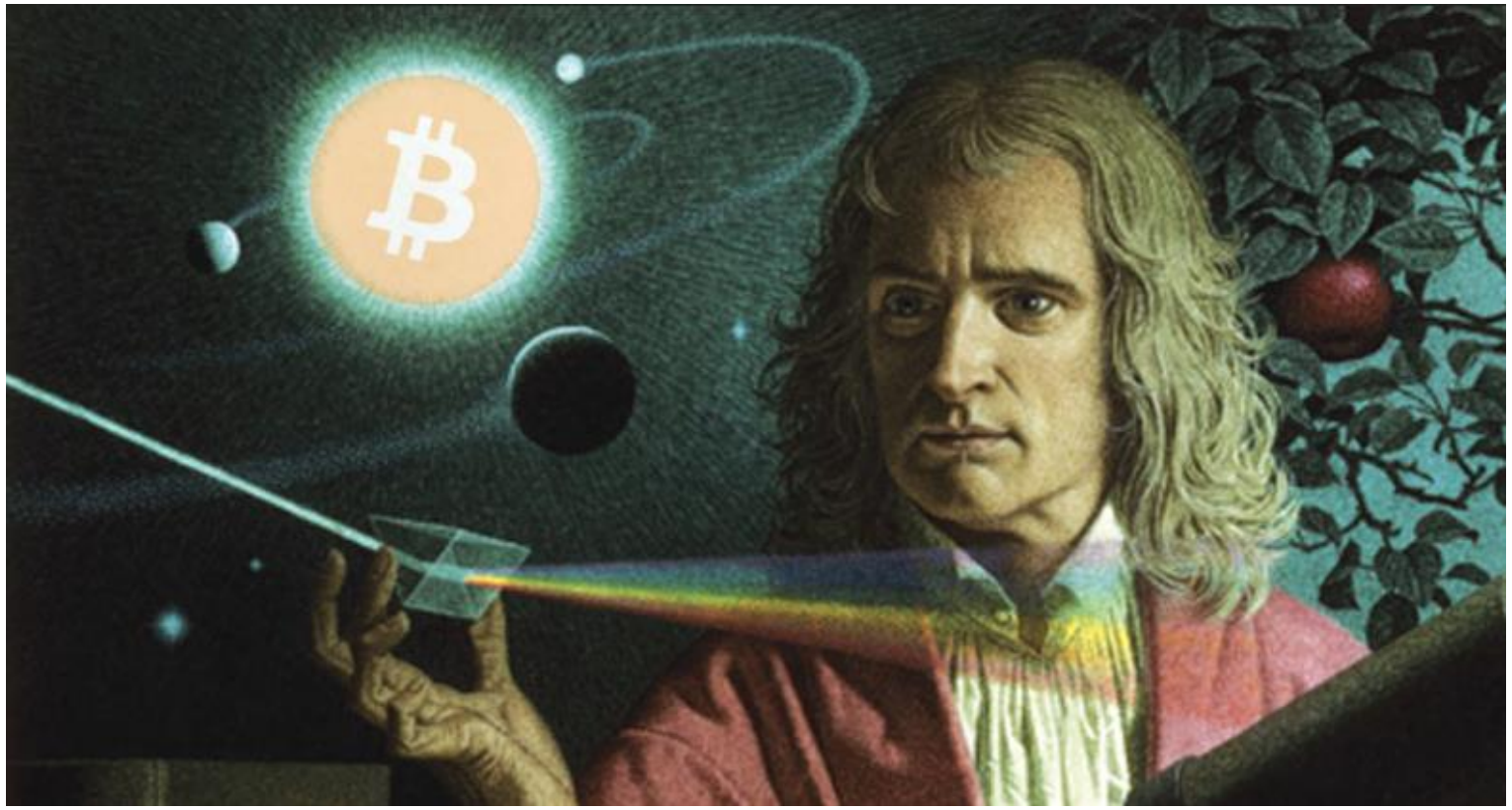
Bitcoin & Preuve de Travail
(En attendant Isaac Newtomoto)



Séminaire Cryptofinance - 18 Octobre 2018 - @laurentmt

La Crypto-apocalypse est proche©

MOTHERBOARD

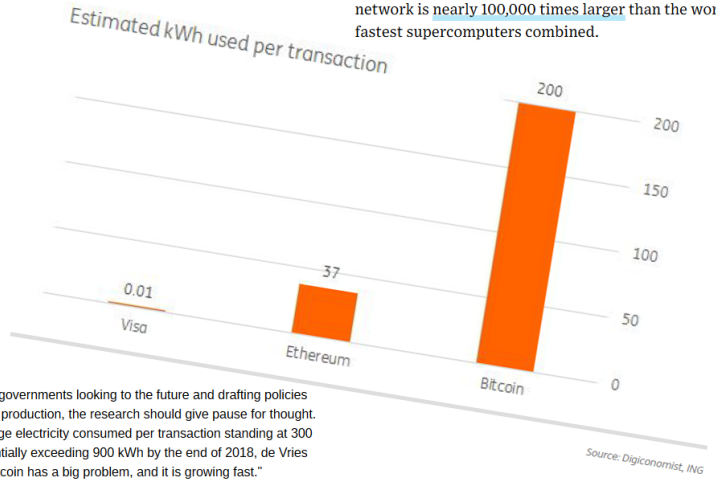
BITCOIN IS UNSUSTAINABLE

One Bitcoin Transaction Consumes As Much Energy As Your House Uses in a Week

As Bitcoin's price increases, its energy consumption is soaring. Bitcoin's power consumption is extremely high compared to conventional digital payment, and one transaction now uses as much energy as your house in a week.

WIRED

Today, each bitcoin transaction requires the same amount of energy used to power nine homes in the US for one day. And miners are constantly installing more and faster computers. Already, the aggregate computing power of the bitcoin network is nearly 100,000 times larger than the world's 500 fastest supercomputers combined.



However, with governments looking to the future and drafting policies around energy production, the research should give pause for thought. With the average electricity consumed per transaction standing at 300 kWh and potentially exceeding 900 kWh by the end of 2018, de Vries concluded: "Bitcoin has a big problem, and it is growing fast."

To make the verification (mining) costly, the verification algorithm requires a lot of processing power and thus electricity. In fact, the website Digiconomist has constructed a Bitcoin Energy Consumption Index, estimating bitcoin energy consumption. And the results are sobering. At the time of writing, verifying one transaction on the bitcoin blockchain consumes about 200kWh.

Current Bitcoin Energy Consumption Index

200kWh Estimated electricity cost per bitcoin transaction

INTERESTING ENGINEERING

NEWS INNOVATION SCIENCE INDUSTRY HOW-TO ▶ VIDEOS SHOP MORE

INNOVATION / CRYPTOCURRENCIES

A Single Bitcoin Transaction Now Consumes as Much Electricity as Your House Does in a Week

As Bitcoin rises so does its exorbitant energy usage. The cryptocurrency has some explaining to do when it comes to energy consumption.

Share on Facebook Share on Twitter +

Mashable

Despite what you might've read, we don't have exact figures on Bitcoin's energy consumption. A site called Digiconomist keeps stats on how much energy Bitcoin is consuming, and it's the primary source for the stories circulating on the subject. Some of these stats look horrific: Bitcoin's current energy consumption is 30.2 terawatt-hours (TWh), which is more than 63 specific countries, and a single Bitcoin transaction consumes enough energy to power nearly 10 U.S. households for an entire day. But we shouldn't blindly trust those numbers.

Etude Digiconomist

Deux « résultats »

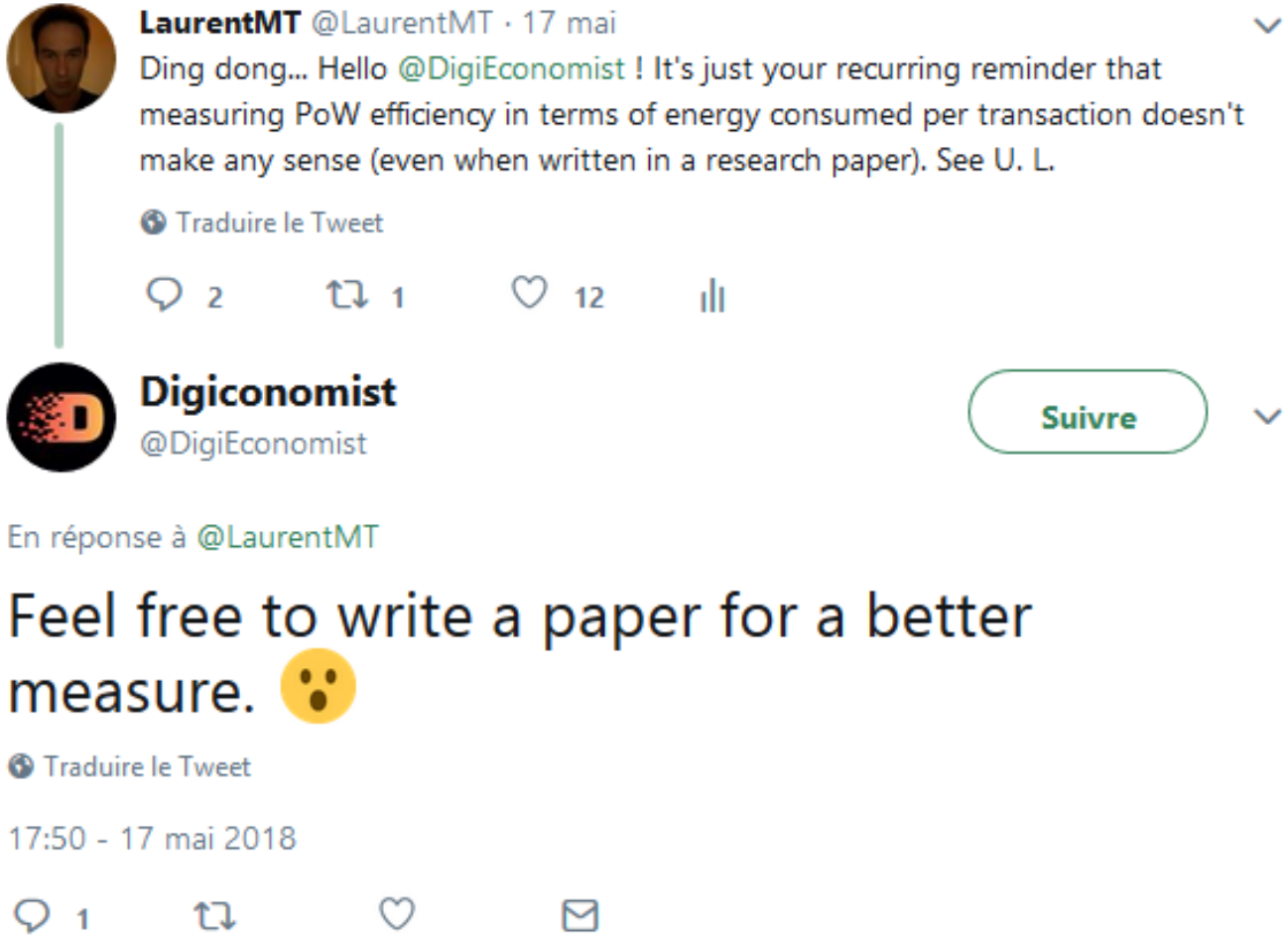
estimation de la consommation globale du PoW Bitcoin

l'ordre de grandeur est probablement assez juste… mais il ne marque pas les esprits

consommation énergétique par transaction (efficience)

marque fortement les esprits… mais n'a aucun sens

Tout le monde aime les Preuves de Travail



Problèmes de cette métrique

Nombre de transactions != Nombre de paiements

Le coût énergétique total est un coût fixe par rapport au nombre de transactions et non pas un coût variable.

Il n’y a surtout aucun relation entre ces deux grandeurs. La métrique promeut une vision confuse du fonctionnement de Bitcoin.

Quelle est l’utilité principale du PoW Bitcoin ?

Théorie de l’extraction d’or numérique

Basée sur la métaphore du minage de l’or physique.

Le coût (énergétique & économique) est le coût « d’extraction » des nouveaux bitcoins.

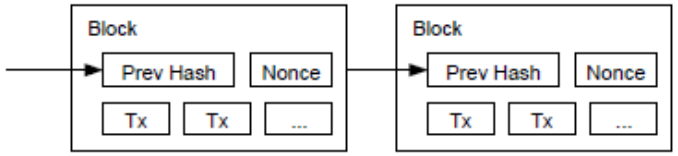
Problème: le minage Bitcoin n’est pas supposé s’arrêter une fois tous les bitcoins créés…

Théorie de la section IV

4. Proof-of-Work

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash [6], rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.

For our timestamp network, we implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it.



The proof-of-work also 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. Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes. We will show later that the probability of a slower attacker catching up diminishes exponentially as subsequent blocks are added.

To compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases.

« La principale utilité du PoW Bitcoin
est de sécuriser
une histoire (mémoire) économique »

Formalisation

Hypothèses (de Travail)

H1: Durant toute son histoire, Bitcoin a été la blockchain publique la plus sécurisée.

H2: Durant toute son histoire, toute puissance de calcul utilisable et significative a été utilisée pour le minage de Bitcoin.

H3: Les revenus extraits du minage de Bitcoin sont égaux au coûts engagés.

H4: Les frais de transactions payés aux mineurs sont négligeables.

H5: Sur une durée suffisamment longue, la puissance de calcul moyenne dédiée au minage de Bitcoin est une fonction monotone croissante.

Formalisation

Notre modèle devrait être capable d'exprimer

des valeurs économiques sécurisées par le système

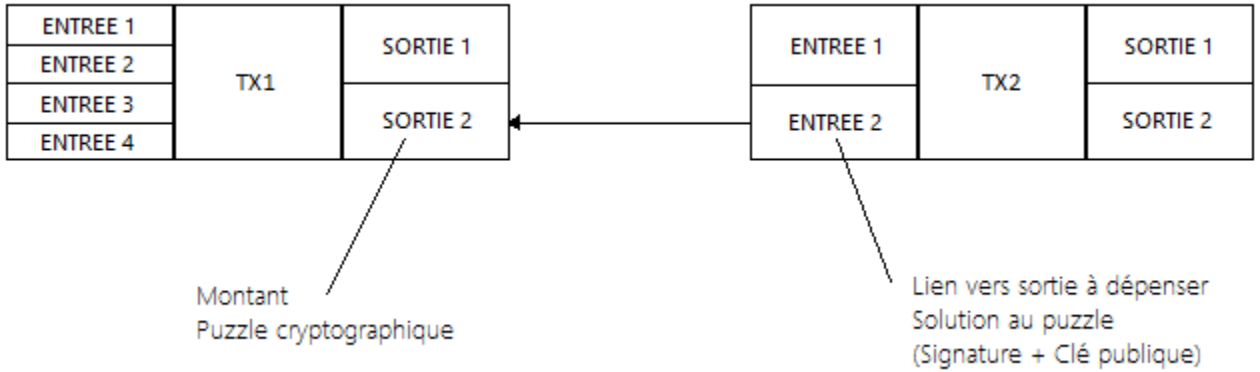
(idéalement de façon atomique ou en agrégats)

la sécurité fournie par le système à ces valeurs économiques

(ou au moins une fonction d'estimation acceptable)

Valeurs économiques

Le concept de sortie de transaction non dépensée (UTxO) semble le candidat tout désigné pour jouer le rôle d'unité atomique de valeur.



Il est possible d'agréger ces unités de valeurs.

Au niveau global, on retrouve le concept d'UTxO Set.

Sécurité

Le PoW Bitcoin a deux propriétés fondamentales qui devraient être prises en compte par tout modèle

une Preuve de Travail est globale

(la sécurité associée à une preuve de travail s'applique à tous les UTxOs)

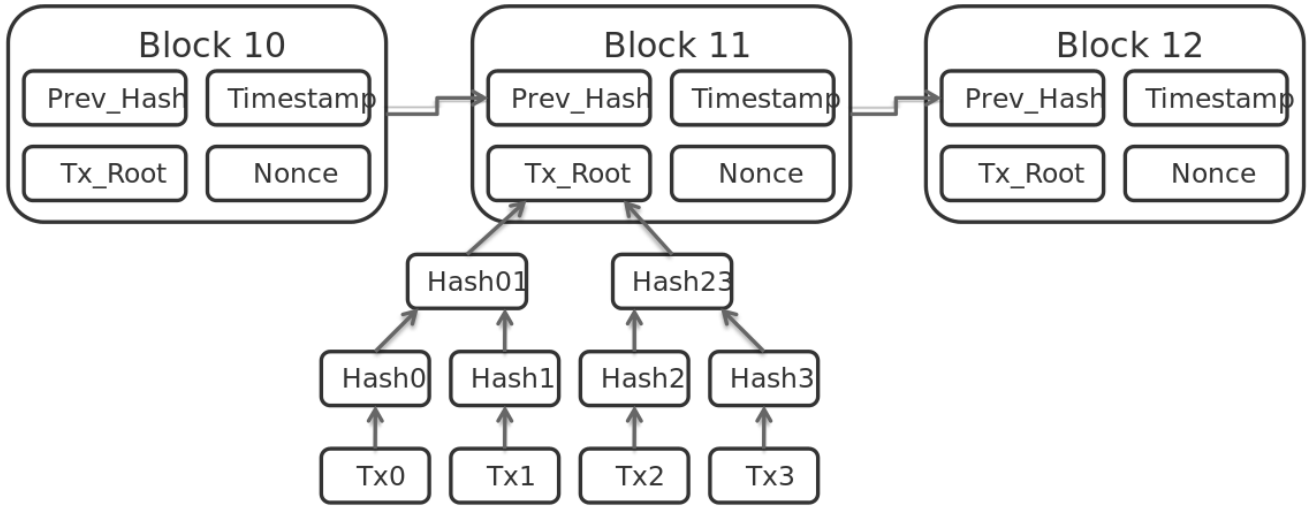
une Preuve de Travail est cumulative

(tant qu'il n'est pas dépensé, un UTxO accumule la sécurité associée à toutes les nouvelles preuves de travail créées)

Le PoW Bitcoin agit de façon assez similaire à un champ gravitationnel homogène

Sécurité

Nous allons répondre à la question: Combien de jours un UTxO créé dans le passé resterait il sécurisé (c.a.d. existant) si 100% de la puissance de calcul actuelle était utilisée pour réécrire l'histoire économique de Bitcoin (blockchain) ?



Dans le contexte de nos hypothèses, 100% de la puissance de calcul actuelle est le cas le plus défavorable.

Utilité – Bitcoins.Days Secured

Intuitions

plus la valeur économique associée à un UTxO est élevée, plus le nombre de BTC.Days Secured est élevé.

plus longtemps un UTxO est sécurisé, plus le nombre de BTC.Days Secured est élevé.

Utilité – Bitcoins.Days Secured d'un UTxO

$$BDS_b(u) = A_u \frac{\sum_{i=b_u}^{b} H_i}{144\, H_b}$$

with:

$BDS_b(u)$: Number of BTC.Days Secured by UTXO u after block at height b

A_u: Amount of UTXO u

b_u: Height of the block containing the transaction creating the UTXO u

H_i: Expected number of hashes associated to block at height i

Utilité – Bitcoins.Days Secured de l'UTxO Set

$$BDS_b = \sum_{u \in U_b} A_u \frac{\sum_{i=b_u}^{b} H_i}{144\, H_b}$$

with:

BDS_b: Total number of BTC.Days Secured by the UTXO set after block at height b

U_b: UTXO set after block at height b

A_u: Amount of UTXO u

b_u: Height of the block containing the transaction creating the UTXO u

H_i: Expected number of hashes associated to block at height i

Efficience du PoW Bitcoin

Métrique 1 : coût unitaire des bitcoins.days secured

Coût Unitaire des bitcoins.days secured

$$UC_b = \frac{R_b}{\frac{H_b}{144\ H_b} \sum_{u \in U_b} A_u}$$

with:

UC_b: Unit cost of the BTC.Days Secured produced by block at height b

R_b: Reward associated to block at height b

H_b: Expected number of hashes associated to block at height b

U_b: UTXO set after block at height b

b_u: Height of the block containing the transaction creating the UTXO u

A_u: Amount of UTXO u

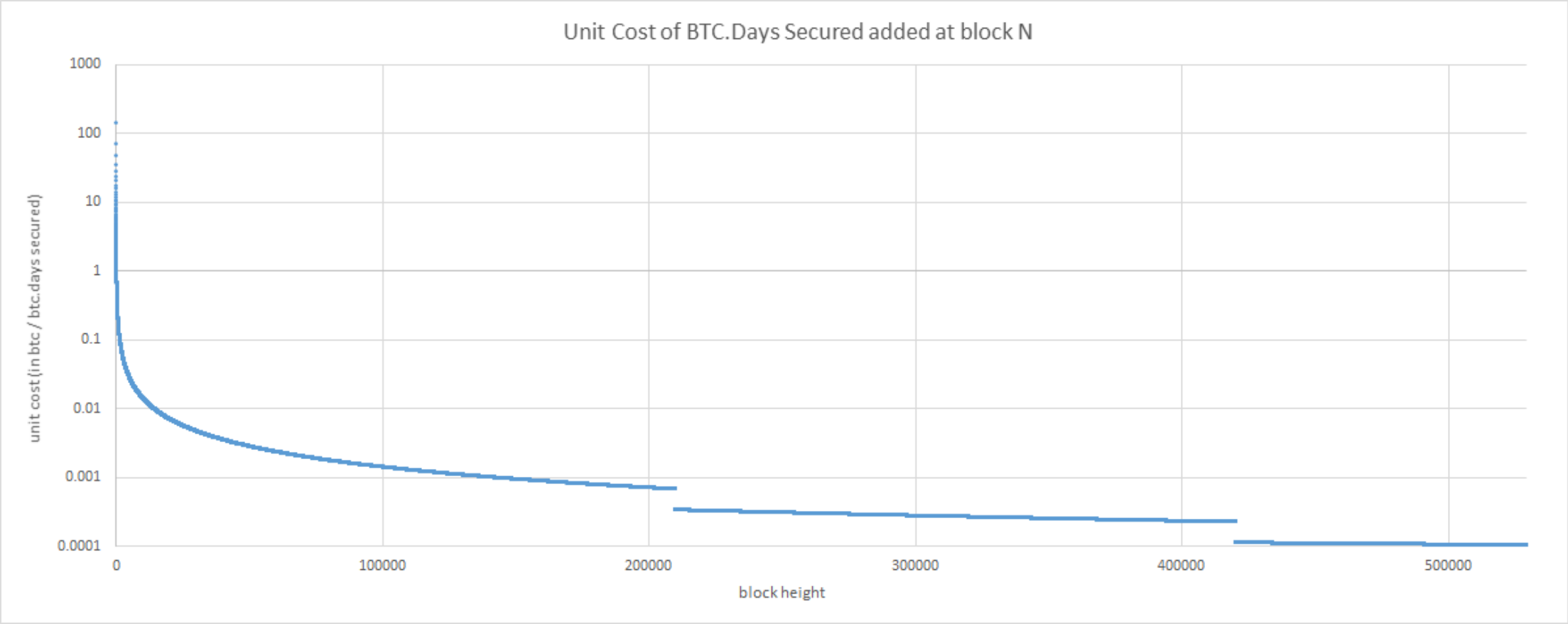
Coût Unitaire des bitcoins.days secured

Par définition $\sum_{u \in U_b} A_u = \sum_{i=1}^{b} R_i$

ce qui nous donne $UC_b = \dfrac{R_b}{\dfrac{H_b}{144\, H_b} \sum_{i=1}^{b} R_i}$

ou encore $UC_b = \dfrac{144\, R_b}{\sum_{i=1}^{b} R_i}$

Coût Unitaire de 1 BTC.Day Secured pour un bloc donné



Métrique 2 : coût moyen des dollars.days secured

Coût Moyen des dollars.days secured

$$AC_b = \frac{\sum_{i=1}^{b} R_i \, P_i}{\sum_{j=1}^{b} \frac{H_j \, P_j \, \sum_{u \in U_b} A_u}{144 \, H_j}}$$

with:

AC_b: Average cost of the Dollars.Days Secured produced up to block at height b

H_j: Expected number of hashes associated to block at height j

R_b: Reward associated to block at height b

P_b: Market Price around block at height b

U_b: UTXO set after block at height b

b_u: Height of the block containing the transaction creating the UTXO u

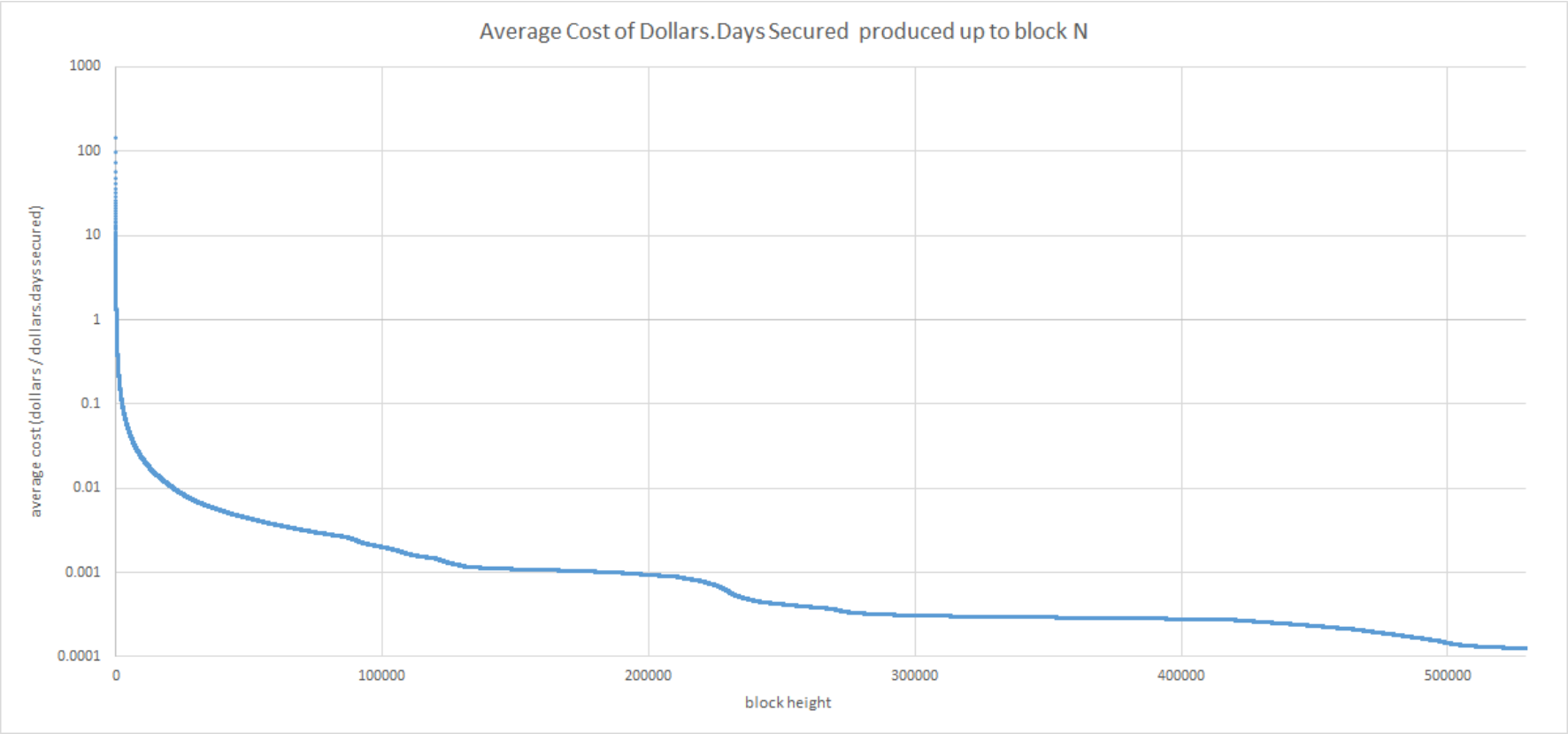
A_u: Amount of UTXO u

Coût Moyen des dollars.days secured

Qui peut être réécrit en $$AC_b = \frac{\sum_{i=1}^{b} R_i \, P_i}{\sum_{j=1}^{b} \frac{H_j \, P_j \, \sum_{k=1}^{j} R_k}{144 \, H_j}}$$

ou encore $$AC_b = \frac{144 \, \sum_{i=1}^{b} R_i \, P_i}{\sum_{j=1}^{b} P_j \, \sum_{k=1}^{j} R_k}$$

Coût Moyen des dollars.days secured



Métrique 3 : Ratio Prix / Performance

Ratio Prix / Performance du PoW Bitcoin

Une métrique économique souvent utilisée pour illustrer le progrès cumulatif associé aux nouvelles technologies.

Ratio Prix / Performance du PoW Bitcoin

Intuition

Nous allons considérer l'UTxO Set après chaque bloc comme un nouveau « produit » offrant une certaine utilité (nb de Bitcoins.Days Secured de l'UTxO Set) pour un prix donné (récompense des miners pour le bloc).

Ratio Prix / Performance du PoW Bitcoin

$$PPR_b = \frac{R_b}{BDS_b}$$

with:

PPR_b: Price-Performance Ratio for block at height b

R_b: Reward associated to block at height b

BDS_b: Total number of BTC.Days Secured by the UTXO set after block at height b

Ratio Prix / Performance du PoW Bitcoin

$$PPR_b = \frac{R_b}{\frac{\sum_{u \in U_b}(A_u \sum_{i=b_u}^{b} H_i)}{144\, H_b}}$$

with:

H_i: Expected number of hashes associated to block at height i

U_b: UTXO set after block at height b

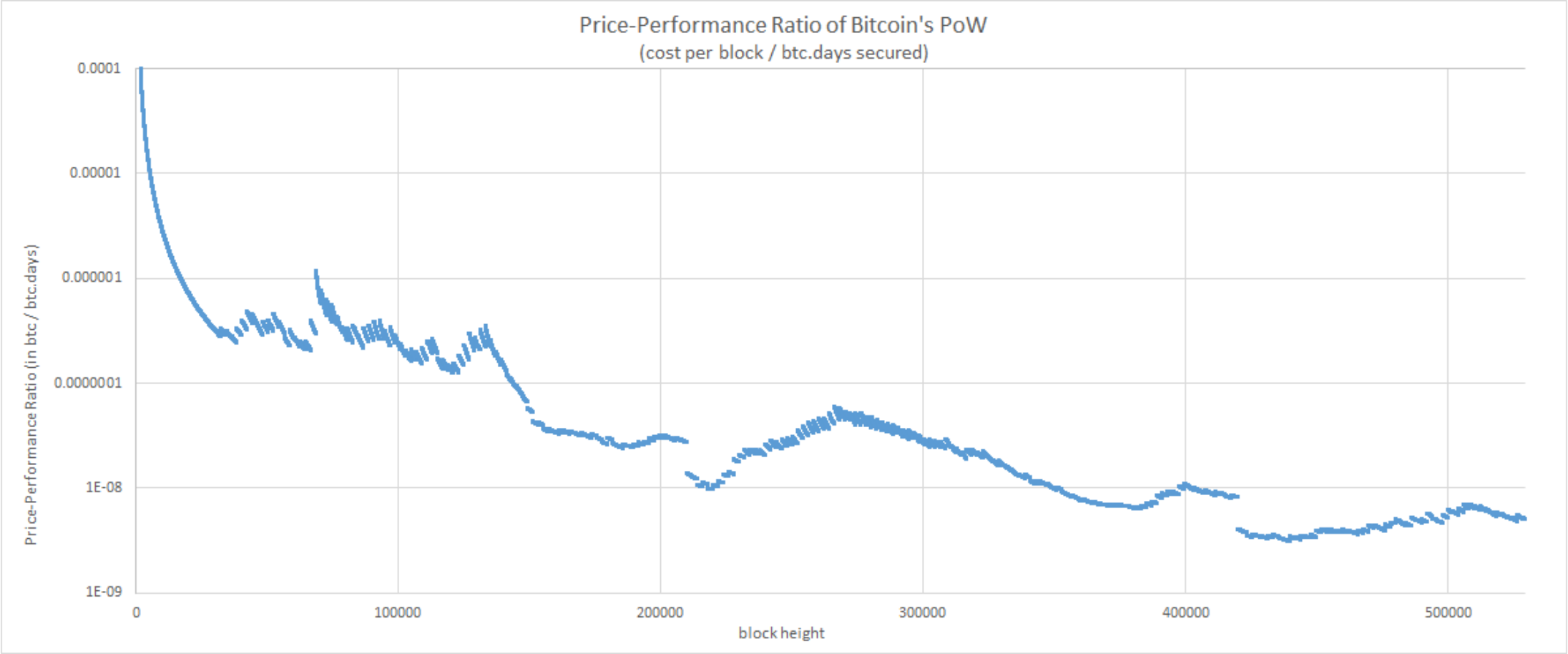
A_u: Amount of UTXO u

b_u: Height of the block containing the transaction creating the UTXO u

Ratio Prix / Performance du PoW Bitcoin

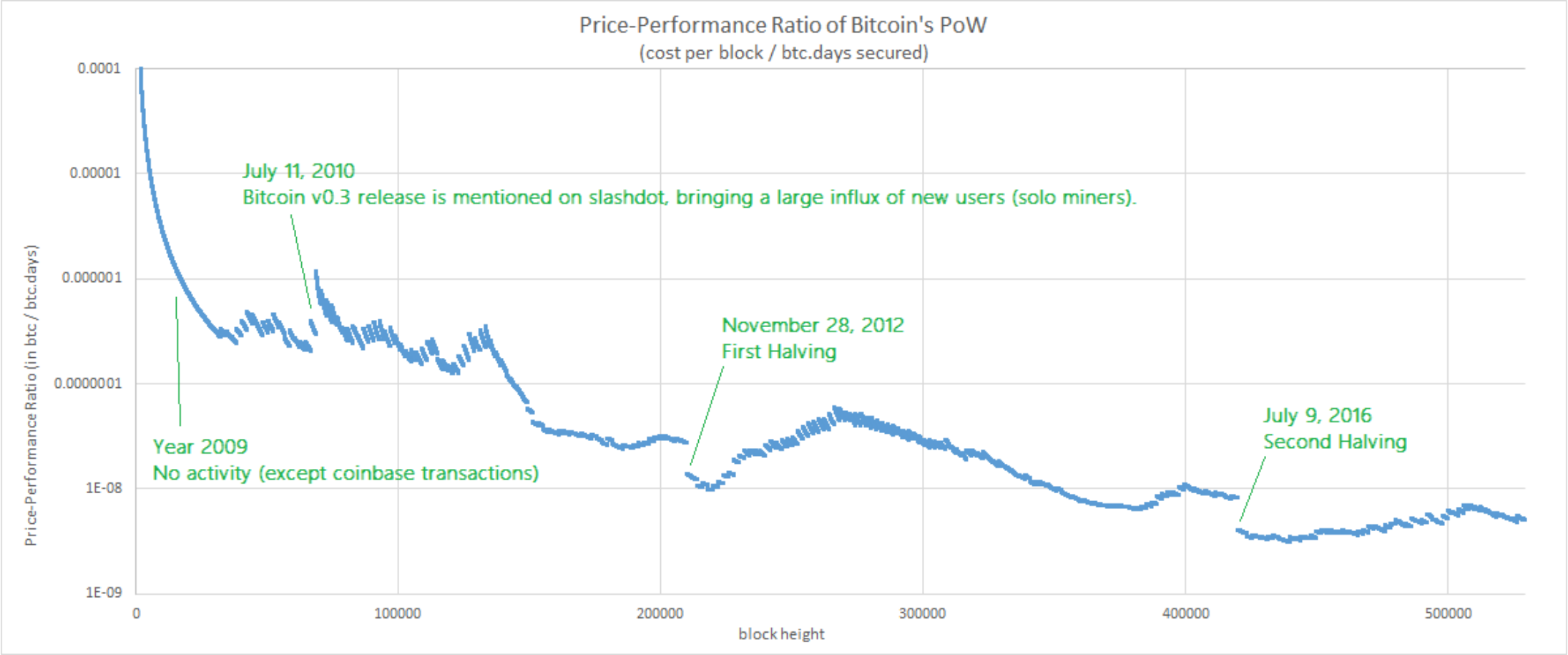
$$PPR_b = \frac{144\ H_b R_b}{\sum_{u \in U_b} (A_u \sum_{i=b_u}^{b} H_i)}$$

Ratio Prix / Performance du PoW Bitcoin



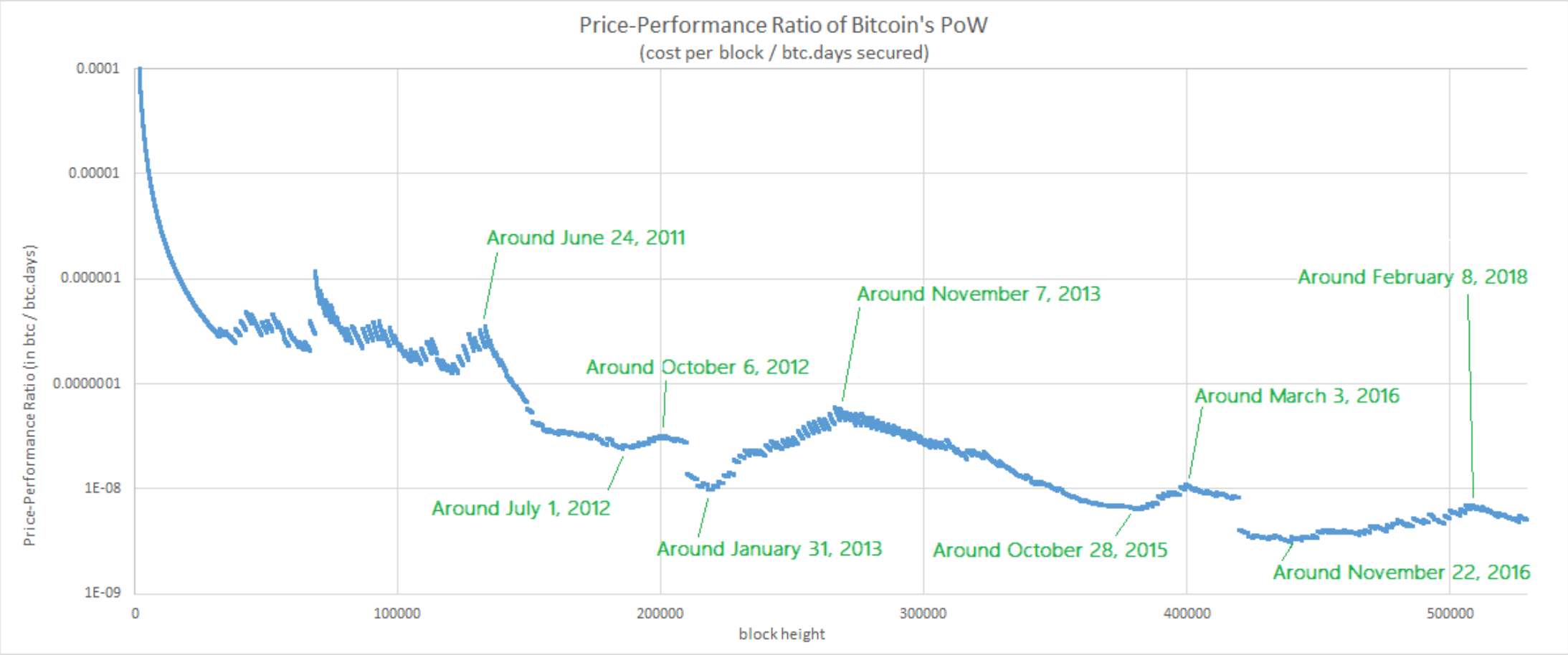
Singularités et discontinuités

PPR – Singularités & discontinuités

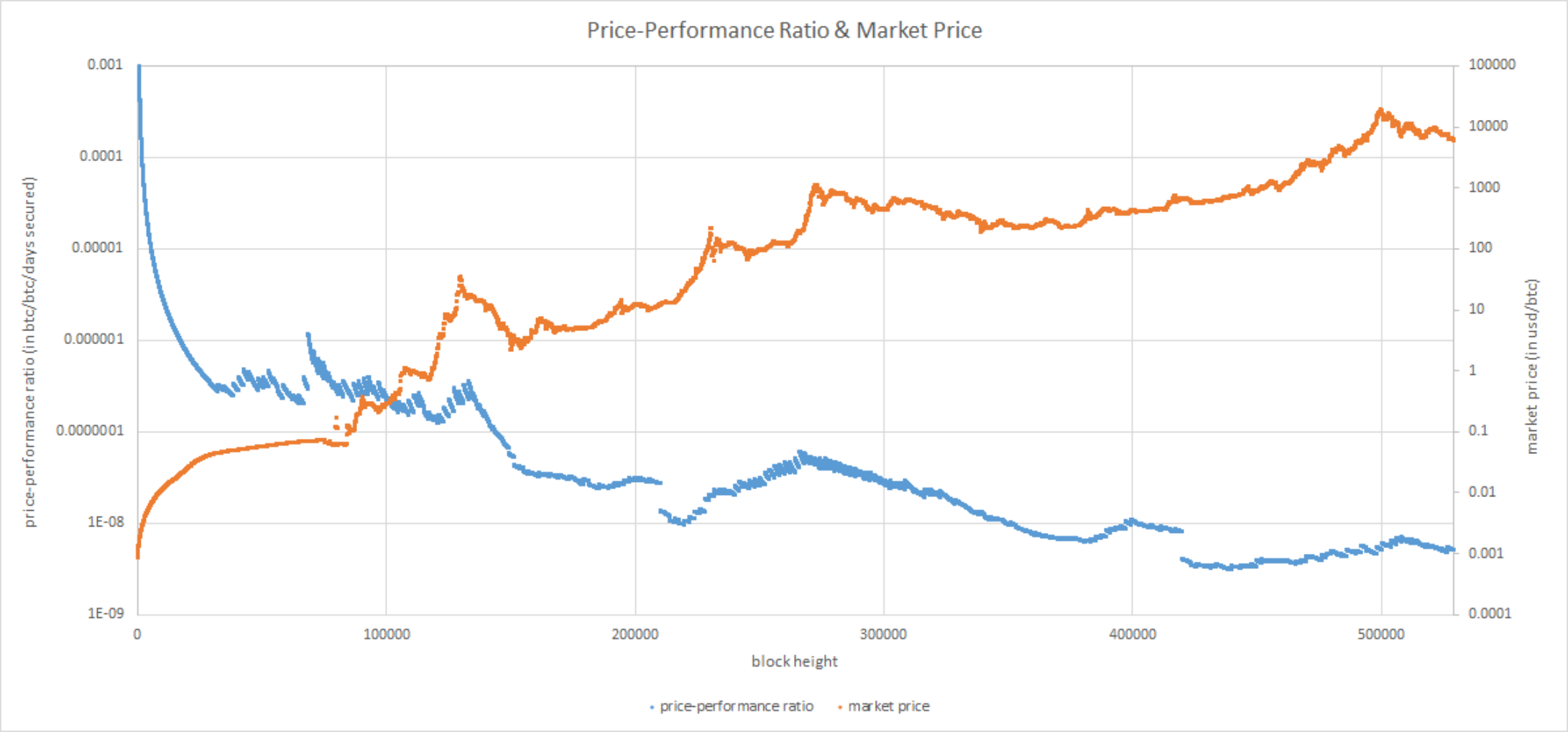


Oscillations & Market Price

PPR - Oscillations



PPR – Market Price



PPR – Market Price

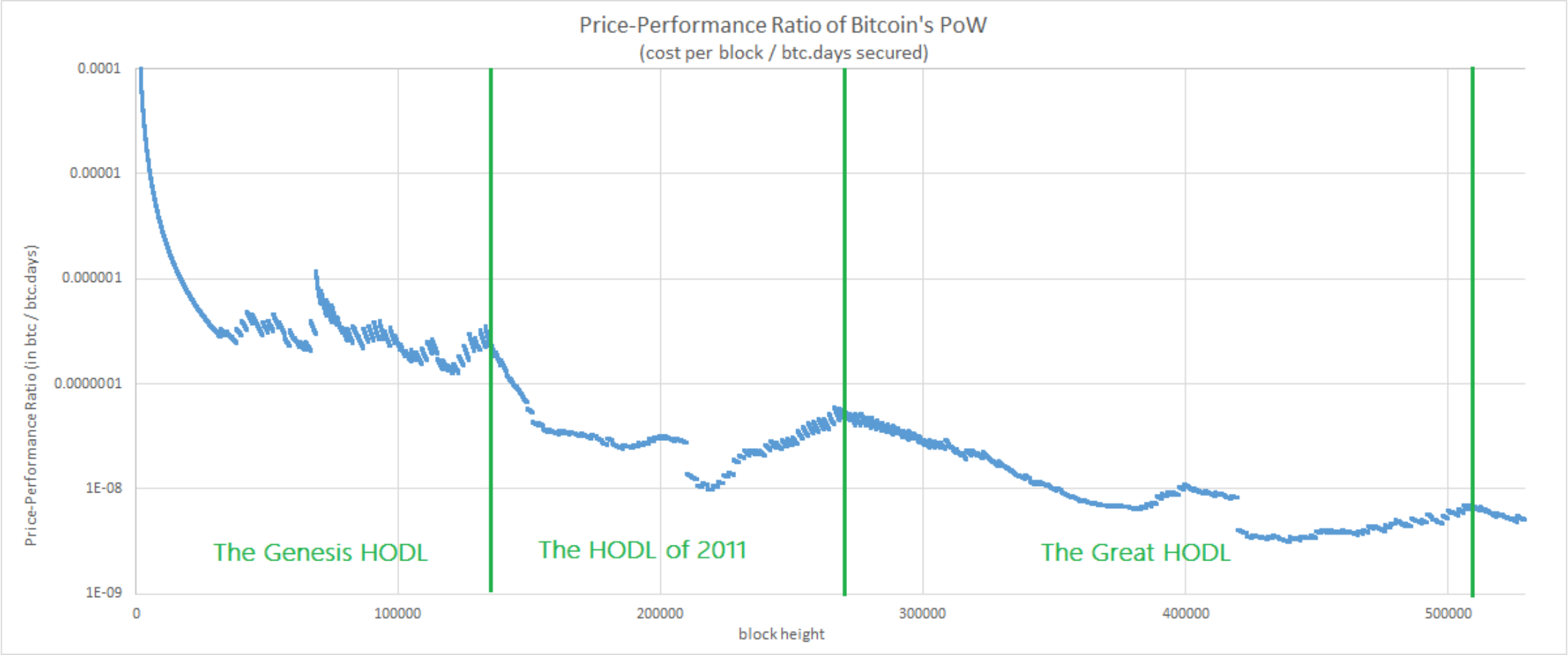
Le chart suggère une corrélation entre PPR et Market Price bien que le Market Price ne soit pas un facteur explicitement utilisé dans notre définition du PPR…

$$PPR_b = \frac{144\ H_b R_b}{\sum_{u \in U_b} (A_u \sum_{i=b_u}^{b} H_i)}$$

Hypothèse: Il existe une influence « indirecte » du Market Price sur le PPR via 2 facteurs présents dans la définition du PPR: le comportement des Hodlers & des Miners.

Influence du hodling

PPR – Hodling (Théorie des Hodl Waves)



PPR – Influence du Hodling sur le PPR

Objectif: Déterminer l'espace d'évolution possible du PPR lorsque le comportement des Hodlers change.

Les bornes de cet espace peuvent être associées à 2 comportements de Hodling « extrêmes »: Zéro Hodling ou Full Hodling.

Zéro Hodling: Bitcoin Stéroïds

Full Hodling: Bitcoin Arctic

PPR Bitcoin Steroids

$$PPR_b = \frac{144\ H_b R_b}{\sum_{u \in U_b} (A_u \sum_{i=b_u}^{b} H_i)}$$

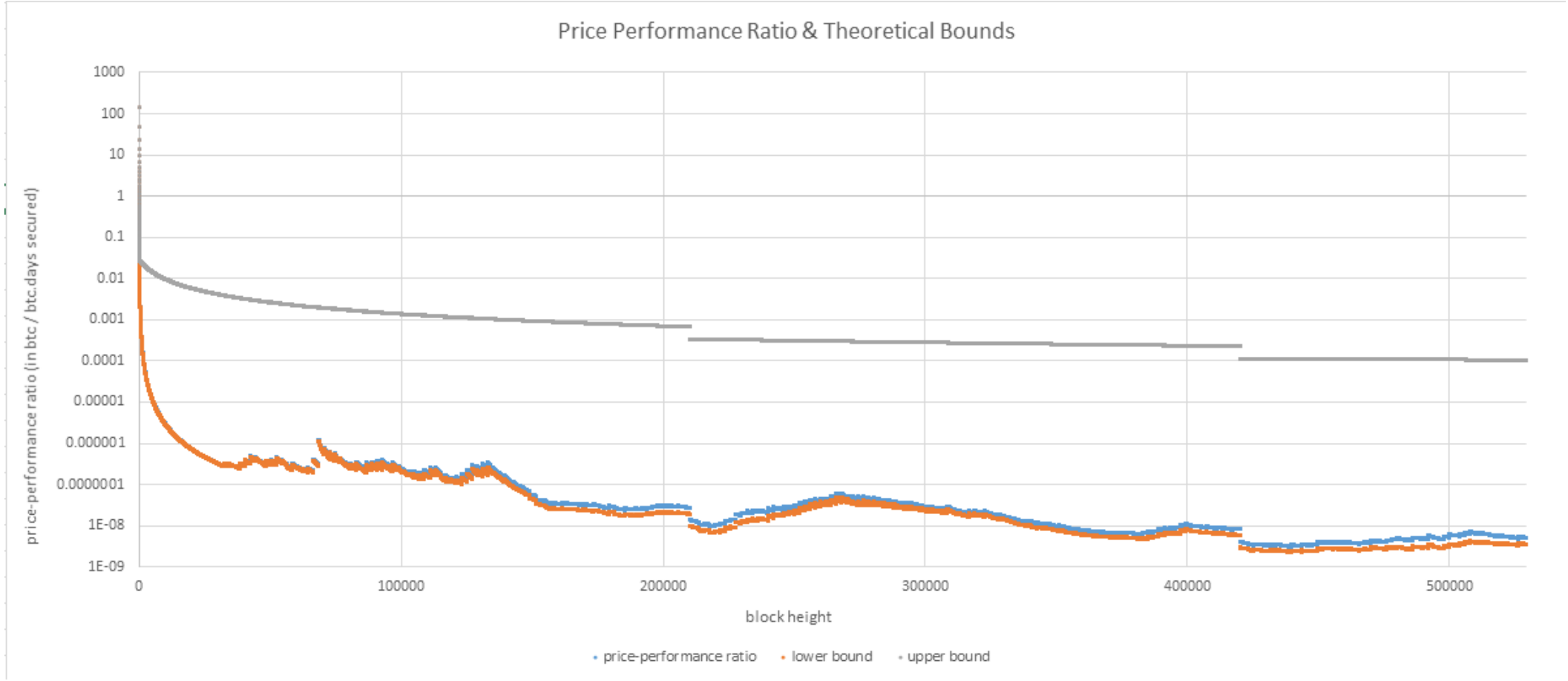
$$PPR_b = \frac{144\ R_b}{\sum_{i=1}^{b} R_i}$$

PPR Bitcoin Arctic

$$PPR_b = \frac{144\ H_b R_b}{\sum_{u \in U_b} (A_u \sum_{i=b_u}^{b} H_i)}$$

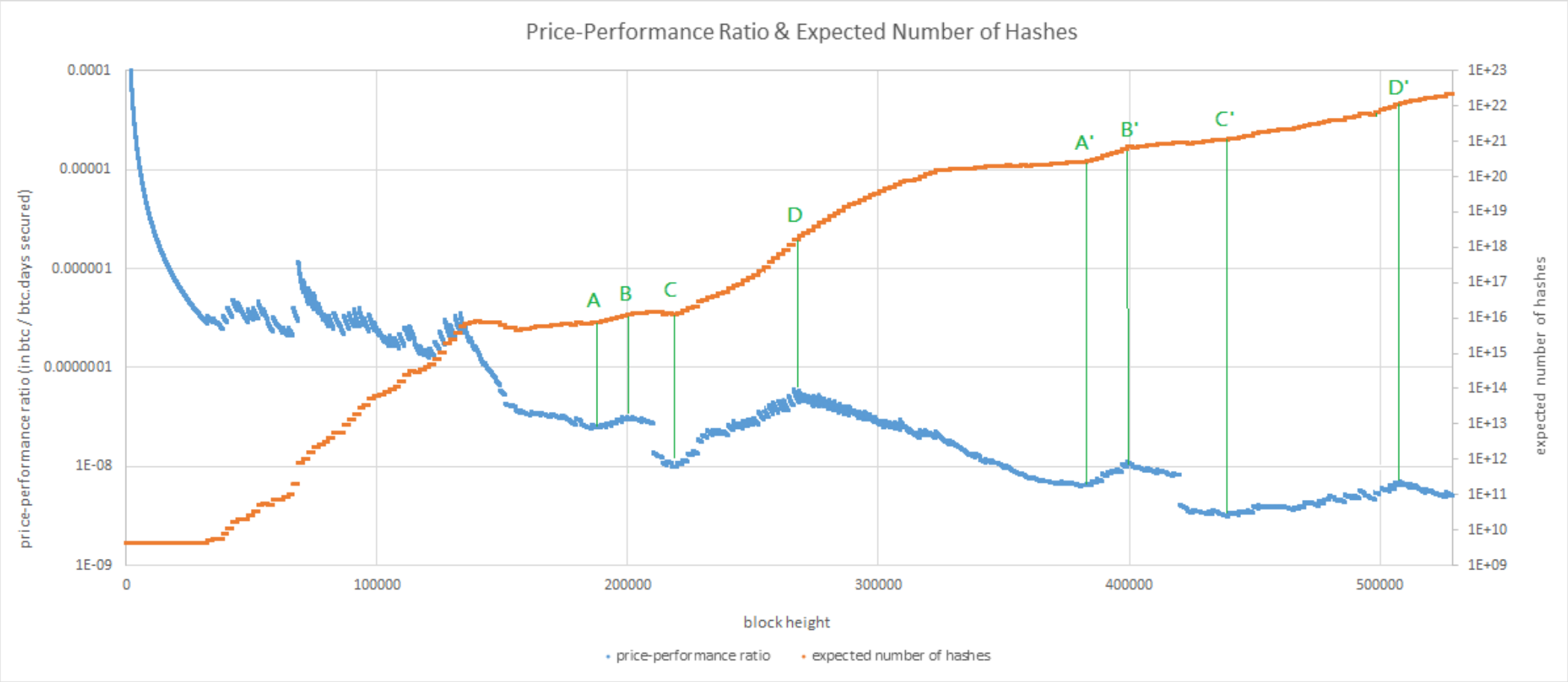
$$PPR_b = \frac{144\ R_b H_b}{\sum_{i=1}^{b} R_i \sum_{j=i}^{b} H_j}$$

PPR – Influence du Hodling



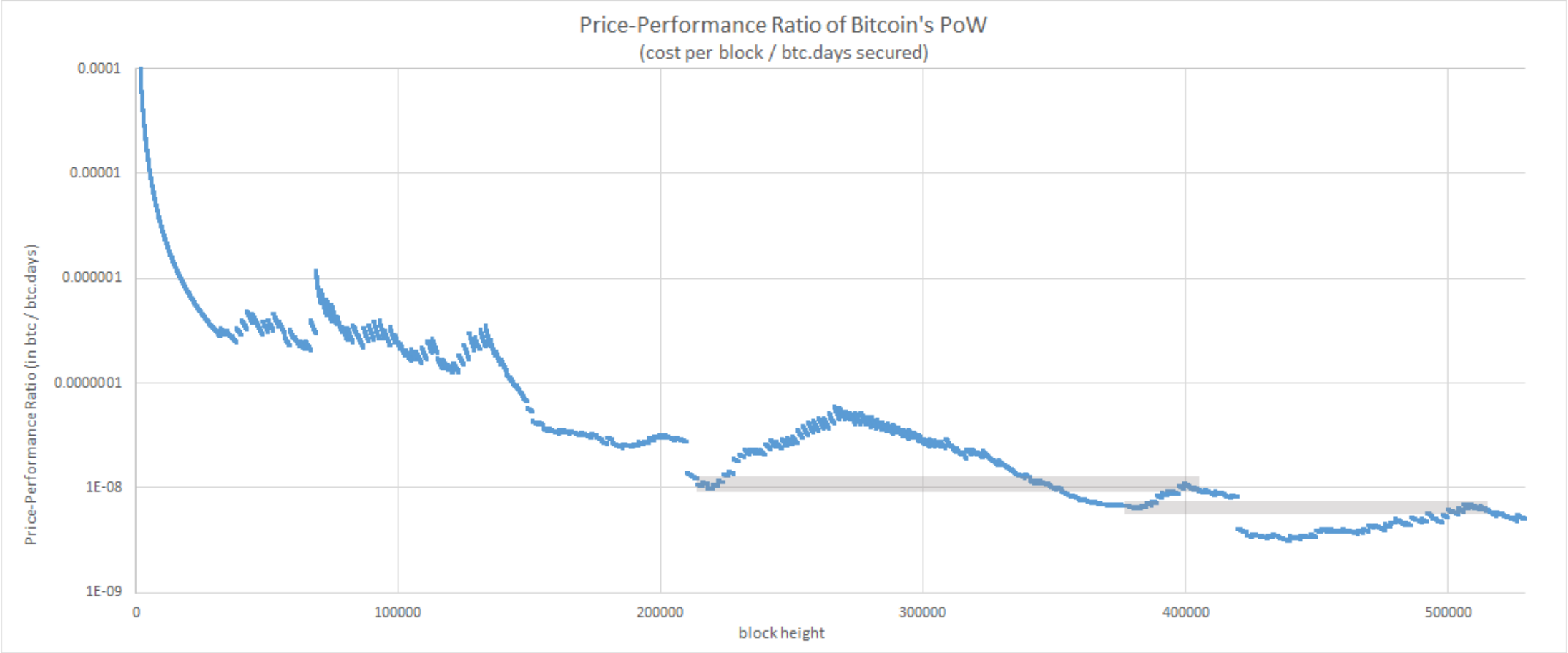
Influence du mining

PPR – Influence du Mining

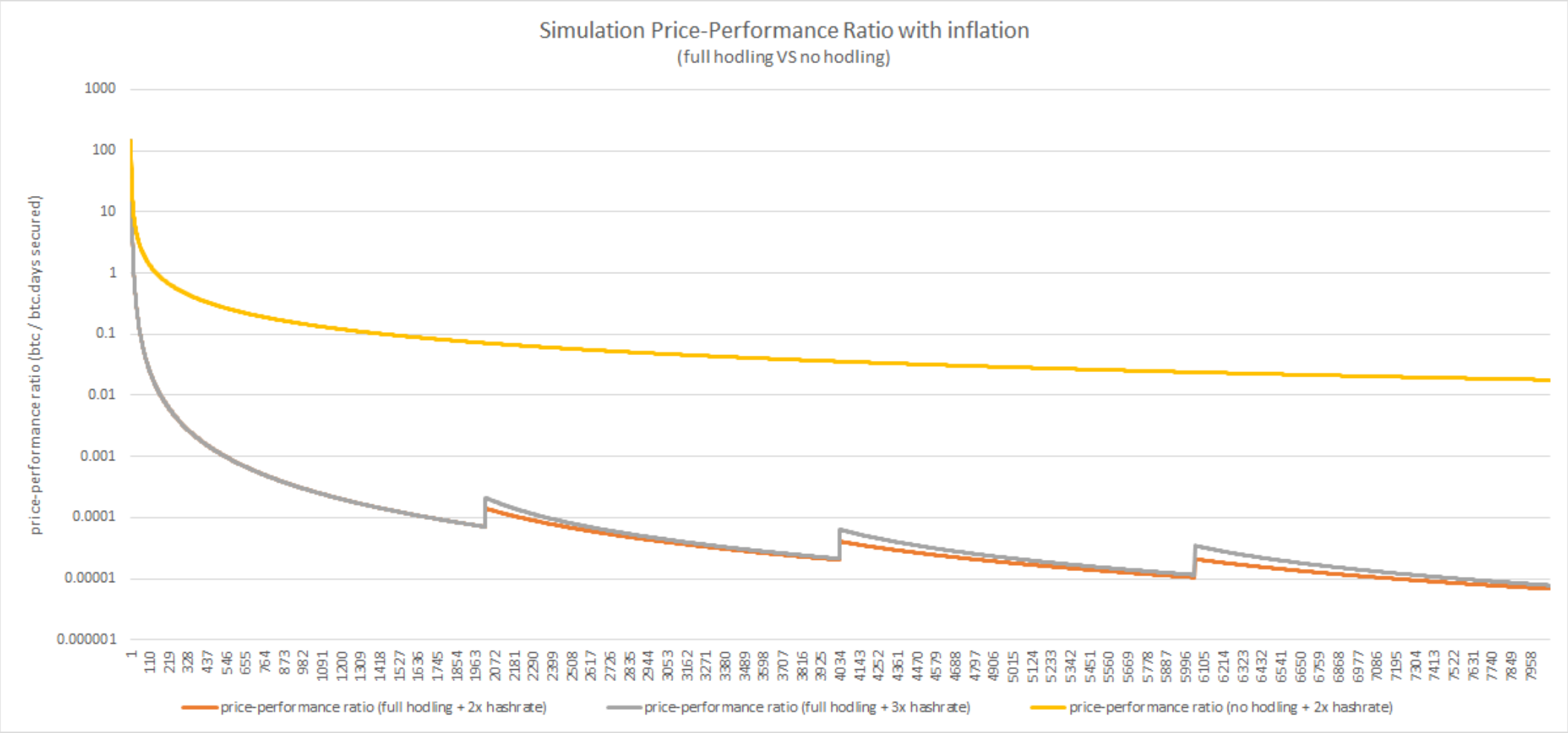


Phénomène de résistance

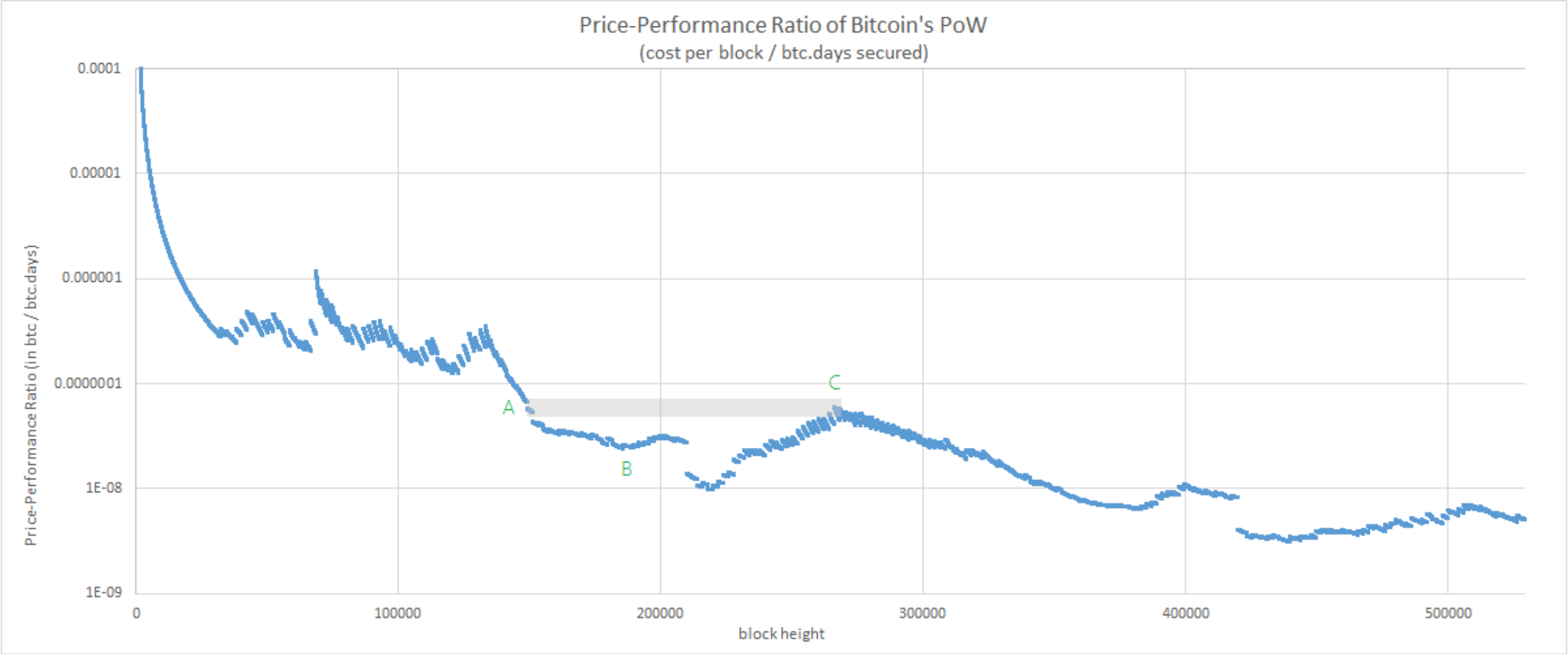
PPR – Phénomène de résistance



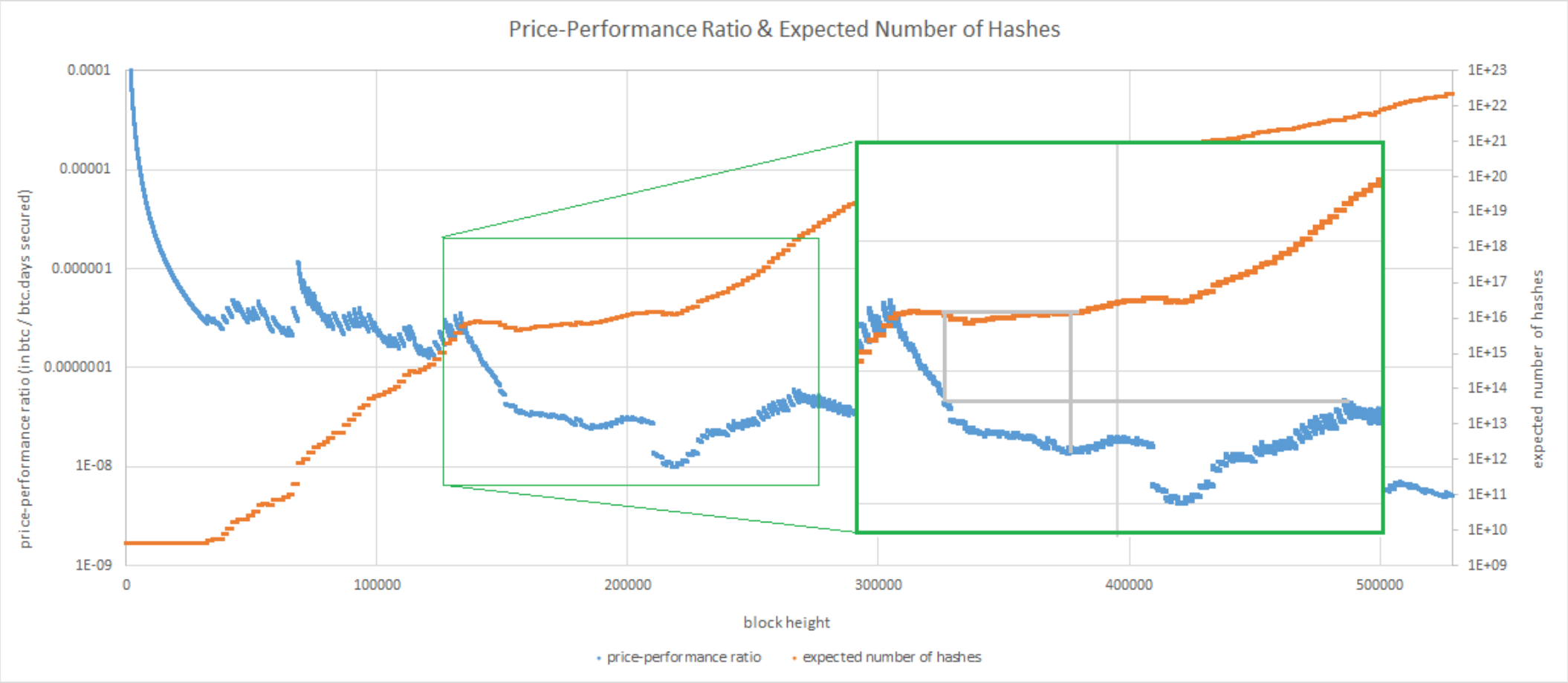
PPR – Spherical Cow



PPR – Phénomène de résistance

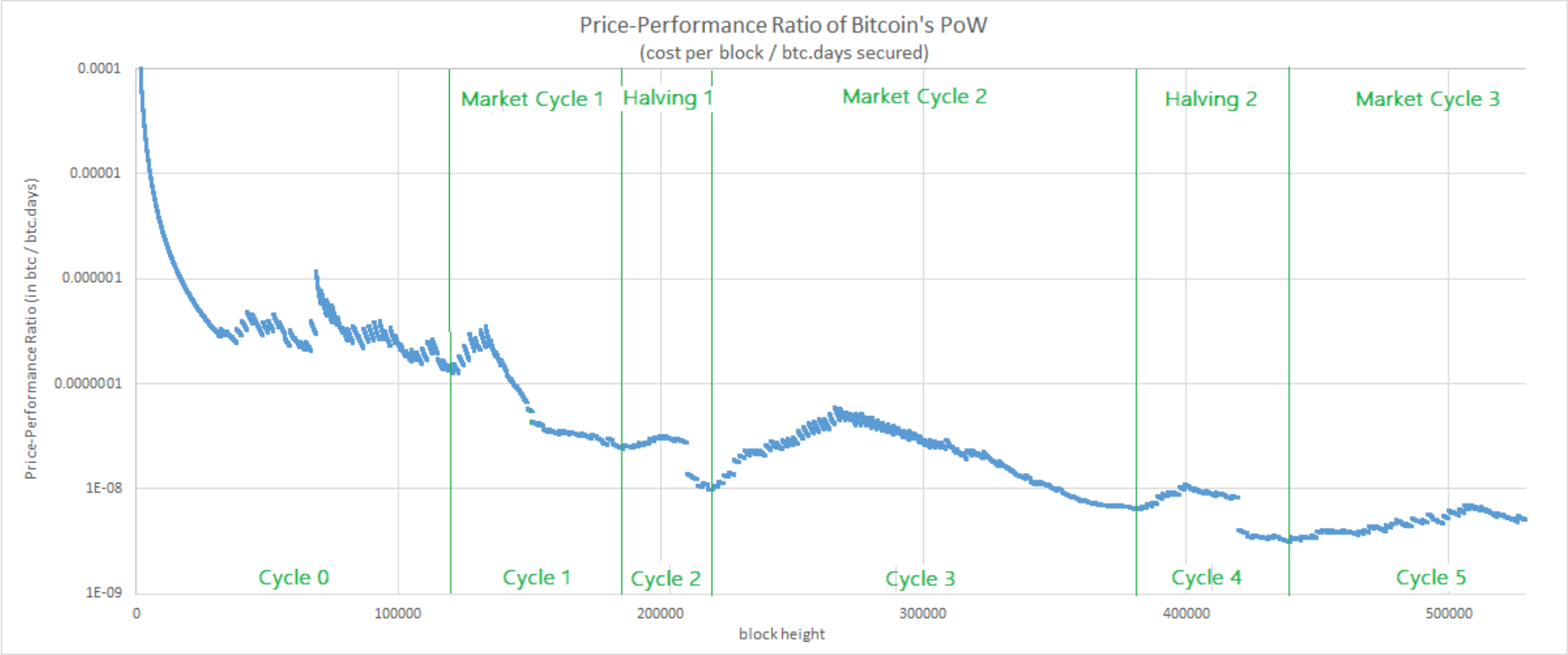


PPR – Phénomène de résistance

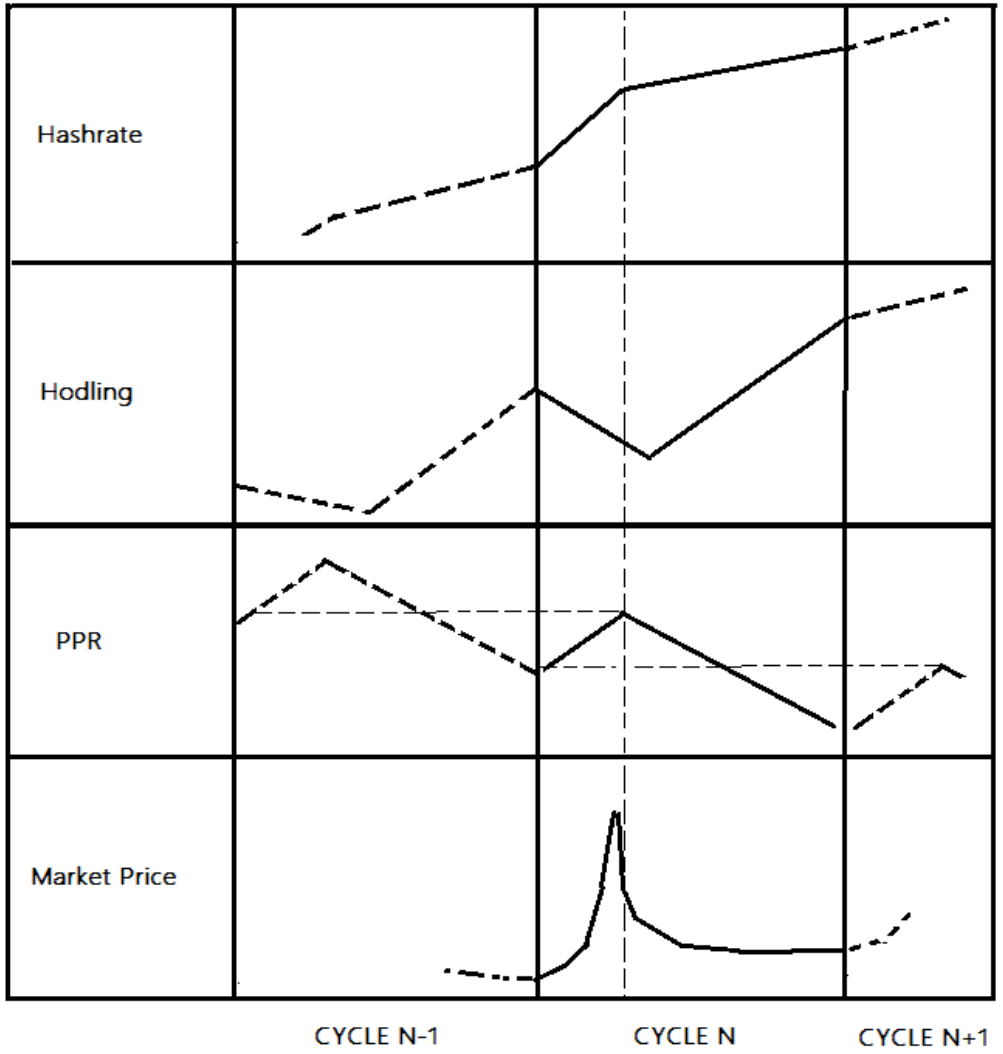


Cycles PPR

PPR – Cycles


Price-Performance Ratio of Bitcoin's PoW
(cost per block / btc.days secured)
Price-Performance Ratio (in btc / btc.days)
0.0001
0.00001
0.000001
0.0000001
1E-08
1E-09
0
100000
200000
300000
400000
500000
block height
Market Cycle 1
Halving 1
Market Cycle 2
Halving 2
Market Cycle 3
Cycle 0
Cycle 1
Cycle 2
Cycle 3
Cycle 4
Cycle 5

PPR – Cycles



Quelques réflexions sur la notion d’efficience

La notion d’efficience

L’efficience n’est pas une valeur « absolue ».

L’efficience est toujours définie dans un contexte donné.

« X est plus efficient que Y » => X et Y fournissent le même résultat, les mêmes propriétés mais X consomme moins de ressources.

Dire que « X est plus efficient que Y » si le résultat ou les propriétés fournies par X et Y ne sont pas les mêmes n’a pas de sens.

Une propriété fondamentale du PoW

Le PoW Bitcoin créé un espace d'interaction économique intrinsèquement ouvert et résistant aux lock-outs.

Même une coalition de 100% du hashrate existant ne peut empêcher l'arrivée d'un nouvel entrant.

- Les seules barrières à l'entrées sont les limites technologiques, financières et géopolitiques du nouvel entrant.

Aucune autre combinaison existante de consensus distribué + système anti-Sybil n'offre aujourd'hui cette propriété.

Conclusions

Conclusions

Mesurer l'efficience du PoW avec un ratio coût/transaction est un non sens total.

Au mieux: incompétence.

Au pire: « rhétorique » déguisée en discours scientifique.

A ce jour, la plupart des « discussions » sur le sujet relèvent de l'obscurantisme intellectuel ou de la pensée magique.

Conclusions

Les résultats présentés restent « superficiels ».

Au-delà du débat sur l'efficience et le coût du PoW Bitcoin, il y a beaucoup à gagner à établir un cadre conceptuel correct aidant à penser la dynamique du « système » Bitcoin.

Tout reste à faire

Bitcoin attend toujours sont Isaac Newtomoto