Laurent TEDESCO
CEO d'Humbrain

Blockchain : La guerre des preuves aura bien lieu

Inséparable du procédé de blockchain, la technique de validation des blocs, désignée « mode de consensus », fait l'objet de nombreux débats. Deux grandes techniques sont en vigueur actuellement, celle dite de la « preuve de travail » (PoW, Proof of Work) et sa principale alternative, la « preuve d'enjeu » (PoS, Proof of Stack). Si la première représente la très grande majorité des blockchains car elle est née avec, la seconde est regardée avec de plus en plus d'intérêt. Le réseau Ethereum, second en volumétrie après le Bitcoin, va même abandonner la première au profit de la seconde. Voyons les enjeux.

L'OBJECTIF : ASSEMBLER AVEC SÉCURITÉ ET PÉRENNITÉ LES BLOCS CONSTITUTIFS

Le concept de Blockchain consiste à composer un assemblage de blocs de données, inaltérable d'une part et éternellement accessible d'autre part. Ces deux besoins induisent deux actions : la mise en œuvre d'un algorithme pour assembler les blocs, suffisamment solide pour qu'elle ne puisse être altérée, d'une part, et son stockage décentralisé, offrant la redondance suffisante pour rester accessible en toutes circonstances, d'autre part.

La réponse à la seconde nécessité est partagée par toutes les blockchains. Il s'agit d'une architecture Peer To Peer ou Pair à Pair, où chaque nœud du réseau est à la fois fournisseur et consommateur d'un service, généralement dispersé géographiquement.

La première nécessité est quant à elle, finalement plus délicate à résoudre. Il faut faire en sorte que la chaine de blocs soit assemblée de manière infalsifiable et ce, dans un contexte multisupport partagé (la même chaine doit exister sur tous les nœuds). L'objectif est de donc désigner un unique nœud qui validera l'ajout d'un nouveau bloc et présentera la nouvelle version de chaine à l'ensemble des autres nœuds. Si cet objectif est partagé par toutes les blockchains, les modalités d'y répondre diffèrent.

LA POW, LE MARTEAU POUR ÉCRASER UNE MOUCHE

C'est la technique mise en œuvre par la première blockchain opérationnelle, à la savoir le Bitcoin. Elle consiste à mettre en concurrence les nœuds du réseau dans une compétition de calcul d'une clé. Cette mise en concurrence est la garantie qu'aucun acteur du réseau ne pourra préempter la composition de la chaine et éventuellement la détourner à son profit car sa puissance individuelle ne peut dépasser celle de l'ensemble. La charge de calcul déployée par un nœud constitue sa *« preuve de travail »* et représente une forme d'engagement sur son sérieux. In fine, seul le nœud qui a trouvé le premier la bonne clé se voit récompensé en Jeton (Bitcoin pour Bitcoin, Ether pour Ethereum). Cette approche reconnue solide, présente cependant plusieurs défauts largement admis :

- Représentative de la chaine composée, la clé à retrouver se complexifie au fil du temps et nécessite des ressources de calcul (processeurs) et une consommation d'énergie en constante augmentation ;
- Les nœuds qui participent à la compétition (appelés *« mineurs »*) sont eux de plus en plus nombreux, démultipliant les consommations d'énergies gâchées ;
- La mise en concurrence reste chronophage : même s'il existe des alternatives plus rapides, le Bitcoin par exemple, s'appuie sur des cycles de 10 minutes pour l'ajout des nouveaux blocs. On est donc loin de pouvoir supporter des transactions en temps réel…

LE POS, LA MISE SOUS SÉQUESTRE VAUT GARANTIE

Dans cette approche de *« preuve d'enjeu », les nœuds participants à la composition de la chaine – appelé « validateurs »* - doivent exposer une certaine somme en token (32 ETH pour Ethereum) comme garantie. L'idée sous-jacente est que si le nœud validateur opère mal, intentionnellement ou pas, en ne validant pas correctement un bloc, la somme qu'il a mise en jeu risque d'être perdue. En pratique, c'est un tirage au sort, plus ou moins affiné, qui détermine quel nœud parmi les candidats déclarés sera validateur d'un nouveau bloc. Plusieurs avantages apparaissent alors par rapport à la preuve de travail :

- Réduction des calculs nécessaires : les nœuds ne sont plus mis en concurrence au travers de calculs inutiles et énergivores, car seuls les validateurs désignés devront opérer ;
- Gain de temps dans les mises à jour : la disparition de calculs complexes d'une part, et l'absence de compétition d'autre part, réduit les délais de traitement et de mise à jour de la chaine ;

La robustesse du procédé ensuite : le PoS offre encore peu de retours d'expérience massive, voire certains déjà négatifs, avec des hacks possibles déjà détectés.
La fondation Ethereum offre même 50000 $ à quiconque décèlerait un bug.

L'acceptation de la communauté Ethereum enfin. Car ce n'est pas gagné : l'évolution bouscule en effet nombre de positions établies ; Le minage a fait émerger au fil des années tout un écosystème (des datacenters entièrement dédiés, des communautés de mineurs, etc…), totalement dévoué à cette industrie du calcul. Les investissements qu'ils ont appelés, attirés par des rémunérations dont les valeurs en monnaie réelle promettaient de beaux rendements, n'ont cessé d'augmenter au fil des années. Abandonner cette approche amènerait donc à rendre obsolète une grande partie de ces investissements. On comprend le grincement de dents…

Une partie de la communauté résiste alors. On s'attend par exemple à création d'une chaine Ethereum alternative (appelées *« Fork »*) qui conserverait le PoW comme technique de validation en marge de la chaine primaire.

Mais en créant plus de confusion que de cohésion, ces développements pourraient avoir un effet délétère sur le réseau et plus généralement l'écosystème des blockchains et des cryptomonnaies. Là où la consolidation permettrait de rassurer nombre d'acteurs encore hésitant à entrer dans le jeu, la situation pourrait faire fuir ceux qui y avaient déjà mis les pieds…

Malgré ces qualités, le procédé n'est pas encore complètement déployé et quelques incertitudes subsistent à ce jour sur sa fiabilité, c'est l'objet du débat PoW vs PoS.

THE MERGE, LE BING BANG D'ETHEREUM

Mutation programmée dès sa naissance, maintes fois reportée, la blockchain Ethereum va passer de la PoW à la PoS, cet automne. L'évènement est très attendu et surveillé, car les enjeux sont colossaux, et plusieurs aspects seront scrutés.
La fluidité de la migration d'abord : même si le PoS est déjà en fonction sur un réseau parallèle d'Ethereum, avec lequel la chaine principale va fusionner (d'où le nom de *« fusion »*), il n'est pas garanti que tout ça se déroule correctement.