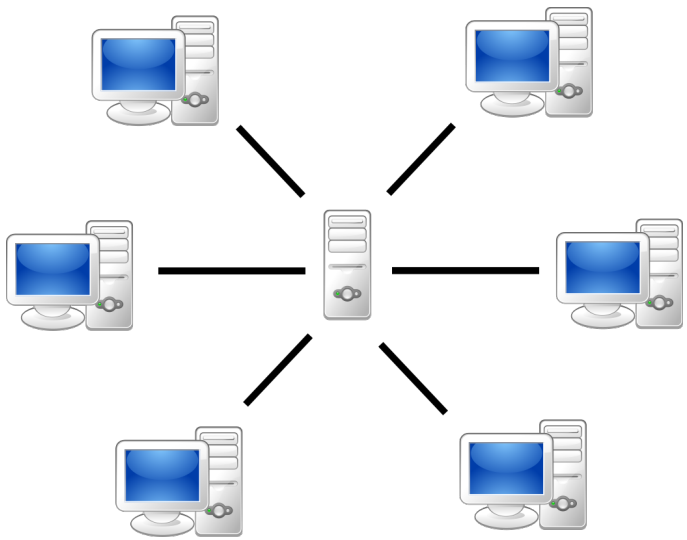
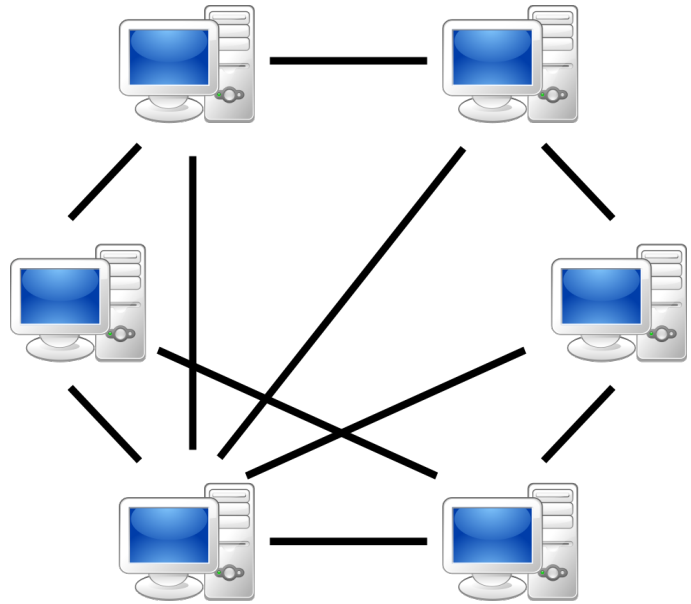
# Amélioration du passage à l'échelle de l'espace pris par la blockchain Bitcoin

Benjamin Loison

# Introduction aux blockchains

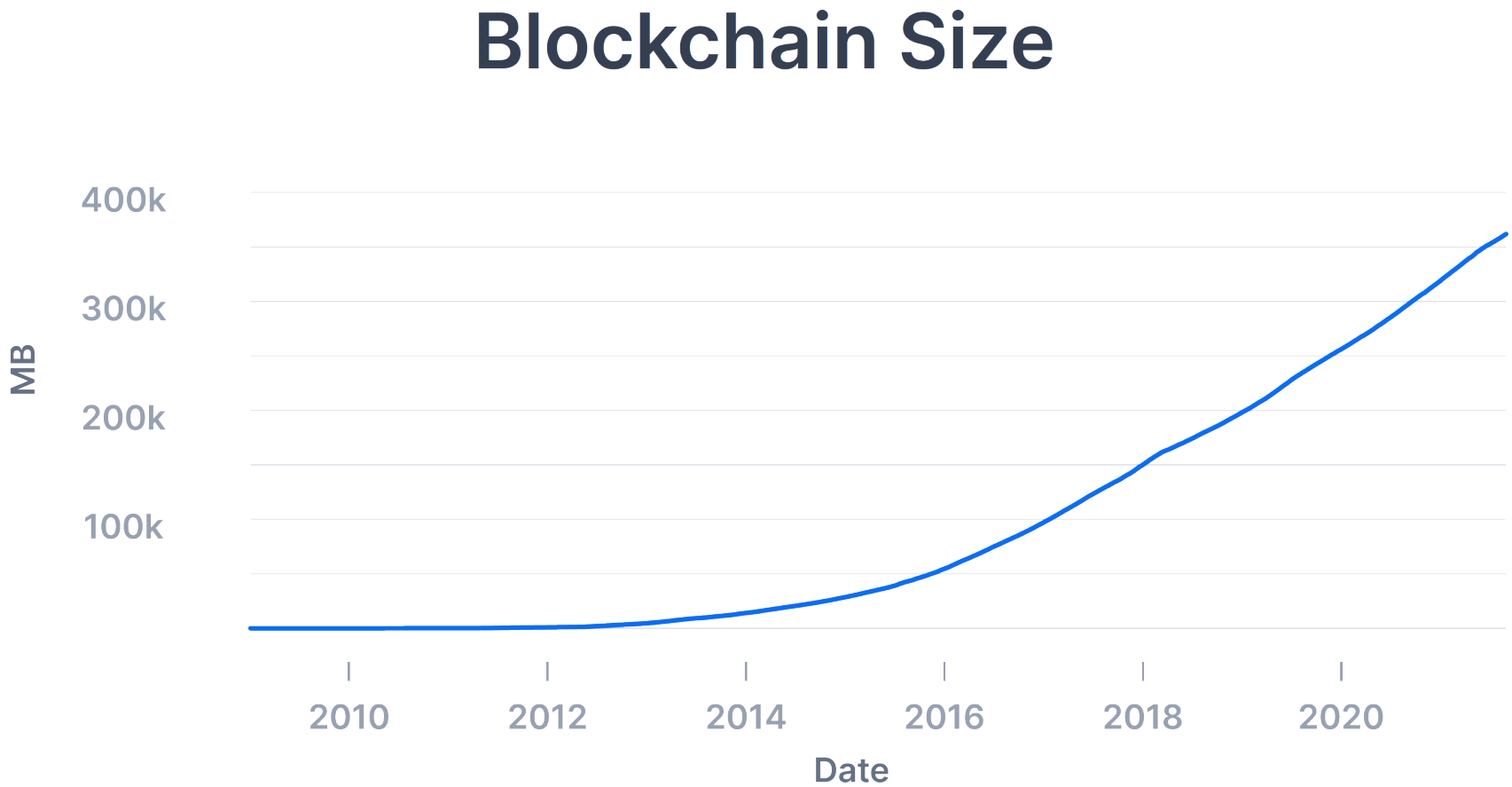


(a) Réseau maître-esclave



(b) Réseau pair-à-pair

# Le problème du passage à l'échelle



# L'idée du stage

- Mining in Logarithmic Space 2021 Aggelos Kiayias, Nikos Leonardos and Dionysis Zindros

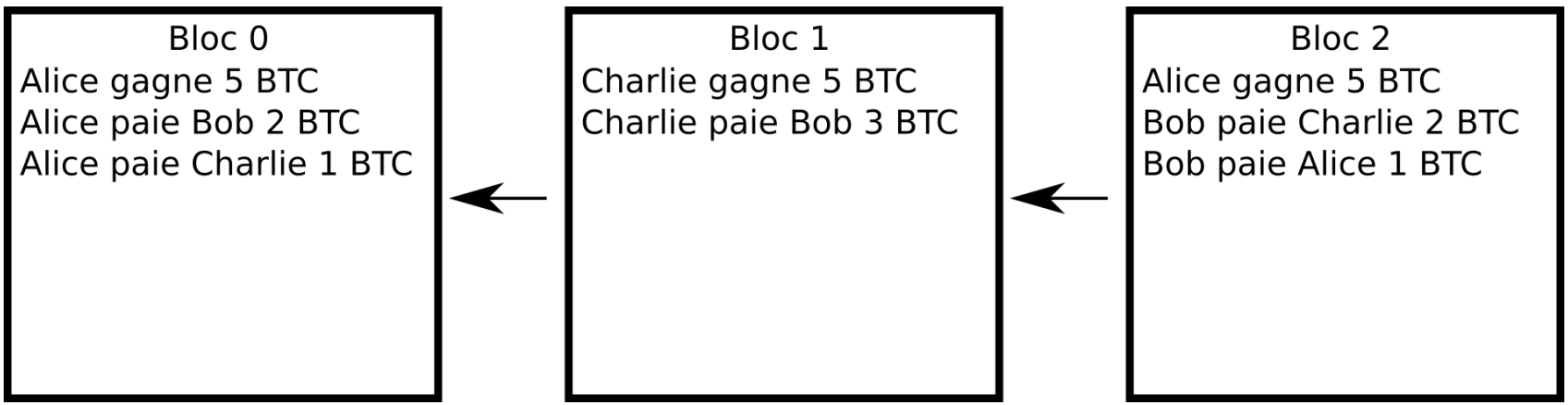
**Historique des transactions**

| Personne 1 donne à | personne 2 | n Bitcoins |
|---|---|---|
| Réseau | Alice | 5 |
| Alice | Bob | 2 |
| Alice | Charlie | 1 |
| Réseau | Charlie | 5 |
| Charlie | Bob | 3 |
| Réseau | Alice | 5 |
| Bob | Charlie | 2 |
| Bob | Alice | 1 |

**Etat courant**

| Personne possède | n Bitcoins |
|---|---|
| Alice | 8 |
| Bob | 2 |
| Charlie | 5 |

# Le fonctionnement de Bitcoin



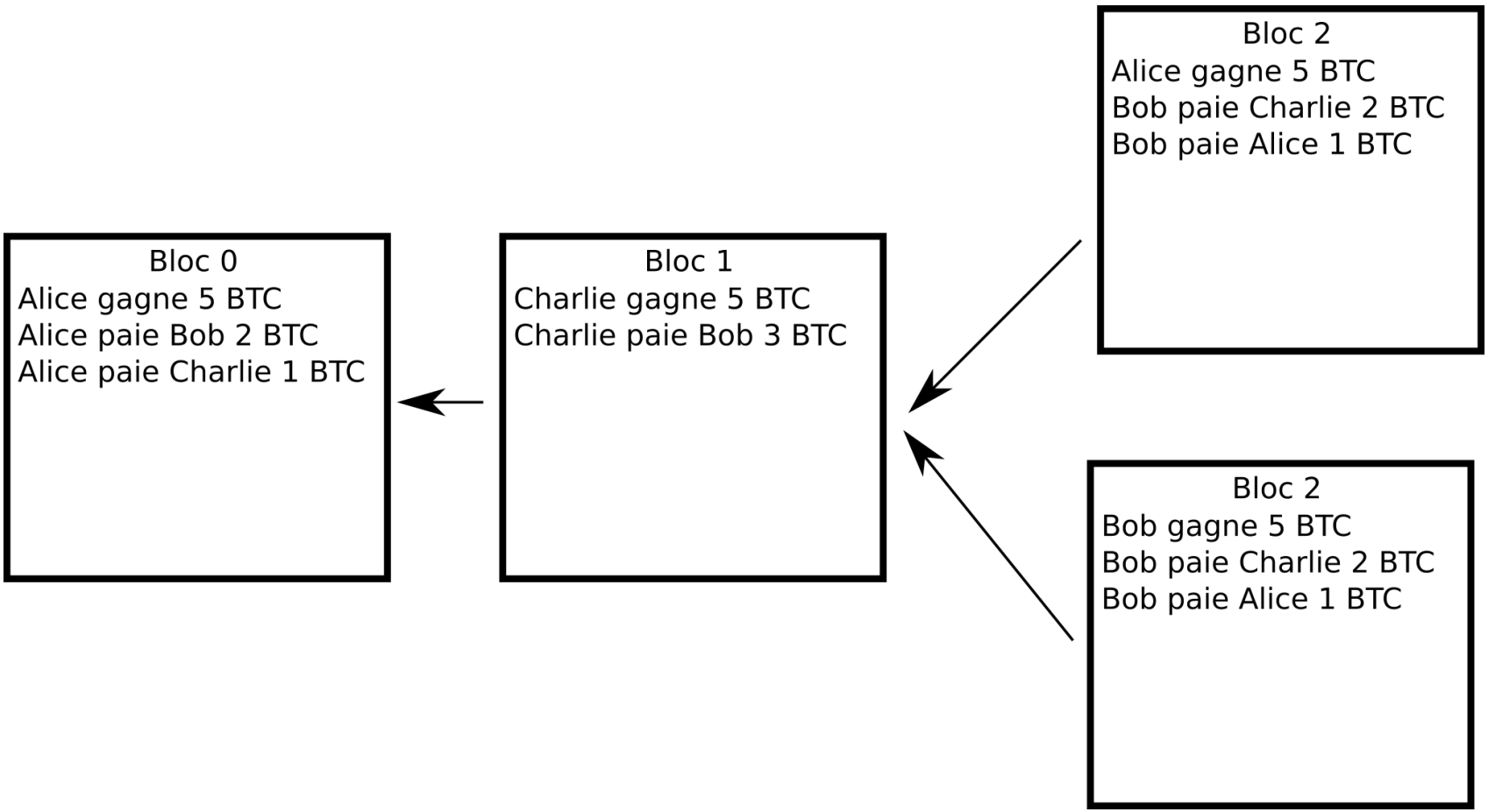
# Miner des blocs

Données:

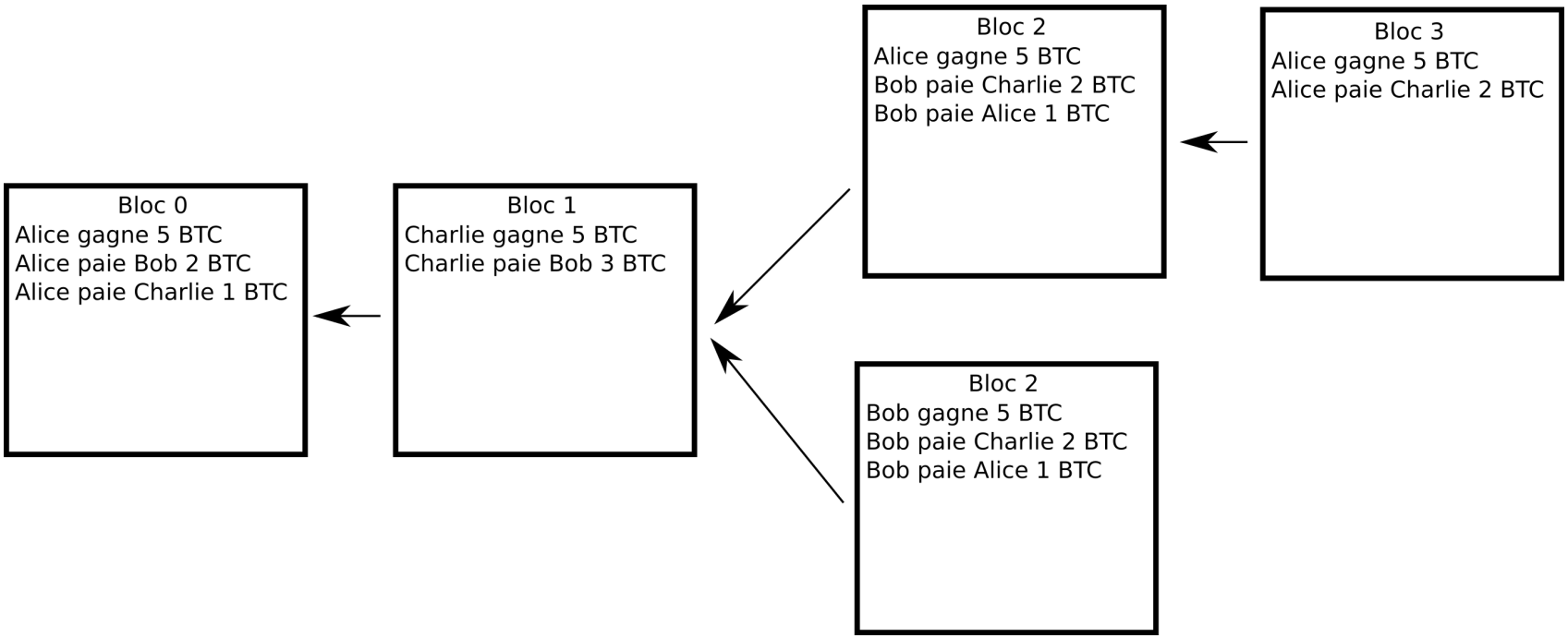
Bloc 0 n
Alice gagne 5 BTC
Alice paie Bob 2 BTC
Alice paie Charlie 1 BTC

| n | haché SHA-256² |
|---|---|
| 0 | 6c7c2450bd52e950a3db47d8dc91cbdb04a792561759... |
| 1 | 6442a403b0cd2bac7b3af363a342769d1955f9851d65... |
| ... | ... |
| 86 | 00e9d707e8f386a73d2455cfa9c06d618285f03e434a... |

# Le problème du fork



# Le problème du fork



# Les atouts de la théorie

| Proposal | Storage | Communication | Can mine? |
|---|---|---|---|
| **BTC Full** | $n(c+\delta)$ | $n(c+\delta)$ | yes |
| **BTC SPV** | $nc$ | $nc$ | no |
| **Ethereum** | $nc+k\delta+a$ | $nc+k\delta+a$ | yes |
| *This work* | $poly\log(n)c+k\delta+a$ | $poly\log(n)c+k\delta+a$ | yes |

**Table 1.** A comparison of our results and previous work. $n$: the number of blocks in the chain; $\delta$: size of transactions in a block; $c$: block header size; $a$: size of snapshot; $k$: common prefix parameter

Figure: Extrait du tableau page 9 de "Mining in Logarithmic Space" (BTC signifiant Bitcoin)
$n = 695590$, $\delta$ entre 0 et 2 Mo, $c = 97$, $a = 4.24$ Go, $k = 6$

# Le problème de l'interlink set

**Fig. 2.** The interlinked blockchain. Each superblock is drawn taller according to its level. A new block links to all previous blocks that have not been overshadowed by higher levels in the meantime.

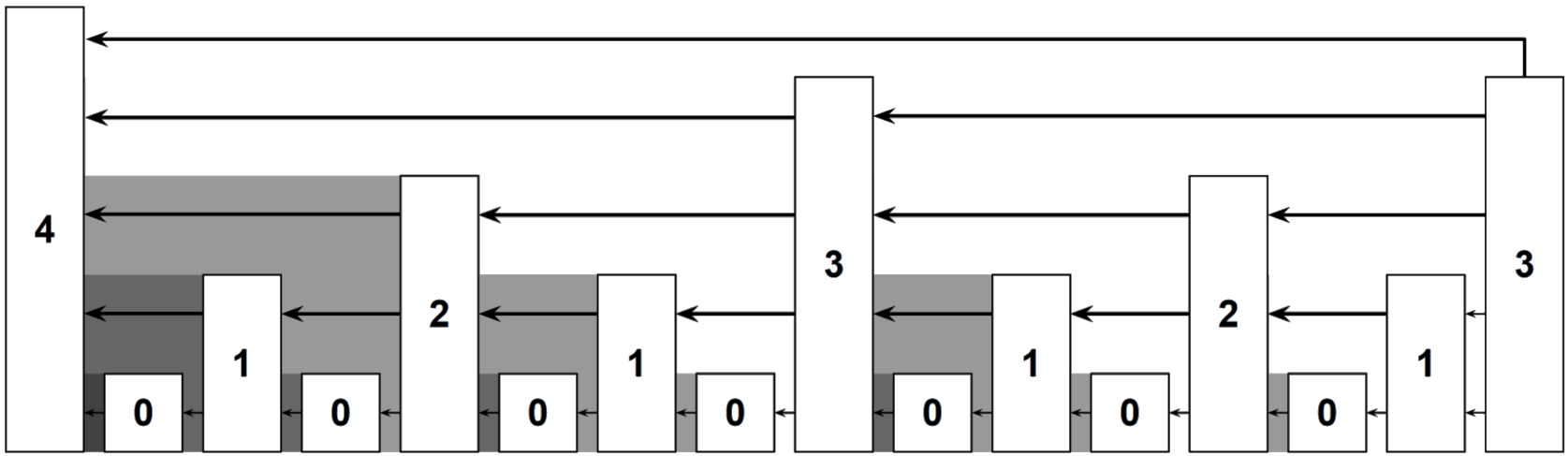



Figure: Ensemble de pointeurs de "Mining in Logarithmic Space" nécessaire à la bonne exécution de leur approche

# Quelques statistiques

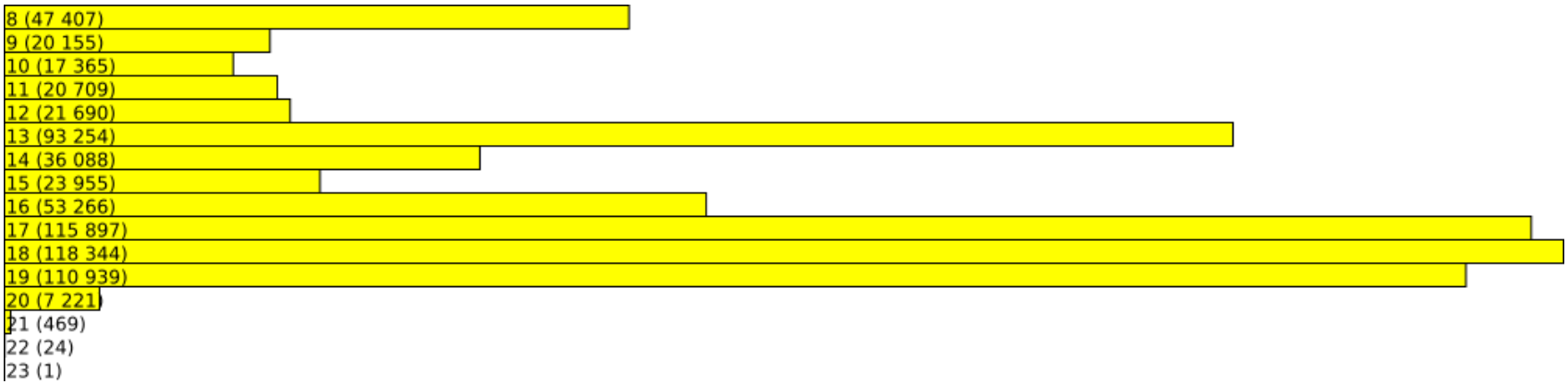



Figure: Répartition des hachés des blocs de Bitcoin par difficulté $m$ ($n$) où $m$ est le nombre de zéros hexadécimaux au début du haché et $n$ le nombre de hachés débutant précisément par $m$ zéros hexadécimaux

# Quelques statistiques

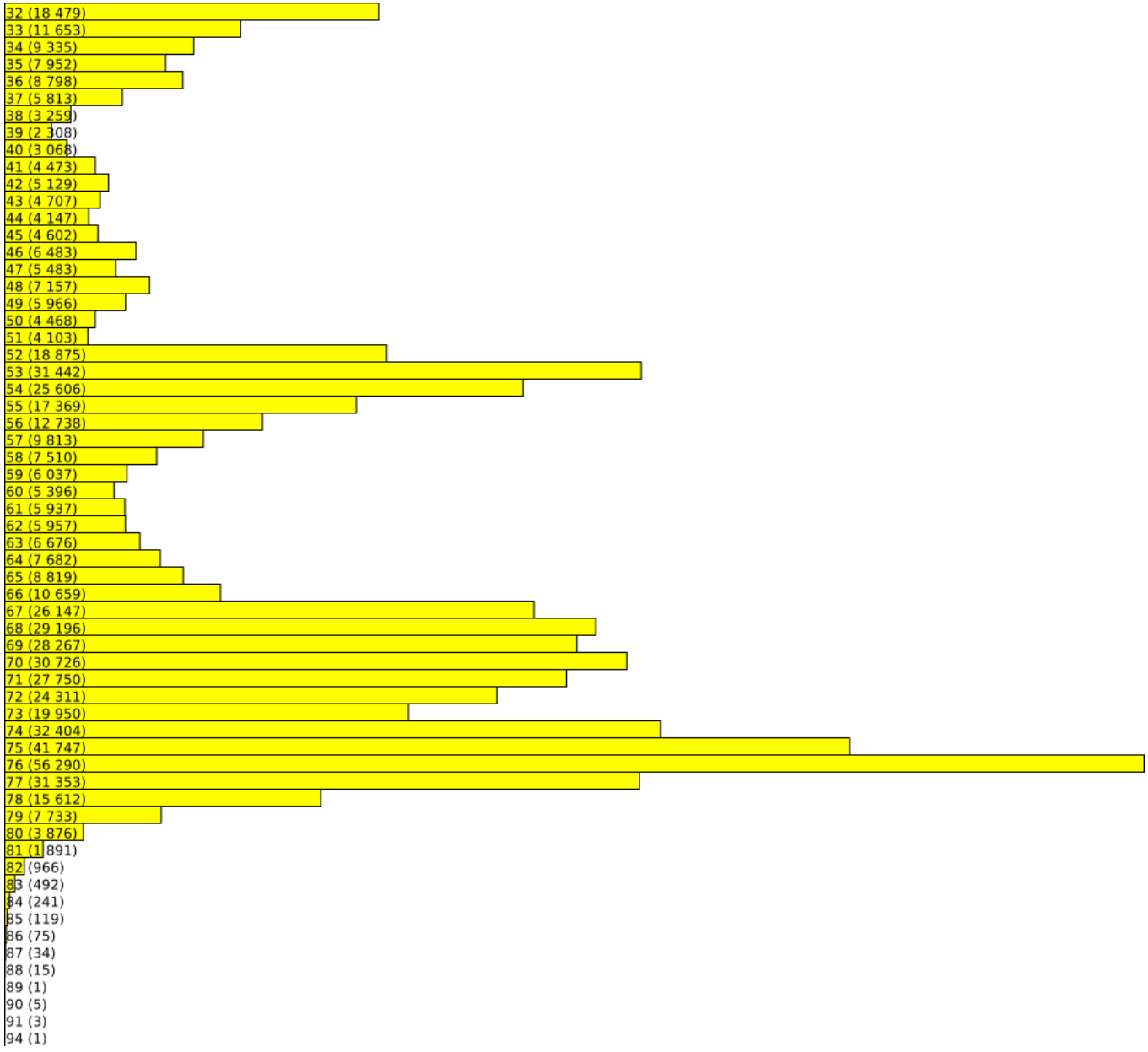



Figure: Répartition des hachés des blocs de Bitcoin par difficulté $m$ ($n$) où $m$ est le nombre de zéros binaires au début du haché et $n$ le nombre de hachés débutant précisément par $m$ zéros binaires

# L'algorithme de compression

**Algorithm 1** Chain compression algorithm for transitioning a full miner to a logspace miner. Given a full chain, it compresses it into logspace state.

**function** $\mathsf{Dissolve}_{m,k}(\mathcal{C})$
  $\mathcal{C}^* \leftarrow \mathcal{C}[:-k]$
  $\mathcal{D} \leftarrow \emptyset$
  **if** $|\mathcal{C}^*| \geq 2m$ **then**
    $\ell \leftarrow \max\{\mu : |\mathcal{C}^{*}\uparrow^{\mu}| \geq 2m\}$
    $\mathcal{D}[\ell] \leftarrow \mathcal{C}^{*}\uparrow^{\ell}$
    **for** $\mu \leftarrow \ell - 1$ down to $0$ **do**
      $b \leftarrow \mathcal{C}^{*}\uparrow^{\mu+1}[-m]$
      $\mathcal{D}[\mu] \leftarrow \mathcal{C}^{*}\uparrow^{\mu}[-2m:] \cup \mathcal{C}^{*}\uparrow^{\mu}\{b:\}$
    **end for**
  **else**
    $\mathcal{D}[0] \leftarrow \mathcal{C}^*$
  **end if**
  $\chi \leftarrow \mathcal{C}[-k:]$
  **return** $(\mathcal{D}, \ell, \chi)$
**end function**
**function** $\mathsf{Compress}_{m,k}(\mathcal{C})$
  $(\mathcal{D}, \ell, \chi) \leftarrow \mathsf{Dissolve}_{m,k}(\mathcal{C})$
  $\pi \leftarrow \bigcup_{\mu=0}^{\ell} \mathcal{D}[\mu]$
  **return** $\pi\chi$
**end function**

Figure: Algorithme 1 de "Mining in Logarithmic Space" permettant de compresser une blockchain.
$C$ est la chaîne de blocs
$C^* \uparrow^{\mu}$ désigne les blocs de niveau de difficulté exactement $\mu$ de $C^*$
$C^* \uparrow^{\mu} \{b :\}$ désigne les blocs de $C^* \uparrow^{\mu}$ plus récents que le bloc $b$

# Les résultats

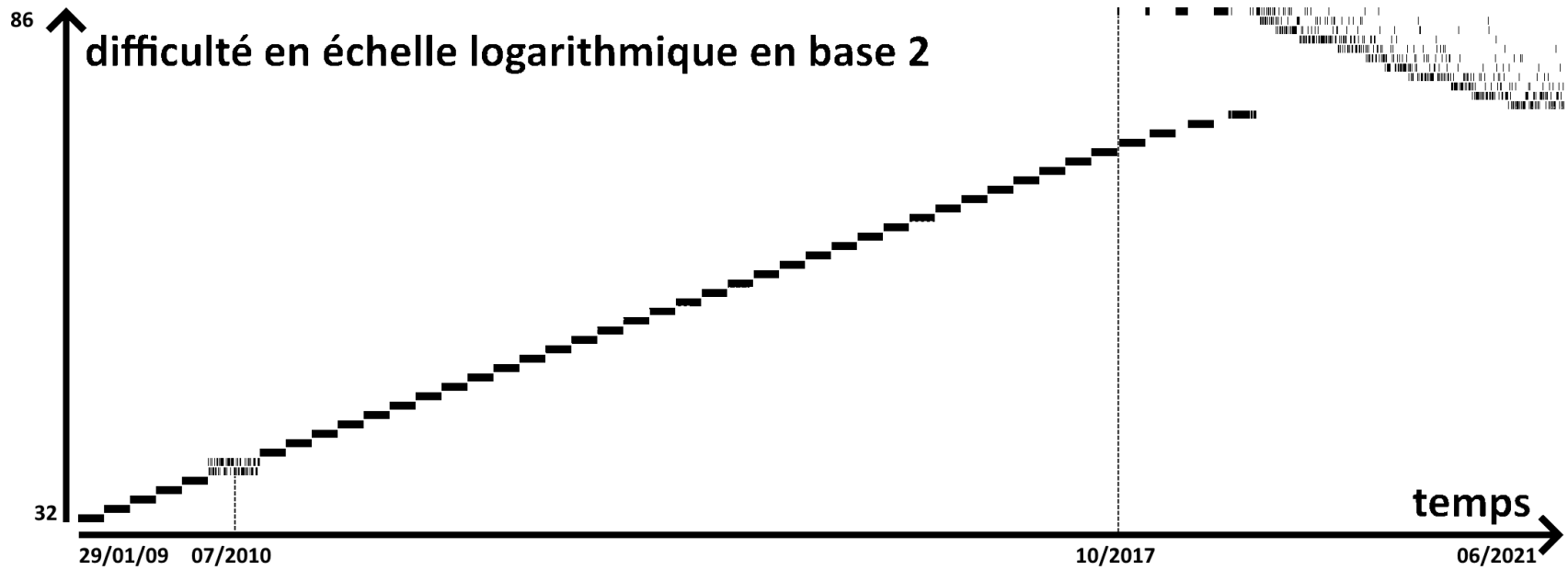



Figure: Répartition des hachés des blocs sélectionnés par l'algorithme 1, où chaque bloc a une largeur de 1 pixel

# Sources des illustrations

- Page 2: Wikipedia: peer-to-peer
- Page 3: Blockchain.com