# Rapport d’essais: partie benchmarks

Le but de ce document est de retracer notre parcours dans l’aspect benchmark du projet, y résumer tout ce qu’on a pu apprendre d'intéressant, et comment celà à orienter notre travail. Nous présenterons en fin de document notre avancée et les résultats que l’on a pu obtenir.

## Première approche, premières métriques

Pour commencer, nous nous somme documentés sur les différentes blockchains existantes, à savoir leur fonctionnement, leurs avantages et inconvénients les une par rapport aux autres. Le paysage des cryptomonnaies est vaste et diversifié, chaque monnaie ayant sa propre blockchain avec des spécificités uniques. Examinons donc quelques-unes de ces cryptomonnaies, en mettant en évidence les caractéristiques de leurs blockchains respectives, ainsi que les métriques intéressantes à étudier pour évaluer leur performance.

Commençons par le Bitcoin (BTC), la première et la plus connue des cryptomonnaies. La blockchain du Bitcoin utilise le consensus de preuve de travail (PoW) et vise à être une monnaie numérique décentralisée. Une spécificité de la blockchain Bitcoin est son algorithme de hachage SHA-256 et sa limite de taille de bloc de 1 mégaoctet (MB). Pour évaluer le Bitcoin, il est pertinent de se pencher sur des métriques telles que la puissance de hachage totale du réseau, le temps moyen de confirmation des transactions et les frais de transaction moyens.

Ensuite, examinons Ethereum (ETH), une plateforme de contrat intelligent qui utilise une blockchain publique. La blockchain d'Ethereum utilise actuellement le consensus de preuve de travail (PoW), mais elle prévoit également une transition vers le consensus de preuve d'enjeu (PoS) avec Ethereum 2.0. Une caractéristique distinctive de la blockchain Ethereum est son support natif des contrats intelligents et des jetons ERC-20. Les métriques clés à considérer pour Ethereum incluent le nombre de contrats intelligents déployés, le volume des transactions et les temps de confirmation.

Poursuivons avec Ripple (XRP), à la fois une cryptomonnaie et une plateforme de règlement en temps réel. La blockchain de Ripple utilise un registre distribué et un protocole de consensus appelé le protocole de consensus de Ripple (RPCA). La spécificité de la blockchain Ripple réside dans sa capacité à faciliter les paiements transfrontaliers rapides et à faible coût. Dans l'évaluation de Ripple, il est pertinent d'analyser des métriques telles que le volume total des transactions effectuées sur le réseau et les frais de transaction moyens.

Ensuite, intéressons-nous à Cardano (ADA), une blockchain qui vise à être une plateforme de contrat intelligent sécurisée et évolutive. La blockchain de Cardano utilise le consensus de preuve d'enjeu (PoS) et se distingue par son approche scientifique et sa vérification formelle pour garantir la sécurité. La spécificité de la blockchain Cardano réside dans son architecture en couches, séparant la couche de règlement (Settlement Layer) de la couche de calcul (Computational Layer). Les métriques importantes pour Cardano incluent le nombre de contrats intelligents déployés, le rendement des stakers et la participation au réseau.

Enfin, examinons Binance Coin (BNB), une cryptomonnaie émise par la plateforme d'échange Binance. La blockchain de Binance Coin, appelée Binance Chain, utilise le consensus de preuve d'enjeu (PoS) et est principalement utilisée pour faciliter les transactions sur la plateforme Binance. Une particularité de la blockchain Binance Chain est son intégration étroite avec l'écosystème Binance, offrant des avantages tels que des frais réduits pour les utilisateurs de la plateforme Binance. Les métriques pertinentes pour Binance Coin incluent le volume des transactions sur la plateforme Binance, l'utilisation du BNB pour les frais de transaction et l'adoption de la cryptomonnaie.

Après une revu des différentes chaînes existante ainsi que de leur spécificité, nous avons dressé une première liste des métriques qu'il aurait été intéressant d'avoir :

- Le temps nécessaire pour arriver consensus
- l'impact de la latence
- le délais de validation des transactions
- une estimation de la différence de consommation d'énergie entre un algo de proof of work et un algo de proof of interaction

## Les forks de chaine, une question primordial

C'est alors que plusieurs questions se sont posées autour de ces métriques. Tout d'abord, le délai pour que nos transactions soient acceptées par l'ensemble du réseau. Après étude, on s'est rendu compte que cela reviendrait à tout simplement à faire varier la difficulté de l'algorithme de consensus, afin que les blocs soient validés plus rapidement. Seulement, cela implique un gros problème: le risque de fork de la chaîne. En effet diminuer la difficulté revient à rendre "l'énigme" plus facile et ainsi à produire et "sceller" plus de blocs, mais de ce fait la probabilité que plusieurs utilisateurs le fassent en même temps augmente. Deux personnes attachent donc a la chaine un bloc différent: ils ont donc tous les deux une chaîne totalement valide, mais différente. Quelles chaînes choisir dans ce cas ? La plupart des crypto-monnaies recommande de toujours choisir la chaîne la plus longue. Oui mais alors comment choisir, si ces deux chaînes continuent de croître toutes les deux ?
Plusieurs mécanismes sont utilisés pour résoudre ces forks et maintenir la cohérence de la blockchain.
Un exemple de gestion des forks temporaires se trouve dans le Bitcoin (BTC). Lorsqu'un fork se produit, les mineurs continuent de travailler sur la branche qu'ils ont choisie initialement. Cependant, la communauté Bitcoin reconnaît la branche qui a accumulé le plus de puissance de calcul comme la branche principale et valide les transactions sur cette branche. Les mineurs qui travaillent sur la branche perdante sont incités à basculer vers la branche principale en raison de la difficulté accrue de miner des blocs sur la branche perdante. Cela permet de converger rapidement vers une seule chaîne.
Un autre exemple est Ethereum (ETH) qui utilise également le consensus de preuve de travail (PoW). Lorsqu'un fork transitoire se produit, les mineurs choisissent généralement de continuer à miner sur la branche avec la plus grande puissance de hachage, car cela leur permet de gagner plus de récompenses minières. Cependant, Ethereum a également connu des forks plus importants, appelés "hard forks", qui sont des mises à jour majeures du protocole. Ces hard forks sont planifiés et nécessitent un consensus de la communauté pour

être acceptés. Les participants de la communauté peuvent choisir de migrer vers la nouvelle version ou de rester sur l'ancienne.
Une autre approche est celle de Ripple (XRP), qui utilise un protocole de consensus de Ripple (RPCA) pour valider les transactions. Le protocole RPCA ne génère généralement pas de forks transitoires, car il sélectionne un ensemble de validateurs uniques pour valider les transactions. Ces validateurs sont choisis en fonction de leur fiabilité et de leur accord avec les autres participants du réseau Ripple, ce qui réduit considérablement les risques de forks temporaires.

## Travail produit, difficultés rencontrés

Suite à une discussion avec l'enseignant Brama ou on lui a présenter nos réflexions et nos pistes, il nous a suggéré d'explorer cette partie de forks de chaîne.
Dans le contexte des crypto-monnaies, un utilisateur est généralement représenté par une adresse de cryptomonnaie. Cette adresse est une chaîne de caractères alphanumériques unique, spécifique à chaque utilisateur, qui lui permet de recevoir, stocker et envoyer des fonds numériques.
L'adresse de cryptomonnaie est essentiellement une clé publique, c'est-à-dire une partie d'une paire de clés cryptographiques. La clé publique est utilisée pour recevoir des fonds et est accessible à tous les utilisateurs du réseau. Cependant, elle ne permet pas de dépenser les fonds.
La clé privée correspondante à la clé publique est ce qui permet à un utilisateur de signer des transactions et de prouver qu'il est le propriétaire des fonds. La clé privée doit rester confidentielle et sécurisée, car toute personne ayant accès à la clé privée peut accéder et dépenser les fonds associés à l'adresse de cryptomonnaie.
C'est donc tout naturellement que l'on s'est tourné vers les questions de création de comptes utilisateurs, en tenant compte de ses aspects là.
Pour cela, nous avons pensé à utiliser la bibliothèque polkadotJS. C'est une bibliothèque spécialement faite pour cela. A première vue, cela répondait parfaitement à notre besoin. Mais on a passé beaucoup de temps à essayer, puis on en est arrivé à la conclusion qu'il fallait impérativement modifier les paramètres de notre blockchain de test implémentant l'algorithme de proof of work. On a ensuite essayé de le faire dans les paramètres de la blockchain, mais c'était hors de notre portée, et l'équipe core avait déjà des tâches plus prioritaires sur le le backend du projet.
Au final on s'est résigné à continuer uniquement avec les 6 comptes prédéfinis, forcément ça devient un peu moins intéressant, d'avoir uniquement 6 comptes.
Mais on a tout de même fait un script, qui lance donc ces 6 nœuds, connectés entre eux (en local bien sûr), et qui participent à une session de consensus.
Ce script nous permet de voir où il y a des forks dans la blockchain, en analysant les logs des nœuds . Tout ça soulève plein d'autres questions: comment notre algorithme de proof of interaction pourra gérer cela ? Comment pourrait-on s'inspirer de ce qui est fait dans d'autres systèmes?
C'était justement ce vers quoi on tendait, en faisant varier la difficulté on aurait aimé trouver des conjectures, faire varier cette difficulté, trouver une équivalence entre la difficulté proof of work et proof of interaction, et enfin comparer les probabilités de forks pour des difficultés équivalentes, afin d'en trouver une optimale pour le POI.

En conclusion, ce travail sur les benchmarks dans le domaine des cryptomonnaies a permis d'explorer différentes blockchains, leurs spécificités et les métriques clés pour évaluer leurs performances. Nous avons examiné des cryptomonnaies telles que Bitcoin, Ethereum, Ripple, Cardano et Binance Coin, en mettant en évidence leurs caractéristiques uniques et les métriques pertinentes pour chacune d'entre elles.

Ce travail nous a permis de mieux comprendre les aspects liés aux benchmarks dans le domaine des cryptomonnaies, en mettant en évidence les métriques importantes et les défis rencontrés dans la gestion des forks de chaîne.

# SOURCES

https://bitcoin.org/bitcoin.pdf
https://ethereum.org/whitepaper/
https://ethereum.org/pdfs/EthereumYellowPaper.pdf
https://doi.org/10.1007/978-3-662-47854-7_32