CREOGN
CENTRE DE RECHERCHE

Note flash du CREOGN

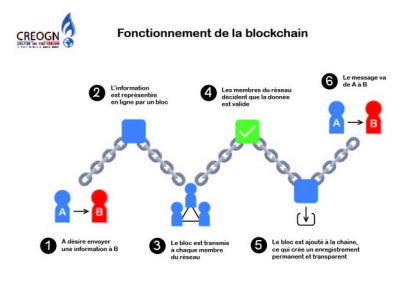
Une question d'actualité : une référence synthétique

N° 2 - Octobre 2022

Mathéo GILBERT

Blockchain et tokens

C'est au travers de la blockchain (*technologie des chaînes de blocs*) que circulent les tokens. Le token est un jeton non fongible (NFT pour *non-fungible token*) auquel est rattachée une identité numérique. C'est une donnée stockée et authentifiée sur une chaîne de blocs. Les cryptomonnaies, qui sont des tokens, ont pour but initial d'être des monnaies pair-à-pair permettant des paiements en ligne directement envoyés les uns aux autres sans passer par des institutions financières ou étatiques. Les régulateurs, les banques centrales et commerciales sont immédiatement concernés par cette innovation. Bitcoin est le réseau blockchain le plus décentralisé (14 000 nœuds) et le premier à avoir été créé. Sa cryptomonnaie, le BTC, domine le marché des cryptoactifs (entre 40 et 50 % de dominance moyenne selon les cours).



En page 3
Infographie de la blockchain

Points clés/à retenir :

• La blockchain est (*initialement conçue pour être*) un réseau informatique décentralisé permettant d'établir de la confiance grâce aux protocoles de consensus et de validation entre entités inconnues, sans intermédiaire(s) ;
• Il existe 4 types de blockchain : les publiques (*décentralisées, sans niveaux d'autorisations, accessibles et lisibles par tous*) ; les privées (*pour un groupe restreint de personnes, décentralisées ou non, avec niveaux d'autorisations possibles*) ; les hybrides (*privées avec méthodes d'autorisations, où l'on peut décider quelles sont les informations publiques ou non*) ; celles de consortium (*aussi appelées blockchains fédérées : une multitude d'organisations peuvent collaborer sur un réseau décentralisé, avec niveaux d'autorisations*) ;
• La traçabilité, la transparence et l'immuabilité des données sont les caractéristiques inhérentes à la blockchain. N'importe qui peut consulter les transactions réalisées grâce aux explorateurs de blocs (exemple : Etherscan pour le réseau Ethereum) ;
• Les mineurs sont ceux qui valident (*protocole de consensus)* les transactions en résolvant une problématique algorithmique. Celui qui réussit le premier est récompensé par la cryptomonnaie de la blockchain. C'est le processus de création monétaire de la blockchain. La méthode de minage dépend du protocole de consensus/ validation (*exemple : preuve de travail ou preuve d'enjeu*) ;
• La tokenisation est le processus informatique de sécurisation des données sur blockchain. Cela permet de digitaliser un élément sur blockchain pour qu'il devienne un token (*œuvre d'art, actif financier, document…*), enregistré et chiffré dans la blockchain, ce qui permet de garantir la sécurité, l'unicité et la propriété du token. Les NFT et les cryptomonnaies sont des tokens ;
• Un NFT est un fichier numérique stocké sur blockchain. C'est la création du jumeau numérique du fichier réel, par exemple une photo, une œuvre d'art, une vidéo, un brevet, un fichier audio. Pour en assurer la propriété, le détenteur peut stocker toute information qui lui est relative dans les métadonnées du NFT. Une

métadonnée est une donnée qui sert à définir ou décrire une autre donnée, quel qu'en soit le support. Une métadonnée peut être la date de production ou d'enregistrement de la donnée. Sur une photo numérique, les métadonnées peuvent être les coordonnées géographiques du lieu de la photo. Toutes les blockchains ne supportent pas les NFT.

Liste non exhaustive des avantages :

• L'existence de tokens de gouvernance : ils permettent de participer à la prise de décision sur les directions et perspectives du réseau ;
• La traçabilité : les blockchains sont des registres ouverts et publics qui documentent la provenance de chaque actif ;
• Les contrats intelligents : ils permettent l'automatisation des transactions et le déclenchement d'actions selon des conditions développées algorithmiquement ;
• L'architecture décentralisée : elle permet la collaboration dans un écosystème d'utilisateurs inconnus ;
• La réduction des frais par l'absence de tiers/intermédiaires ;
• La très faible consommation énergétique pour les protocoles de preuve d'enjeu ;
• La rapidité des échanges et transactions.

Liste non exhaustive des risques :

• Les doubles dépenses (*double spending)* : défaut technique permettant aux utilisateurs de dupliquer l'argent. Types d'attaques à double dépense : attaque Finney, attaque de course, attaque à 51 ;
• L'attaque à 51 : répandue dans les petites chaînes de blocs lorsque les attaquants génèrent plus de 51 % de la capacité de minage et acquièrent ainsi une majorité de la capacité de validation (pouvoir de décision sur les réseaux blockchain) ;
• Certains réseaux naissent déjà avec une gouvernance par un groupe restreint. La possibilité de se faire voler ses fonds est alors plus forte que sur un réseau où les fonds sont répartis en majorité au sein de la communauté des utilisateurs ;
• Une cyberattaque sur un portefeuille de cryptomonnaies : lorsqu'un utilisateur télécharge une application corrompue (*cheval de Troie*) pour recueillir des données de l'utilisateur victime. Sur un portefeuille virtuel, il peut s'agir de la clé de chiffrement ;
• La décentralisation signifie une multiplication des points de contact et, de fait, une multiplication des points de vulnérabilité ;
• Une utilisation de la blockchain pour des usages qui nécessitent de relier la réalité au réseau requiert un intermédiaire. Si l'intermédiaire est humain, la difficulté réside dans l'attestation de sa bonne volonté. Si l'intermédiaire est informatique (*exemple des oracles*), il peut être l'objet d'une cyberattaque ;
• *Dataprivacy* : la sécurité et la protection des données personnelles peuvent être remises en question, tout protocole informatique pouvant être l'objet d'une cyberattaque ;
• Le quantique : une fois créé, il remettra en question la sécurité de l'intégralité des technologies de l'information et sera en mesure de casser les mots de passe.

CREOGN
CENTRE DE RECHERCHE

Fonctionnement de la blockchain