

Résumé:

IPFS (InterPlanetary File System) est un protocole de stockage de fichiers décentralisé qui permet de stocker et de partager des fichiers de manière efficace. Il utilise une architecture basée sur une adresse de hachage plutôt qu'une adresse IP traditionnelle pour accéder aux fichiers, ce qui permet une résistance aux pannes et une répartition efficace de la charge. Il utilise également un système de stockage en réseau basé sur la technologie de la blockchain pour assurer l'intégrité et l'authenticité des fichiers. En résumé, IPFS est un système de fichiers décentralisé qui permet de stocker et de partager des fichiers de manière efficace et fiable.

Abstract:

IPFS (InterPlanetary File System) is a decentralized file storage protocol that allows for efficient storage and sharing of files. It uses a hash-address based architecture rather than traditional IP addresses to access files, which enables resistance to failures and efficient load distribution. It also employs a blockchain-based network storage system to ensure file integrity and authenticity. In summary, IPFS is a decentralized file system that enables efficient, and reliable storage and sharing of files.

Web 3.0

Le web 3.0 est un terme "flou" mais tend vers l'idée d'un web décentralisé exploitant la technologie de blockchain.

Blockchain: A l'inverse de celle qu'on a dans le web 2.0, c'est-à-dire une base de données centrale qui partage les données avec chaque utilisateur, est une technologie dans laquelle chaque utilisateur possède une copie de la base de données. Un algorithme de consensus est utilisé dans le but de résoudre les conflits et décider d'un accord sur le contenu de la blockchain.

Avant de s'intéresser à cette technologie "futuriste" et la comprendre, il faut remonter aux origines du web.

Les origines : La première idée d'internet

L'idée de base d'internet était d'avoir un réseau de machines interconnectés ou chacun pouvait partager des connaissances en hébergeant un serveur (web par exemple) sur sa machine.

L'internet d'aujourd'hui

Les outils mis en place à l'époque n'étaient pas vraiment adaptés. L'internet d'aujourd'hui est très éloigné de l'idée à la base de son invention.

Voici son fonctionnement actuel: une machine serveur, de puissance bien supérieure, au centre et des machines clientes tout autour. Ainsi, dans la majorité des cas, les machines clientes ne communiquent pas directement entre elles mais passent par le serveur, qui relaye l'information.

Les différentes organisations

Il y a donc plusieurs façons d'organiser les échanges dans un réseau. Chacune possédant ses avantages et ses inconvénients.

Dans l'organisation centralisée il n'y a qu'une machine serveur. Les clients passent par la même machine. Une organisation comme celle-ci est relativement simple à mettre en place mais elle est très inefficace pour plusieurs raisons :

- **La latence:** l'information ne peut être transmise plus vite que la lumière. Si le serveur et le client sont très éloignés, l'information peut mettre du temps à arriver.
- **Le coût:** comme tous les clients sont connectés à la même machine, celle-ci doit être extrêmement performante. Cela demande également un débit internet très important.
- **La fiabilité:** si la machine serveur tombe en panne le site web sera inaccessible jusqu'à ce que cette dernière soit réparée
- **Le monopole:** quelques entreprises possèdent les serveurs, gardent d'énormes bases de données inaccessibles et ont tous les droits dessus. Par exemple, si demain wikipedia décide de tout arrêter, le site ne sera plus disponible et énormément de connaissances seront perdues.

En ce qui concerne l'organisation décentralisée, il s'agit d'une méthode semblable à la première à la différence que le serveur central est découpé en plusieurs serveurs plus petits répartis à différents endroits.

Elle est plus compliquée à mettre en place que la première mais peut être utilisée dans des applications d'une envergure beaucoup plus large. Si l'on prend l'exemple de youtube, il serait impossible de l'héberger de façon centralisée, il n'existe simplement pas de serveur assez puissant.

- Cela règle également en grande partie le problème de la **latence** car les serveurs se rapprochent des utilisateurs. Par exemple, pour un utilisateur en France, il est plus rapide d'accéder à un fichier se situant à Paris qu'à Los Angeles.
- Le **coût** reste cependant très élevé. En effet, il faut plusieurs serveurs, et donc plusieurs bâtiments avec dans chaque bâtiment une équipe de techniciens...
- De plus, cette méthode est plus **fiable**. Si un serveur tombe en panne, un autre pourra prendre le relai immédiatement.
- En revanche, elle ne change rien au problème du **monopole**.

La dernière méthode est celle à laquelle nous allons nous intéresser: l'organisation distribuée.

- Il n'y a pas de serveur, on récupère les fichiers sur l'ordinateur de la personne la plus proche qui en possède un exemplaire. La latence est donc minimale.

- Pour la même raison, il n'y a aucun coût et aucun risque qu'un serveur soit inaccessible.
- Le problème du monopole est également résolu puisque les données appartiennent à tout le monde et chacun peut décider de les sauvegarder et de les redistribuer.

IPFS

IPFS signifie **InterPlanetary File System** ou **Système de Fichier InterPlanétaire** en français. IPFS est un ensemble de protocoles visant à remplacer http qui a été désigné pour permettre le web distribué. Il est inspiré de plusieurs technologies récentes comme les hashtable distribuées, le protocole bittorrent, git, ou les blockchain

Adressage

La principale caractéristique d'IPFS est la manière dont sont adressés les fichiers. HTTP adresse les fichiers par adresse IP. Ce qui permet d'aller chercher le fichier sur une machine spécifique.

IPFS adresse les fichiers par contenu, peu importe où ils se trouvent. Le fichier est passé dans une fonction de hachage. Cette fonction va par la suite générer une clé unique qui identifie le fichier, autrement dit une signature numérique. Ainsi, si une personne, même à l'autre bout du monde, hache le même fichier, elle aura exactement la même clé IPFS. IPFS peut donc ensuite retrouver qui possède le fichier correspondant à cette clé.

Proximité

Un avantage à cela est la proximité des données. Avec HTTP, un ordinateur ira toujours chercher un fichier à la même source tandis qu'avec IPFS, une fois qu'un ordinateur a téléchargé un fichier, il pourra lui aussi participer à sa distribution. Cela permet de télécharger le fichier depuis la machine (voir les machines pour les gros fichiers) la plus proche ce qui permet de réduire la latence. C'est donc de cette propriété que vient le nom de "Système de Fichier InterPlanétaire".

Si quelqu'un voulait accéder à internet depuis mars par exemple, il y aurait entre 3 et 20 minutes d'attente pour charger une simple page internet, avec des périodes d'indisponibilité quand mars est hors de portée. IPFS résoudrait en grande partie ce problème en ayant des copies des fichiers sur place au lieu d'aller les chercher sur un serveur terrestre.

Persistance

Un argument important mis en avant par les créateurs d'IPFS est la persistance des données. En effet, même si la personne qui a publié les données à l'origine les supprime, elles seront toujours accessibles avec le même lien si au moins une personne les a sauvegardé

Cependant la plupart des utilisateurs n'ont pas d'intérêt à sauvegarder et héberger des centaines de fichiers. C'est pourquoi il est possible de "louer" de l'espace de stockage et de la bande passante à IPFS, qui s'occupera de stocker, dupliquer et répartir les fichiers

automatiquement. Le fait de prêter cet espace génère de l'argent sous la forme d'une monnaie virtuelle appelée filecoin.

Exemples

IPFS est une technologie qui est encore en développement mais elle est déjà en grande partie fonctionnelle et plusieurs applications l'utilisent déjà.

Par exemple, d.tube qui est une alternative à youtube mais de manière distribuée. On retrouve également la version turque de wikipédia, puisque ce dernier a été bloqué par le gouvernement turque. Des utilisateurs ont alors décidé de le publier de nouveau, mais cette fois, sur IPFS.

Limites

Malgré tous ces avantages IPFS possèdent des inconvénients non négligeables:

- Comme tout repose sur le nombre d'utilisateurs, IPFS est très lent puisqu'il y en a encore peu à l'heure actuelle.
- IPFS est juste une solution de stockage de fichier, on ne peut pas y effectuer de calculs. Le web d'aujourd'hui est pourtant de plus en plus dynamique. Un site comme youtube, avec un historique de navigation et des recommandations personnalisées, pourrait difficilement exister sur IPFS. On pourrait imaginer des solutions de calcul décentralisé construites par dessus IPFS, mais là encore on a des problèmes, pour reprendre l'exemple de youtube, il faudrait rendre l'historique de navigation public pour effectuer des calculs dessus. Une potentielle solution pourrait être l'encryption homomorphique, qui permet d'effectuer des opérations mathématiques sur des données cryptées, et d'avoir le bon résultat après decryption. On pourrait aussi effectuer un maximum de calculs côté client, mais toutes ces choses restent compliquées à mettre en place.
- Les données mises en ligne ne peuvent pas être supprimées, même par la personne qui les a postées. Cela évite les erreurs 404 et les pertes de données mais les actions sont irréversibles.
- Le contenu est pour cette raison très difficile à réguler. C'est un des avantages puisque cela empêche la censure, mais c'est aussi un inconvénient puisque certains types de contenus sont illégaux pour de bonnes raisons.
- IPFS est fonctionnel mais il manque encore des pièces au puzzle pour le rendre utilisable. Il faudrait notamment mettre à jour les navigateurs web pour qu'ils le supportent nativement, ce que Opera et Brave font déjà, et développer de nouveaux outils.

- IPFS est très difficile d'utilisation pour une personne lambda, difficile de savoir où commencer, et tout ce qui a un rapport de près ou de loin avec IPFS a tendance à vous bombarder de termes techniques.
- Pour finir il est plus difficile de financer du contenu grâce aux publicités car il est beaucoup plus simple de les désactiver. Il existe encore une fois des alternatives en développement permettant de rémunérer les créateurs de contenu avec des crypto-monnaies, avec STEEM par exemple.
- Ce problème s'étend aussi aux hébergeurs de contenu, c'est pour ça que IPFS inclut le FileCoin, mais ça reste plus compliqué que les pubs. C'est d'autant plus un problème si on veut rajouter du calcul distribué.

Conclusion

En conclusion, il existe plusieurs technologies à l'étude qui sont déjà à un stade avancé et ont le potentiel de résoudre une grande partie des problèmes d'internet mais ces technologies sont nouvelles, peu matures et incomplètes et il y a encore beaucoup de problèmes techniques ou éthiques à résoudre avant de pouvoir en profiter pleinement.