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

Pierre Depaz

Paris-3 Sorbonne-Nouvelle - THALIM

February 28, 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[4] ou les législations de la RGPD ou du DGA; ou encore critiques programmatiques, telles que les bloqueurs de publicités[5] ou des applications liées à des performances politiques[6]. 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[7]. 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 et les limitations et les alternatives à un objet donné à un moment donné, se

[1] Des analyses notamment confirmées par Dominique Cardon[3].

focalisant souvent sur un ou plusieurs points contentieux majoritaires. La critique sémantique est 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 et computationelle. 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[8], 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[9], ainsi que les possibilités de déterminisme technologique en comparant les usages abstraits imaginés par le protocole avec 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, et plus spécifiquement quant aux façons de considérer, 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 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[10], 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 principe technique (chaîne d'information cryptographiée) et d'analyser à quel point ce but et ce moyens résultent, ou non, en des conséquences culturelles (c'est-à-dire de récits imaginaires communs) ou pratiques (en types et nombres d'applications développées) 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 la mise en pratique et les possibles limites de la confrontation au réel que chaque protocole présente avec travers ses applications. Ensuite, nous approfondirons notre comparaison en considérant la composante spatio-temporelle telle qu'elle est impliquée dans chaque protocole, et les impli-

cations d'une telle comparaison en ce qui concerne le déterminisme des technologie.

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 vers 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, et révèle que c'est un projet lui-même constitué d'un amalgames de protocoles existants, afin notamment de réguler la création et la vérification d'identité de chaque pair du réseau, la connection et la localisation de pairs au sein du réseau, l'échange d'information entre pairs, et surtout la représentation des objets conservés par les pairs, intégrant étroitement les questions de versions et de nomination, dans ce qui est considéré un des piliers de l'approche IPFS, le *content-addressing*[11]. Bien que sa nature décentralisée rend difficile son utilisation exacte, IPFS avait environ 40,000 noeuds dans le réseau en 2020[12].

IPFS recombine des technologies existantes dans une approche holistique, puisant depuis divers domaines de la cryptographie et de la théorie des graphes, pour permettre la disponibilité à tout un chacun d'un seul ensemble globalisé de fichiers. 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, pour pallier aux limitations identifiées du web actuel. Celui-ci est considéré comme éphémère et temporel, l'antithèse du but d'IPFS—le web permanent et l'accessibilité universelle de toute information[2]. Parmi ces technologies, on voit surtout 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, mais comportent aussi d'autres implications sociales qui vont venir se heurter à la vision du protocole.

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, afin de pallier à la disparition du contenu à l'adresse spécifiée—un phénomène manifesté sous la forme de la familière 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 héberge la liste des objets disponibles, contrairement au système DNS d'Internet, qui fonctionne lui de manière hautement centralisée[3]. 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 sys-

[2] emph"A web where [...] publishing valuable information does not impose hosting it on the publisher but upon those interested, where users can trust the content they receive without trusting the peers they receive it from, and where old but important files do not go missing.[11]

[3] DNS est aussi étroitement lié à des organisations gouvernementales et économiques, tel que l'ICANN

tème de dettes et de crédits[4]. 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.

Cette permanence, c'est-à-dire la disponibilité de chaque objet accessible par n'importe quel membre du réseau, aussi longtemps que ces membres décident de le conserver, est donc rendue possible par des techniques liant unicité de l'objet et mécanismes économiques de partage basé sur des dynamiques de marché, afin de pallier à ces myriades d'erreurs 404 du Web contemporain.

2.2 IPFS: vision du monde et réalité

Les raisons pour lesquels IPFS cherche à garantir un accès universel et atemporel à tout utilisateur est basée sur quatre critiques de l'Internet actuel, et toutes reliées au concept d'architecture centralisée, telle que Benet l'explique dans une de ses premières interventions publiques en 2016 à Stanford[13], puis en 2019 à IPFS Camp[11]. Il y a, au sein de la manière dont IPFS se présente, une dimension téléologique indéniable: lors de sa présentation à la première conférence IPFS, il y passe les dix premières minutes à inscrire IPFS dans la directe lignée des 10 millions d'années d'existence de l'espèce humaine[5]. Pour compléter cette approche darwinienne, il pose alors le Web actuel comme inefficient en termes de coût par bande passante, du fait de son architecture client/serveur centralisée. Cette même architecture centralisée est effectivement consid-

[4] Comparé au système d'échange *tit-for-tat* de Bittorrent.

[5] Allant notamment jusqu'à considérer que la technologie de l'écriture a permis l'évolution de la culture.

érée prone à la disparition d'un document lorsque ce dernier n'est plus hébergé par le serveur le fournissant. Enfin, il est considéré 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 que certaines sont des critiques 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 décisions socio-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. Puisque chacun est considéré responsable à titre égal de la mise à disposition de l'information du réseau, IPFS permet à chacun d'accéder à tout en permanence, 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).

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[6]. 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[14]. 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

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

créateur du Web, Solid[15].

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 spécifique. Un réseau distribué doit, lui, se reposer sur le partage constant d'information, y compris une information qui n'est pas immédiatement pertinente aux utilisateurs les hébergeant—et donc sans incitation intrinsèque. En universalisant les contenu, on dépersonalise donc le rapport au contenu et sa responsabilité. 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 (*marketplace*, selon les termes de la documentation[16]), et dont l'auteur lui-même reconnaît dans le white paper qu'elle serait particulièrement adaptée à une cryptomonnaie. Celle-ci sera développée sous la forme d'un FileCoin au même moment qu'IPFS[17]—la composante principale du partage de contenu est donc d'inspiration financière—un système de troc tel que BitTorrent ne fonctionne plus dès lors qu'il s'agit d'acquérir une multiplicité de fichiers, plutôt qu'un seul.

Ce que nous voyons donc ici, c'est que le protocole IPFS vise à 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 financière à travers une cryptomonnaie, et non à travers la manière dont HTTP le faisait, c'est à dire la responsabilité individuelle de l'hébergeur, ou la manière de BitTorrent, en se focalisant sur un seul fichier et un traqueur d'information centralisé. Le système de FileCoin propose au 01/02/2022 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, dans le sens où il y a bien un vaste espace de mémoire mis-à-disposition, c'est alors l'utilisation de ce protocole

qui va nous intéresser—ce qui est fait de cet espace de mémoire. 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.[18]

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 afin d'analyser la cohérence ou discordance entre théorie et pratique.

2.3 Applications

Après s'être penchés 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[**?**]. Plus particulièrement, IPFS concentre son 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.

Cette vision d'un monde qui serait mieux si toute information était permanente se reflète dans plusieurs types d'applications. D'une part, Juan Benet présente dès 2014 le travail de l'*Internet Archive* comme étant es-

sentiel dans le développement des connaissances humaines à l'ère informatique. Un projet est donc ouvert sur GitHub où les développeurs et dévloppeusent discutent de l'implémentation en 2015, avant qu'il soit abandonné en 2017, au mêne moment que se pose la question de "qui" va héberger cette archive—nominativement la communauté IPFS, mais en pratique les employés de Protocol Labs[7], retournant donc à un hébergement centralisé. Si cette entreprise échoue pour des raisons pratiques, une autre application du protocole se déroule lors de la copie du site turc de Wikipedia sur IPFS alors que la version HTTP est censurée par le gouvernment Erdogan. Dans ce cas précis, il s'agit alors d'une mise en place à responsabilité individuelle (une initiative d'un développeur de nationalité turque), récupérée ensuite par Protocol Labs. Si leur annonce sur leur blog[8] se targue d'etre pair-au-pair et décentralisée, l'organisation est, en pratique, encore une fois sla seule à héberger ce contenu, qui devient donc centralisé et client/serveur.

La question de la censure se pose à l'inverse pour le reste du contenu hébergé sur IPFS. En effet, le protocole se base sur l'immutabilité des contenus, ce qui mène donc à la conséquence de second-ordre de suppression de contenu illégal. Un problème compliqué résumé sur le répositaire GitHub du projet par l'utilisateur *geebotron*, à propos de la modification des fichiers disponibles:

> Every single file that could exist on IPFS has the potential to offend someone. [9].

En effet, la conception d'un protocole sur la permanence d'une information se heurte alors de manière frontale à la question de la censure et de la propriéte intellectuelle. Mis face à l'existence de législation regardant la propriété intellectuelle, la réponse d'IPFS est donc de développer

[7] Voir notamment les dicussions sur https://github.com/ipfs-inactive/archives/issues/88

[8] https://blog.ipfs.io/24-uncensorable-wikipedia/

[9] `https://github.com/ipfs-inactive/faq/issues/36#issuecomment-217677401`

un soit un protocole additionnel (*une whitelist*) pour déterminer l'utilisation des fichiers, ou plus simplement en fermant la conversation:

> It is not my intention to start a political philosophy discussion—but rather only to articulate the design space and why IPFS falls in a particular set of decisions. If the issue gets more off topic, i'll just close it, or rename it.[19]

Enfin, la question de l'applicabilité du protocole BitSwap se retrouve dans le développement de services d'entreprise centralisés[10]:

> "If you don't pin your content to IPFS, it goes bye-bye. And if the server pinning your resources ever goes offline and no one else has it pinned, it's gone forever. That's why a market has opened up for services like Pinata, which aim to be permanent pinning services. So you still end up with a centralized business framework even if the technology itself is decentralized, in that, if you don't have the means to provide your own distributed infrastructure, you're going to have to pay someone who does."

En fin de compte, ce que nous voyons dans ce développement, c'est que la réalité technique d'IPFS est soit non-avenante (cf. les mesures d'hébergement de l'Internet Archive), soit centralisée au niveau économique plus qu'au niveau technique, allant jusqu'à ressembler aux protocoles de libre-échange BitSwap. Ayant observé l'insertion sociale d'un protocole technique, nous nous tournons désormais vers la description technique d'un protocole social, SSB.

[10] `https://www.reddit.com/r/ipfs/comments/ruxlej/ipfs_is_an_alternative_for/`

3 SSB: implémentation technologique d'un protocole social

3.1 Description

SSB (ou Secure Scuttlebutt) est un protocole de communication créé par Dominic Tarr en 2014, la même année qu'IPFS. Alors que Juan Benet est un développeur issu de la Silicon Valley, Tarr est un navigateur néo-zélandais qui pose la disponibilité hors-ligne, ainsi que la nature sémantique des objets comme messsages, en tant que fondation du protocole, sous le terme de (*local first*). Face aux même difficultés de mesures que présente tout système décentralisé, les membres de l'organisation autour de SSB (le *Secure Scuttlebutt Consortium*) estiment à la fin de 2019 le nombre de pairs sur le réseau à au moins 10,000[20].

SSB, tout en étant un protocole de communication et de distributions de fichiers, tout comme IPFS, se démarque alors tout d'abord par son positionnement dans la famille des *gossip protocols*, des protocoles de ragots. Ceux-ci sont basés sur la distribution des rumeurs, ou des épidémies, essentiellement une sélection au hasard des pairs à qui l'information va se propager. L'approche est donc posée: il s'agit de définir un protocole technique comme simulation de phénomènes naturels, partant du principe que l'*information va avoir, en son sein, des schémas sociaux*[21].

SSB pose donc comme axiome de départ la disponibilité hors-ligne: le protocole et ses applications doivent être utilisables lorsque l'on n'est pas connecté à l'Internet, du fait que les personnes sortant en mer, telles que le créateur du protocole, n'ont plus accès à ce réseau. Ainsi, tout stockage et accès de données se fait uniquement de manière locale, et la mise à jour, ou synchronization de ces données vont être effectués quand, et si, il y a une connexion effectué à un ou une autre membre du réseau. SSB réplique, de manière protocolaire, l'expérience d'une vie en mer, expérience locale si il en est, en ne permettant la synchronisation entre deux pairs que

si ceux-ci sont connectés au même réseau LAN.

SSB est également un protocole décentralisé de partage de données. Il fonctionne par pairs qui s'assignent une signature cryptée, afin de constituer leur identité—si on perd sa clé, on perd tout accès à son compte, corrélat de la responsabilité de l'utilisateur de ses propres données. La manière dont les pairs se découvrent, en revanche, ne se situe qu'au niveau local, c'est à dire qu'ils émettent des paquets UDP (une alternative au paquest TCP de l'Internet) jusqu'à ce qu'ils soient reçus par un autre pair. Une fois que la connexion est établie entre deux pairs, un échange de messages ou de blobs (*binary large objects*). Il est également possible de se connecter à un pair à travers un portail Internet, il ne s'agit donc pas directement d'une critique protocolaire qui cherche à remplacer HTTP, mais plutôt à le complémenter[11].

Enfin, les messages eux-mêmes sont basés sur une conception similaire à la blockchain, et à une utilisation semblable du versionnage des fichiers d'IPFS. Chaque message est relié cryptographiquement au message précédent et au message suivant, formant donc non pas une *chain*, mais un *feed* (flux). De cette manière, les objets ne sont plus uniquement considérés comme étant des entités flottantes, uniques, mais bien des entités relationelles qui tirent leur nature sémantique de leur contexte social.

SSB est donc un protocole qui se base sur des phénomènes naturels, et qui conditionne avant tout la décentralisation non pas à l'étendue universelle, mais bien à la responsabilité *locale*, manifesté dans le protocole même par une préférence pour UDP comme signalétique, par une relation cryptographique, et par un stockage local de toutes données. Les discours autour de SSB renforcent cette préférence pour une approche sociale plutôt qu'une approche technique.

[11] Ceux-ci existent sous forme de *pub*, jeu de mot entre "bar" et "publiciste"

3.2 Communication

Le discours de SSB et la manière dont est présenté le protocole est un miroir intéressant d'IPFS: plutôt qu'une démonstration technique, il s'agit plutôt de prendre un cas d'étude, une relation amoureuse, pour montrer comment SSB supporte une conception intime de la communication, plutôt qu'une conception technique[22]. La page de documentation du site de SSB, au lieu de se présenter sous la forme d'un article académique publié de manière autonome sur un site de recherche scientifique, accueille la visiteur avec le message suivant:

> Scuttlebutt aims to harmonize four perspectives of life: Environment reflecting Technology reflecting Community reflecting Society.
>
> We acknowledge the natural, the virtual, and the social environments. Our responsibility is to recognize which resources are abundant, which are sufficient, and adapt accordingly through efficiency.

Alors, en effet, il y a également une possibilité de consulter une documentation plus poussée et plus rigoureusement technique, ainsi que l'article présentant le protocole SSB, publié dans les annales de la conférence Information-Centric Networking de l'ACM en 2019[23]. Cependant, il est intéressant de s'arrêter sur ce premier message d'accueil. Au vu de la place attribuée au terme *technologie*, coincé entre *environnement* et *communauté*, la position est bien plus relationelle que le *protocole hypermedia concu pour préserver et développer le savoir de l'humanité* d'IPFS, holistique et donc auto-suffisant.

Nous pouvons identifier cette prise de parole par une emphase sur la relation entre deux agents. Déjàm la première version du protocole SSB se base sur un article de Tarr considérant le problème d'authentification et

d'échange d'informations entre deux pairs[12] plutôt que sur la représentation d'une information. De cette manière, si ces deux protocoles, IPFS et SSB considèrent tous deux la mise en place d'un système de communications, IPFS se focalise sur ce qui est communiqué (messages/objets comme membres d'un graphe acyclique dirigé), tandis que SSB se focalise sur les individus voulant échanger un message.

En tant que critique, c'est un double présupposé fondamental d'un internet *contemporain* que SSB critique: l'idée que toute information, et donc tout membre du réseau qui héberge ou demande une information, doit être disponible en permanence et à l'échelle globale. Ce présupposé, considèrent Tarr et ses collaborateurs, a notamment des répercussions sur l'autonomie des membres du réseau par rapport à l'influence de monopoles économiques, et à laquelle ils veulent redonner une prépondérance (ce *local first* mentionné plus haut) par le biais d'une propagation par défaut sur un réseau local que par réseau global[13].

Comme le développe Zach Mandeville dans son essai financé par SSB *The Future Will be Technical*, on note également dans l'écosystème SSB une croyance non seulement en le développement des technologies pour améliorer le futur, mais également une prise en compte de la technique en tant qu'élément de la culture:

> Dev discussions and tutorials are an essential part of our community, and should not be obscured or downplayed[24].

La technique est ici un élément fortement culturel et l'adhésion à un protocole est donc une adhésion à une vision partagée du monde, à un imaginaire collectif[25]. En conséquence, le champ d'application évolue aussi. De manière symmétrique à la perception d'IPFS, qui veut un protocole qui

[12] Voir l'article mis à disposition ici: https://dominictarr.github.io/secret-handshake-paper/shs.pdf

[13] Voir notamment le commentaire d'Ian Bogost sur le sujet, consultable à `https://www.theatlantic.com/technology/archive/2017/05/meet-the-counterantidisintermediationists/527553/`

concerne l'univers entier, SSB s'addresse au *Scuttleverse*. On peut considérer ce *Scuttleverse* comme une cosmos qui est mis au monde par le biais d'un lien technique basé sur un lien social—où, par exemple, les *groupes d'utilisateurs* s'appellent des *tribus*, rappelant les travaux de Yuk Hui sur la cosmotechnique, quant à cette capacité des systèmes techniques de supporter des manières d'être, de faire et de penser des utilisateurs de cette technologie.

Cette étroite connexion entre technologie et culture, cette considération du protocole comme artefact relationnel, se manifeste également dans la documentation du protocole. Celle-ci oscille entre rigueur technique et clins d'oeil charmants: présentation de la documentation comme une *carte au trésor*, ou encore la représentation de l'échange de clés cryptographiées comme relation érotique[14].

Enfin, un dernier example comparatif se trouve dans la manière dont ces protocoles font vivre leur communauté, notamment en termes d'évenements organisés pour du *community-building*. Pour les deux protocoles, cela se manifeste sous formes de camps. Le *IPFS Camp* consiste à rencontrer des *pionniers*, prêts à *hacker* pendant cinq jours, le tout sponsorisé par des entrerprises dont IPFS est le fond de commerce[15]; tandis que, de sont côté, le *Scuttlebutt Camp* est un rassemblement sans véritable fin déterminée, ni agenda particulier[16]. Même si la pandémie de la Covid-19 a été responsable de la non-tenue de ces évènements, nous voyons toujours la différence entre IPFS et SSB en termes de différences entre contenu et individus, but et procédé.

[14] Voir le visuel suivant: `https://dev.scuttlebutt.nz/assets/handshake-erotica.png`

[15] Voir aussi https://camp.ipfs.io/

[16] La version SSB se trouve à l'addresse suivante: https://two.camp.scuttlebutt.nz

3.3 Applications

Autant SSB et IPFS proposent directement une implémentation des clients (c'est-à-dire de logiciels manifestant les protocoles sous leur forme concrète et active), autant les domaines d'application de SSB sont beaucoup plus concentrés que ceux d'IPFS. Tandis qu'IPFS, fidèle à sa vision d'expansion globale, privilégie la quantité d'applications possibles (plus de 55 listées sur le site d'IPFS[17]), SSB se concentre sur la qualité, en ne listant qu'une application principale suggérée: un réseau social—c'est à dire un échange de messages entre personnes individuelles (SSB présente 32 applications, dont 13 autour du concept de réseau social[18]).

Cette visée de l'application est clairement établie dès les premières pages de "comment rejoindre SSB". Sans rentrer dans les détails du protocole, sont proposées directement les différentes applications pour rejoindre le *Scuttleverse*, avec en second plan le genre d'applications qui découlent de l'implémentation d'un protocole techniquement plus large que ses visées sociales (e.g. contrôle de version de code, maintenance et distribution de bibliothèques de code, allant même jusqu'à rejoindre le rôle d'IPFS par le biais de *ssbdrv*[19], un système de fichiers basé sur SSB.[20]).

Particulièrement, la fin de l'introduction à SSB consiste autant en un type différent de protocole: une fois que l'installation et l'inscription sont finies, le discours de SSB mentionne non pas le protocole technique, mais un protocole social, mentionné par le terme *tradition*, celle de se présenter sur le canal *#new-people*, mettant une fois de plus en avant l'aspect social rendu possible par un protocole, plutôt qu'existant dans une stricte isolation technique.

[17] https://docs.ipfs.io/concepts/usage-ideas-examples/

[18] Voir `https://handbook.scuttlebutt.nz/applications`

[19] https://github.com/cn-uofbasel/ssbdrv/

[20] https://handbook.scuttlebutt.nz/applications

4 Final

Bien que les deux protocoles étudiés ici, IPFS et SSB, soient similaires dans leur intention pratique de développer un protocole permettant la distribution décentralizée et cryptographiée d'information entre pairs d'un réseau, la posture théorique des projets se tient néanmoins en porte-à-faux. Je voudrais donc conclure sur cette tension entre similarité technologique et différences culturelles, entre déterminisme et imagination.

4.1 L'internet, l'espace et le temps

Manuell Castells estimait, dès la fin des années 1990, que la société connectée, société dont les conditions matérielles de réalisation sont TCP/IP et HTTP, a fait entrer une grande partie du monde, dans une ère d'espaces de flux et de temps atemporel (*space of flows and timeless time*)[26]. L'espace de ces sociétés est un espace qui permet, par des moyens technologiques, de réaliser une simultanéité sans pour autant demander une contiguité, accompagné d'une temporalité qui, tendant à l'immédiateté, tend à s'effacer[27].

D'après Castells, même si l'espace se transforme, au début des années 1990, du matériel au dématérialisé, l'inter-opérabilité des lieux de décisions d'élites invisible ces centres d'opérations ne change pour autant pas leur statut de *centres*, de noeuds principaux par lesquels doivent transiter les noeuds secondaires afin de communiquer. Cette situation de réseau centralisé étant elle-même une conséquence tant de dynamiques économiques et de services marchands, que d'un protocole (HTTP) impliquant la limitation de la duplication de l'information hébergée[21].

C'est cette centralization qui est le premier objet des critiques des deux protocoles étudiés ici. Ceux-ci nous montrent cependant qu'une telle situation de simultanéité peut, par ces mêmes moyens techniques, être repen-

[21] Excepté pour ce qui est des téléchargements et des caches

sée de diverses manières, et notamment en prenant en compte les communautés imaginées en tant qu'utilisatrices de ces protocoles, les priorités discursives des mainteneurs et mainteneuses des protocoles, considérant donc de manière plus holistique la conception d'un protocole, son implémentation et ses applications comme éléments indissociables d'un même discours.

D'une part, IPFS suggère que le réseau peut pousser encore plus loin cette dynamique, se basant sur une interprétation particulière de la vision originelle de Tim Berners-Lee, pour aboutir à un dispositif où le réseau est intégré directement dans chaque poste via un système de fichier. De cette manière sont contournés les côtés négatifs de la centralization, notamment la disparition de contenus, et la lenteur de de téléchargement des données va être résolue par un système d'identification et d'accès à ces contenus.

D'autre part, SSB approche le problème sous l'angle inverse. Il s'agit de pallier à l'impératif d'être connecté en permanence, à travers de larges conglomérats économiques, une nécessité qui obfusque la réalité que la synchronisation "authentique" entre individus est toujours repoussée un peu plus, créant un désir d'immédiateté accru, un phénomène théorisé notamment par Dominic Pettman[28]. SSB propose une vision du monde où l'espace et le temps de chacun des membres du réseau n'est pas identique, et où la proximité physique est une condition suffisante à l'échange d'information.

Des positions similaires sur la centralisation, mais opposées sur la mise-à-disposition, donc. IPFS recherche une quasi-universalité (ou, selon leur dires, une inter-planétarité), alors que SSB recherche l'implémentation technique et culturelle d'une priorité au local. Et pourtant, ces deux protocoles, ces deux visions divergentes se basent sur des algorithmes extrêmement similaires, nous permettant alors de nous poser la question du déterminisme technologique en jeu ici.

4.2 Déterminismes socio-technologiques

Dans les deux cas, nous avons à faire à des protocoles basés sur le principe de l'*append-only log*, c'est à dire une suite d'entités qui ne peut que s'accroître, et dont les entités précédentes dans la liste sont immuables. Ces listes immuables le sont rendues par l'utilisation de techniques cryptographique non dissimilaires à celles utilisés par les technologies dérivées de la blockchain. Et pourtant, un protocole est un objet socio-technique qui s'applique également à un *problem domain*, le domaine d'application de l'algorithme au-delà de son aspect strictement technologique et computationnel. La principale différence n'est donc pas la technologie mais le domaine d'application, et le choix de l'application: IPFS applique son protocole au contenu, possédant une relation à d'autres contenus (fichiers ou dossiers), et une relation à soi-même (établissant par la-même l'immutabilité, et la pérennité du contenu en question). À l'opposé, SSB utilise ces outils techniques pour définir l'individu, chaque noeud du réseau, comme propriétaire des l'information—socialisée, c'est-à-dire une chaine d'informations basées sur un graphe social, d'individus concrets.

La communauté d'IPFS, lorsqu'il s'agit de développer des applications pour le protocole, se retrouve toujours à considérer une approche globale, centralisée, pour un moteur de recherche[22], ou encore à s'enquérir d'une architecture de réseau social qui semble être trop compliqué pour être véritablement centralisé[23]. Particulièrement révélateur est un des deux exemples donnés par les membres d'IPFS comme exemple de la résilience du protocole face à la censure: lors du référendum catalan de 2017, le site pour s'enregistrer en tant que que votant ou votante avait été censuré par les autorités de Madrid, et le site avait été mis en ligne sur IPFS en

[22] `https://discuss.ipfs.io/t/would-there-be-an-interest-in-an-ipfs-search-engine/8058/32`

[23] Voir aussi `https://discuss.ipfs.io/t/social-media-architecture-with-ipfs/4625/84` une discussion qui termine en la description d'un service d'hébergement de fichiers, néanmoins avec la mention de SSB et leur appréciation!

tant qu'alternative permanente d'un contenu victime de censure; pourtant, comme le note l'utilisateur Akira:

> Unfortunately, most users back then used the HTTP gateway gateway.ipfs.io 6, which was also censored, but tech-savvier users avoided censorship using a regular IPFS daemon and installing the simple IPFS Companion browser extension. IPFS is now way easier to use.[24]

La technologie était donc là, mais l'usage ne semble pas avoir suivi. De manière plus générale, l'écosystème d'IPFS semble se focaliser plus sur l'existence d'applications, que sur leur usage, tel que le montre également la page *Awesome IPFS*, dont environ la moitié des applications sont désormais désuettes ou non-maintenues[25] sur la centaine de disponible.

Plus qu'un déterminisme technologique, SSB semble incarner une approche mutuellement informative entre technique et culture qui est réminiscente de la théorie de l'acteur-réseau, à travers laquelle protocoles et humains co-existent et co-agissent dans un seul et même système[29]. Tel que le présente la documentation du protocole, ce dernier est efficace non pas strictement par ses vertus techniques mais:

> One of its first applications was as a social network, and it has also become one of the most compelling because the people who hang out there are not jerks.[26]

Cet enchevêtrement entre développements technologiques et interactions sociales est présente dès la genèse de SSB, racontée par Dominic Tarr[27]: il développe des concepts technologiques, les présente et intègre des contributions d'autres individus et collaborateurs, puis développe le

[24] https://discuss.ipfs.io/t/how-censorship-resistant-is-ipfs-intended-to-be/7892/5
[25] https://awesome.ipfs.io/apps/
[26] https://scuttlebutt.nz/docs/protocol/
[27] https://handbook.scuttlebutt.nz/stories/scuttlebutt-genesis

protocole d'avantage, dans un mouvement de balance qui contraste avec l'aspect plus téléologique d'IPFS.

5 Conclusion

Cette étude comparative de deux protocoles nous a, en fin de compte, permis de révéler la manière dont un dispositif technique présente des présupposés profonds quant à la manière dont la communication d'une information doit se dérouler, que ce soit en se focalisant sur le message (IPFS) ou sur les interlocuteurs ou interlocutrices (SSB).

D'autre part, nous avons pu élucider comment cette rhétorique du protocole plus ou moins s'aligner à la rhétorique des utilisateurs (notamment en ce qui concerne la censure sur IPFS, ou en ce qui concerne la centralization des données, ou l'application à des domaines plus spécifiques), et identifier certaines cohérences et incohérences entre les discours autour du protocole et les applications développées par ce protocole.

Finalement, nous avons vu comment ces protocoles entrent en dialogue avec la question du déterminisme technologique, que ce soit sur une trajectoire téléologique (IPFS), ou sur une trajectoire plus écologique (SSB). En fin de compte, donc, une technologie de communication est plus qu'une technologie, c'est aussi une culture.

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] Dominique Cardon. *Culture numérique*. Presses de SciencesPo, March 2019.

[4] Niva Elkin-Koren. Creative Commons: A Skeptical View of a Worthy Pursuit. SSRN Scholarly Paper ID 885466, Social Science Research Network, Rochester, NY, February 2006.

[5] Rohit Gupta and Rohit Panda. Block the blocker: Studying the effects of Anti Ad-blocking. *arXiv:2001.09434 [cs]*, January 2020. arXiv: 2001.09434.

[6] Critical Art Ensemble. Electronic Civil Disobedience & Other Unpopular Ideas, 1996.

[7] Harsh Gupta. (Lack Of) Representation of Non Western World in process of creation of Web standards. *arXiv:1609.01996 [cs]*, August 2016. arXiv: 1609.01996 version: 1.

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

[9] Ian Bogost. *Persuasive Games: The Expressive Power of Videogames*. MIT Press, August 2010. Google-Books-ID: uLdNEAAAQBAJ.

[10] Dianna R. Mullet. A General Critical Discourse Analysis Framework for Educational Research. *Journal of Advanced Academics*, 29(2):116–142, May 2018. Publisher: SAGE Publications.

[11] Juan Benet. IPFS - Content Addressed, Versioned, P2P File System. *arXiv:1407.3561 [cs]*, July 2014. arXiv: 1407.3561.

[12] Sebastian Henningsen, Martin Florian, Sebastian Rust, and Björn Scheuermann. Mapping the Interplanetary Filesystem. *arXiv:2002.07747 [cs]*, February 2020. arXiv: 2002.07747.

[13] stanfordonline. Stanford Seminar - IPFS and the Permanent Web, October 2015.

[14] Protocol Labs. History | IPFS Docs.

[15] Tim Berners-Lee. One Small Step for the Web..., 2018.

[16] Protocol Labs. Bitswap | IPFS Docs, 2019.

[17] Protocol Labs. Filecoin: A Cryptocurrency Operated File Storage Network. Self-published, Protocol Labs, 2014.

[18] Tony Willenberg. IPFS: The Internet Democratised, May 2018.

[19] Juan Benet. Editing/deletion of content and power dynamics - Help / Old FAQ, May 2017.

[20] Zenna Fiscella. 35C3 - Scuttlebutt, December 2018.

[21] Web3 Foundation. Secure Scuttlebutt Peer to Peer Infrastructure by Dominic Tarr at Web3 Summit 2019, September 2019.

[22] Zach Mandeville. A Scuttlebutt Love Story.

[23] Dominic Tarr, Erick Lavoie, Aljoscha Meyer, and Christian Tschudin. Secure Scuttlebutt: An Identity-Centric Protocol for Subjective and Decentralized Applications. In *Proceedings of the 6th ACM Conference on Information-Centric Networking*, ICN '19, pages 1–11, New York, NY, USA, September 2019. Association for Computing Machinery.

[24] Zach Mandeville. The Future Will be Technical.

[25] Stuart Hall. *Representation: Cultural Representations and Signifying Practices*. SAGE, April 1997.

[26] Manuel Castells. *Communication Power*. Oxford University Press, Oxford, New York, July 2009.

[27] Paul Virilio. *Speed and Politics, New Edition*. MIT Press, October 2006. Google-Books-ID: EkDaAAAAIAAJ.

[28] Dominic Pettman. *Infinite Distraction*. John Wiley & Sons, November 2015. Google-Books-ID: bG0BCgAAQBAJ.

[29] Bruno Latour. *Reassembling the social an introduction to actor-network-theory*. Clarendon lectures in management studies. New York: Oxford University Press, 2005.