L'Ethereum, un système efficace et sécurisé pour les transactions et les contrats intelligents

Dea Bllaca, Milos Cerovic

Etudiant-e-s en ingénierie des médias, 1ère année, HEIG-VD

Aussi futuriste qu'elle paraisse, la technologie de la *blockchain* semble prendre de l'ampleur dans nos quotidiens, en passant par les cryptomonnaies, les applications décentralisées, ou encore les *smart contracts*. Malgré la difficulté à comprendre la manière dont elle fonctionne et sous son allure effrayante, la *blockchain* demeure à la fois très transparente et sécurisée. Comme acteur principal de cette technologie, l'Ethereum se positionne comme étant un des leaders des *blockchains* et cryptomonnaies favorisant les échanges par les pairs.

I. INTRODUCTION

C'EST en 2008 que le concept de *blockchain* est apparu aux yeux du monde, considéré dès lors comme une innovation de rupture qui révolutionne nos systèmes de transmission et d'échange à une échelle internationale[1]. Satoshi Nakamoto, le créateur dont l'identité reste encore à ce jour inconnue, a mis sur pied le système décentralisé le plus sophistiqué possible (en termes de technologie) qu'il y ait pu avoir jusque-là ; un système de base de données qui contient l'historique de tous les échanges effectués entre ses utilisateurs et tout ceci sans le besoin d'intermédiaires. Et c'est parce que cette technologie est en train de bouleverser notre société qu'il est important de comprendre ce qu'elle implique dans divers domaines d'applications, et surtout comment concrètement des morceaux de codes informatiques peuvent changer – et même faciliter – la manière de faire nos échanges et transactions.

II. LA BLOCKCHAIN

La technologie de la *blockchain* consiste à stocker et transmettre des informations en ligne de manière décentralisée, sécurisée et transparente, permettant ainsi à des utilisateurs de partager des données sans intermédiaire. Ils ont ainsi accès à cette grande base de données informatique qui contient les informations de tous les échanges ayant été effectués depuis sa création. Autrement dit, c'est un historique comportant des données telles que l'expéditeur, le destinataire, le contenu de l'envoi, la date ou encore l'heure.

Concrètement, cette base de données est composée de chaînes de blocs contenant des *datas* pouvant être identifiées et analysées par tous les utilisateurs du réseau qui reçoivent respectivement une copie dès qu'une transaction se fait – d'où la notion de transparence. Chaque personne peut ainsi consulter l'ensemble des échanges présents et passés sur l'intégralité de la chaine, mais en plus ils font office de validateurs par consensus. Il est quasi impossible de frauder en falsifiant ces blocs car ils sont identifiés par un *hash*, une suite de caractères uniques en guise de clé cryptée au début et à la fin d'un bloc.

L'utilisation de la *blockchain* permet d'améliorer la rapidité des transactions car la validation de ces dernières ne prend que quelques secondes ou minutes. La sécurité du système est également un point fort dans cette technologie grâce au contrôle mutuel [2] établit par l'ensemble des utilisateurs, ou plus communément appelés « nœuds » ou « mineurs ». Ces personnes se chargent de valider en consensus tous les échanges commis entre deux personnes tierces. Si quelqu'un essaye de falsifier une information dans l'historique des transactions (soit un bloc), les utilisateurs pourront contester l'information car ils vont s'appuyer sur leurs copies pour rendre invalide la manipulation échéante. On peut aussi parler d'une meilleure productivité dans l'organisation des échanges qui reposent désormais sur des protocoles informatiques, et contrairement aux intermédiaires traditionnels (banque, institutions, médiateurs, etc.), le mécanisme de gestion des transactions est beaucoup moins lent, coûteux et faillible.

III. CE QUE LA BLOCKCHAIN IMPLIQUE

La *blockchain* implique alors de grands changements dans notre société, particulièrement dans les secteurs bancaires, des assurances, de la logistique, de la santé, et bien d'autres encore [3]. Cette technologie ouvre la porte à une facilité transactionnelle grâce à l'absence d'intermédiaire, soit un gain de temps dans le traitement des échanges et des coûts réduits. Dans le secteur bancaire, il n'y aurait, en théorie, plus besoin d'une institution centralisant tous les échanges bancaires, système coûteux pour les acteurs procédant à cet échange. Des entreprises comme *Monaygram* ou *Western Unio*n pourrait voir leur fin puisque les transactions de pair à pair peuvent désormais se faire directement sans charges supplémentaires grâce à la technologie *blockchain*. Dans le domaine des assurances, l'avantage peut se distinguer au niveau de l'automatisation des procédures de remboursement si les conditions sont bien établies par le biais de *smart contracts* (voir point V.). La traçabilité est un avantage hautement utile pour des domaines comme la logistique ou encore l'agroalimentaire, et grâce à cette technologie, les entreprises peuvent former et suivre un historique des produits sans risque de perte, de falsification, ou autre.

Socialement parlant, la technologie de la *blockchain* est très polémique et partage la population entre les fervents d'innovation et les conservateurs traditionnels. Il est clair qu'une telle technologie peut faire peur, notamment par sa complexité et sa capacité à modifier profondément divers systèmes que nous exploitons actuellement. Cependant, les avantages de la *blockchain* sont innombrables et peuvent

permettre à n'importe qui d'optimiser les échanges quels qu'ils soient.

IV. BITCOIN ET ETHEREUM, CRYPTOMONNAIES EN TÊTE

La première cryptomonnaie qui est apparue est le Bitcoin. Elle a été créée en 2009 par un homme mystérieux du nom de Satoshi Nakamoto. Il décrit son idée dans un rapport appelé *"White paper"* [4] où il souhaite supprimer les tiers de confiance - soit des personnes physiques ou morales agissant comme intermédiaires - dans les transactions en utilisant la technologie de la *blockchain*.

Six ans après la création du Bitcoin, un fan a décidé de créer sa propre blockchain : l'Ethereum. La monnaie correspondante s'appelle donc Ether. Vitalik Buterin s'est basé sur le bitcoin est a décidé de l'améliorer. En plus de supprimer les tiers de confiances, il y ajoute deux nouvelles notions, la première étant les applications décentralisées. Elles ont la particularité d'être open source et de fonctionner à travers le réseau de *blockchain* sans avoir besoin d'être hébergées dans une centrale [5]. Il peut exister tout type d'applications décentralisées : transfert d'argent, location de vélo, jeux en ligne et autres [6]. La seconde nouveauté est la notion de *smart contract*, un moyen simple et rapide de sécuriser les transactions. Dès 2017, les *smart contracts* ont permis de créer une nouvelle manière d'identifier une valeur unique dans le monde digital. L'Ethereum propose donc des NFT (Non-Fongible Tokens), des jetons uniques et indivisibles en lien virtuel dans le cadre des *smart contracts* (voire point V.).

Le 6 avril 2021, l'Ether a battu son propre record en atteignant les 2'153 $US, contre 1'386,02 $US en 2018. Concernant le bitcoin, il a atteint le 13 mars 2021 la somme de 61'711,87 $US. Ces prix ont tendances à beaucoup varier en fonction de l'offre et la demande actuelles sur le marché.

V. CAS CONCRET : LES SMART CONTRACTS

La *blockchain* Ethereum est la meilleure en termes de protection de transactions. Aujourd'hui, si un utilisateur souhaite vendre ses habits sur internet, il va utiliser les multitudes d'applications de vente de seconde-main disponibles. S'il trouve un potentiel acheteur, ce dernier ne va vouloir payer qu'à la réception du colis. Mais qu'est-ce qui garantit au vendeur que l'acheteur ne va pas fuir avec le colis sans payer ? Et bien c'est ici que les *smart contracts* entrent en action. Pour illustrer ce système, l'exemple suivant permet de comprendre le fonctionnement : lors de l'envoi du colis, le vendeur va mettre un « cadenas » sur son colis et il ne pourra être déverrouillé qu'au moment où l'acheteur accepte l'échange et envoie l'argent en retour. S'il refuse de payer, le colis ne pourra jamais s'ouvrir et le postier le retournera à l'expéditeur.

En 2017, AXA Assurance a lancé l'application Fizzy. Elle permet d'indemniser les utilisateurs si leurs vols de ligne ont plus de deux heures de retard. Parfois, pour qu'une compagnie vous dédommage cela peut s'étendre sur plusieurs mois, voire une année. Le *smart contract*, quant à lui, entre en action dès le moment où l'on sait que l'avion a deux heures de retard. C'est à ce moment que vous êtes remboursé sans même passer par les procédures administratives, souvent jugées trop longues.

Puis, on retrouve de l'autre côté les NFT (Non-Fongible Tokens). C'est un jeton d'authentification unique correspondant à un seul bien virtuel, et par conséquent immatériel. En 2017, sort Cryptokitty, un jeu en ligne où on peut élever, collectionner, vendre ou acheter des chats virtuels. Ce jeu a comme particularité que chaque chat est unique. Il n'en existe pas deux pareils, et chacun ne peut appartenir qu'à une seule personne.

En février 2021, un artiste[1] a vendu une œuvre d'art digital à plus de 6,6 millions $US. Contrairement à une œuvre d'art conventionnelle, il n'y a pas de certificat d'authentification physique. Le NFT fait office de certificat où il recense le nom de l'auteur et la date de création. Sur internet, tout peut se vendre en utilisant des NFT ; le tweet d'Ellen DeGeneres avec plus de 3 millions de retweets, votre premier post Facebook, ou vos créations artistiques.

VI. CONCLUSION

Quel futur proche nous prépare cette nouvelle révolution technologique ?

Il est évident qu'une telle révolution technologique peut faire peur car elle bouleverse nos systèmes traditionnels d'échange. Cependant, la *blockchain* prend déjà une grande ampleur en tant qu'innovation révolutionnaire que beaucoup de personnes utilisent déjà à une large échelle. Il y aura sans aucun doute moins de personnes tierces et d'intermédiaires, voire pas du tout, lors de transactions ou échanges via la *blockchain*.

Dans un futur proche, il se pourrait que la monnaie physique puisse faire l'objet de remises en question, puisque les cryptomonnaies offrent bien plus d'avantage en termes de coût, d'efficacité, et de sécurité. Cela mène à questionner également les tiers de confiance ; à quel point peut-on leur faire confiance ? Peuvent-ils se mettre à niveau afin qu'ils puissent prendre avantage sur la technologie de la blockchain ? Il se peut qu'à moyen ou long terme, les Etats pourraient mettre en place une cryptomonnaie nationale afin de maintenir l'économie intérieure et internationale.

RÉFÉRENCES

[1] BITCONSEIL, 2019. « Smart Contract : Qu'est-ce qu'un contrat intelligent ? » *BitConseil* [en ligne]. Le 3 juillet 2019. [Consulté le 7 avril 2021]. Disponible à l'adresse : https://heig.ch/Glrzl

[2] FRANCE, 2018. « Qu'est-ce qu'une application décentralisée (DApp) ? » *France* [en ligne]. [Consulté le 15 mars 2021]. Disponible à l'adresse : https://heig.ch/K2LNQ

[3] BLOCKCHAIN, 2016. « Qu'est-ce qu'Ethereum ? » *France* [en ligne]. Le 4 mars 2016. [Consulté le 6 mars 2021]. Disponible à l'adresse : https://heig.ch/lMy0z/

[4] GOUV. FRANÇAIS, 2019. « Qu'est-ce que la blockchain ? » *Bery* Infos [en ligne]. Le 20 septembre 2019. [Consulté le 6 mars 2021]. Dispnible à l'adresse : https://heig.ch/rY8VK

[5] ethereum.org. « Qu'est-ce qu'Ethereum? ». [Consulté le 6 mars 2021]. Disponible à l'adresse : https://ethereum.org.

[6] Fillière d'Ingénierie des médias. « Médiamorphoses 2020 » *HEIG-VD* [en ligne]. Le 13 juillet 2020 [Consulté le 2 mars 2021]. Disponible à l'adresse : https://heig.ch/RwVvw

[7] REBECCA GARCIA, 2020. « Les smart contracts gagnent tous les secteurs ». *Bilan* [en ligne]. Le 17 juin 2020 [Consulté le 22 mars 2021]. Disponible à l'adresse : https://heig.ch/YMWnO

[8] CARLO LOMBARDI, 2021. « Les cryptomonnaies sont sans valeur ». *Le Temps* [en ligne]. Le 7 février 2021. [Consulté le 1er mars 2021]. Dispnible à l'adresse : https://heig.ch/RWd7J

[9] PASIN, PATRICK, et GOMEZ, 2018. « Les cryptomonnaies changent déjà le monde ». *Diplomatie* n° 94 (2018): 8084 [en ligne]. [Consulté le 4 mars 2021].

[10] CRYPTOPAST, 2018. « Le cours des crypto-monnaies fluctue en permanence, mais pourquoi ? ». Cryptopast [en ligne]. Le 14 mars 2018 [Consulté le 6 mars 2021]. Disponible à l'adresse : https://heig.ch/VJryo

[1] Mike Winkelmann ou Beeple

[11] PIGNEL, Marion, 2019. « La technologie Blockchain », Juin 2019 : 31. [Consulté le 15 mars 2021].
[12] ROUSSEAUX LES BONS TUYAUX, 2017. L'Ethereum en 5 minutes (ETH) | RLBT. *Youtube* [en ligne]. Le 19 juillet 2017. [Consulté le 6 mars 2021]. Disponible à l'adresse : https://heig.ch/OX1o3
[13] SHOBHIT, Seth, 2020. « How Do Cryptocurrency Mining Pools Work? ». *Investopedia* [en ligne]. Le 29 octobre 2021. [Consulté le 6 mars 2021]. Disponible à l'adresse : https://heig.ch/ApxZg
[14] WIKIPEDIA. « Ethereum » [en ligne]. [Consulté le 6 mars 2021]. Disponible à l'adresse : https://heig.ch/LKQgo
[15] LE TEMPS. « De la blockchain aux monnaies virtuelles » [en ligne]. [Consulté le 6 mars 2021]. Disponible à l'adresse : https://heig.ch/1nxKb
[16] BITCONSEIL, 2019. « DApp : qu'est-ce qu'une application décentralisée ? ». *BitConseil* [en ligne]. Le 3 juillet 2019. [Consulté le 6 mars 2021]. Disponible à l'adresse : https://heig.ch/JA1mA
[17] MA, Richard, 2019. « Council Post : How Blockchain is changing the game for social impact initatives ». *Forbes* [en ligne]. Le 25 septembre 2019. [Consulté le 15 mars 2021. Disponible à l'adresse : https://heig.ch/dWXq5
[18] RAJARSHI, Mitra, 2019. « Contrats intelligents : la technologie Blockchain qui remplacera les avocats ». *BlockGeeks* [en ligne]. Le 4 mars 2019. Disponible à l'adresse : https://heig.ch/6GxXG
[19] TROY, Sue, 2016. « Blockchain : qu'est-ce qu'un Smart Contract et à quoi ça sert ? » *LeMagIT* [en ligne]. Consulté le 22 mars 2021. Disponible à l'adresse : https://heig.ch/QkZ2k
[20] NAKAMOTO, Satoshi. « Bitcoin: A Peer-to-Peer Electronic Cash System », date unknown s. d., 9. Disponible à l'adresse : www.bitcoin.org
[21] REIFF, Nathan. « Bitcoin vs. Ethereum: What's the Difference? » *Investopedia* [en ligne]. [Consulté le 7 avril 2021]. Disponible à l'adresse : https://heig.ch/Lm5pv
[22] CRYPTERIUM. « 12 Best DApps To Try In 2020 [Reviews Included] | News Blog | Crypterium ». No date. [Consulté le 7 avril 2021]. Dispnible à l'adresse : https://heig.ch/OA4mj
[23] PIGNEL, Marion, 2019. « La technologie Blockchain », Juin 2019 : 31. [Consulté le 15 mars 2021].
[24] GOUV. FRANÇAIS, 2019. « Qu'est-ce que la blockchain ? » *Bery* Infos [en ligne]. Le 20 septembre 2019. [Consulté le 6 mars 2021]. Dispnible à l'adresse : https://heig.ch/rY8VK
[25] PASIN, PATRICK, et GOMEZ, 2018. « Les cryptomonnaies changent déjà le monde ». *Diplomatie* nº 94 (2018): 8084 [en ligne]. [Consulté le 4 mars 2021].
[26] NAKAMOTO, Satoshi. « Bitcoin: A Peer-to-Peer Electronic Cash System », date unknown s. d., 9. Disponible à l'adresse : www.bitcoin.org
[27] BITCONSEIL, 2019. « DApp : qu'est-ce qu'une application décentralisée ? ». *BitConseil* [en ligne]. Le 3 juillet 2019. [Consulté le 6 mars 2021]. Disponible à l'adresse : https://heig.ch/JA1mA
[28] CRYPTERIUM. « 12 Best DApps To Try In 2020 [Reviews Included] | News Blog | Crypterium ». No date. [Consulté le 7 avril 2021]. Dispnible à l'adresse : https://heig.ch/OA4mj