# **Open Source** :

La désignation ***open source***, ou **code source ouvert**, s'applique aux [logiciels](https://fr.wikipedia.org/wiki/Logiciel) (et s'étend maintenant aux [œuvres de l'esprit](https://fr.wikipedia.org/wiki/%C5%92uvres_de_l%27esprit)) dont la [licence](https://fr.wikipedia.org/wiki/Licence_de_logiciel) respecte des critères précisément établis par l'[Open Source Initiative](https://fr.wikipedia.org/wiki/Open_Source_Initiative), c'est-à-dire les possibilités de libre redistribution, d'accès au [code source](https://fr.wikipedia.org/wiki/Code_source) et de création de travaux dérivés. Mis à la disposition du grand public, ce code source est généralement le résultat d'une collaboration entre [programmeurs](https://fr.wikipedia.org/wiki/D%C3%A9veloppeur).

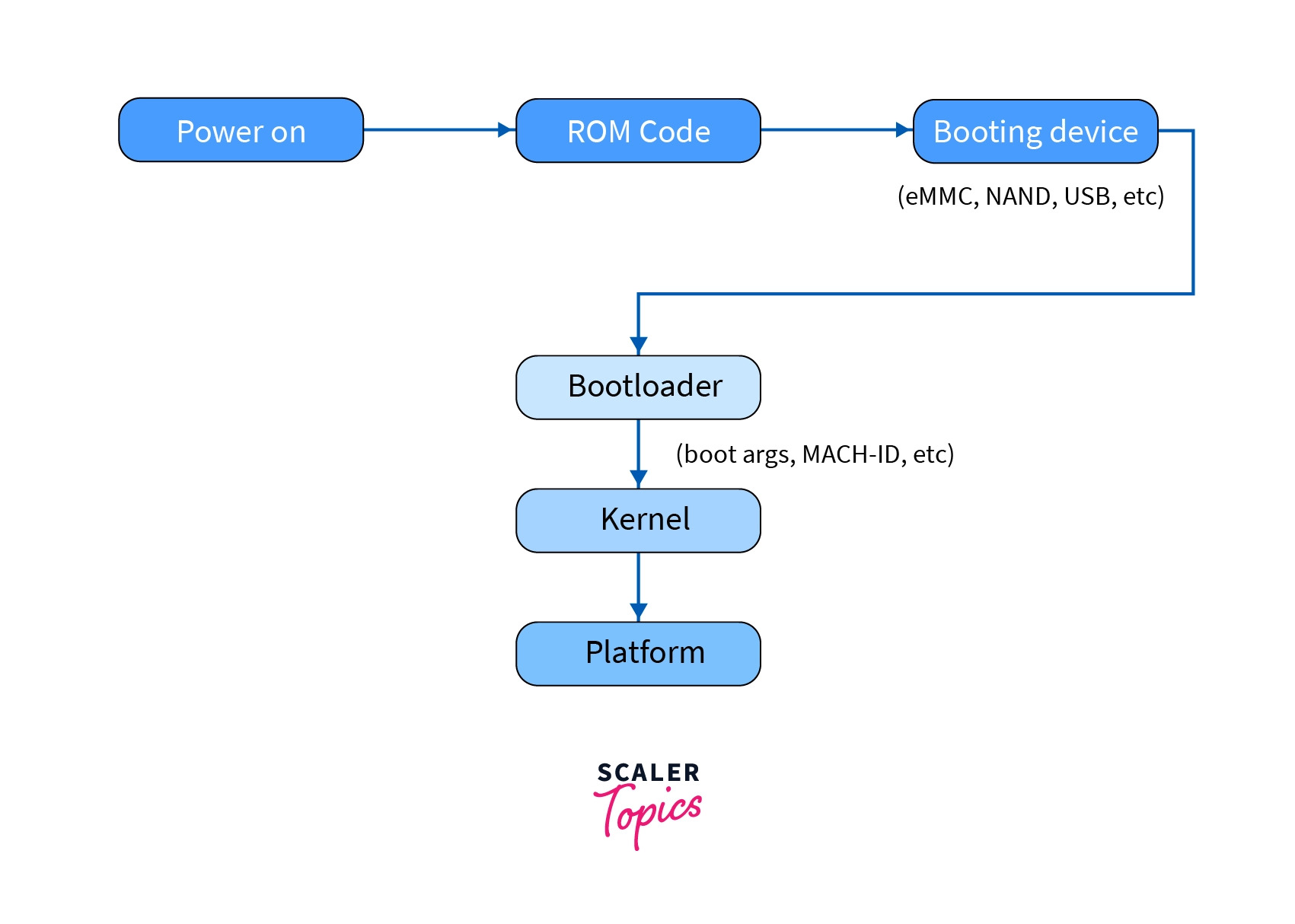
<https://fr.wikipedia.org/wiki/Open_source>

# 404 :

Dans le [World Wide Web](https://fr.wikipedia.org/wiki/World_Wide_Web), l’erreur 404 signale que la [ressource](https://fr.wikipedia.org/wiki/Ressource_du_World_Wide_Web) demandée, généralement une [page Web](https://fr.wikipedia.org/wiki/Page_Web), n'a pas été trouvée. Elle est souvent accompagnée d'un message avec les mots « pas trouvé » ou *not found* en anglais. Le numéro 404 est défini par la [liste des codes](https://fr.wikipedia.org/wiki/Liste_des_codes_HTTP) du [protocole de communication](https://fr.wikipedia.org/wiki/Protocole_de_communication) [Hypertext Transfer Protocol](https://fr.wikipedia.org/wiki/Hypertext_Transfer_Protocol) (HTTP)

<https://fr.wikipedia.org/wiki/Erreur_HTTP_404>

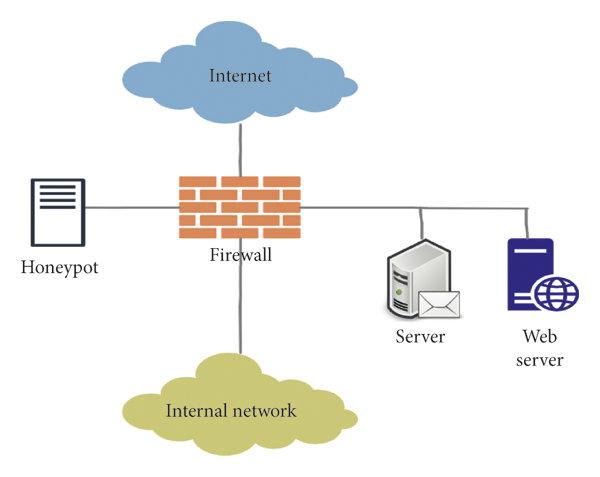
# **Bootloader** :

Les données du [système d’exploitation](https://www.ionos.fr/digitalguide/serveur/know-how/quest-ce-quun-systeme-dexploitation/) doivent être chargées directement dans la [mémoire vive](https://www.ionos.fr/digitalguide/serveur/know-how/quest-ce-quune-memoire-vive/) lors du démarrage de l’appareil. Cela est possible grâce à ce que l’on appelle un chargeur d’amorçage ou bootloader, qui fait office de programme de démarrage. Ainsi, le bootloader se lance généralement juste après le démarrage d’un appareil, **quel que soit son support** comme un disque dur, CD/DVD ou [clé USB](https://www.ionos.fr/digitalguide/serveur/know-how/creer-une-cle-usb-bootable/). Ce support va chercher dans le **firmware** de l’ordinateur (par ex. le BIOS) les informations qui concernent l’emplacement du chargeur d’amorçage. Ce processus est généralement désigné sous le nom d’« amorçage ».

# **man in the middle (terme utilisé dans la cybersécurité) :** L'**attaque de l'homme du milieu** (**HDM**) ou *man-in-the-middle attack* (**MITM**), parfois appelée **attaque du monstre du milieu** ou *monster-in-the-middle attack*[1](https://fr.wikipedia.org/wiki/Attaque_de_l%27homme_du_milieu#cite_note-cloudflare-1),[2](https://fr.wikipedia.org/wiki/Attaque_de_l%27homme_du_milieu#cite_note-ifs-2) ou **attaque de l'intercepteur**, est une attaque qui a pour but d'intercepter les communications entre deux parties, sans que ni l'une ni l'autre puisse se douter que le [canal de communication](https://fr.wikipedia.org/wiki/Canal_de_communication) entre elles a été compromis. Le canal le plus courant est une connexion à [Internet](https://fr.wikipedia.org/wiki/Internet)

<https://fr.wikipedia.org/wiki/Attaque_de_l%27homme_du_milieu>

# **Honey pot (terme utilisé dans la cybersécurité)** :

(en français, au sens propre « **pot de miel**[1](https://fr.wikipedia.org/wiki/Honeypot#cite_note-1) », et au sens figuré « **leurre** ») est une méthode de [défense active](https://fr.wikipedia.org/wiki/D%C3%A9fense_active) qui consiste à attirer, sur des ressources ([serveur](https://fr.wikipedia.org/wiki/Serveur_informatique), [programme](https://fr.wikipedia.org/wiki/Programme_informatique), service), des adversaires déclarés ou potentiels afin de les identifier et éventuellement de les neutraliser.

Le terme désigne à l'origine des dispositifs informatiques spécialement conçus pour susciter des [attaques informatiques](https://fr.wikipedia.org/wiki/Attaque_informatique). Son usage s'est étendu à des techniques relevant de l'[ingénierie sociale](https://fr.wikipedia.org/wiki/Ing%C3%A9nierie_sociale_(s%C3%A9curit%C3%A9_de_l%27information)) et du [renseignement humain](https://fr.wikipedia.org/wiki/Renseignement_humain)

<https://fr.wikipedia.org/wiki/Honeypot>

<https://ca-fr.norton.com/blog/iot/what-is-a-honeypot#:~:text=Un%20honeypot%20est%20un%20logiciel,attir%C3%A9s%20par%20des%20cyber%2Dapp%C3%A2ts.>

# **Firewall** : Un pare-feu, ou "firewall" en anglais, est un système de sécurité réseau qui surveille et contrôle le trafic entrant et sortant d'un réseau privé. Il agit comme une barrière entre votre réseau et Internet, bloquant les accès non autorisés et les attaques malveillantes.

**Voici les principales fonctions d'un pare-feu :**

**Filtrage du trafic**: Le pare-feu analyse chaque paquet de données entrant et sortant du réseau et le compare à un ensemble de règles prédéfinies. Il autorise ou bloque le passage des paquets en fonction de ces règles.

**Protection contre les intrusions**: Le pare-feu peut détecter et bloquer les tentatives d'intrusion et d'attaques malveillantes, telles que les attaques par déni de service (DoS) ou les scans de ports.

**Contrôle des applications**: Le pare-feu peut autoriser ou bloquer l'accès à certaines applications ou services, comme les jeux en ligne ou les réseaux sociaux.

**Journalisation**: Le pare-feu peut enregistrer les événements de sécurité, tels que les tentatives de connexion non autorisées ou les attaques bloquées.

**mais il existe deux types principaux de pare-feu :**

Pare-feu matériel: Il s'agit d'un appareil physique qui est installé entre votre réseau et Internet.

Pare-feu logiciel: Il s'agit d'un programme qui est installé sur chaque ordinateur du réseau.

Les pare-feu sont un élément essentiel de la sécurité informatique. Ils peuvent vous aider à protéger votre réseau contre les attaques malveillantes et les accès non autorisés.

<https://www.cisco.com/c/fr_fr/products/security/firewalls/what-is-a-firewall.html>

# Proxy :

**Qu'est-ce qu'un proxy ?**

Un proxy est un serveur intermédiaire qui agit comme un pont entre votre ordinateur et Internet. Lorsque vous utilisez un proxy, vos requêtes Web sont envoyées au serveur proxy, qui les transmet ensuite au site Web que vous souhaitez visiter. Le site Web répond ensuite au serveur proxy, qui transmet la réponse à votre ordinateur.

**Voici quelques-uns des avantages de l'utilisation d'un proxy :**

**- Confidentialité:** Un proxy peut masquer votre adresse IP, ce qui rend plus difficile pour les sites Web de vous suivre et de collecter vos données.

**- Sécurité**: Un proxy peut vous protéger des sites Web malveillants en filtrant le trafic Web.

Contournement des restrictions: Un proxy peut vous aider à contourner les restrictions géographiques ou les pare-feu.

**- Amélioration de la performance**: Un proxy peut mettre en cache les pages Web et les contenus Web, ce qui peut améliorer la vitesse de chargement des pages Web.

**L'utilisation d'un proxy peut présenter certains inconvénients, notamment :**

**- Réduction de la vitesse:** L'utilisation d'un proxy peut ralentir votre connexion Internet.

**- Compatibilité**: Certains sites Web et applications ne fonctionnent pas avec les proxies.

**- Anonymat**: L'utilisation d'un proxy ne garantit pas l'anonymat complet.

<https://fr.wikipedia.org/wiki/Proxy>

<https://www.avg.com/fr/signal/proxy-server-definition>

# DDoS

**Qu'est-ce qu'une attaque DDoS ?**

Une attaque par déni de service distribué (DDoS) est une tentative malveillante de perturber le trafic normal d'un serveur, service ou réseau ciblé en le submergeant avec un flot de trafic Internet.

**Fonctionnement d'une attaque DDoS :**

**- Réseau de machines compromises:** L'attaquant utilise un réseau de machines compromises, appelées "bots", pour générer le trafic malveillant.

**- Cible:** Le trafic est dirigé vers la cible, surchargeant ses ressources et la rendant indisponible pour les utilisateurs légitimes.

**- Types d'attaques:** Il existe différents types d'attaques DDoS, comme les attaques par inondation UDP (User Datagram Protocol), les attaques SYN flood et les attaques HTTP GET.

**UDP** est un protocole de transport sans connexion, ce qui signifie qu'il n'établit pas de connexion préliminaire entre l'expéditeur et le destinataire avant de transmettre des données.

**Fonctionnement d'UDP :**

- L'expéditeur encapsule les données dans un paquet UDP avec l'en-tête approprié.

- L'expéditeur envoie le paquet UDP au réseau.

- Le réseau achemine le paquet UDP vers le destinataire.

- Le destinataire reçoit le paquet UDP et extrait les données.

**SYN flood**  
Dans le cas d'une attaque SYN Flood la situation est comparable à celle d'un employé qui travaille dans la réserve et qui reçoit les demandes du comptoir du magasin.

L'employé reçoit une demande, va chercher le paquet et attend une confirmation avant de le transmettre au comptoir. Il reçoit ensuite de nombreuses autres demandes de colis sans confirmation jusqu'à ce qu'il ne puisse plus transporter aucun colis, qu'il soit débordé et que les demandes commencent à rester sans réponse.

**Attaques HTTP GET :**

Une attaque HTTP GET est une attaque DDoS qui utilise des requêtes HTTP GET légitimes pour surcharger un serveur web.

**Fonctionnement :**

L'attaquant utilise un grand nombre de machines compromises pour envoyer des requêtes HTTP GET vers une page web ou un service web du serveur cible.

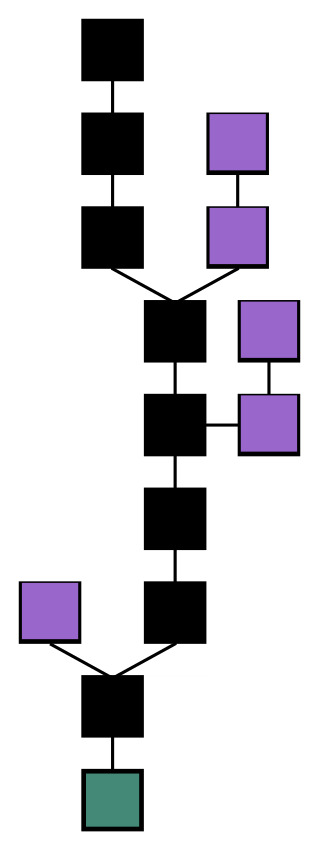
Le serveur, en recevant ces requêtes, doit traiter chacune d'entre elles, ce qui surcharge ses ressources et le rend indisponible pour les utilisateurs légitimes.

<https://www.cloudflare.com/fr-fr/learning/ddos/what-is-a-ddos-attack/>

<https://www.cloudflare.com/fr-fr/learning/ddos/udp-flood-ddos-attack/>

<https://www.cloudflare.com/fr-fr/learning/ddos/glossary/user-datagram-protocol-udp/>

# Blockchain

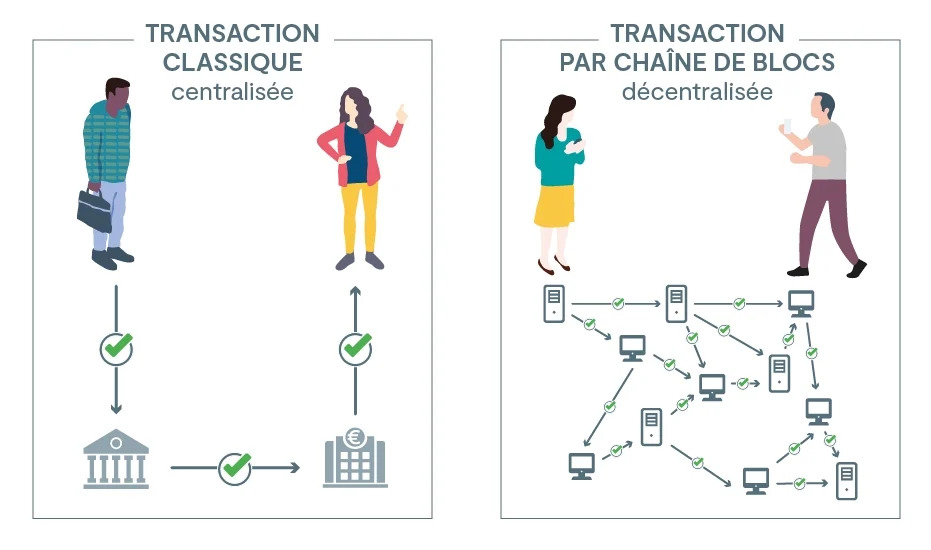
Une **blockchain** ou **chaîne de blocs** (en*française*), est une technologie de stockage et de transmission d'informations sans autorité centrale. Techniquement, il s'agit d'une [base de données distribuée](https://fr.wikipedia.org/wiki/Base_de_donn%C3%A9es_distribu%C3%A9e) dont les informations envoyées par les utilisateurs et les liens internes à la base sont vérifiés et groupés à intervalles de temps réguliers en blocs, formant ainsi une chaîne. 

**Voici les principales caractéristiques d'une blockchain :**

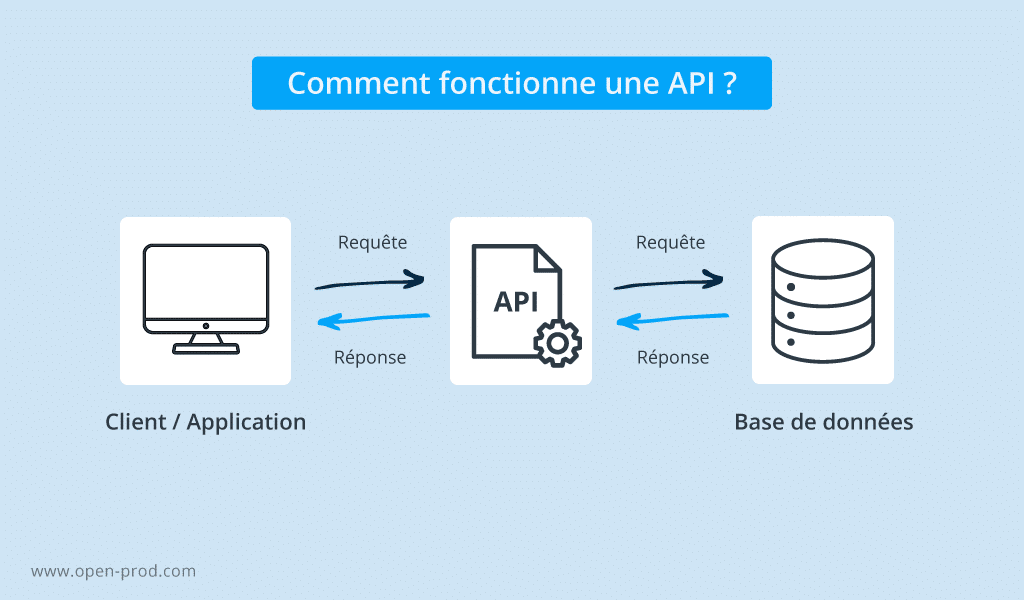
**- Décentralisation**: La blockchain n'est pas contrôlée par une seule entité, mais par un réseau d'ordinateurs répartis dans le monde entier. Cela la rend plus résistante à la censure et à la manipulation.

**- Sécurité**: Les données de la blockchain sont protégées par la cryptographie, ce qui rend très difficile leur falsification ou leur suppression.

**- Transparence**: Toutes les transactions de la blockchain sont accessibles à tous les participants du réseau.

**- Immuabilité**: Une fois qu'une transaction est ajoutée à la blockchain, elle ne peut plus être modifiée..

# API

****

**Qu'est-ce qu'une API ?**

Une API, ou Interface de Programmation d'Application, est un ensemble de règles et de définitions qui permet à deux logiciels de communiquer entre eux. Elle agit comme un intermédiaire qui facilite l'échange de données et de fonctionnalités entre différentes applications.

**Voici quelques exemples d'utilisations d'API :**

**Météo**: Une application météo peut utiliser une API pour obtenir les données météorologiques d'un service météorologique.

**Réseaux sociaux**: Une application de réseau social peut utiliser une API pour se connecter à votre compte Facebook ou Twitter.

**Paiement en ligne**: Un site de commerce électronique peut utiliser une API pour traiter les paiements via un service de paiement en ligne.

<https://fr.wikipedia.org/wiki/Interface_de_programmation_d%27application>

[https://www.redhat.com/fr/topics/api/what-are-application-programming-interfaces](https://fr.wikipedia.org/wiki/Interface_de_programmation_d%27application)

[https://www.mulesoft.com/fr/resources/api/what-is-an-api](https://fr.wikipedia.org/wiki/Interface_de_programmation_d%27application)