Critiques protocolaires d'Internet: Comparaison des projets IPFS et SecureScuttleButt

Pierre Depaz

Paris-3 Sorbonne-Nouvelle - THALIM

February 22, 2022

1 Introduction

Avec toutes ses implications économiques, sociales et politiques, l'Internet et le Web[1] sont avant tout des protocoles de communication, c'est-à-dire un ensemble de règles permettant à deux parties ou plus de requérir et fournir des données dans un même réseau. Cette suite de protocoles voit le jour autour de TCP/IP à la fin des années 1960 sous l'égide de la recherche militaire étasunienne, tandis que les deux protocoles HTTP et HTTPS qui constituent l'infrastructure du Web sont développés et distribués par le Centre Européen de la Recherche Nucléaire, une institution publique de recherche. Ces deux documents sont mis-à-jour, avec la version 6 de l'Internet Protocol et la version 2 de l'HyperText protocol étant actuellement (2022) en cours d'adoption.

Pourtant, l'utilisation de ces protocoles ont découlé sur des utilisations bien différentes de leurs usages intialement envisagés—i.e. la sûreté des données en cas d'attaque militaire soviétique et l'accès à des articles et

de la documentation de recherche en physique. Cette évolution est notamment documentée par Lawrence Lessig, dans son ouvrage *Code and Other Laws of Cyberspace*[2], en ce qu'il identifie différentes forces capables de faconner l'évolution de l'Internet et du Web: des forces légales, marchandes, sociales et technologiques[1].

Les dérives de surveillance, de limitation de partage et de monopole des applications issues des protocoles Internet et Web sont donc bien documentées. Face à celles-ci s'élèvent alors plusieurs types de critiques: critiques sémantiques, sous la forme de blogs, de livres, d'articles et de conférences; critiques légales, telles que les licences GPL ou Creative Commons ou les législations de la RGPD ou du DGA; ou encore critiques programmatiques, telles que les bloqueurs de publicités. Bien qu'il y ait eu des solutions légales avancées en réponse critiques à ces évolutions des usages des technologies d'Internet, telles que l'ensemble des licenses Creative Commons, dans la lignée de GPL et licenses copyleft, il n'en reste pas moins que les forces technologiques peuvent influencer fortement les possibilités d'agir des utilisateurs de ces dernières. Par example, Harsh Gupta s'interroge sur le manque de représentation des contients africains, sud-américains et asiatiques (respectivement 0%, 0% et 0%) lors des délibération ayant pour objet l'implémentation de l'Encrypted Media Extensions. L'EME est un standard de communication pour contenus protégés par une propriété intellectuelle, une propriété intellectuelle de tradition exclusivement occidentale désormais établie en tant que vérité technique plutôt que réglementation économico-politique. Dans ce cas-là, il semble que le protocole en lui-même comporte une capacité d'influence et de détermination du comportement de l'utilisateur.

Ces différentes critiques sont donc toutes des manières d'exposer limitations et alternatives à un objet donné à un moment donné, se focalisant souvent sur un ou plusieurs points majoritaires. La critique sémantique est

[1] Des analyses notamment confirmées par Dominique Cardon.

argumentative, et offre des stratégies discursives, la critique légale déploie un appareil d'arguments valides en termes législatifs, et la critique programmatique promeut l'utilisation de de dispositifs d'actions (dont les logiciels font partie) pour remédier aux limitations identifiées de manière pratique. Le type de critique sur lequel je vais me pencher ici est celui de la *critique protocolaire*.

Partant du principe, selon Galloway, qu'un protocole encode des manières de faires qui contraignent ses utilisateurs à la suivre sous peine d'être exclus de la communication se déroulant à travers ce protocole[3], j'envisage ici la critique protocolaire comme la conception et la distribution d'infrastructures abstraites (devant être implémentées *a posteriori*) qui addressent les limitations identifiées d'une infrastructure existante.

De ce question de critique protocolaire découlent plusieurs questions que nous aborderons à travers la comparaison de deux études de cas: celle du protocole IPFS (Interplanetary Filesystem) et celle du protocole SSB (Secure Scuttlebutt). Il s'agira d'examiner, dans les deux cas, les capacités expressives des protocoles numériques en tant que sous-ensemble des systèmes computationnels, en se basant notamment sur les travaux d'Ian Bogost en rhétorique procédurelle[2], ainsi que les possibilités de déterminisme technologique en comparant les usages abstraits imaginés par le protocole et ses implémentations concrètes, et donc de considérer à quel point ces protocoles proposent des nouveaux imaginaires possibles pour l'échange d'information sur des réseaux numériques, notamment quant aux façons d'imaginer, techniquement, l'espace et le temps. Comment se constitue une critique protocolaire? Quels sont les environnements, documents et actions sociales, économiques et techniques qui doivent être déployés pour subvenir à la pérennisation d'un protocole?

Afin d'élucider ces questions, nous procéderons à une analyse du discours des deux écosystèmes d'IPFS et SSB. Ces écosystèmes comportent

[2] Ian Bogost

des éléments discursifs décrivant leurs protocoles respectifs tant au niveau normatif (le protocole en lui-même), que prescriptif (les usages imaginés par les concepteurs), descriptif (la représentation du projet à travers sites webs, entretiens dans la presse et promotion individuelle) ou encore argumentatifs et participatifs (discussions entre concepteurs et utilisateurs autour des intentions et usages des protocoles). Le cadre d'interprétation de ces documents est donc celui d'une analyse critique du discours, telle qu'elle est développée par Dianna Mullet[3], partant de l'hypothèse que ces différents facettes du discours d'une même organisation permet alors de mettre à jour une certaine cosmogonie suggérée avec, à sa base, un protocole comme élément socio-technique similaire.

Cette approche d'analyse critique du discours a lieu au sein d'une analyse comparative, et cela pour deux raisons. Premièrement, il s'agit de mettre en exergue les éléments communs au déploiement d'un protocole: pendant technique, pendant communicationel, et pendant social, et de voir comment le contenu et la forme de ces éléments peuvent varier selons les présupposés des concepteurs. Deuxièmement, il s'agit de considérer de considérer l'implication d'un même but (communication d'un message d'un émetteur à un récepteur), avec un même algorithme (SHA-512) et d'observer à quel point ce but et ce moyens résultent, ou non, en des conséquences drastiquement différentes.

Il s'agira donc d'approcher le sujet en deux temps. Tout d'abord, nous examinerons les visions paradigmatiques des deux projets, en commencant par IPFS, suivi de SSB. Ces examinations se feront de manière identique, à travers la description du protocole, puis l'identification du mythe fondateur, et du support technique et discursif de ce dernier, pour enfin conclure sur l'applicabilité et les possibles limites de la confrontation au réel que chaque protocole présente. Ensuite, nous approfondirons notre comparaison en considérant: (1) la composante spatio-temporelle telle qu'elle est impliquée

[3] À l'exception du fait de légitimer, non pas des inégalités sociales, mais des choix techniques.

dans chaque protocole, (2) les propriétés d'un tel mode de critique.

2 IPFS: une disponibilité permanente de l'objet

2.1 Description du protocole - 700

L'*InterPlantery File System*, ou système de fichiers interplanétaires est un protocole de distribution d'information qui considère comme primordial la disponibilité permanente de tout objet, et oriente donc son organisation technique dans cette optique. La première version du protocole est spécifiée en 2014 par Juan Benet, sous la forme d'un *white paper*, publication scientifique distribuée sur le site communautaire arXiv.org. Ce document est fondateur de l'approche d'IPFS, un projet lui-même constitué d'un amalgames de protocoles existants, régulant la création et la vérification d'identité de chaque pairs, la connection et la localisation de pairs au sein du réseau, l'échange d'information, la représentation des objets conservés par les pair, intégrant étroitement les questions de versions et de nomination.

Ce que cela signifie, c'est que IPFS recombine des technologies existantes pour permettre la disponibilité à tout un chacun d'un unique ensemble de fichiers à travers le globe. D'après les termes de Juan Benet,

> IPFS is similar to the Web, but IPFS could be seen as a single BitTorrent swarm, exchanging objects within one Git repository. In other words, IPFS provides a high through-put content-addressed block storage model, with content-addressed hyper links. This forms a generalized Merkle DAG, a data structure upon which one can build versioned file systems, blockchains, and even a Permanent Web.

Ce que nous notons *a priori*, c'est donc un enchevêtrement de technologies, néanmoins pour pallier aux limitations identifiées du web actuel, un

web considéré comme éphémère et temporel, l'antithèse du but d'IPFS—le web permanent. Quelles sont alors les technologies nécéssaires pour développer ce web permanent? Elles sont au nombre de quatre: une DHT, *Distributed Hash Table*, un système d'incitation de partage BitSwap, et une représentation d'objets à travers un graphe acyclique de Merkle, eux-mêmes accédés à travers une infrastructure de clés publiques. Ces innovations techniques vont se combiner pour réaliser la vision d'un protocole assurant un partage de l'information global et permanent, intégrés au système de fichiers "normal" de l'utilisateur.

L'infrastructure de clé publique permet avant tout d'adresser les objets désirés par leur *contenu* plutôt que par leur *addresse*, un choix sur lequel nous reviendrons rapidement, afin de pallier à la disparition du contenu à l'adresse spécifiée—un phénomène manifesté sous la forme d'une erreur 404 par le protocole HTTP. Les identifiants uniques de chaque objet sont ensuite répertoriés, de manière distributive, sur cette DHT, de sorte à ce que chacun des membres du réseau contiennent la liste des objets disponibles, contrairement au système DNS d'Internet, qui fonctionne de manière hautement centralisée. Le transfert des objets se fait ensuite par le méchanisme BitSwap, qui récompense les membres du réseaux partageant le plus de contenus, et pénalisant ceux qui ne le font pas, à travers un système de dettes et de crédits. Enfin, la représentation de ces objets (qui peuvent être un fragment de texte, un fichier MP3, une section d'image, etc.) est *immuable*.Cela signifie que chaque objet, une fois inscrit au sein du réseau, ne peut être supprimé par son auteur, et ne disparait qu'une fois que tous les membres du réseaux ont cessé de l'héberger. Si une version subséquente de cet objet est ajoutée sur le réseau, il s'agit d'un tout nouvel objet, avec une nouvelle addresse, et existe donc en parallèle de l'objet précédent.

Le résultat est donc un protocole de communication assurant la disponibilité de chaque objet accessible par n'importe quel membre du réseau, aussi longtemps que ces membres décident de le conserver.

Avant de se tourner sur les manières dont ce protocole est présenté, penchons-nous d'abord sur les applications pratiques d'un tel protocole. La documentation du site IPFS propose une liste exhaustive de cas d'usages, potentiels ou déjà réalisés. On y retrouve notamment le partage de fichiers par un individu, de la collaboration en temps-réel sur le même fichier ou encore l'utilisation comme messagerie. Cependant, la principale raison d'être d'IPFS est bien celle d'un protocole, c'est-à-dire en tant qu'infrastructure afin d'héberger, gérer et distribuer du contenu à travers le monde—par exemple, Netflix étudiait en 2021 la possibilité de synchroniser ses conteneurs Docker à l'échelle globale via IPFS[4]. Le dernier champ d'application de l'IPFS est celui des dApps, ou applications décentralisées traditionellement basées sur des systèmes de blockchain, ce qui annonce une certaine contingence de l'écosystème des blockchains avec celui d'IPFS.

2.2 IPFS: vision du monde et réalité

La raison d'être d'un tel protocole garantissant accès universel et atemporel à tout utilisateur est basée sur quatre critiques de l'Internet actuel, et toutes reliées au concept d'architecture centralisée. Tout d'abord, l'Internet actuel est considéré comme inefficient en termes de coût par bande passante, du fait de son architecture client/serveur centralisée. Cette même architecture centralisée est prone à la disparition d'un document lorsque ce dernier n'est plus hébergé par le serveur central. Enfin, le développement économique de l'Internet et du Web aujourd'hui tendent à une centralisation et un monopole de l'accès à l'information qui sont considérées comme un obstacle à l'innovation.

Déjà, nous voyons dans ces critique que certaines sont des critique technologiques valides (questions de bande-passante et de pérennité du contenu en ligne), mais les deux dernières sont plus floues, et plus difficilement attribuables à une technologie plutôt qu'à un ensemble de dé-

[4] https://blog.ipfs.io/2020-02-14-improved-bitswap-for-container-distribution/

cisions économiques, telles qu'identifiées par Lessig. Néanmoins, la vision du monde proposée par IPFS est celle d'un réseau de connexions perpétuel et quasi-instantané. Là où l'Internet établit une relation de hiérarchie entre serveur et client, en ce que le client est subordonné aux politiques d'autorisation du serveur (notamment par la composante des *headers* du protocole HTTP), IPFS permet à chacun d'accéder à tout en permanence, puisque chacun est responsable à titre égal de la mise à disposition de l'information du réseau.

D'une certaine manière, le protocole IPFS propose donc une approche solidaire de la distribution d'information, faisant la part belle au contenu plutôt qu'à l'adresse de ce contenu[5]. La réponse critique apportée aux limitations d'Internet mentionnées plus haut—lenteur et disparition—est donc radicalement opposée. Il s'agit désormais de faire en sorte que chaque objet mis à disposition sur le réseau puisse y rester tant qu'au moins un individu décide de le fournir au réseau, en se reposant sur le peer-to-peer, un protocole aussi mentionné dans le *white paper*. Cette emphase revêt un caractère particulier lorsque Benet compare IPFS au rêve originel du Web, par lequel Tim Berners-Lee imagine un réseaux de pairs[6]. Et pourtant, nulle part dans les spécifications HTTP 1.0 et 1.1 figurent la mention de pairs, ou d'échange réciproque d'information. Cela semble alors être une sorte de révisionnisme historique, peut-être influencé par le projet du créateur du Web, Solid[7].

IPFS addresse également le problème d'incitation à la distribution d'un contenu qui n'est pas celui que l'on possède, ou que l'on désire. Sous le régime protocolaire du web, le serveur est toujours considéré comme ayant un intérêt à distribuer son propre contenu, tandis que le client sait qu'il s'addresse à un serveur spécifique afin de récupérer un contenu spé-

[5]Par exemple, la différence entre *Madame Bovary* et *843.809 FLAU DUME* du système d'adresse Dewey.

[6]https://docs.ipfs.io/project/history/

[7]https://www.inrupt.com/one-small-step-for-the-web

cifique. Un réseau distribué doit, lui, se reposer sur le partage constant d'information qui n'est pas immédiatement pertinente aux utilisateurs les hébergeant—et donc sans incitation. Afin de pallier à cette limitation, IPFS propose BitSwap, une manière d'accumuler du crédit ou du débit en tant que réputation, au sein d'une logique de libre-échange, dont l'auteur lui-même reconnaît dans le white paper qu'elle serait particulièrement adaptée à une cryptomonnaie, qui sera développée sous la forme d'un FileCoin au même moment qu'IPFS[8]—la motivation première du partage de contenu est donc financière.

Nous voyons donc qu'IPFS en tant que protocole promeut la permanence du contenu hébergé sur la plateforme indépendamment du ou de la propriétaire, considérant qu'une telle permanence peut être accomplie par le biais d'incitation monétaire à travers une cryptomonnaie. Le système de FileCoin propose actuellement un espace de stockage de 39 Petabytes pour un peu plus de 818000 objets distincts, soit une moyenne de 53 Gib par objet. Si le protocole d'incitation marche, c'est alors l'utilisation de ce protocole qui va nous intéresser. En effet, comme le dit Tony Willenber en 2016, dans sa présentation d'IPFS:

> The IPFS is not just a theoretical or academic experiment. It is a working software system (although still in alpha) that can be downloaded and switched on right now. *Tony Willenberg*

Si une des vertus de la critique protocolaire est d'être pratique et immédiate, de se manifester directement en des produits et des usages, ce sont vers ces usages, et le rapport qu'ils ont avec la vision originelle du protocole, que nous nous tournons.

[8] https://filecoin.io/filecoin-jul-2014.pdf

2.3 Applications

problem with censorship - https://www.youtube.com/watch?v=HUVmypx9HGI - also he says ”technologies get adopted because you make the thing faster” - kinda true in ssb (first load) but not always true

References

[1] Roy T. Fielding and Julian Reschke. Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing. Request for Comments RFC 7230, Internet Engineering Task Force, June 2014. Num Pages: 89.

[2] Lawrence Lessig. *Code and Other Laws of Cyberspace*. Basic Books, Inc., USA, 1999.

[3] Alexander R. Galloway. *Protocol: How Control Exists after Decentralization*. Leonardo. MIT Press, Cambridge, MA, USA, February 2004.