IPFS

CID (Content Identifiers)

DHT : Distributed Hash Tables

Cette tableau contient les paires clé/valeur entre un fichier et le détenteur de ce fichier. Cette table est distribué sur le réseau. Comme cette table est décentralisé, il peut fonctionner même lorsque des noeuds lachent ou quittent le réseau.

Grâce à cet élément, les noeuds peuvent stocker et partager des données sans coordination centrale

BitSwap

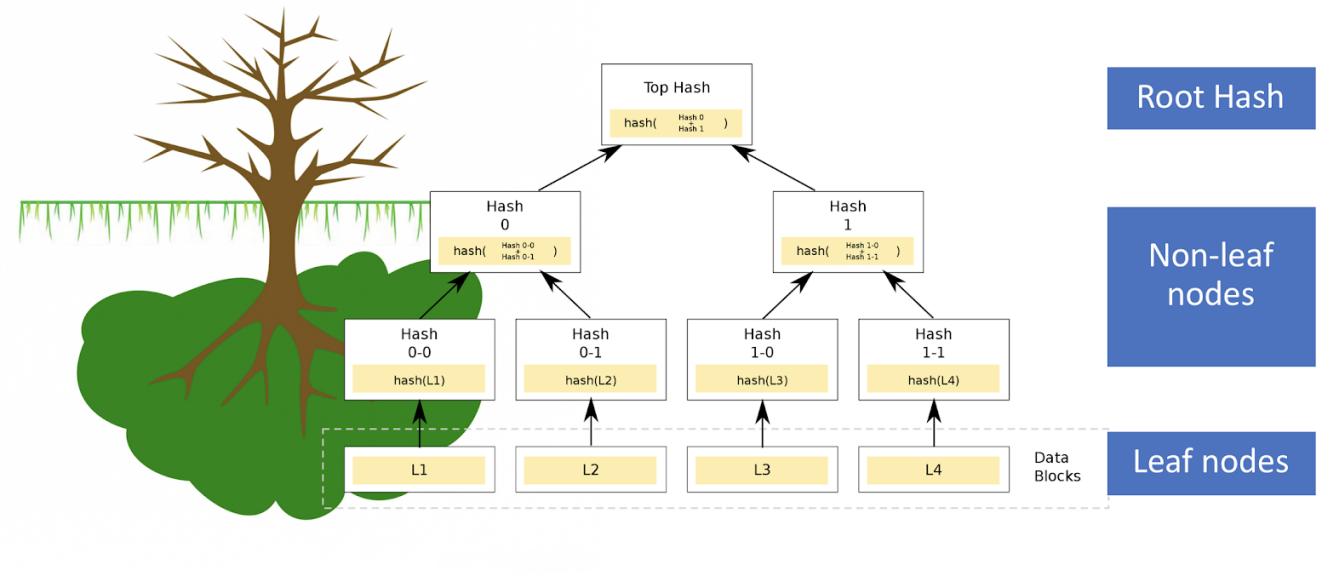
L'échange de données sur l'ensemble des noeuds du réseau est géré avec BitSwap (élément fondamentale de Filecoin)

Merkle DAG

Merkle Tree

S'assure que les blocks échangés sur le réseau en p2p sont corrects, intactes, non altérés (utilisation de fonction de hachage cryptographic)

Les feuilles de l'arbre représentent les blocs d'un fichier. Chaque blocs est alors hashé pour devenir des noeuds (non-leaf nodes). On peut ensuite combiner et hacher ces noeuds jusqu'à représenter cette donnée par un seul haché racine (root hash).



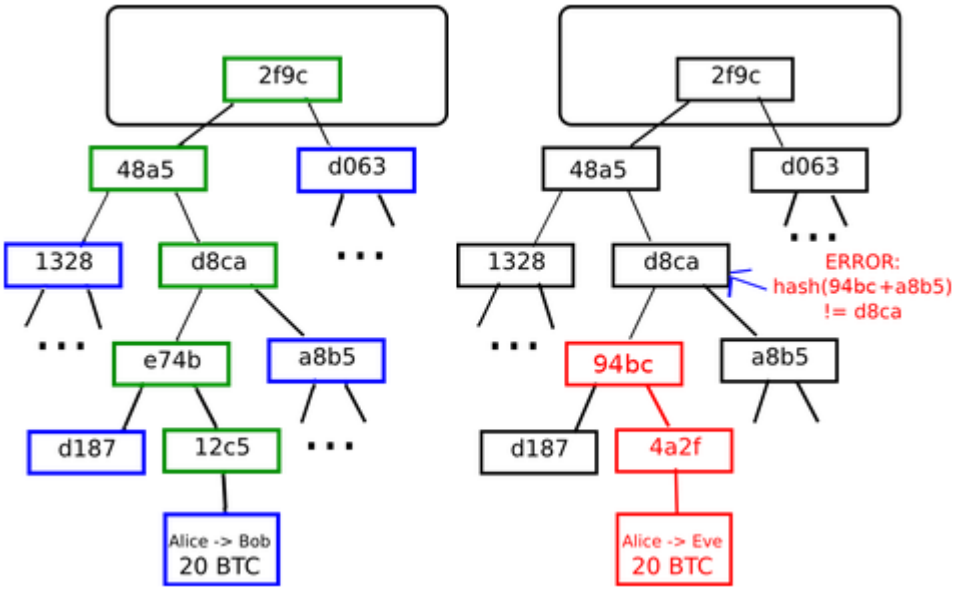
Source : hackernoon.com

Directed Acyclic Graph

C'est une façon de modéliser des séquences d'informations (topologique?) non-cycliques.

Un Merkle DAG est simplement une structure de données où les hachés sont utilisés pour références des blocs de données ainsi que des objets dans un DAG.
Les avantages sont :

- Tout contenu sur IPFS est identifié par un hash unique.
- Les données ne sont pas altérables car les hashs seraient impactés



Source: ethereum.org

La structure Merkle DAG permet également la mise en place d'un système de contrôle de version distribué (VCS) (type Github)

Self-certifying File System (SFS)

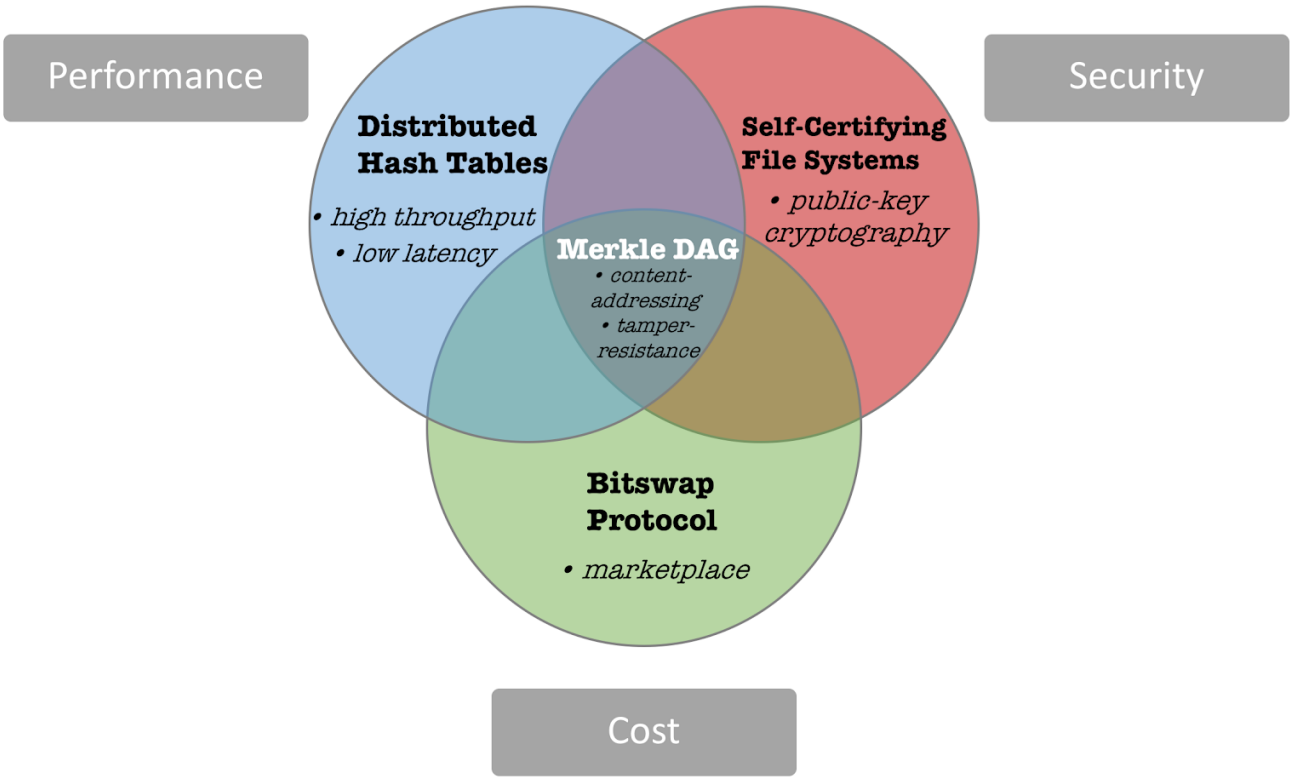
C'est un système de fichiers que ne requiert pas de permissions speciale pour l'échange de données. C'est données sont autocertifiés du fait que ces données sont déjà authentifiées par le nom du fichier (le hash je suppose).

IPFS par de cette base en utilisant des clé publiques cryptographiques pour auto-certifier les objets que publie un noeud sur le réseau. Tout bloc peut être identifié mais il en est de même pour les noeuds. Chaque noeud du réseau à une paire de clés privée et publique aisni qu'un identifiant du noeud (qui n'est autre que le haché de la clé publique du noeud). Chaque noeud peut ainsi utiliser leur clé privée pour signer tout objet (donnée) qu'il publie. On peut alors vérifier l'authenticité de la donnée avec la clé publique de l'émetteur.

IPNS

Permet aux données d'être instantanement pre-authentifiées et vérifié grâce aux clés publiques cryptographiques.

Résumé du système



Source : hackernoon.com

Challenges

On IPFS there is also little incentive for nodes to maintain long term backups of data on the network. Nodes can choose to clear cached data to save space, meaning theoretically files can end up 'disappearing' over time if there are no remaining nodes hosting the data. At current adoption levels this isn't a significant issue but in the long term, backing up large amounts of data requires strong economic incentives.

Source : hackernoon.com

Filecoin

Verifying storage on Filecoin

Proof of replication

- proof of work + storage + spacetime
    - comment rendre tout ça décentralisé
- les deux noeuds doivent pinner le fichier (voir services de pinning)
- en cas de panne, les voisins du noeud impacté font un signalement au réseau qui va résulter à une demande du réplication de la part de l'unique noeud détenant toujorus l'information.
- encrypter les fichiers

Sources

IPFS

- https://hackernoon.com/a-beginners-guide-to-ipfs-20673fedd3f
- https://proto.school/tutorials