A N D S I

Association Nationale des Dirigeants en Sciences de l'Information
www.andsi.fr

La Blockchain, succès, échecs et évolution.

Compte rendu rédigé par ANDSI & Pierre Delort

En bref…

Benjamin RAMEIX, DSI de Prévoir, reprendra sa conférence sur la blockchain, pour évoquer ses succès et ses échecs. Il fera un point sur les évolutions de ce qu'il ne présente plus uniquement comme une technologie.

Concepts

La blockchain est un registre distribué qui appartient à tous les utilisateurs au sein d'un réseau de *peer-to-peer*, de façon décentralisée, et avec des mises à jour régulières. Elle repose sur la confiance. Contrairement à une base de données, chacun possède une visibilité sur ce qu'elle contient. L'immutabilité représente son point fort. Ainsi, les implémentations ne peuvent pas être modifiées.

Cryptographie

Le hash se définit comme la création d'une empreinte numérique à partir d'un message initial. Sa signature permet de garantir l'authenticité de l'émetteur.

La blockchain constitue un assemblage d'unités logiques appelées blocs qui comportent les signatures des émetteurs et un horodatage, et qui font l'objet d'un hashage. Le bloc suivant récupère le hash du bloc précédent, et les modifications de hash sont répercutées en cascade.

Validation

Une fois le bloc validé, il est soumis à l'ensemble du réseau.

Consensus

Les règles sont différentes selon les blockchains. Pour le Bitcoin, elles reposent sur les preuves de travail. Les valideurs sont des personnes qui détiennent suffisamment de cryptomonnaie pour être en mesure de la redistribuer s'ils commettent une erreur. Le Bitcoin est assis sur un hash et des transactions. Le protocole défini est que le prochain utilisateur valide le bloc, la règle étant similaire pour chacun des nœuds du réseau. Les mineurs testent les hashs. Une fois qu'ils ont trouvé la bonne valeur, ils préviennent les autres nœuds du réseau qui effectuent une vérification. Le risque est que l'acteur le plus puissant, comme un ordinateur quantique, prenne le pouvoir.

Concepts

La chaîne étant publique, chacun peut rejoindre le réseau. Dans les faits, il existe aussi des blockchains privées. Par exemple, les grands assureurs français se sont réunis au sein d'un consortium pour créer un registre de traçabilité.

Promesses

L'enjeu est de recréer de la confiance grâce à un algorithme participatif. Le succès de la blockchain tient davantage aux attentes qu'elle suscite, car elle est à ce jour peu développée dans les entreprises. Ses principales mises en pratique concernent la *supply chain*.

Applications

Les opinions des médias au sujet des monnaies électroniques sont partagées. En dépit de leur caractère spéculatif, elles connaissent un essor. Ainsi, 10 à 12 % des Français en possèdent. L'objectif qui a présidé à leur création était d'empêcher un effondrement semblable à celui de la banque Lehman Brothers. Néanmoins, la société, FTX, spécialisée dans les cryptomonnaies, a aussi fait faillite.

Le livre blanc sur le Bitcoin signé par Satoshi Nakamoto constitue une référence. Une communauté s'est créée autour de spécifications plus développées, d'un réseau et de plateformes. Bien que cette monnaie ne soit pas reconnue en France, il est possible de la convertir en euros. Aux États-Unis, des paiements peuvent être effectués en Bitcoin. L'anonymat favorise son usage dans le cadre de trafics. Il est ainsi utilisé pour acheter des produits illégaux.

D'autres monnaies numériques existent, à l'exemple de Tether qui est indexée sur la monnaie réelle, ou d'Ethereum qui permet de déclencher automatiquement la réalisation d'un service à la suite d'un paiement.

Un règlement européen applicable depuis 2014 a posé des définitions afin d'éviter les abus sur le marché et de protéger les investisseurs, par l'intermédiaire de logiques d'agrément pour les plateformes. Le système qui se voulait indépendant se trouve ainsi réglementé.

La blockchain est utilisée pour la traçabilité alimentaire, par exemple par Carrefour et Walmart. Chaque intermédiaire y est intégré. Une logique de consortium est appliquée dans le secteur du transport. Dans le luxe, ce même système permet d'enregistrer l'ensemble des produits, en ajoutant des certificats d'authenticité, et en suivant le nom du propriétaire lors des transactions officielles. Dans l'énergie, Engie s'est appuyé sur une start-up pour assurer le suivi et la traçabilité de la consommation des énergies vertes dans une optique de défiscalisation. La filiale d'EDF Exaion offre des services numériques à destination des entreprises.

La blockchain est en mesure de contrôler efficacement le résultat d'une élection. Elle utilisée à cette fin en Estonie et aux États-Unis. Si elle permet la traçabilité des médicaments, peu de systèmes ont toutefois été développés dans ce domaine. Le remboursement automatique des retards d'avions par Axa représente un cas d'usage dans le secteur des assurances.

Les *non-fungible tokens* (NFT) sont des actifs numériques qui répondent à une logique de propriété, par exemple, la toute première publication sur Twitter.

Faiblesses

Le secteur d'activité est déterminant dans le choix de mettre en place une blockchain. Les cryptomonnaies en constituent l'application la plus lucrative. Aucun véritable standard n'a été à ce jour défini. Les cryptomonnaies renvoient une image négative et sont associées à la fraude. Leur décentralisation s'avère factice, car elles sont dans les faits contrôlées par une oligarchie.

Atouts

Certains cas d'usage ont démontré l'efficacité d'une blockchain pour renforcer la sécurité. La trace numérique garantit aussi l'authenticité. Les algorithmes sont amenés à acquérir une valeur de preuve de plus en plus importante à l'avenir.

Débat

Int : Dans la mesure où chacun possède la base, est-il facile de tester les mots de passe ?
BR : Si le registre est réparti entre tous les utilisateurs, en revanche une modification par l'un d'eux n'entraîne pas de modifications pour les autres, car peu disposent de la faculté de valider les blocs.

Int : Les coûts de transaction du Bitcoin augmentent.
BR : Ce dernier s'est éloigné de l'objectif de son créateur qui voulait créer une monnaie stable et non spéculative.

Int : Comment des vols de cryptomonnaie peuvent-ils être commis ?
BR : Ils sont réalisés en récupérant l'identité numérique qui constitue une clef privée.

Int : D'où provient la valeur de la preuve de travail ?
BR : Cette dernière étant rémunérée, le mineur a tout intérêt à ne pas casser la blockchain.
Int : Existe-t-il un autre mode de preuve ?
BR : Oui. La preuve d'enjeu repose sur une validation par une minorité de personnes qui sont rémunérées pour établir la vérité.

Présentation de l'orateurs

Benjamin RAMEIX, ingénieur ENSMA de formation et diplômé de l'EN3S, a débuté sa carrière dans le consulting, puis dans l'assurance de personnes et la protection sociale sur plusieurs postes de DSI. Il fait maintenant partie du groupe Prévoir.