GOFFETTE Matthias

État de l'art

Keywords ::

cryptocurrency, bitcoin, ethereum, proof of work, blockchain

Mots-clefs :

cryptomonnaie, bitcoin, ethereum, preuve de travail, blockchain

Résumé :

Jusqu'à maintenant, l'argent d'une personne était le plus souvent confié à une banque en laquelle l'individu à confiance. Pour palier aux inconvénients que cela peut représenter, une nouvelle forme de monnaie, les cryptomonnaies, ont été crées.

En 1998, Wei Dai propose un protocole de gestion anonyme et électronique de monnaie : la "b-money", décentralisée, de façon à ce que personne n'ait plus de pouvoir sur la monnaie que d'autres. A sa suite, Nick Szabo propose BitGold, qui influencera ensuite Bitcoin. BitGold est le premier système à nécessiter une preuve de travail cryptographique. Bitcoin est lancé en 2009 par Satoshi Nakamoto, et est à présent la cryptomonnaie majeure. Deux mécanismes importants sont implantés : la blockchain et la preuve de travail.

La blockchain est un fichier contenant la liste de toutes les transactions. Ainsi, en remontant la blockchain, il est possible de tracer les transactions d'un utilisateur, de connaître son solde, tout en ignorant son identité. Ceci permet à chacun de vérifier que l'argent qu'utilise un utilisateur existe bel et bien.

Pour que le système fonctionne de manière entièrement décentralisée, il est nécessaire que chaque ordinateur du réseau aide au contrôle du cahier des comptes de Bitcoin, pour vérifier que personne ne fraude : c'est le système de preuve de travail. Les ordinateurs du réseau résolvent un problème informatique, dans le but de valider un bloc de transactions. La première machine à résoudre le problème remporte 25 bitcoins, pour inciter à participer à ce contrôle. La difficulté de la résolution du problème est régulièrement réévaluée pour maintenir une durée de 10 minutes entre chaque obtention de résultat.

Ces principes permettent de sécuriser au maximum les transactions et les comptes des utilisateurs, mais cependant, Bitcoin n'est pas sans inconvénients. En effet, la blockchain prend de la place (71 Go en Juin 2016) et doit être installée sur chaque ordinateur du réseau. De plus, le mécanisme de preuve de travail nécessite de réaliser des calculs en continu, ce qui est énergivore, mobilise une partie de la puissance de calcul de l'ordinateur, et ralenti le flux de transactions. Aujourd'hui, la majorité des calculs sont fait par des machines spécialisées, souvent regroupées en pools. La principale faille de Bitcoin serait qu'une personne prenne le contrôle de 51% de la puissance de calcul du réseau et, bénéficiant ainsi d'une puissance de calcul supérieure aux 49% restant, puisse valider de fausses transactions. Ceci semble peu probable, cependant, les utilisateurs pouvant s'associer en pool, partageant leurs calculs, un de ces regroupement à réussi à contrôler le réseau plusieurs heures durant. Le but ne semble pas d'avoir été d'émettre des transactions frauduleuses, mais ceci montre que le risque est néanmoins présent.

Pour tenter de trouver des réponses à ces problèmes, de nombreuses cryptomonnaies ont été créées dans le but de devenir des alternatives à Bitcoin, en en améliorant certaines composantes. Le terme général pour les désigner est « altcoins », il y en a plus de 400 actuellement. La plupart reprennent le code de Bictoin et n'en améliorent qu'un aspect mineur, comme l'algorithme de hashage, la rapidité des transactions, ou encore la quantité d'unités de monnaie en circulation. Elles ne survivent en général pas longtemps, à l'exception de quelques unes, comme Litecoin, qui propose des transactions plus rapides, ou Darkcoin, qui permet des transactions totalement anonymes. La prolifération de monnaies alternatives permet de décentraliser encore plus la cryptomonnaie, ce qui est un des buts de Bitcoin, et d'expérimenter des méthodes de fonctionnement différentes, que Bitcoin pourrait peut-être utiliser plus tard.

Ethereum est l'une des dernières cryptomonnaies en date, souvent présentée comme étant le "Bitcoin 2.0". Ethereum a été créée en partant de rien, en reprenant cependant des concepts importants de Bitcoin tels que la preuve de travail ou la blockchain, mais va au-delà des limites de Bitcoin en ne se cantonnant pas à des échanges monétaires. En effet, Ethereum permet l'exécution de programmes créés pas la communauté, qu'on utilise en dépensant de l'Ether, la monnaie d'Ethereum. Ces « contrats » s'exécutent automatiquement après payement, sans action humaine, coupant donc toute possibilité de triche.

De plus, Ethereum désire migrer d'une preuve de travail à une preuve de confiance (proof of stake). Celle-ci ne se base plus sur des calcul pour atteindre un consensus de la blockchain, mais sur une méthode de sélection du prochain bloc valide : sélection d'un bloc aléatoire, selon certains paramètres, qui peuvent être l'âge du bloc, la quantité de flux entrants et sortants, ou le résultat de votes. C'est une alternative qui pourrait se développer dans le futur pour faire des cryptomonnaies pesant moins sur la consommation énergétique.