Les passerelles blockchains, victimes deÂ hacks Ã rÃ©pÃ©tition

Description

Une passerelle blockchain est une application dont lâ€™objet est de reprÃ©senter le token dâ€™une blockchain dâ€™origine vers le token dâ€™une blockchain de destination. Des pirates profitent de dÃ©faillances humaines ou de la vulnÃ©rabilitÃ© desÂ *smart contracts*Â sur lesquels ces applications sont construites pour dÃ©tourner des fonds en crypto-actifs dont le montant record sâ€™Ã©IÃ¨ve Ã 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 maniÃ¨re autonome, avec des tokens, des protocoles informatiques et des rÃ¨gles de gouvernance diffÃ©rents. Les passerelles blockchains,Â *blockchain bridge*Â ou encoreÂ *cross-chain applications*, constituent une des rÃ©ponses Ã lâ€™absence dâ€™interopÃ©rabilitÃ© entre les diverses blockchains publiques. Plus prÃ©cisÃ©ment, pour reprendre la dÃ©finition de lâ€™entrepreneur de lâ€™Ã©conomie dÃ©centralisÃ©e James Prestwich,Â *Â«Â une passerelle blockchain est une application qui utilise la communication interchaÃ®nes pour reprÃ©senter les jetons dâ€™une autre chaÃ®neÂ Â»*. Il nâ€™est en effet pas possible pour une personne dÃ©tenant des bitcoins dâ€™effectuer un rÃ¨glement auprÃ¨s dâ€™une autre personne qui souhaiterait recevoir des Ether (ETH), le crypto-actif de la blockchain Ethereum.Â Lâ€™intÃ©rÃªt dâ€™une application interchaÃ®nes est de passer dâ€™une blockchain Ã une autre, sans avoir Ã vendre ou convertir de token, et donc, sans dÃ©pendre de la volatilitÃ© des cours, dâ€™Ã©conomiser les frais de transaction.Â Par exemple, un utilisateur envoie un Bitcoin (BTC) vers une appliÂcation interchaÃ®nes qui le verrouille dans unÂ *smart contrat*Â (voirÂ *La rem*Â nÂ°44, p.97) et crÃ©e, pour un montant Ã©quivalent, un Wrapped Bitcoin (WBTC) â€“Â *wrapped*, pourÂ Â«Â emballÃ© / enveloppÃ©Â Â», dans la blockchain de destination, en lâ€™occurrence Ethereum. Il pourra alors utiliser ce Wrapped Bitcoin sur les applications dÃ©centralisÃ©es dÃ©veloppÃ©es au sein de lâ€™Ã©cosystÃ¨me dâ€™Ethereum et rebasculer par la suite vers le token de la blockchain initiale. Les applications interchaÃ®nes sont particuliÃ¨rement utilisÃ©es dans le domaine de la finance dÃ©centralisÃ©e (DeFi), qui permet aÌ€ quiconque en a les moyens, et indÃ©pendamment du pays ouÌ€ il se trouve ou de sa nationalitÃ©, dâ€™emprunter, de prÃªter et dâ€™investir, dâ€™assurer et dâ€™Ã©changer des crypto-actifs sans passer par un intermÃ©diaire, les transactions Ã©tant sÃ©curisÃ©esÂ *viaÂ* lâ€™usage dâ€™une blockchain et deÂ *smart contracts.*

Ces applications interchaÃ®nes se distinguent selon quâ€™elles fonctionnent de maniÃ¨re centralisÃ©e ou dÃ©cenÂtralisÃ©e. Les applications centralisÃ©es requiÃ¨rent de leurs utilisateurs quâ€™ils fassent confiance Ã une entitÃ© centrale, afin dâ€™assurer la sÃ©curitÃ© des tokens en sÃ©questre, alors que les applications interchaÃ®nes dÃ©cenÂtralisÃ©es Ã©liminent lâ€™opÃ©rateur central et sâ€™appuient

sur la programmation deÂ *smart contracts*Â qui verrouillent les tokens de la blockchain dâ€™origine et Ã©mettent les tokens sur la blockchain de destination.Â Quâ€™elles soient centralisÃ©es ou dÃ©centralisÃ©es, ces applications sont sujettes Ã de nombreux piratages, impliquant des dÃ©faillances humaines comme le vol de clefs privÃ©es, ou des failles de sÃ©curitÃ© dans la programmation desÂ *smart contracts*,Â avec toujours pour consÃ©quence le transfert et le dÃ©tournement de fonds en crypto-actifs.Â La valeur totale des crypto-actifs dÃ©tournÃ©s en 2022 a atteint le record de 3,8 milliards de dollars.Â Selon Chainalysis, une sociÃ©tÃ© amÃ©ricaine spÃ©cialisÃ©e dans lâ€™analyse des donnÃ©es des blockchains, ces attaques proviennent pour une large part de la CorÃ©e du Nord et notamment du groupe de pirates informatiques appelÃ©s Lazarus (voirÂ *La rem*Â nÂ°33, p.81 etÂ *La rem* Â nÂ°44, p.50).

Des hacks Ã rÃ©pÃ©tition

En 2021, le studio de jeux vidÃ©o Sky Mavis a dÃ©cidÃ© de dÃ©placer le jeu Axie Infinity, construit sur la blockchain Ethereum, vers leur propre blockchain appelÃ©eÂ Ronin. Les joueurs ont Ã©tÃ© invitÃ©s Ã utiliser une application interchaÃ®nes Ethereum-Ronin pour bÃ©nÃ©ficier des nouveaux tokens. Or lâ€™application interchaÃ®ne de Ronin, centralisÃ©e, ne comptait que neuf validateurs dont quatre Ã©taient des dirigeants du studio de jeux. Les attaquants ont rÃ©ussi Ã pirater les clefs privÃ©es de cinq validateurs sur les neuf, Ã sâ€™autoriser Ã transfÃ©rer les fonds, et Ã mettre la main sur lâ€™Ã©quivalent de 625 millions de dollars. En juin 2022, lâ€™application interchaÃ®nes Horizon, qui crÃ©e des ponts entre les blockchains Harmony (ONE), Ethereum (EHT), Binance Chain (BNB) ou encore Bitcoin (BTC), sâ€™est fait subtiliser lâ€™Ã©quivalent de 100 millions de dollars, alors que lâ€™application avait fait lâ€™objet dâ€™un audit par la sociÃ©tÃ© PeckShield, spÃ©cialisÃ©e dans la dÃ©couverte et la correction de failles de sÃ©curitÃ©. En aoÃ»t 2022, lâ€™application interchaÃ®nes dÃ©centralisÃ©e Nomad a Ã©tÃ© victime dâ€™un dÃ©tournement de tokens Ã©quivalent Ã 200 millions de dollars. Les pirates se sont appuyÃ©s sur la mise Ã jour dâ€™unÂ *smart contract* Â prÃ©sentant une vulnÃ©rabilitÃ©, grÃ¢ce Ã laquelle les attaquants ont pu crÃ©er de fausses transactions et vider le portefeuille de Nomad en un rien de temps.

Quel avenir ?

Nombre de spÃ©cialistes estiment que le dÃ©veloppement dâ€™un Ã©cosystÃ¨me de blockchains passe par la communication interchaÃ®nes, permettant ainsi Ã tout un chacun de passer dâ€™une blockchain Ã lâ€™autre en conservant les crypto-actifs de dÃ©part, verrouillÃ©s en tant que sous-jacents. Mais si les applications interchaÃ®nes nâ€™ont pas Ã prouver leur utilitÃ©, leur conception technique laissepourtant Ã dÃ©sirer. Jusquâ€™ici, la cible principale des attaquants nâ€™Ã©taient autres que lesplateformes dâ€™Ã©changes centralisÃ©es (CEX), comme Binance ou Kraken. Ces derniÃ¨res ayantconsenti dâ€™importants efforts en matiÃ¨re de sÃ©curitÃ©, les attaquants se tournent dorÃ©navant vers dâ€™autres catÃ©gories de victimes ou de cibles, au comportement parfois amateur, et donc vers ces applications interchaÃ®nes puisquâ€™elles donnent accÃ¨s, de maniÃ¨re centralisÃ©e ou dÃ©centralisÃ©e, aux fonds verrouillÃ©s de leurs utilisateurs.

Dâ€™autres, comme Vitalik Buterin, le fondateur de la blockchain Ethereum, se montrent nettement plus sceptiques quant Ã lâ€™opportunitÃ© dâ€™utiliser des applications interchaÃ®nes. Pour ce dernier, elles prÃ©sentent des risques trop importants en matiÃ¨re de sÃ©curitÃ©, dâ€™autant que si le problÃ¨me se pose dÃ©jÃ pour la commuÂnication entre deux blockchains, quâ€™en sera-t-il avec quatre, cinquante ou cent blockchains ?Â *Â«Â Il finira par y avoir des applications dÃ©centralisÃ©es avec de nombreuses interdÃ©pendances entre ces chaÃ®nes, et une attaque des 51 %Â* [attaque visant Ã dÃ©penser deux fois le mÃªme solde]*Â mÃªme sur une seule chaÃ®ne crÃ©erait une contagion systÃ©mique qui menacerait lâ€™Ã©conomie de cet Ã©cosystÃ¨me en entier.Â Â»*Â Si bien queÂ *Â«Â lâ€™activitÃ© interchaÃ®nes a donc un effet anti-rÃ©seauÂ : tant quâ€™elle est peu rÃ©pandue, elle est assez sÃ»re, mais plus elle est rÃ©pandue, plus les risques augmententÂ Â»*Â expliquait-il en janvier 2022 sur Reddit, un forum de discussion.Â *Â«Â Je suis optimiste quant Ã un Ã©cosystÃ¨me blockchain multichaÃ®nes (il y a vraiment quelques communautÃ©s distinctes avec des valeurs diffÃ©rentes et il vaut mieux quâ€™elles vivent sÃ©parÃ©ment plutÃ´t que de se disputer lâ€™influence sur la mÃªme chose), je suis pessimiste quant aux applications interchaÃ®nes.Â Â»*

Comme si lâ€™avenir lui avait donnÃ© raison, selon un rÃ©cent rapport de Chainalysis, les trois plus importants dÃ©tournements de crypto-actifs en 2022, Ronin (625Â 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 dÃ©tournÃ©s cette mÃªme annÃ©e, concernent des applications interchaÃ®nes.

SourcesÂ :

- Â« The fundamental security limits of bridges Â», Vitalik Buterin, Reddit,Â old.reddit.com/r/ethereum, January 7, 2022.
- Â« Explaining cryptoâ€™s billion-dollar bridge problem Â», Corin Faife, theverge.com, April 11, 2022.
- Â« Quâ€™est-ce quâ€™un bridge (pont) pour cryptomonnaies et comment Ã§a fonctionne ? Â», Jessy Aouali, cryptoast.fr, 30 juillet 2022.
- Â« Nouveau piratage dans la crypto : le Â«Â bridgeÂ Â» Nomad vidÃ© de 190 millions de dollars Â», RaphaÃ«le Karayan, usine-digitale.fr, 2 aoÃ»t 2022.

- Â« Selon Chainalysis, les bridges cross-chain sont la principale cause de hack dans lâ€™Ã©cosystÃ¨me crypto Â», Maximilien PruÃ©, cryptoast.fr, 4 aoÃ»t 2022.
- Â« Cryptos : les Â«Â bridgesÂ Â» entre blockchains, nouvelle cible privilÃ©giÃ©e des hackers Â», ClÃ©ment Perruche, lesechos.fr, 4 aoÃ»t 2022.
- Â« Are Blockchain Bridges Safe ? Why Bridges Are Targets of Hacks Â», Marcus Chan, coindesk.com, August 17, 2022.
- Â« Crypto Bridge Hacks 101 : Types and Causes Â», worldcoin.org, December 13, 2022.
- Â« Crypto hacks stole record $3.8 billion in 2022 Â», Josh Smith, reuters.com, February 7, 2023.Â

Categorie

1. Techniques

date crÃ©Ã©e
11 mai 2023
Auteur
jacquesandrefines