

## Attaque Sybil sur un réseau pair-à-pair

### Description

L'impact des réseaux pair-à-pair, socle des blockchains publiques, est de se passer de l'autorité centralisée pour fonctionner. Les attaques dites « Sybil » consistent à créer de fausses identités pour corrompre le réseau.

Le propre d'une architecture informatique pair-à-pair est d'opérer des échanges entre plusieurs ordinateurs connectés au système sans passer par un serveur central. Tous les ordinateurs d'un réseau pair-à-pair, appelés « nœuds », jouent tout à la fois le rôle de client et de serveur, c'est-à-dire le rôle d'émetteur et de récepteur. Une application largement répandue dans le domaine des architectures informatiques pair-à-pair est celui du partage de fichiers, bête noire des industries culturelles depuis l'avènement d'internet et le lancement, en juin 1999, du premier logiciel utilisé à grande échelle, Napster, puis, à l'été 2002, du protocole de transfert de données BitTorrent. Dans le domaine des réseaux filaires ou sans fil, la structure du réseau est dite « maillée » lorsqu'elle consiste en la connexion de tous les nœuds (aussi nommés « hôtes ») en pair-à-pair, sans hiérarchie centrale. Tous les hôtes du réseau sont à la fois client et serveur, permettant une bien meilleure résilience des communications si l'un des points tombe en panne. Aujourd'hui, les réseaux pair-à-pair sont également au cœur du fonctionnement de la plupart des blockchains publiques, comme Bitcoin, Ethereum ou encore Tezos.

Toutes ces applications dont l'architecture technique repose sur un réseau pair-à-pair doivent faire face, notamment, à une menace de sécurité propre à cette topologie distribuée baptisée « attaque Sybil », au cours de laquelle une personne crée plusieurs comptes ou raccorde plusieurs nœuds ou ordinateurs au sein du réseau pour tenter d'en prendre le contrôle. Le nom de ce type d'attaque informatique est une référence à un roman biographique paru en 1973 aux États-Unis, écrit par Flora Rheta Schreiber, qui raconte l'histoire de la psychothérapie de Shirley Ardell Mason (1923-1998), également connue sous l'alias « Sybil Isabel Dorsett », une artiste publicitaire atteinte d'un trouble de la personnalité multiple, ou trouble dissociatif de l'identité. Une attaque Sybil désigne ainsi l'activité de nœuds malhonnêtes au sein d'un réseau pair-à-pair qui se font passer pour des nœuds individuels et indépendants alors qu'ils sont en réalité sous le contrôle d'une seule entité malintentionnée, et dont l'objectif est d'influencer les décisions prises sur le réseau, de désanonymiser les utilisateurs du réseau ou encore d'en corrompre le fonctionnement, voire d'en bloquer le protocole.

En 2014, le réseau Tor, réseau informatique mondial et décentralisé qui permet à ses utilisateurs

dâ€™anonymiser lâ€™origine de leur connexion, a subi une attaque Sybil pendant plusieurs mois. Lâ€™objectif des attaquants, qui sont parvenus Ã prendre le contrÃ le Ã lâ€™aide de nâ€™uds malveillants dâ€™environ la moitiÃ des relais Tor, Ãtait dâ€™espionner le trafic des donnÃes et de dâ€™sanonymiser un grand nombre dâ€™utilisateurs. Dâ€™aprÃs Sombrecritz, collaborateur du site linuxadictos.com, *Ã placer un grand nombre de nâ€™uds contrÃ les par un opÃrateur permet aux utilisateurs de dâ€™sanonymiser Ã lâ€™aide dâ€™une attaque de classe Sybil, ce qui peut Ãtre fait si les attaquants contrÃ lent le premier et le dernier nâ€™ud de la chaÃne dâ€™anonymisation. Le premier nâ€™ud de la chaÃne Tor connaÃt lâ€™adresse IP de lâ€™utilisateur, et ce dernier connaÃt lâ€™adresse IP de la ressource demandÃe, qui permet de dâ€™sanonymiser la demande en ajoutant une certaine Ãtiquette cachÃe sur le cÃtÃ du nâ€™ud dâ€™entrÃe pour les en-tÃtes de paquets qui restent inchangÃs tout au long de la chaÃne dâ€™anonymisation, puis lâ€™analyse de celui-ci cÃtÃ de nâ€™ud de sortie.* Ces nâ€™uds malveillants, une fois identifiÃs, ont ÃtÃ dÃconnectÃs du rÃseau Tor.

Le risque dâ€™attaques Sybil existe sur les protocoles blockchain dont le fonctionnement repose Ãgalemment sur une architecture pair-Ã-pair. Comment les nâ€™uds dâ€™une blockchain se font-ils confiance et acceptent-ils les nouveaux blocs de transactions diffusÃs sur le rÃseau ? Comment repÃrer dâ€™Ãventuels nâ€™uds malveillants qui tentent dâ€™inscrire de fausses transactions Ã leur profit dans le registre public ? Pour se prÃmunir de ce type dâ€™attaque, les blockchains publiques mettent en Ãuvre un mÃcanisme de consensus, celui notamment de la preuve de travail (*proof of work*). Le mÃcanisme de consensus de la preuve de travail exige que chaque nâ€™ud impliquÃ dans la validation des transactions rÃsolve une Ãnigme cryptographique, coÃteuse en Ãnergie, afin de participer au processus de minage. Celui qui rÃsout cette Ãnigme cryptographique valide le bloc de transactions et perÃsoit une rÃcompense pour ce travail. Or, si la crÃation dâ€™identitÃs multiples est toujours possible, il est aujourdâ€™hui quasiment impossible pour un attaquant de fournir une puissance de calcul suffisante pour inscrire Ã lâ€™insu de tous de fausses transactions dans une blockchain publique. Le mÃcanisme de consensus de la preuve de travail, mis en Ãuvre au sein dâ€™un protocole blockchain, permet ainsi de se dÃfendre de maniÃre trÃs efficace contre les attaques Sybil. Comme le prÃcise le site academy.binance.com, *Ã il nâ€™empÃche en rien un attaquant de tenter ce type dâ€™attaque mais a pour objectif de la rendre extrÃmement difficile, voire impossible*. Câ€™est par cet ingÃnieux moyen que, depuis 2009, la blockchain publique Bitcoin se prÃmunit avec succÃs contre les attaques Sybil et permet de garantir lâ€™inviolabilitÃ des transactions sur son rÃseau.

Sources :

- *Ã Les attaques Sybil* Ã, Binance Academy, academy.binance.com/fr, 2018, mise Ã jour en 2021.
- *Ã Sybil Attacks and Defenses in Internet of Things and Mobile Social Networks* Ã, Ali Alharbi, Mohamed Zohdy, Debatosh Debnath, Richard Olawoyin, George Corser, *International Journal of Computer Science Issues*, vol. 15, issue 6, zenodo.org, November 30, 2018.
- *Ã Lâ€™attaque de Sybil â€ Free TON est-il vulnÃrable ?* Ã, Vitaly Romanov, freeton.house/fr/

21 mars 2021.

- « Tor 11.0.2 a déjà été publié et est livré avec quelques correctifs », Sombrecrizt, [linuxadictos.com/fr](https://linuxadictos.com/fr), 5 décembre 2021.

## Categorie

1. Techniques

**date créée**

20 juillet 2022

**Auteur**

jacquesandrefines