Mini Rapport concernant l'usage d'une machine du cloud

Adrien Pavao

Juin 2017

1 Introduction

A la fin du TER intitulé *"Utilisation de Spark pour du Map-Reduce sur des objets combinatoire"*, j'ai continué à utiliser la machine qui était à ma disposition sur le cloud du LAL. Ces utilisations étaient principalement les suivantes:

- **Du machine learning :** En effet, les calculs déployés pour faire de l'apprentissage automatique s'avèrent souvent très longs. L'accès à un serveur sur lequel on peux lancer des calculs de plusieurs jours est donc très utile. La plupart des calculs étaient faits dans le cadre d'un projet pour la faculté (reconnaissance d'image sur la base de données CIFAR-10), d'autres m'ont permis d'approfondir ma prise en main de la bibliothèque python Sklearn.
- **Du minage de crypto-monnaie :** Les monnaies virtuelles sont des sortes de monnaies sur un réseau informatique, dont les transactions sont validées à l'aide de principes de la cryptographie. Un miner est donc un programme qui valide des transactions et qui en échange, se voit être rémunéré dans la monnaie en question. Ces calculs sont complexes et demandent de la puissance de calcul. C'est sur cette utilisation du serveur, plus ambigu, que portera la suite de ce rapport.

2 Motivation et objectifs

Plusieurs points ont attirés ma curiosité.

- La première question qui m'intéressait était tout simplement de savoir comment on met en place un miner, afin d'en comprendre mieux le fonctionnement.
- Bien que le principe général reste le même, il existe des centaines de crypto-monnaies au propriétés souvent bien différentes. Elles ne sont pas toutes

basées sur le même algorithme de cyptographie. On peux alors se demander laquelle est la plus rapide à miner (dans l'absolu), ou encore laquelle est théoriquement la plus rentable (relativement à son prix sur le marché).

- Le minage peut s'exécuter sur GPU ou sur CPU. Ici, nous n'utilisons que le CPU. La question suivante peut sembler triviale aux premiers abords: Combien de coeurs du processeur faut-il mettre à la tâche pour obtenir la meilleure fréquence de minage ? J'ai donc tenté d'y répondre à l'aide de tests.

3 Mise en place du miner

Pour faire miner un ordinateur, il est nécessaire d'avoir:

- **Un logiciel de mining :** C'est le programme qui va exécuter les différents algorithmes afin de sécuriser des transactions.
- **Une mining pool :** La complexité des calculs étant très grandes, les miners se rejoignent en "pool" pour miner ensemble avant de se répartir équitablement les rémunérations. Ceux qui ont fourni la plus grande puissance de calcul récupèrent la plus d'argent virtuel.
- **Un porte-feuille** (ou wallet) : Avec les crypto-monnaies, il n'y a pas de compte en banque et encore moins de liquidité. Votre argent est stockée dans un porte-feuille virtuel, qui possède une adresse sur laquelle on peux vous transférer de l'argent.

Le logiciel de mining affichera un certain **taux de hash**. Le taux de hash est l'unité de mesure de calculs par seconde que votre matériel peut effectuer lorsqu'il résout un problème mathématique (H/s). Celui-ci dépend donc du matériel (puissance du GPU ou CPU) mais également de l'algorithme sur lequel est basée la monnaie ou encore de sa difficulté actuelle. Nous en verrons un peu plus à ce sujet dans la section suivante.

4 Différentes monnaies

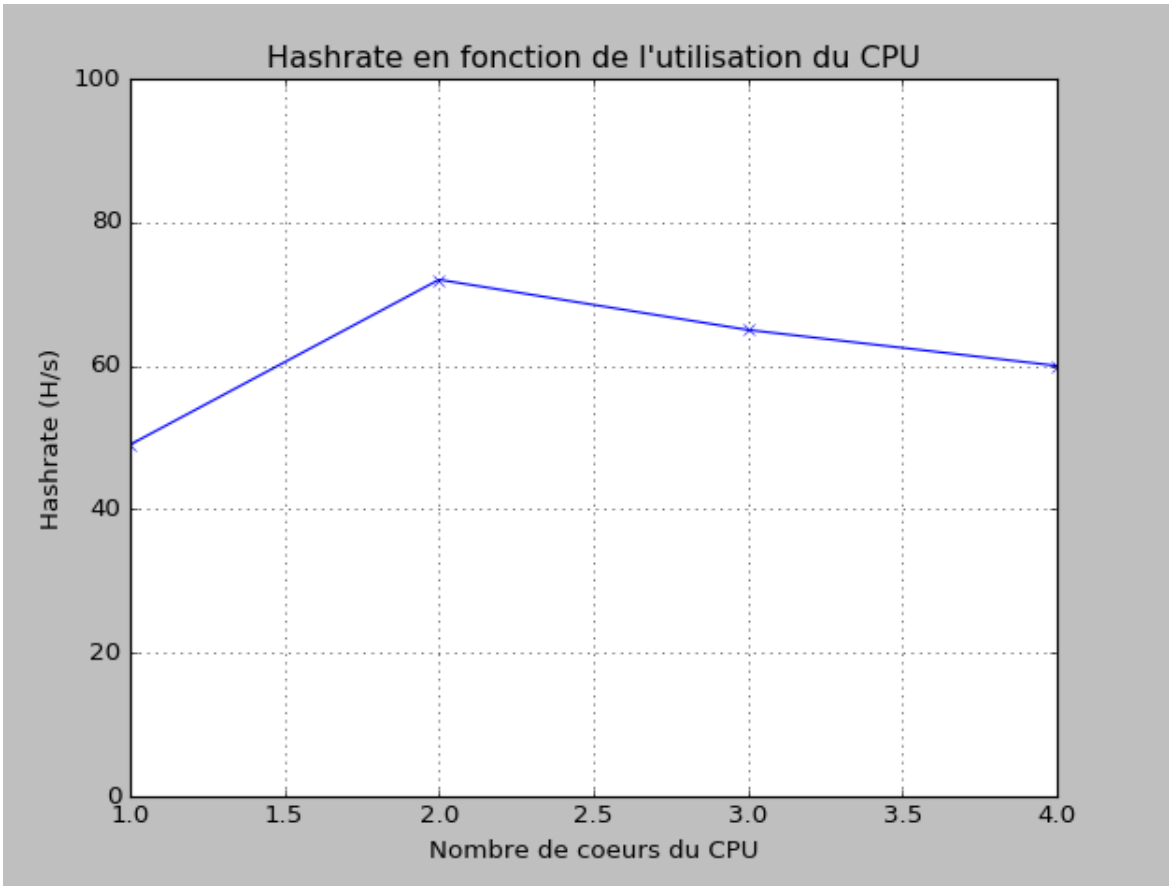
Lorsqu'on parle de crypto-monnaie, on pense tout de suite au BitCoin. Cependant, depuis la création de celui-ci des centaines d'autres monnaies ont vu le jour.
Chaque monnaie possède un cours (l'évolution de son prix) et un certain algorithme permettant de la miner. Plus une monnaie a été minée par le passé et plus la difficulté à la miner par la suite est grande. J'ai pu ainsi me rendre compte des différences colossales que l'on peut rencontrer d'une monnaie à l'autre concernant le minage de celle-ci. Je malheureusement n'ai pas gardé de statistiques précises sur les tests que j'ai effectué. S'il est facile de savoir quelle monnaie est la plus rapide à miner dans l'absolu, il est bien pus difficile

de trouver la plus rentable. Les cours sur le marché fluctuent constamment, et une monnaie rentable à un moment donné peut ne plus l'être le lendemain et réciproquement. Il faudrait faire des tests précis et sauvegarder des données pour en savoir plus.
J'ai également pu apprendre qu'il existe des monnaies permettant le **merged mining**. Cela signifie que pour la même puissance de calcul, on mine en parallèle deux monnaies. Il faut bien-sûr que celles-ci soient basées sur le même algorithme.

5 Variation du nombre de coeurs

Le logiciel de minage permet de choisir le taux d'utilisation du processeur que l'on souhaite. Nous avions en tout 8 coeurs sur la machine. Il aurait été souhaitable d'avoir tracé un graphe du taux de hash en fonction du nombre de coeurs utilisés, cependant je n'ai pas enregistré les valeurs. Ce qu'il était intéressant de noter est le fait que le plus efficace était d'utiliser la moitié des coeurs, soit 4. Je n'ai pas su expliquer la raison de cette amélioration. L'utilisation pleine du processeur semble trop contraignante, il faut un peu de marge pour que tout fonctionne normalement.
Pour avoir tout de même des chiffres à présenter dans ce rapport, j'ai exécuté un minage du Monero (il s'agit d'une monnaie) avec 1, 2, 3 et 4 coeurs (ma machine n'en possède que 4). On peut à présent comparer les H/s. Avec le logiciel **htop**, on voit que les coeurs demandés sont utilisés à 100%.

Figure 1: Hashrate en fonction de l'utilisation du CPU



Les résultats sont cohérents avec ceux obtenus sur la machine du LAL. On voit que le taux de hash est au plus haut lorsque l'on utilise la moitié des processeurs (ici 2, plutôt que 4).

6 Analyse et conclusion

En conclusion, l'étude des crypto-monnaies et de leurs différents minages est concret et satisfaisant. Les diverses questions auxquelles j'ai répondu durant mes tests m'en ont appris et m'ont introduit à un domaine que je ne connaissais que très peu. Il est toute fois dommage que je n'ai pas gardé de données à la suite des tests. A l'avenir, j'essaierai d'avancer moins à l'aveugle lorsque j'explorerais une nouvelle technologie. De plus, j'aurais normalement du deman-

der la permission avant d'utiliser cette machine en dehors du cadre du TER, aussi bien pour le machine learning que pour le minage.
Je trouve personnellement que les résultats du taux de hash en fonction du nombre de coeurs utilisés est très intéressant, cependant je ne sais pas l'expliquer. Il serait envisageable d'approfondir la question.