pour réussir doit re-miner *tous* les blocs suivants jusqu'à dépasser la branche dominante.

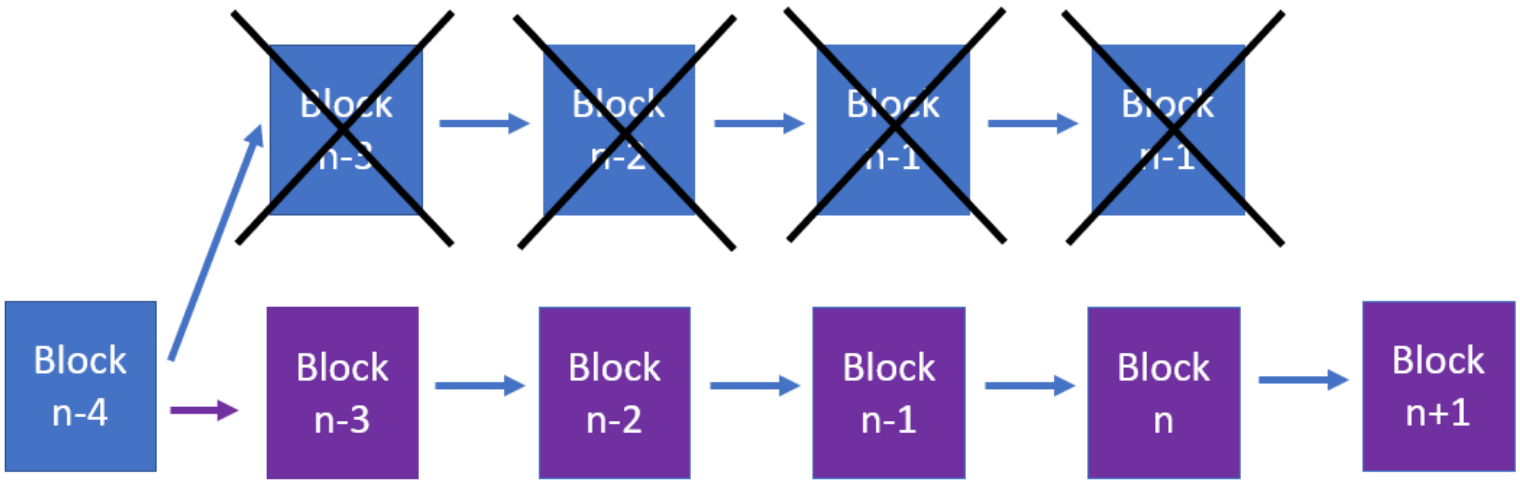


Retour sur pourquoi un délai moyen entre deux blocs de 10 minutes ?

Compromis entre :

- finalisation rapide des transactions
- limitation du nombre de forks accidentels

En cas de succès, la chaîne est *réorganisée* : l'ensemble des noeuds abandonnent la chaîne obsolète et minent le bloc suivant sur celui de l'attaquant.



Attaquer à 51 % une blockchain peut être une opération profitable :

1. transférer des bitcoins sur une plateforme d'échange
2. les échanger contre des dollars
3. les transférer dans un compte intraçable
4. réécrire l'historique des transactions en annulant le transfert initial des bitcoins vers la plateforme

Deux exemples d'attaques à 51 %

1. Bitcoin Gold (mai 2018) : double dépense de 18 millions de dollars en BTG.

2. Ethereum Classic (janvier 2019) : double dépense de plus de 200 000 ETC, soit environ 1,1 million de dollars à l'époque (3693 blocs réorganisés, soit 24h environ).

La probabilité d'une attaque est plus élevée sur les blockchains à preuves de travail faiblement capitalisées, car la puissance de hash totale qui sécurise les transactions est limitée.

Hard forks et soft forks

Supposons que la communauté des développeurs d'une blockchain rédige une mise à jour de l'application qui modifie les critères de validité des blocs, par exemple en faisant varier la taille maximale des blocs.

L'application est ensuite mise à disposition des nœuds à qui il appartient de la télécharger et utiliser.

Si tous les noeuds appliquent la mise à jour à une date convenue, la blockchain est mise à jour sans perturbations.

Que se passe-t-il si les nœuds ne sont pas d'accord sur l'intérêt de la mise à jour ?

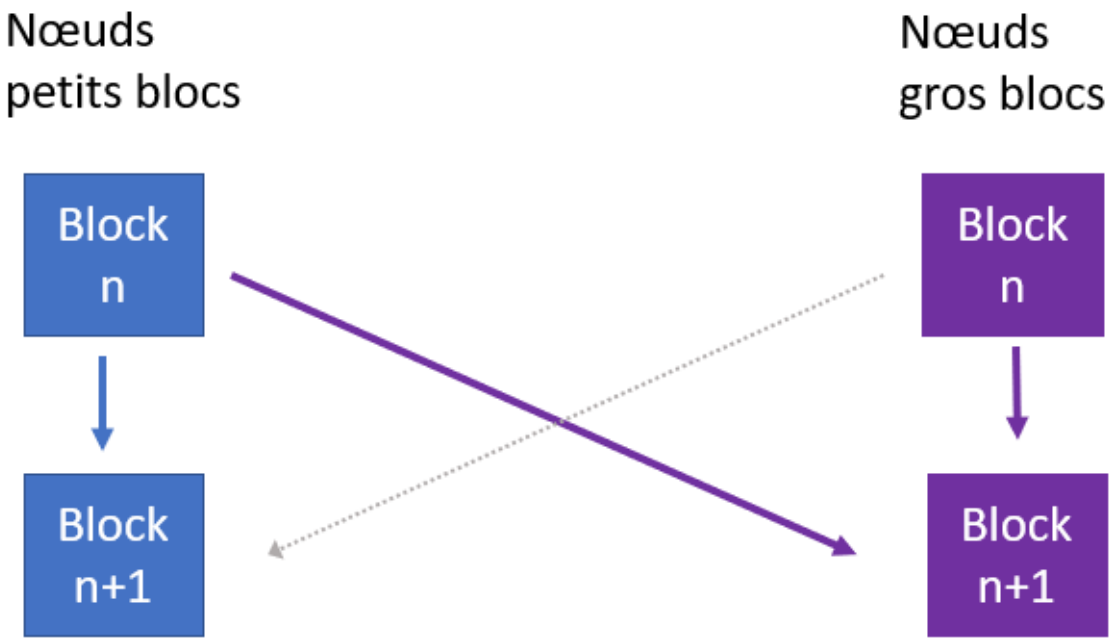
Supposons que :

- le changement consiste en une diminution de la taille maximale des blocs qui passent de 1 à 0,5 Mb
- seulement 10 % des noeuds appliquent initialement la mise à jour

La mise à jour sera-t-elle au final adoptée ?

▷ Les nœuds "grands blocs" minent des blocs au-dessus des blocs transmis par les nœuds "grands blocs" et "petits blocs"

▷ Les nœuds "petits blocs" minent des blocs au-dessus des blocs transmis par les noeuds "petits blocs" seulement.



▷ Les blocs minés par les nœuds "petits blocs" servent de bases pour les blocs minés par *tous* les nœuds

▷ Les chaînes initiées par les nœuds "petits blocs" avancent plus vite que celles initiées par les nœuds "grands blocs"

▷ Les nœuds "grands blocs" minent des blocs sur des chaînes perdantes, ...

▷ ... ou adoptent la mise à jour.

Supposons maintenant que :

- le changement consiste en une *augmentation* de la taille maximale des blocs qui passent de 1 à 2 Mb
- 80 % des noeuds appliquent initialement la mise à jour

La mise à jour sera-t-elle au final adoptée ?

Que pourrait-il arriver ?

Différence entre soft forks et hard forks

- les soft forks introduisent des modifications qui *restreignent* les critères de validité
- les hards forks introduisent des modifications qui *élargissent* les critères de validité des blocs (pas de rétro-compatibilité des versions)

Avec un soft fork, les noeuds sont incités à adopter la mise à jour.

réf

Conséquence des hard forks

▷ scission de la chaîne (*contentious hard fork*) : deux communautés de nœuds maintiennent une blockchain différente.

▷ duplication des coins : si quelqu'un possède 10 btc à la date de la scission, il a maintenant 10 btc dans chacune des deux blockchains (base de données dupliquées).

▷ division de la puissance de calcul $\longrightarrow$ affaiblissement du réseau et risque accru d'attaques à 51 %.

Exemple de hard forks : Bitcoin Cash relève la taille des blocs à 8 Mb (août 2017).

Rank	Nom	Symbole	Cap. Marché	Prix
1	Bitcoin	BTC	€63,938,781,307.50	€3,865.20
2	Ethereum	ETH	€27,669,017,792.12	€293.06
3	Bitcoin Cash	BCH	€8,483,139,902.74	€512.30
4	XRP	XRP	€7,399,409,694.37	€0.193
5	Litecoin	LTC	€3,419,911,292.79	€64.81

vu le 03/09/2017

source

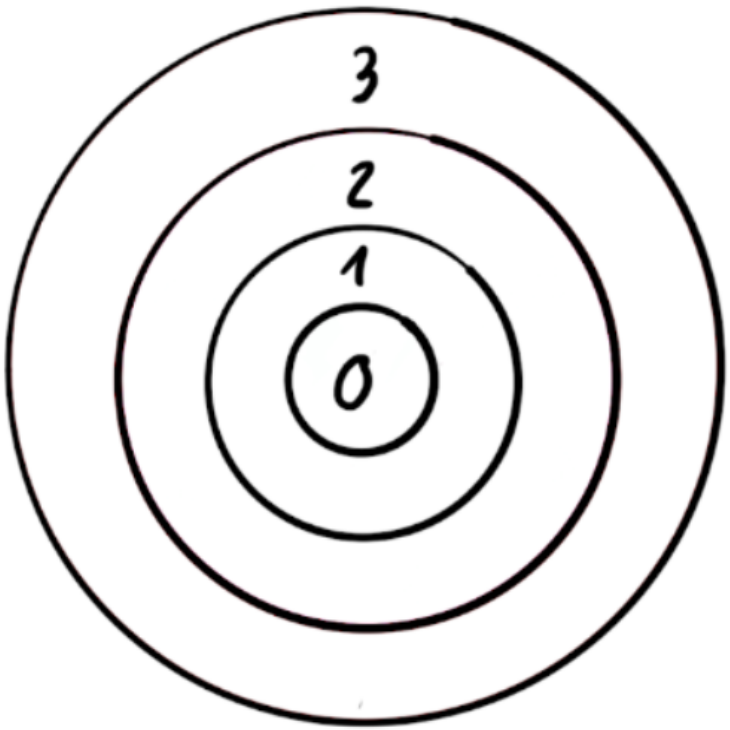
La mise à jour Segwit (*Segregated witness*)

▷ amélioration du protocole Bitcoin introduite en 2017 pour résoudre plusieurs problèmes, notamment l'augmentation de la taille des blocs.

⟶ soft fork qui s'est transformé ... en hard fork (création de Bitcoin Cash).

source

Sécurité des blockchains : le modèle de l'oignon



3: Cryptographic guarantees

2: Consensus guarantees

1: Economic guarantees

0: Social guarantees

vu le 27/05/2023

source

▷ Garanties du consensus : finalisation des transactions

Ce que peut faire une attaque à 51 % :

- censurer des transactions
- arrêter la chaîne (miner des blocs vides)

Protection contre les attaques à 51 % : une puissance totale de hash élevée → des revenus suffisants accordés aux mineurs

source

Ce que ne peut pas faire non plus une attaque à 51 % :

- s'approprier les pièces d'un propriétaire

= garanties cryptographiques (clés privées)

Ce que ne peut toujours pas faire une attaque à 51 % :

- imposer des blocs invalides (modifier les règles de consensus)

Exemples de blocs invalides :

- augmenter la taille des blocs
- créer des pièces *ex nihilo* pour se les approprier

▷ Modifier les règles de consensus : créer une nouvelle blockchain (*hard fork*)

▷ Garanties économiques : incitations financières données aux noeuds de protéger plutôt que d'attaquer la chaîne.

2019 : plus de 50 % de la puissance de hash était concentrée dans quelques fermes de minage dans la région du Sishuan (Chine).

Supposons qu'un mineur contrôle 51 % du hashrate : attaquer la blockchain ferait chuter le prix de bitcoin et ses revenus

source

▷ Consensus social : degré d'engagement d'une communauté d'utilisateurs

= dernier rempart sécurisant la blockchain

⟶ réduit les risques de hard forks

⟶ rejette les tentatives de hard fork

⟶ déclenche un hard fork en cas d'attaque majoritaire (steemit/hive)

source : 1, 2

$\longrightarrow$ plus le nombre d'utilisateurs qui vérifient la validité des blocs est important, plus la blockchain est résiliente face à des attaques à 51 %

$\longrightarrow$ rend impossible la propagation dans le réseau de blocs invalides

Bitcoin : 17 000 noeuds

sources : 1, 2, 3


Always has been
Wait, is Bitcoin a social contract?

Conclusion

Bitcoin, la réunion de quatre innovations

- cryptographie asymétrique (clés privées/publiques)
- chaîne de blocs (hashs chaînés, Harber et Stornetta)
- preuve de travail (Hashcash, Adam Back)
- règle de consensus Nakamoto (la chaîne valide est la plus longue)

sources : 1, 2

Le futur : la ligne de crête des revenus perçus par les mineurs :

▷ stables ou croissants (hausse du prix de btc et/ou accroissement des frais de transaction)

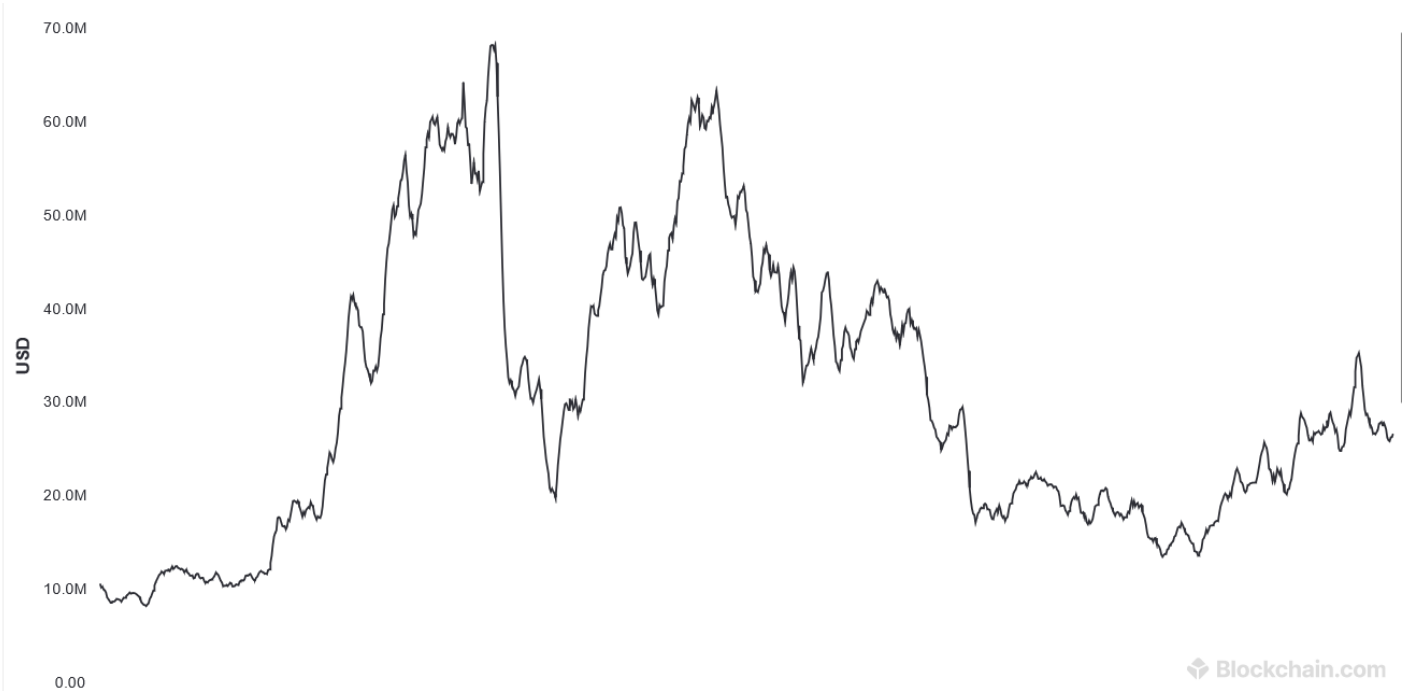
$\longrightarrow$ hausse des dépenses en matériel et énergie (-)

▷ décroissants (*halvening*)

A long-terme, les mineurs recevront uniquement les frais de transaction

$\longrightarrow$ baisse des dépenses en énergie (+) mais dégradation de la sécurité de la blockchain (-)

Revenus journaliers perçus par les mineurs



Moyenne sur 7 jours (source)

Calcul (ex) : 72 blocs/j $\times$ 6.25 $\times$ 26 000 (px btc) + 2m (fees) = 14m

La puissance de hash déployée diminue après chaque *halvening* (à prix donné)