Les secrets de la blockchain

Henri Kelle
Secrétaire de rédaction de la Revue NDP
« Les Nouvelles Dynamiques du Paiement »

Si aujourd'hui, tout le monde doit connaître de nom le Bitcoin, encore peu nombreux sont ceux qui comprennent son fonctionnement. Avant d'entrer dans un premier niveau de détail des mécanismes cryptographiques mis en œuvre par la technologie blockchain, sur laquelle il repose, commençons par un peu de vocabulaire pour resituer les différents éléments et acteurs du système.

Qu'est-ce que la blockchain ?

Elle peut être considérée comme un journal public de toutes les transactions Bitcoin, rangées en ordre chronologique. On parle aussi de « ledger » : un grand registre de compte, décentralisé, dans lequel sont enregistrés tous les soldes comptables des utilisateurs (qui peuvent posséder une multitude de comptes). C'est le réseau lui-même et non pas une « autorité » en particulier qui va se charger de la mise à jour, contrairement aux systèmes bancaires centralisés, où des serveurs informatiques centraux sont contrôlés par une seule entité. Tout le monde peut ainsi vérifier les transactions, qui y ont eu lieu et consulter l'état de chaque compte. La base de données est accessible à tous, sans intermédiation. Le registre est contrôlé de façon collective par tous ceux qui sont capables de fournir de la puissance de calcul depuis un ordinateur, ce sont les mineurs.

Mining, minage et mineurs

Les mineurs sont les personnes qui fournissent le réseau Bitcoin en puissance de calcul. Ce faisant, ils lui permettent de réaliser la mise à jour de la base de données de la blockchain. Par analogie au système bancaire, ils jouent le rôle d'intermédiaire financier, sans pour autant connaître l'identité des personnes effectuant des transactions en bitcoins. Les traitements qu'ils effectuent servent à produire des confirmations de transactions afin de les afficher dans le registre des comptes. Lorsqu'un block de transactions est confirmé, les mineurs remportent un total de 25 nouveaux bitcoins. Actuellement, il y a environ 15 millions de bitcoins en circulations, et il n'en existera au total jamais plus de 21 millions. Bien entendu, tout le monde peut être mineur sans aucune autorisation ou autre exigence préalable qu'une connaissance solide du monde informatique. Plus il y a de mineurs disposés à accomplir cette tâche, plus le niveau de concurrence et la difficulté pour confirmer des transactions s'accroît.