
Les passerelles blockchains, victimes de hacks à répétition

Description

Une passerelle blockchain est une application dont l'objet est de représenter le token d'une blockchain d'origine vers le token d'une blockchain de destination. Des pirates profitent de défaillances humaines ou de la vulnérabilité des *smart contracts* sur lesquels ces applications sont construites pour détourner des fonds en crypto-actifs dont le montant record s'élève à 3,8 milliards de dollars en 2022.

Bitcoin (BTC), Ethereum (ETH), Polygon (MATIC), Cosmos (ATOM) ou encore Solana (SOL) sont des blockchains publiques qui fonctionnent toutes de manière autonome, avec des tokens, des protocoles informatiques et des règles de gouvernance différents. Les passerelles blockchains, *blockchain bridge* ou encore *cross-chain applications*, constituent une des réponses à l'absence d'interopérabilité entre les diverses blockchains publiques. Plus précisément, pour reprendre la définition de l'entrepreneur de l'économie décentralisée James Prestwich, « *une passerelle blockchain est une application qui utilise la communication interchaînes pour représenter les jetons d'une autre chaîne* ». Il n'est en effet pas possible pour une personne détenant des bitcoins d'effectuer un règlement auprès d'une autre personne qui souhaiterait recevoir des Ether (ETH), le crypto-actif de la blockchain Ethereum. L'intérêt d'une application interchaînes est de passer d'une blockchain à une autre, sans avoir à vendre ou convertir de token, et donc, sans dépendre de la volatilité des cours, d'économiser les frais de transaction. Par exemple, un utilisateur envoie un Bitcoin (BTC) vers une application interchaînes qui le verrouille dans un *smart contrat* ([voir La rem n°44, p.97](#)) et crée, pour un montant équivalent, un Wrapped Bitcoin (WBTC) – *wrapped*, pour « emballé / enveloppé », dans la blockchain de destination, en l'occurrence Ethereum. Il pourra alors utiliser ce Wrapped Bitcoin sur les applications décentralisées développées au sein de l'écosystème d'Ethereum et rebasculer par la suite vers le token de la blockchain initiale. Les applications interchaînes sont particulièrement utilisées dans le domaine de la finance décentralisée (DeFi), qui permet a? quiconque en a les moyens, et indépendamment du pays ou? il se trouve ou de sa nationalité, d'emprunter, de prêter et d'investir, d'assurer et d'échanger des crypto-actifs sans passer par un intermédiaire, les transactions étant sécurisées *via* l'usage d'une blockchain et de *smart contracts*.

Ces applications interchaînes se distinguent selon qu'elles fonctionnent de manière centralisée ou décentralisée. Les applications centralisées requièrent de leurs utilisateurs qu'ils fassent confiance à une entité centrale, afin d'assurer la sécurité des tokens en séquestre, alors que les applications interchaînes décentralisées éliminent l'opérateur central et s'appuient sur la programmation de *smart contracts* qui verrouillent les tokens de la blockchain d'origine et émettent les tokens sur la blockchain de destination. Qu'elles soient centralisées ou décentralisées, ces applications sont sujettes à de nombreux piratages, impliquant des défaillances humaines comme le vol de clefs privées, ou des failles de sécurité dans la programmation des *smart contracts*

, avec toujours pour conséquence le transfert et le détournement de fonds en crypto-actifs. La valeur totale des crypto-actifs détournés en 2022 a atteint le record de 3,8 milliards de dollars. Selon Chainalysis, une société américaine spécialisée dans l'analyse des données des blockchains, ces attaques proviennent pour une large part de la Corée du Nord et notamment du groupe de pirates informatiques appelés Lazarus ([voir La rem n°33, p.81](#) et [La rem n°44, p.50](#)).

Des hacks à répétition

En 2021, le studio de jeux vidéo Sky Mavis a décidé de déplacer le jeu Axie Infinity, construit sur la blockchain Ethereum, vers leur propre blockchain appelée Ronin. Les joueurs ont été invités à utiliser une application interchaînes Ethereum-Ronin pour bénéficier des nouveaux tokens. Or l'application interchaîne de Ronin, centralisée, ne comptait que neuf validateurs dont quatre étaient des dirigeants du studio de jeux. Les attaquants ont réussi à pirater les clefs privées de cinq validateurs sur les neuf, à s'autoriser à transférer les fonds, et à mettre la main sur l'équivalent de 625 millions de dollars. En juin 2022, l'application interchaînes Horizon, qui crée des ponts entre les blockchains Harmony (ONE), Ethereum (EHT), Binance Chain (BNB) ou encore Bitcoin (BTC), s'est fait subtiliser l'équivalent de 100 millions de dollars, alors que l'application avait fait l'objet d'un audit par la société PeckShield, spécialisée dans la découverte et la correction de failles de sécurité. En août 2022, l'application interchaînes décentralisée Nomad a été victime d'un détournement de tokens équivalent à 200 millions de dollars. Les pirates se sont appuyés sur la mise à jour d'un *smart contract* présentant une vulnérabilité, grâce à laquelle les attaquants ont pu créer de fausses transactions et vider le portefeuille de Nomad en un rien de temps.

Quel avenir ?

Nombre de spécialistes estiment que le développement d'un écosystème de blockchains passe par la communication interchaînes, permettant ainsi à tout un chacun de passer d'une blockchain à l'autre en conservant les crypto-actifs de départ, verrouillés en tant que sous-jacents. Mais si les applications interchaînes n'ont pas à prouver leur utilité, leur conception technique laisse pourtant à désirer. Jusqu'ici, la cible principale des attaquants n'étaient autres que les plateformes d'échanges centralisées (CEX), comme Binance ou Kraken. Ces dernières ayant consenti d'importants efforts en matière de sécurité, les attaquants se tournent dorénavant vers d'autres catégories de victimes ou de cibles, au comportement parfois amateur, et donc vers ces applications interchaînes puisqu'elles donnent accès, de manière centralisée ou décentralisée, aux fonds verrouillés de leurs utilisateurs.

D'autres, comme Vitalik Buterin, le fondateur de la blockchain Ethereum, se montrent nettement plus sceptiques quant à l'opportunité d'utiliser des applications interchaînes. Pour ce dernier, elles présentent des risques trop importants en matière de sécurité, d'autant que si le problème se pose déjà pour la communication entre deux blockchains, qu'en sera-t-il avec quatre, cinquante ou cent blockchains ? *« Il finira par y avoir des applications décentralisées avec de nombreuses interdépendances entre ces chaînes, et une attaque des 51 % [attaque visant à dépenser deux fois le même solde] même sur une seule chaîne créerait une contagion systémique qui menacerait l'économie de cet écosystème en entier. »* Si bien

que « l'activité interchaînes a donc un effet anti-réseau : tant qu'elle est peu répandue, elle est assez sûre, mais plus elle est répandue, plus les risques augmentent » expliquait-il en janvier 2022 sur Reddit, un forum de discussion. « Je suis optimiste quant à un écosystème blockchain multichaînes (il y a vraiment quelques communautés distinctes avec des valeurs différentes et il vaut mieux qu'elles vivent séparément plutôt que de se disputer l'influence sur la même chose), je suis pessimiste quant aux applications interchaînes. »

Comme si l'avenir lui avait donné raison, selon un récent rapport de Chainalysis, les trois plus importants détournements de crypto-actifs en 2022, Ronin (625 millions de dollars), Wormhole (321 millions de dollars) et Nomad (190 millions de dollars), ainsi que les deux tiers de la valeur totale des crypto-actifs détournés cette même année, concernent des applications interchaînes.

Sources :

- « The fundamental security limits of bridges », Vitalik Buterin, Reddit, old.reddit.com/r/ethereum, January 7, 2022.
- « Explaining crypto's billion-dollar bridge problem », Corin Faife, theverge.com, April 11, 2022.
- « Qu'est-ce qu'un bridge (pont) pour cryptomonnaies et comment ça fonctionne ? », Jessy Aouali, cryptoast.fr, 30 juillet 2022.
- « Nouveau piratage dans la crypto : le « bridge » Nomad vidé de 190 millions de dollars », Raphaële Karayan, usine-digitale.fr, 2 août 2022.
- « Selon Chainalysis, les bridges cross-chain sont la principale cause de hack dans l'écosystème crypto », Maximilien Prué, cryptoast.fr, 4 août 2022.
- « Cryptos : les « bridges » entre blockchains, nouvelle cible privilégiée des hackers », Clément Perruche, lesechos.fr, 4 août 2022.
- « Are Blockchain Bridges Safe ? Why Bridges Are Targets of Hacks », Marcus Chan, coindesk.com, August 17, 2022.
- « Crypto Bridge Hacks 101 : Types and Causes », worldcoin.org, December 13, 2022.
- « Crypto hacks stole record \$3.8 billion in 2022 », Josh Smith, reuters.com, February 7, 2023.

Categorie

1. Techniques

date créée

11 mai 2023

Auteur

jacquesandrefines