3INDF BlocNote, activité 5 : preuve d'enjeu (PoS, proof of stake)

But : comprendre le consensus basé sur la preuve d'enjeu (proof of stake, PoS).

5.1 Théorie

La principale critique concernant les chaîne de blocs basées sur la preuve de travail (PoW) est leur utilisation d'énergie électrique démesurée. Certaines chaînes de blocs comme Ethereum optent pour le consensus basé sur la preuve d'enjeu (PoS).

Dans ce type de chaînes, les nœuds n'ont plus besoin d'effectuer un calcul mathématique pour qu'un nouveau bloc soit inséré dans la chaîne : les mineurs s'appellent maintenant **validateurs**. Le nœud-validateur qui validera le prochain bloc est tiré au hasard parmi tous les blocs qui mettent de côté une partie de leurs avoirs en cryptomonnaie. La chance de remporter la loterie est proportionnelle au montant mis en garantie par le nœud. Notons que le montant gelé n'est plus disponible pour effectuer des transactions.

Comme dans les chaînes de blocs à PoW, le validateur reçoit une récompense pour chaque bloc faisant partie de la fourche la plus longue de la chaîne de blocs. Si un validateur ne fait pas son travail, n'est pas en ligne, ne détecte pas un bloc invalide, ou laisse délibérément un bloc invalide dans la chaîne de blocs, il perd une partie ou la totalité de la cryptomonnaie de sa PoS.

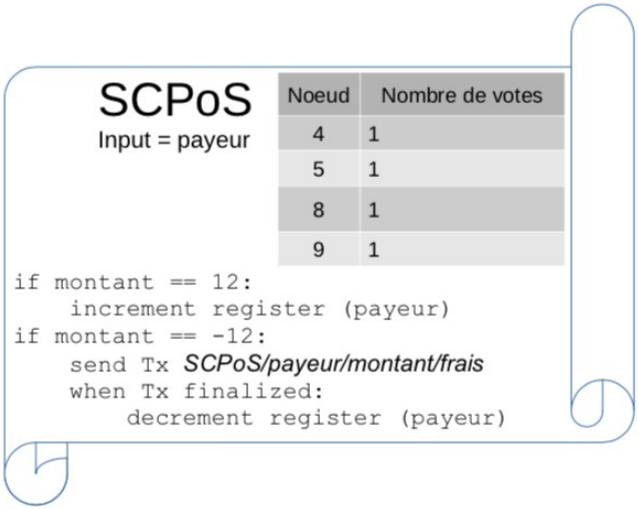
Les PoS sont insérées dans la chaîne de blocs grâce à des contrats intelligents spécialisés.

5.2 BlocNote

Dans BlocNote, une garantie de 12 R$ donne droit à une ballotte supplémentaire pour la lotterie des validateurs. Un validateur qui insère un bloc invalide se voit infliger une amende de 5 R$.

Les garanties des validateurs sont gérées par le contrat intelligent « SCPoS », qui contient les champs suivants :

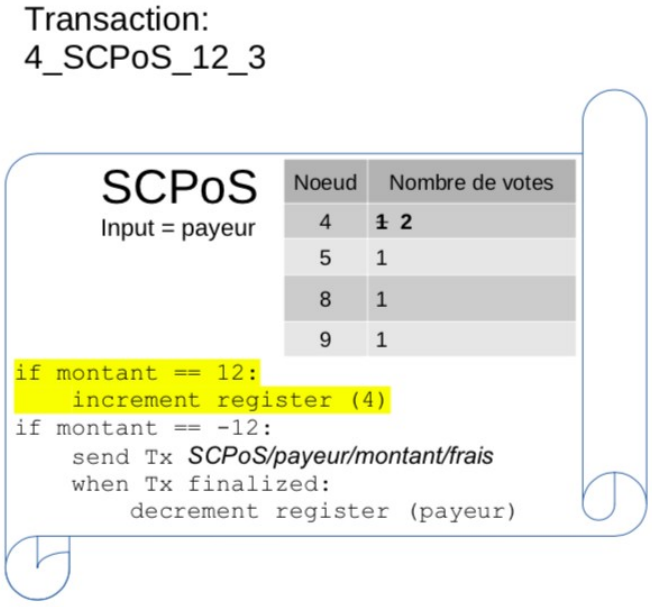
- l'adresse du payeur / validateur
- le registre du nombre de votes de chaque validateur
- le code qui effectue automatiquement les tâches suivantes :
  1. incrémenter le registre du nombre de ballotes de chaque validateur,
  2. décrémenter le nombre de ballottes si le validateur souhaite récupérer sa garantie.



Par exemple, si le validateur 4 souhaite augmenter son nombre de ballotes, il soumet la transaction « 4_SCPoS_12_3 » :

- le payeur est le validateur 4
- le destinataire est le SCPoS
- le montant est de 12 R$
- le validateur décide des frais de transaction, ici de 3 R$.

Cette transaction déclenche automatiquement le code du SCPoS, qui augmente le nombre de ballotes pour le validateur 4 dans le registre.



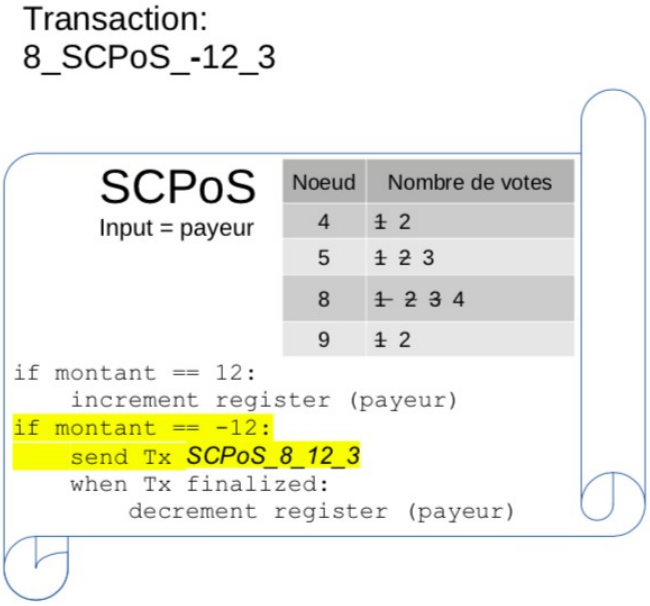
Le remboursement d'une garantie se fait en deux temps :

1. le validateur soumet d'abord une transaction avec comme destinataire le SCPoS,
2. puis le SCPoS soumet automatiquement une deuxième transaction avec comme destinataire le validateur afin de lui rembourser la garantie.

Le validateur doit donc prévoir des frais de transaction (à son choix) pour soumettre la transaction.

Par exemple, si le validateur 8 souhaite récupérer la garantie associée à un de ses droits de vote, il soumet la transaction « 8_SCPoS_-12_3 » :

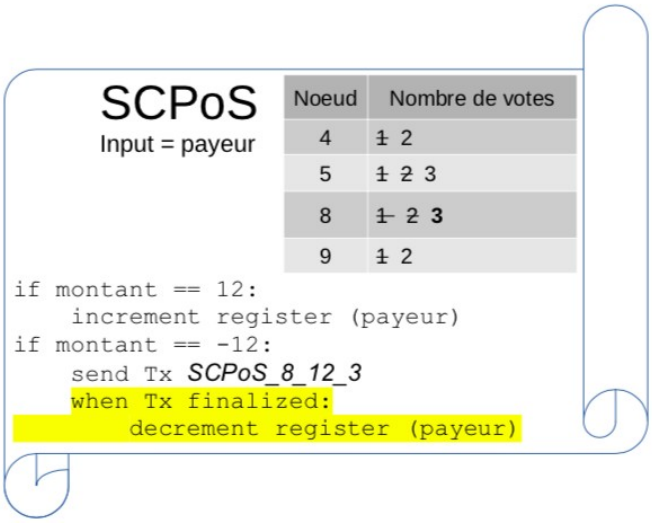
- le payeur est le validateur 8
- le destinataire est le SCPoS
- le montant est de -12 R$
- le validateur décide des frais de transaction (3 R$ pour cet exemple).



Cette transaction déclenche automatiquement le code du SCPoS, qui soumet la transaction « SCPoS_8_12_0 » :

- Le payeur est le SCPoS
- le destinataire est le validateur 8
- le montant est de 12 R$
- pour simplifier, aucun frais de transaction ne sont nécessaires.

Lorsque la transaction « SCPoS_8_-12_0 » est finalisée, le validateur 8 a récupéré les 12 R$ de sa garantie, et le registre est mis à jour : le nombre de ballotes du validateur 8 passe de 3 à 2.



5.3 Activité

But : posséder le plus de R$ possible à la fin de l'activité.

Matériel :

- tableau d'affichage de la chaîne de blocs
- une « urne de tous les validateurs » contenant un jeton par droit de vote, chacun identifié au validateur.
- Variantes 2 et 3 un tableau d'affichage mempool pour les transactions
- variante 3 : un tableau d'affichage « machine virtuelle » où est affiché le SCPoS

5.3.1 Variante 1

Dans cette variante, il n'y a pas de transactions ni de contrats intelligents.

1. Au début de l'activité, chaque nœud/validateur possède une ballote ;
2. le validateur du prochain bloc est tiré au hasard dans l'urne ;
3. le validateur choisit un bloc-parent, et lui enchaîne un nouveau bloc, mais cette fois sans calculer de PoW ;
4. lorsque le solde d'un nœud est suffisant, il peut acheter des ballottes supplémentaires ;
5. À la fin de l'activité, le solde de chaque nœud est compté : 10 R$ par blocs finalisé, desquels on soustrait 12 R$ par ballote acheté. Le validateur ayant le plus de R$ l'emporte !

5.3.2 Variante 2

Dans cette activité, les règles sont les mêmes que dans la variante 1 pour enchaîner les blocs, mais les garanties sont gérées par des transactions, comme dans l'activité 3. Le nœud qui souhaite acheter une ballotte supplémentaire doit donc soumettre une transaction dans le mempool.

Déroulement :

1. Au début de l'activité, chaque nœud/validateur possède une ballote.
2. Les nœuds et les validateurs gèrent les transactions comme dans l'activité 3, mais cette fois, les validateurs ne calculent pas de PoW : le validateur du prochain bloc est tiré au hasard dans l'urne.
3. Le validateur choisit un bloc-parent puis enchaîne un bloc contenant au moins la transaction de récompense, et 0, 1 ou 2 transaction(s) choisies dans la mempool.
4. Les autres validateurs sont tenus de vérifier la validité des transactions insérées dans le bloc. Si un validateur a inséré une transaction non-valide, il doit payer une amende de 5 R$ et son bloc en entier est éliminé de la chaîne, même si certaines transactions sont valides.

5. En plus des transactions d'échange de R$ (comme dans l'activité 3), les nœuds/validateurs peuvent soumettre des transactions pour gagner des ballotes supplémentaires. Le nœud obtient sa ballote supplémentaire lorsque la transaction est finalisée.

   Par exemple, si le validateur 4 souhaite augmenter son nombre de ballotes, il soumet la transaction « 4_0_12_3 » :

   - le payeur est le validateur 4
   - le destinataire est la chaîne de blocs elle-même (numéro 0)
   - le montant est de 12 R$
   - le validateur décide des frais de transaction, ici de 3 R$.

   Attention : les R$ mis en gage ne sont plus disponibles pour les transactions.

6. À la fin de l'activité, le nombre de blocs validés par chaque validateur est compté. Cette fois, le solde des nœuds donne directement le nœud gagnant !

5.3.3 Variante 3

Dans cette variante, les garanties des validateurs sont gérées par le SCPoS. Le déroulement est le même que celui de la variante 2, à deux différences près :

- à l'étape 5, les validateurs doivent maintenant soumettre une transactions avec le SCPoS comme destinataire, comme expliqué plus haut ;
- les validateurs peuvent récupérer leur PoS en soumettant une transaction au SCPoS.

Dans la vraie vie...

Les jetons mis en garantie font chacun l'objet d'un contrat intelligent.

La récompense pour la validation d'un bloc est calculée selon la participation du validateur à la chaîne de blocs ; elle n'est pas fixe, comme c'était le cas avec la PoW.