GERMINOLEGRAND



Geste de savoir

# Hole-punching décentralisé

11 juin 2023

# Table des matières



## Introduction

En parcourant les pages liées à l'IPFS dans ma quête des réseaux décentralisés (un sujet passionnant pour moi depuis que je sais coder), je suis tombé sur un papier publié en 2022 décrivant une méthode de hole-punching décentralisé que j'ai eu envie de vous partager.

Le Hole-Punching en bref c'est une technique qui permet de contourner le problème que la plupart des ordis des particuliers (et des entreprises) se trouvent derrière une Box (qui fait office de NAT et de pare-feu) qui ne laisse pas passer les connexions dans les deux sens.

Problème auquel on se heurte quand on est jeune (hello le moi de 2009), qu'on n'a pas d'argent pour se payer un serveur (coucou le moi d'avant 2012), et encore moins une infrastructure cloud à même de fournir une haute disponibilité pour des services centralisés (salut moi-même de 2023), et qu'on se dit que le peer-to-peer est une solution pour développer des MMO pas cher (ahah, coucou le moi absolument pas réaliste de 2012), ou encore que l'avenir de l'humanité dépend de notre capacité à concevoir une décentralisation à tous les niveaux (politique, économique, technologique, …), y compris donc les réseaux qui devraient pouvoir résister à la censure étatique et des GAFAM, aux guerres et aux catastrophes naturelles.

J'avais implémenté, avec un petit frisson d'interdit, du Hole-Punching avec le protocole UDP pour mon petit moteur réseau en C++ il y a longtemps[1]. Évidemment j'étais débutant et il m'avait semblé bien plus facile de bricoler mes propres protocoles pour cela plutôt que de comprendre d'obscures RFC de protocoles existants (pas si répandus que cela à l'époque). J'ai découvert par la suite qu'il existait des protocoles comme STUN, TURN, etc. et après tout, on voit ce type de protocoles massivement déployés via le streaming et les torrents en p2p[2].

Le Hole-Punching consiste généralement à ce que les deux pairs se connectent à un serveur public, que celui-ci retransmette les informations nécessaires aux deux pairs pour qu'ils puissent se faire respectivement passer pour le serveur pour la suite de leurs communications. De sorte que les deux box ont l'impression de communiquer avec le serveur alors qu'en réalité les deux pairs discutent directement entre eux.

Je redécouvre au passage avec ce papier qu'il est possible de faire du Hole-Punching avec du TCP (même si c'est casse-gueule), et que QUIC, une alternative au TCP, basée sur l'UDP, est en train de prendre de l'ampleur (enfin !).

> Un petit mot de mise en garde: depuis quelques années, les technologies décentralisés ont un peu trop tendance à attirer une communauté maudite des internets, j'ai nommé les fans de blockchains, de cryptos, de NFT et autres drames écologiques ou dystopies utra-libérales. À la fois ça me dégoûte/déprime une fois sur deux lorsque je vais sur des sites comme celui qui héberge le papier à lire ici, et en même temps il me semble crucial de ne pas y laisser moisir les avancées de recherche fondamentale en décentralisation des réseaux.

## 1. Résumé (la traduction est mienne)

Nous présentons un mécanisme de Hole Punching décentralisé construit dans la bibliothèque de réseau pair-à-pair libp2p. Le Hole Punching est crucial pour les réseaux pair-à-pair (peer-to-peer), permettant à chaque participant de communiquer directement avec n'importe quel autre participant, même s'ils sont séparés par des NAT et des pare-feux. Le protocole de hole punching décentralisé de libp2p met en oeuvre des protocoles similaires à STUN (RFC 8489), TURN (RFC 8566) et ICE (RFC 8445), sans nécessiter d'infrastructure centralisée. Spécifiquement, il ne nécessite aucune connaissance préalable des participants au réseau autre qu'au moins un noeud (n'importe lequel arbitrairement) pour initier la découverte des pairs. Le point clé est que les protocoles utilisés pour du hole punching, nommément les protocoles de découverte d'adresse et de relai, peuvent être construits de façon à ce que leur besoins en ressources soient négligeables. Ce qui rend possible pour chaque participant au réseau de faire tourner ceux-ci, permettant ainsi la coordination des tentatives de hole punching, en supposant qu'au moins une petite fraction des nœuds n'est pas située derrière un pare-feu ou un NAT.

https://research.protocol.ai/publications/decentralized-hole-punching/

## Conclusion

Bonne lecture!

N'hésitez pas à réagir si ces problématiques de décentralisation des réseaux vous parlent 🍊

1. Arg, ça fait au moins 10 ans, ça me rajeunit pas 🍊 !
2. avec PopcornTime par exemple…

# Liste des abréviations

**IPFS** InterPlanetary FileSystem. 1

**RFC** https://fr.wikipedia.org/wiki/Request_for_comments. 1, 2