

Bitcoin Basis 14 - Proof of Stake (FR)

Preuve d'enjeu ou "Proof of Stake" est souvent mentionné en relation avec Bitcoin. Des systèmes tels que Ethereum ou Cardano en sont des exemples.

La preuve d'enjeu récompense les détenteurs de plus grandes parts et remplace le minage par des validateurs.

Les validateurs sont des dispositifs qui aident à former le réseau et approuvent les blocs.

Le mécanisme de consensus de la preuve d'enjeu aura déjà décidé quel validateur propose un nouveau bloc sur leur blockchain avant même qu'il ne soit ajouté.

Il utilise donc la possession et l'engagement comme base pour l'attribution des blocs et la vérification des transactions, sans travail fourni comme dans le cas de Bitcoin.

La preuve d'enjeu présente de nombreuses variantes, telles que la répartition proportionnelle des subventions, la délégation des votes ou une redistribution aléatoire des revenus de type loterie.

Elle nécessite moins de puissance informatique que la preuve de travail, mais en contrepartie, elle ne bénéficie pas d'une répartition décentralisée équitable, sûre et résistante. Elle manque également d'autorégulation et d'un grand livre complètement fiable. En d'autres termes, elle est plus passive.

La preuve d'enjeu peut être utile comme système interne d'entreprise, par exemple pour le suivi du transport international de marchandises.

Cependant, elle n'est pas adaptée en tant qu'unité monétaire alternative, car il n'y a pas de rareté réellement établie et les règles sont souvent arbitrairement modifiées.

Un tel réseau n'est souvent pas suffisamment décentralisé pour fonctionner de manière indépendante des créateurs ou des grands détenteurs intéressés.

Avec Bitcoin, les mineurs rivalisent pour sécuriser le réseau. Avec la preuve d'enjeu, des milliers de projets se font concurrence pour obtenir votre attention et votre argent à court terme.