

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

Pierre Depaz

Paris-3 Sorbonne-Nouvelle - THALIM

February 18, 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 initialement 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 façonner l'évolution de l'Internet et du Web: des forces légales, marchandes, sociales et technologiques<sup>1</sup>.

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 licences Creative Commons, dans la lignée de GPL et licences copyleft, il n'en reste pas moins que les forces technologiques peuvent influencer fortement les possibilités d'agir des utilisateurs de ces dernières. Par exemple, Harsh Gupta s'interroge sur le manque de représentation des continents africains, sud-américains et asiatiques (respectivement 0%, 0% et 0%) lors des délibérations 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 économique-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

---

<sup>1</sup>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 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 faire 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 adressent 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 procédurale<sup>2</sup>, d'examiner 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

---

<sup>2</sup>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, partant de l'hypothèse que ces différentes 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 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 communicationnel, et pendant social, et de voir comment le contenu et la forme de ces éléments peuvent varier selon 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.

et maintenant dire le plan

## 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.