FORCE NETWORK

Un nouvel internet où la vie privée et l'anonymat sont préservés et où la censure n'est pas possible

Qu'est-ce que Force Network ?

Force Network est destiné à être un réseau décentralisé à grande échelle dans lequel les participants sont encouragés à fournir et utiliser divers services en toute sécurité de manière anonyme et sans tiers de confiance.

Force Network est capable d'anonymiser n'importe quel protocole ou service réseau (e.g. navigation internet, jeux en ligne, vidéo à la demande).

Qu'est-ce que qui rend Force Network si flexible ?

Force Network permet à n'importe qui d'établir des contrats avec une grande variété de nœuds réseaux afin de fournir des services anonymes avec n'importe quel protocole souhaité. Cette flexibilité permet également de créer des services qui enveloppent les données en utilisant d'autres protocoles réseaux pour renforcer l'anonymat. Cela signifie qu'un tiers ne peut même pas savoir que vous utilisez Force Network. La préservation de la vie privée a une importance grandissante dans un monte où les gouvernements espionnent systématiquement leurs citoyens, les plateformes en ligne collectent et vendent les informations personnelles et les hébergeurs sont responsables du contenu généré par les utilisateurs et peuvent subir des conséquences légales.

Pourquoi Force Network est-il unique ?

Services réseau décentralisés et évolutifs

Initialement compatible HTTP/HTTPs, peut-être facilement rendu compatible avec n'importe quel protocole réseau tels que IPFS, DVPN, LAN, E-mail, messagerie cryptée, contenu à la demande, et plus.

Complètement anonyme

L'adresse IP du client n'est jamais révélée à nœud de paiement ou au serveur hébergeant le contenu et inversement. Les données ne peuvent pas être suivies, corrélées ou décryptées par quelconque intermédiaire grâce aux cryptages successifs.

Réseau résistant à la censure

Le contenu hébergé sur le réseau Force est résistant à la censure car l'adresse IP de l'hébergeur n'est jamais directement révélée.

Routage intelligent pour permettre évolutivité, résilience et performances prévisibles

Les informations sur la santé des nœuds permettent aux nœuds de paiement de générer le meilleur chemin dans le réseau de manière dynamique. Il est possible d'activer une géolocalisation approximative pour minimiser la latence.

Modèle d'encouragement à la participation intelligent

Les jetons Force sont utilisés pour favoriser un réseau sûr, résilient et stable. Les transactions permettent de payer pour divers services, récompenser les nœuds ou échanger des clés ou des adresses si nécessaire.

Prix automatique et capacité de revenue

Le tarif dynamique des services assure le meilleur prix pour une demande donnée. La transparence permet aux nœuds d'ajuster leur prix pour maximiser leur revenu.

Quelques données sur FOR

Quantité en circulation :	121,548,338 FOR
Quantité maximale :	200,000,000 FOR
Caution Masternode :	500,000 FOR

Échanges

Crypto-bridge
Stocks.Exchange
Nouveaux échanges à venir

Potential Use Cases

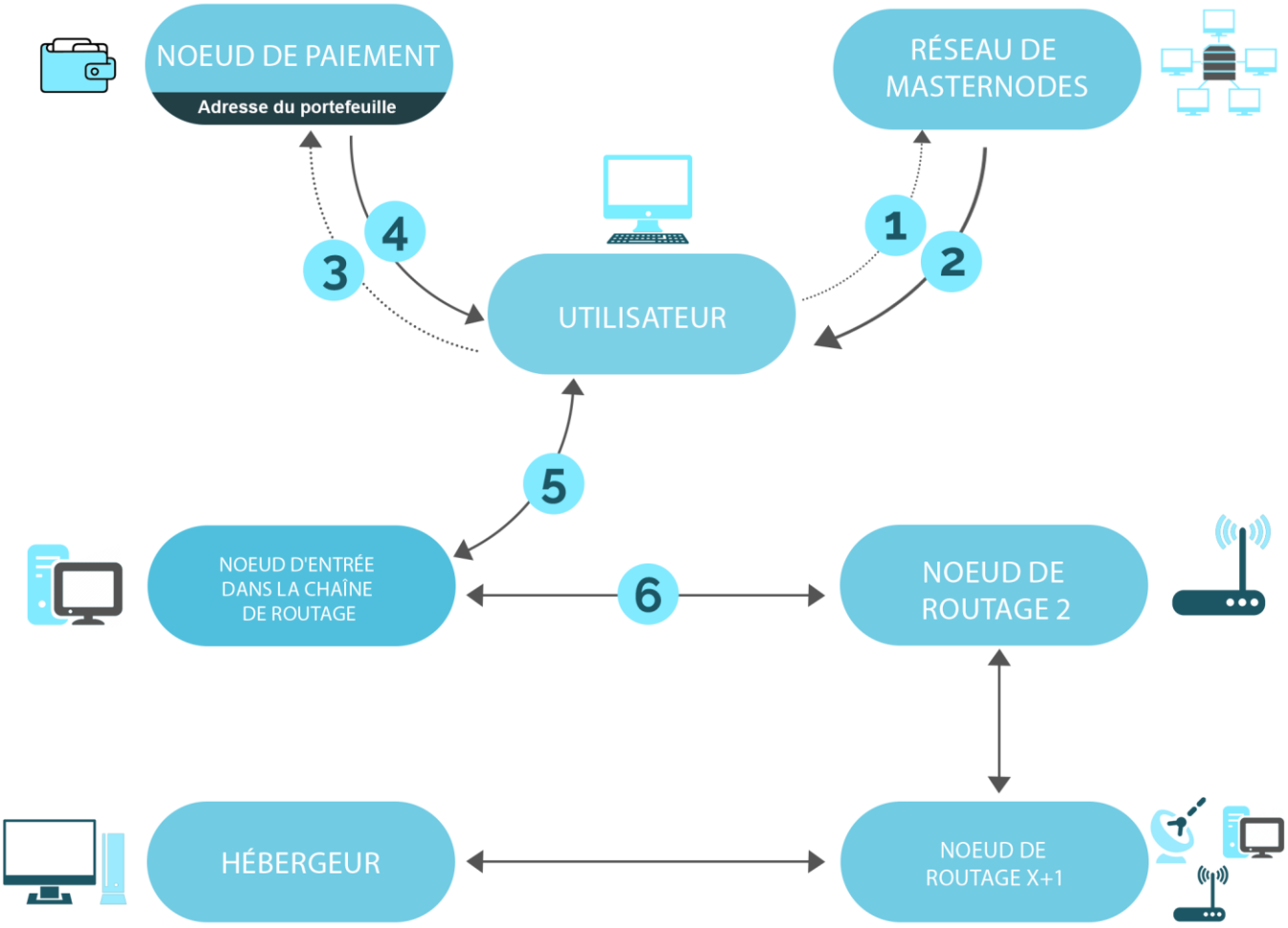
- Préserve la vie privée et garantit l'anonymat
- Cryptage sûr et à zéro divulgation des e-mail et messages
- Distribution de la vidéo à la demande anonymement
- Hébergement d'un serveur de jeux vidéos sans divulgation de l'IP

Relevant Links

Website
White Paper
Discord Channel
Telegram Group
Reddit

Visualisation de Force Network

Exemple simplifié d'un accès anonyme à du contenu



1. L'utilisateur demande la liste des services du masternode le plus proche en utilisant n'importe quel navigateur internet.

2. Le masternode lui envoie l'adresse du portefeuille d'un des noeuds de paiement responsable du maintien du service demandé par l'utilisateur.

3. L'utilisateur envoie des jetons Force au portefeuille du noeud de paiement. Cela done un sinal à ce dernier pour établir un contrat avec une chaîne de routage qui pourra transmettre l'information de manière anonyme.

4. Le noeud de paiement envoie à l'utilisateur l'adresse IP du noeud d'entrée ainsi que les clés qui permettront le cryptage des données le long de la chaîne.

5. L'utilisateur peut maintenant envoyer et recevoir des données cryptées plusieurs fois depuis le noeud d'entrée comme si il s'agissait de la destination finale.

6. Les requêtes sont transmises le long de la chaîne, chaque noeud de la chaîne ne décrypte qu'une couche.