Gouvernance des technologies Blockchain

Approche de EOS

Par: Pascal Ngu Cho, Consultant Blockchain Senior.

A- Introduction

Une technologie blockchain peut être définie comme plusieurs composantes fonctionnant ensemble pour enregistrer et reconnaître la propriété d'un bien numérique. Parmi ces composantes, on a l'algorithme de consensus, le registre des transactions, l'incitatif à la participation et le réseau.

L'objectif de tout consensus blockchain est de trouver des réponses à des questions telles que : Quand faut-il produire le bloc? Qui doit produire le bloc? Comment définir un bloc valide? Comment gérer l'évolution du protocole? Comment gérer les divergences de production etc?

C'est à ces questions que cherche à répondre chaque jour les blockchains publiques telles Bitcoin, Ethereum, EOS et autres. Certaines réponses sont apportées par consensus sur la chaîne et d'autres par consensus hors-chaîne. Les questions liées à la cédule de production et à la validité des blocs vont se faire par algorithme de consensus (PoW, PoS, DPoS, BFT), tandis que celles liées à l'évolution et à gestion des conflits vont se faire par un mode de gouvernance dit « On-Chain » ou « Off-Chain ».

Nous vous présenterons les principaux algorithmes de consensus, ainsi que les modes de gouvernance utilisés par les principales technologies blockchain, en particulier le consensus et le mode de gouvernance de la blockchain EOS.

B- Algorithme de consensus

L'algorithme de consensus est au cœur de tout système blockchain. En tant que système distribué, la blockchain dépend d'un algorithme de consensus pour réaliser la coopération entre différents ordinateurs du réseau. Les plus connus sont :

- **PoW** : Proof of Work ou Preuve de travail, utilisé par Bitcoin et Ethereum 1.0
- **PoS** : Proof of Stake ou Preuve de particpation, utilisé par Tezos et Ethereum 2.0
- **DPoS** : Delegated Proof of Stake ou Preuve de participation déléguée, utilisé par EOS et Tron
- **BFT** : Byzantine Fault Tolerance ou Tolérance aux pannes, utilisé par BSC et Terra.

1- PoW ou Consensus de la preuve de travail.

Aussi appelé consensus de Nakamoto, le consensus de la preuve de travail ou PoW (Proof of Work) est la méthode innovante de validation des transactions

et sécurisation des transactions introduite par le Bitcoin. Il est aujourd'hui utilisé par d'autres protocoles comme **Ethereum 1.0** ou **Litecoin**.

Dans la preuve de travail, les ordinateurs (mineurs) du réseau compétitionnent pour résoudre des calculs mathématiques complexes afin de trouver la solution à une égnime pendant un moment donné. Lorsqu'un mineur trouve la solution, il le diffuse sur le réseau. Les autres mineurs vérifient et ajoute le bloc à la chaîne, et l'exercice recommence. Plus il y a de mineurs, plus la difficulté à trouver la solution augmente. Le consensus de la preuve de travail est le consensus le plus éprouvé. Il est ouvert et tout le monde peut joindre le réseau sans permission.

Le défi principal du consensus de la preuve de travail est son mode de gouvernance sur l'évolution du protocole et la gestion des conflits. Ces activités sont généralement menées hors chaîne.

2- PoS ou Consensus de la preuve de participation.

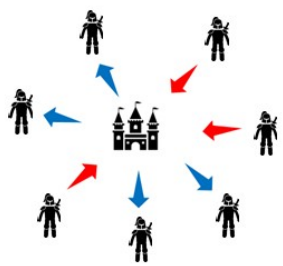
Dans le consensus de la preuve de participation ou PoS (Proof of Stake), le producteur de bloc est choisi aléatoirement basé sur sa participation (nombre de jeton en dépôt) et son âge participation. Lorsqu'un bloc est produit, les autres participants valident avant que celui si soit ajouté à la chaîne.

L'incitatif économique est la motivation pour qu'un nœud malveillant ne valide pas de blocs ou ne crée pas de transactions frauduleuses. En cas de détection d'un nœud frauduleux, ce dernier perd une part de ses dépôts ainsi que sa capacité à produire des blocs. Les participants ou les nœuds peuvent voter pour accepter ou refuser les changements proposés. Cependant, tous les nœuds n'ont pas le même pouvoir de vote.

Le consensus de la preuve de participation est moins éprouvée que la preuve de travail (PoW) et la preuve de travail déléguée (DPoS) car il est encore à ses balbutiements. Il a été utilisé pour la première fois par le projet Peercoin en 2013. Aujourd'hui, il est en expérimentation dans plusieurs réseaux tels que **Tezos** ou **Ethereum 2.0**.

Les principaux avantages du consensus de la preuve de participation sont l'efficacité énergétique et la sécurité. Il est aussi plus abordable, donnant la possibilité à plusieurs utilisateurs de participer à sa sécurité.

3- BFT ou Consensus de la tolérance aux pannes



La tolérance aux pannes byzantines ou **BFT** (Byzantine Fault Tolerance) est un système capable de tolérer des pannes dans un réseau. Quand des ordinateurs sont organisés en réseau, plusieurs raisons peuvent amener à son dysfonctionnement: bris matériel, attaque externe ou communication d'informations erronées de manière

intentionnelle ou non. Quel est le degré de tolérance acceptable lorsque certains nœuds du réseau sont dysfonctionnels? C'est à cette question que répond le consensus BFT. Un bloc ajouté ne peut être remis en cause et il n'est pas possible de créer une scission (hard-fork) sur la blockchain comme avec la preuve de travail (cas de Bitcoin & Bitcoin Cash ou de Ethereum & Ethereum Classic).

4- DPoS-BFT : Cas de EOS

Le réseau EOS utilise le consensus DPoS qui lui permet de créer des blocs à tous les 0.5 seconde. En y ajoutant une tolérance aux pannes byzantine asynchrone, on obtient le **DPoS-BFT** qui permet d'offrir l'irréversibilité des transactions après seulement une seconde.

Une tolérance Byzantine survient lorsqu'un ou plusieurs producteurs de blocs ont des comportements anormaux, tels que la signature de transactions invalides. Si moins de 1/3 des producteurs se comportent de manière anormale ou malveillante, les mécanismes BFT protégeront alors le système.

Le consensus EOS est divisée en 2 parties: la **sélection des producteurs** de blocs et la **réalisation du consensus** de production (temps de production, cédule de production, résolution de conflit, fork etc…).

Toutes les chaînes qui roulent sur le système d'exploitation EOS.IO comme EOS, Proton, Telos, Wax et autres utilisent l'algorithme de consensus DPOS-BFT. Cet algorithme est une intégration de Byzantine Fault Tolerance au DPoS traditionnel.

Il est plus rapide que la plupart des algorithmes de consensus parce que les producteurs de blocs ne compétitionnent que pour faire partir du groupe principal de **21 producteurs** de blocs, élus par les détenteurs de jetons. Ceux ayant obtenu le plus grand nombre de votes travaillent collectivement pour valider et sécuriser le réseau des transactions. Combiné au BFT, le consensus DPoS atteint des performances optimales sans sacrifier la sécurité.

B- Évolution des protocoles Blockchain

Les technologies blockchain permettent de développer une approche économique inclusive et démocratique car les participants peuvent partager les bénéfices. Leurs évolutions nécessitent des mécanismes permettant de s'assurer qu'elles continuent de répondre aux besoins de ses utilisateurs. C'est en ce moment qu'interviennent les modes de gouvernance. Les consensus algorithmiques tels que PoW, PoS, et DPoS vont gérer les opérations de validation et de sécurisation des transactions tandis que la gestion des mises à jour, des mises à niveau et des cas conflictuels va se faire par un mode de gouvernance dit «sur-chaîne» ou «hors-chaîne».

1- Gouvernance hors-chaîne ou «off-chain»

La gouvernance hors-chaîne désigne un processus dans lequel les parties prenantes du réseau se coordonnent de manière informelle (forum, courriel, chat etc…) pour décider comment gérer les mises à niveau. C'est le principal mode de gouvernance utilisé par Bitcoin et Ethereum.

1-1 - Avantages & inconvénient de la gouvernance «off-chain»

- Avantage: Les modifications sont plus difficiles à apporter au protocole. Ce qui assure une certaine stabilité pour les utilisateurs.

- Inconvénient : La principale préoccupation des modes de gouvernance hors-chaîne est la centralisation au niveau des développeurs et des mineurs, le manque de transparence dans les processus de mise à jour.

2- Gouvernance sur-chaîne ou «on-chain»

La gouvernance sur-chaîne ou «on-chain» désigne un processus dans lequel les mises à niveau du protocole se produisent automatiquement en réponse au vote des détenteurs de jetons. Les règles de modifications sont encodées dans le protocole de la chaîne et chaque proposition de mise à jour doit être acceptée ou refusée par vote par les participants.

Pour mieux comprendre le mode de gouvernance «on-chain», prenons l'exemple des débats qui ont lieu entre 2017-2019 sur la taille des blocs du réseau Bitcoin. Une partie des développeurs voulait augmenter la taille des blocs afin d'avoir un plus haut débit des transactions. L'autre partie défendait le maintient des blocs de petites tailles, en proposant l'utilisation des couches secondaires tel que le réseau Lightning comme solution pour augmenter le débit des transactions. Si les mises à jour du Bitcoin se faisaient à travers une gouvernance «on-chain», les détenteurs de jetons auraient voté sur les 2 options et c'est celle avec le plus de vote qui aurait été déployée.

2-1- Avantages & inconvénient de la gouvernance « on-chain »

- Avantages : La gouvernance «on-chain», améliore la transparence et la confiance dans la mise à niveau du protocole. Elle offre des délais d'exécution plus rapides pour les changements. Elle réduit de manière significative les possibilités de scission (hard-fork).

- Inconvénients : Le taux de participation aux votes peut être faible compte tenu du niveau de connaissance minimalement requis pour une décision éclairée. Les nœuds et utilisateurs avec des parts plus importants peuvent avoir un impact négatif sur le court des activités.

D- Gouvernance du protocole EOS

1- Présentation

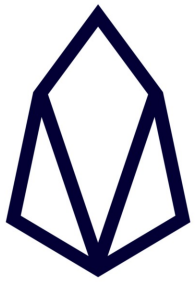
Lancé en juin 2018, EOS fait partie des technologies blockchain dite de 3ème génération. Elles se distinguent par leurs performances (capacité à effectuer un haut débit d'opérations en très peu de temps).

Comme première implémentation du système d'exploitation EOS.IO, la chaîne EOS a démontré en production sa capacité à traiter +4000 transactions/seconde, contre 10-15 transactions/seconde pour la chaîne Ethereum et 7 transactions/sec pour la chaîne Bitcoin.

Comme plateforme de développement de contrats intelligents, EOS est capable de supporter sur sa couche de base autant les opérations d'une place boursière que celles d'un réseau social ou d'un jeu.

Principales caractéristiques :

- Transactions à haut débit
- Faible temps de latence
- Zéro frais de transactions
- Système hiérarchique de gestion des permissions
- Langage de programmation: C++/WASM
- Supporte la virtualisation (EOS VM)
- Protocole modulaire et flexible
- Gouvernance intégrée et programmable
- Faible consommation d'énergie.



2- Mode de gouvernance

Plusieurs participants prennent part à la gouvernance du protocole EOS:

- Les producteurs de blocs (BP), qui exploitent les nœuds, valident et sécurisent les transactions.
- Les développeurs, responsable du développement des algorithmes de base de la blockchain.
- Les utilisateurs ou participants, qui utilisent et investissent dans les jetons de l'écosystème.

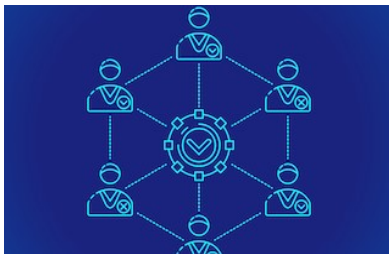
Les parties prenantes au processus de gouvernance EOS reçoivent des incitatifs économiques à participer. Par exemple, les validateurs de blocs, reçoivent des récompenses pour la production et la sécurité du réseau. Les développeurs peuvent soumettre des propositions d'améliorations et recevoir du financement, les utilisateurs peuvent recevoir une part des récompenses associées à l'utilisateur des ressources du réseau ou à la participation aux échanges. Les modifications au protocole doivent être approuvées par au moins 15/21 producteurs de blocs pour que cela prenne effet.

Le protocole intègre en son sein les conditions d'utilisateur EOS appelé EUA (EOS User Agreement), une sorte de constitution qui régit les relations entre les utilisateurs du protocole. Les membres de la communauté EOS bénéficient aussi de la première implémentation du système de gouvernance à démocratie fractal – **EdenOS** - proposé par Daniel Larimer, architecte du logiciel libre EOS.IO; pour la gouvernance des communautés blockchain.

3- Cas d'utilisation du modèle de gouvernance EOS

Le protocole offre plusieurs cas de gouvernance qui nécessite la participation des utilisateurs du réseau: La mise à niveau du protocole, le referendum sur les conditions générale d'utilisations (EUA), la sélection des productions de blocs, la sélection des leaders de la communauté (Eden), la sélection des projets à financer (Projet Pomelio), etc.

E- Conclusion



L'implémentation des modes de gouvernance varie d'une blockchain à l'autre. Bitcoin et Ethereum permettent à quiconque de soumettre des modifications au protocole. Toutes les demandes de modification dépendent du soutien qu'elles reçoivent de la communauté, des mineurs, des opérateurs de nœuds et des développeurs principaux.

Dans le cas de EOS, les mises à niveaux sont testés et déployés par les producteurs de blocs, qui sont constamment votés par les détenteurs de jetons. On parle de démocratie liquide. Le protocole doit rapidement s'adapter aux besoins de ses utilisateurs. La gouvernance «on-chain» est apparue comme alternative aux modèles de gouvernance informelle. Les questions liées à la cédule de production et à la validité des blocs sont répondues par algorithme de consensus (PoW, PoS, DPoS), tandis que celles liées à l'évolution et à gestion des conflits sont effectuées par mode de gouvernance (on-chain et/ou off-chain).

Références :

EOS consensus : https://steemit.com/eos/@attic-lab/eos-io-consensus-algorithm
BFT-DPoS : https://medium.com/eosio/dpos-bft-pipelined-byzantine-fault-tolerance-8a0634a270ba
EdenOS : https://www.edeneos.org/