**Présentation succincte des cryptomonnaies**

Une **cryptomonnaie** est un actif numérique conçu pour servir de moyen d’échange et qui utilise la cryptographie pour sécuriser les transactions et contrôler la création d’unités supplémentaires de cette monnaie. Les cryptomonnaies sont un sous-ensemble des monnaies digitales ; elles constituent également un sous-ensemble de monnaies alternatives et de monnaies virtuelles.

Le bitcoin est devenu la première cryptomonnaie décentralisée en 2009. Depuis, d’autres cryptomonnaies ont été créées. On les appelle souvent des *altcoins*, un mot-valise recouvrant les termes *alternative* et *bitcoin*. Le bitcoin et ses dérivés utilisent le contrôle décentralisé, contrairement aux systèmes bancaires centralisés/monnaies électroniques centralisées. Le contrôle décentralisé est lié à l’utilisation de la base de données des transactions en blockchain qui sert de journal distribué.

La cryptomonnaie décentralisée est produite collectivement par l’ensemble du système de cryptomonnaie, à un rythme défini lors de la création du système et qui est connu du grand public. Dans des systèmes bancaires et économiques centralisés tels que le système de la FED américaine, des conseils de direction ou des gouvernements contrôlent l’offre de monnaie en imprimant des unités de monnaie fiduciaire ou en demandant des ajouts aux registres bancaires numériques. Dans le cas des cryptomonnaies décentralisées, les sociétés ou les pouvoirs publics ne peuvent pas produire de nouvelles unités, et n’ont jusqu’ici pas assure de suivi pour d’autres sociétés, banques ou entreprises qui détiennent des avoirs mesurés grâce à ces cryptomonnaies. La technique sur laquelle reposent les cryptomonnaies a été créée par le groupe ou l’individu connus sous l’appellation de Satoshi Nakamoto.

En mars 2015, il existait des centaines de spécifications pour les cryptomonnaies : la plupart sont similaires à la première cryptomonnaie décentralisée à avoir été pleinement déployée, le bitcoin, dont elles découlent. Dans les systèmes de cryptomonnaies, la sécurité, l’intégrité et le solde des journaux de transactions sont assurés par une communauté de parties qui ne se font pas confiance et que l’on appelle des mineurs ; ce sont des personnes comme vous et moi qui utilisent leur ordinateur pour aider à valider et horodater les transactions puis les ajouter au journal de transaction selon un mécanisme particulier d’horodatage.

La sécurité des journaux de cryptomonnaie repose sur l’hypothèse que la majorité des mineurs essaient honnêtement de tenir le journal correctement, puisqu’il y a une incitation financière à la clé.

La plupart des cryptomonnaies sont conçues pour diminuer progressivement la production de monnaie, le montant total de monnaie en circulation étant ainsi plafonné, sur le modèle des métaux précieux. Par rapport aux monnaies ordinaires détenues par des institutions financières ou sous forme d’espèces, les cryptomonnaies peuvent être plus difficiles à saisir par les services répressifs, du fait de l’évolution des technologies de cryptages.

Cette difficulté nouvelle pour les services répressifs est illustrée par l’affaire Silk Road : le volume de bitcoins d’Ulbricht était détenu séparément et crypté. Les cryptomonnaies telles que le bitcoin sont pseudonymes, même si des ajouts ont été proposés tels que le Zero coin, qui permettraient un véritable anonymat.

Source : https://en.wikipedia.org/wiki/Cryptocurrency