1INDF activité 2 : consensus

2.1 Théorie

Un **noeud** est un ordinateur ou groupe d'ordinateurs, géré(s) par une ou plusieurs personne(s)), qui possède une copie locale de la chaîne de blocs et la tient à jour, ainsi que le logiciel de la chaîne de blocs. Tous les nœuds sont interconnectés et composent le réseau de la chaîne de blocs. Leur rôle est de vérifier la validité des nouveaux blocs et des transactions qu'ils contiennent (voir activité 3).

Le mineur est un type de nœud qui se spécialise dans le minage de blocs.

Des participants à la chaîne de blocs peuvent s'ajouter ou se retirer à tout moment. Ceux qui se retirent puis reviennent doivent accepter la chaîne de blocs telle qu'elle a évolué au moment de leur retour.

La chaîne de blocs est **décentralisée** : il n'existe pas de version « officielle » de la chaîne de blocs, personne ne possède la chaîne de blocs : elle existe dans les copies locales de tous les nœuds participants. La chaîne de blocs est transparente : le registre est public et le logiciel est libre (open source), les modifications sont décidées par les participants à la chaîne de blocs.

La chaîne de blocs est validée **sans tiers de confiance** : personne en particulier n'est chargé d'approuver les nouveaux blocs. Le système s'auto-régule parmi les participants : le nœud dont le mineur a inséré un nouveau bloc partage le nouveau bloc avec les nœuds voisins, qui vérifient la validité du bloc ajouté, l'ajoutent à leur copie locale, puis le partagent avec les nœuds voisins, et ainsi de suite jusqu'à ce que le nouveau bloc se retrouve sur la majorité des copies locales de la chaîne de blocs.

Il arrive que des nœuds possèdent des versions différentes de la chaîne de blocs. Dans ce cas, la version la plus populaire gagne naturellement, car plus de blocs seront construits sur cette chaîne, qui présentera la fourche la plus longue. Les nœuds possédant des versions différentes vont donc abandonner ces versions et adopter la version de la chaîne de blocs comportant la fourche la plus longue.

2.3 Activité

Le but de la deuxième activité est de comprendre le fonctionnement d'un système de transactions par consensus, sans tiers de confiance.

Les règles et le but sont les mêmes que celles de l'activité 1, à une différence près : la chaîne de blocs n'est pas affichée sur un panneau à la vue de tous, mais chaque nœud a sa propre copie locale de la chaîne de blocs.

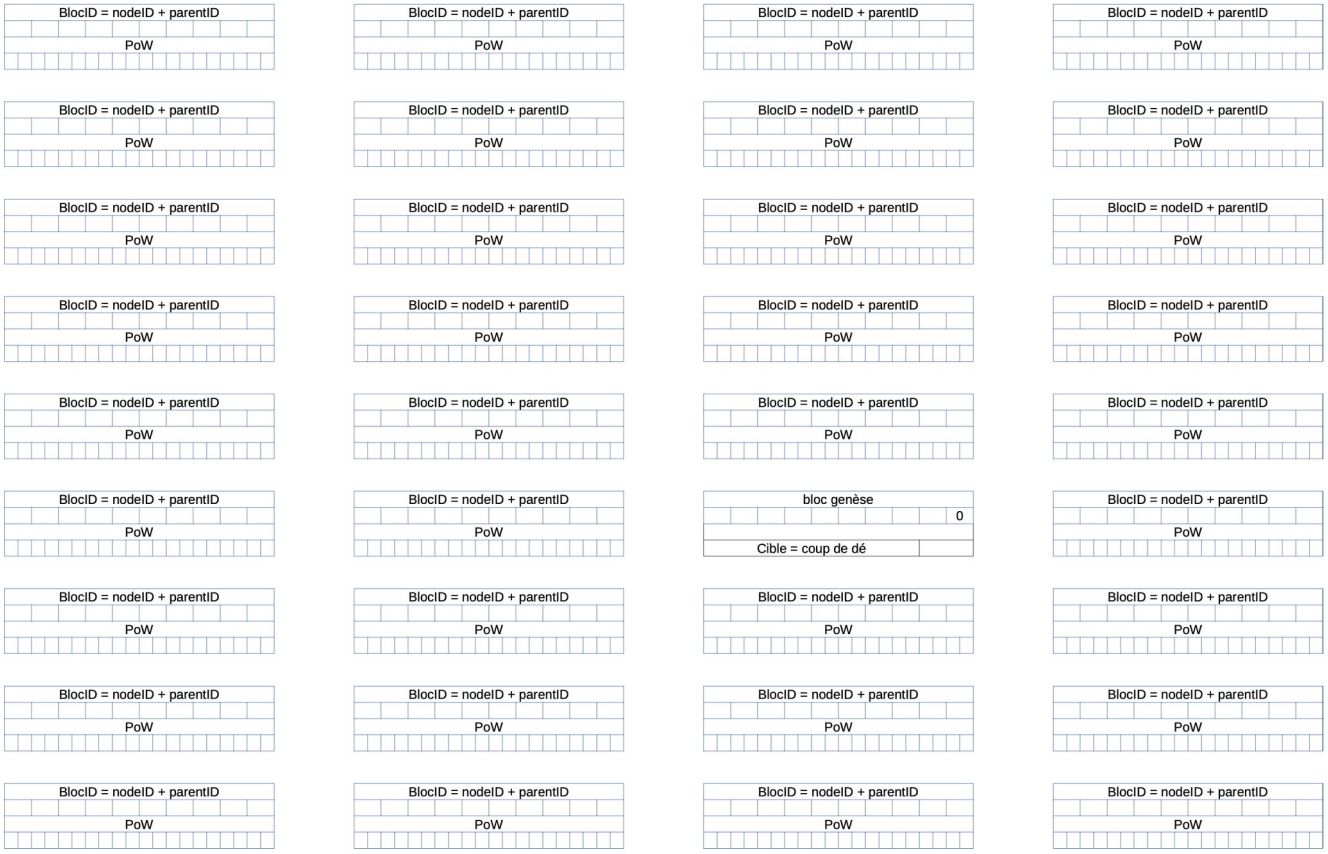
Les élèves travaillant pour un nœud ont avantage à se spécialiser et travailler en parallèle : certains vérifient les nouveaux blocs pendant que d'autres tentent de miner des blocs dans la fourche la plus longue.

Matériel :

- une copie locale de la chaîne de blocs (feuille A4) pour chaque nœud,

- pour la variante 2 seulement : un tableau « nouveaux blocs » (tableau blanc et aimants, ou panneau en liège et punaises, ou poster et scotch)
- papier brouillon (pour les calculs), crayon, calculatrice.

Copie locale de la chaîne de blocs :



2.3.1 Variante 1

1. Les mineurs calculent les nouveaux blocs comme dans l'activité 1, préparent les petits feuillets, mais ne les affichent pas : ils passent les feuillets à leurs voisins.
2. Lorsqu'ils reçoivent un bloc sur un feuillet, les nœuds doivent impérativement en vérifier la validité ***avant*** de commencer à miner un nouveau bloc :
   a) vérifier le « bloc ID » et la « PoW » du bloc ;
   b) si le « bloc ID » et la « PoW » sont valides, le nœud ajoute le bloc sur sa copie locale de la chaîne de blocs ;
   c) si le « bloc ID » ou la « PoW » est faux ou fausse, le mineur ne l'insère pas dans sa copie locale.
3. Les nœuds passent les feuillets qu'ils ont reçus et vérifiés à leurs voisins.
4. Pendant que les nœuds vérifient et diffusent les blocs des feuillets qui circulent, les mineurs calculent de nouveaux blocs, en tenant compte des nouveaux blocs insérés sur leurs copies locales de la chaîne de blocs.
5. À la fin de l'activité, les copies locales de la chaîne de blocs sont comparées :
   - La chaîne de blocs qui se retrouve sur le plus de copies locales devient officielle, les

autres sont éliminées.

- Si aucune chaîne de blocs n'est identique à une autre, les chaînes de blocs les plus similaires sont conservées, et ensuite celle qui contient la fourche la plus longue est conservée, les autres sont éliminées.

2.3.1 Variante 2

Les règles sont les mêmes que celles de la variante 1, mais au lieu de passer les feuillets entre eux, les noeuds les affichent sur le tableau « nouveaux blocs », les uns à la suite des autres, mais sans les relier à leurs blocs-parents respectifs.

2.4 A retenir

Les nœuds ont avantage à vérifier les blocs insérés par les autres nœuds, d'une part pour s'assurer que personne ne triche, mais aussi pour s'assurer que leur copie locale de la chaîne de blocs est à jour, et que leurs futurs blocs sont construits sur des blocs valides, sinon les blocs minés risquent de se retrouver sur une fourche plus courte ou abandonnée.

La chaîne de blocs est **publique,** car n'importe qui peut devenir un mineur et enchaîner un nouveau bloc. Tous les nœuds ont une copie de la chaîne et vérifient sa validité à chaque mise à jour. C'est ce qui fait sa force : plus il y a de nœuds qui participent à la chaîne de blocs, plus il y a d'entités qui vérifient sa validité, plus elle devient **inaltérable**.

Il est possible que plusieurs versions de la chaîne de blocs coexistent. La version la plus populaire (i.e. celle qui correspond à la copie locale du plus grand nombre de nœuds) deviendra dominante, car plus de mineurs y ajouteront des blocs, produisant la chaîne la plus longue.