Force Network: une suite de protocoles Internet décentralisés v0.1

Michael Dye, Johndis, Bumbr, Jared Grey

31 mars 2018

Résumé

Dans cet article, nous présentons un nouveau cadre pour un ensemble de protocoles Internet décentralisés appelés ≪Force Network≫. Ce réseau sera anonyme, évolutif, flexible et permettra aux utilisateurs d'accéder aux données et aux services d'une manière privée et résistante à la censure. Un jeton d'utilité sous-jacent, la devise Force, ou Force Coin (FOR), sert à plusieurs fins qui vont d'un mécanisme d'incentivisation pour la prestation de services et la qualité de ceux-ci, à un outil d'accord sur le consensus réseau simultané et sert de moyen sûr de transfert des clés de cryptage entre les nœuds participants. Force Network permettra aux gens du monde entier d'accéder à l'information et de sécuriser toutes sortes de réseaux, même sous les régimes les plus oppressifs, permettant à l'information d'exister sans suppression et manipulation non autorisée. Force Network permettra aux gens du monde entier d'accéder à de l'information non-censurée ou manipulée sans autorisation et de sécuriser toutes sortes de réseaux, même sous les régimes les plus oppressifs.

I Introduction

Force Network aspire à être un ensemble entièrement anonyme, évolutif et flexible de protocoles offrant un accès résistant à la censure aux données et services en réseau. Nous nous référons à cet ensemble de protocoles en tant que Services de Réseaux Evolutifs et Décentralisés (Decentralized Scalable Network Services – DSNS). L'équipe en charge du réseau Force mettra au point un jeton utilitaire sous-jacent appelé Force Coin (FOR), l'infrastructure du réseau de distribution, et le système qui permettra aux netnodes de fournir une liste en constante expansion de différents protocoles de réseaux. Les développeurs indépendants seront en mesure de construire des applications utilisant Force Network et se basant sur n'importe quelle autre plateforme tierce de partie. Après une connexion initiale réussie au réseau Force, la connexion aux netnodes de service valables se fera de manière aussi intuitive qu'une connexion à un réseau local physique (LAN).

Alors que les réseaux centralisés sont enclins à la censure, à des restrictions d'accès au contenu et aux points de défaillance singuliers, leur avantage par rapport à leurs homologues décentralisés est qu'ils sont mieux placés pour engager des ressources haut-de-gamme continues, tout en ayant une redondance et une disponibilité en cas de panne totale en raison de leur nature centralisée. Vu que Force Network sera un réseau décentralisé où la participation des fournisseurs de services est volontaire, nous décrirons notre solution proposée afin de continuer d'inciter lesdits fournisseurs de maintenir leurs services à long terme et de prévenir les interruptions de service et les dégradations de l'expérience utilisateur en découlant.

Le premier protocole à mettre en œuvre sera le Protocole HTTP (Hypertext Transfer Protocol). Cela signifie que n'importe qui sera en mesure de se connecter au réseau Force en utilisant un cadre de navigateur web customisé et dans le portefeuille. Ce navigateur sera multi-plate-forme pour les appareils mobiles ainsi que ceux de bureau, et interagira avec notre réseau ainsi que l'Internet régulier, avec comme différence que le contenu venant du réseau des netnodes décentralisés sera distribué de façon cryptée de bout en bout. Lors de l'utilisation du réseau Force, le contenu transféré ou téléchargé sera indéchiffrable par des entités extérieures telles que les fournisseurs de services Internet.

Un internet réparti et privé n'est que le début. Force Network vise également à permettre aux netnodes d'héberger n'importe quel protocole réseau prédéfini. Les netnodes Force seront regroupés par le protocole qu'ils fournissent (ruche de service réparti – Distributed Service Hive/DSH), ainsi que par les

niveaux d'autorisation d'accès, appliqués au niveau du réseau.

Voici des exemples de protocoles que le réseau pourrait supporter :

— Système de fichiers interplanétaires (InterPlanetary File System - IPFS) ;
— Réseaux privés virtuels décentralisés (Decentralized Virtual Private Networks - DVPN) ;
— Jeux LAN ;
— Courrier électronique et messagerie sécurisée, éventuellement protocole HushList ;
— Streaming de divers médias ;
— Services de réseau de distribution de contenu (Content Deliver Network - CDN) ; et
— Réseautage pour l'internet des objets (Internet of Things – IOT).

II Points clés de différentiation par rapport à la compétition

Force Network est destiné à être un réseau décentralisé à grande échelle, où les participants sont encourages à fournir et à consommer un large éventail de services en réseau de manière confiante, privée et sécurisée. Force Network vise à atteindre ces objectifs via l'incitation économique. Pour que le réseau soit auto-entretenu et réussisse dans aspect, il doit démontrer sa valeur face à d'autres solutions qui opèrent dans un espace similaire.

Dans l'intérêt d'évaluer le potentiel de marché du réseau Force et de sa capacité à faire la différence dans le paysage actuel, nous avons créé une liste de plusieurs points clés qui, selon nous, sont de forts différentiateurs par rapport aux concurrents existants, ce qui permettra la viabilité à long terme du réseau Force.

1. Confidentialité totale du réseau et cryptage des données. Force Network est la seule devise de protocole entièrement privée, cryptée de bout en bout, avec du contenu résistant aux tentatives de perturbation venant de forces en dehors du réseau. Force Network prend des mesures exemplaires et extensives pour s'assurer que :
   — L'adresse IP des clients n'est jamais directement révélée ;
   — L'adresse IP des fournisseurs de contenu n'est jamais directement révélée ;
   — Les données ne peuvent pas être retracées vers le client ou l'hôte ;
   — Les données ne peuvent être déchiffrées par aucun intermédiaire.
2. Entièrement indépendant des solutions traditionnelles et limitées techniquement. D'autres projets tentent de fournir un Internet décentralisé utilisant des navigateurs Web réguliers. Bien que l'utilisation de navigateurs Web existants serait idéal du point de vue de l'utilisateur, celle-ci présente trop de problèmes logistiques pour les services de réseau sécurisés et privés que nous souhaitons fournir.
   — Protocoles DNS : l'utilisation de cadres Web existants force le réseau à se conformer et être sujet aux contraintes imposées par les protocoles Web existants, y compris DNS. Le DNS a été historiquement le premier point d'attaque pour la censure de contenus. Certaines solutions, telles que DNSchain, tentent de résoudre ce problème, mais ne peuvent pas le faire d'une manière entièrement cryptée qui masque l'IP de destination finale. En outre, bien qu'il permette aux sites de conserver leur domaine existant si nécessaire, le risque de centralisation est très présent, ce qui ne répond pas à nos critères pour un réseau véritablement autonome et résistant à la censure.
   — Cryptage SSL : l'utilisation de navigateurs Web réguliers signifie que le seul schéma de cryptage disponible est le SSL. Cela nécessite une modification du navigateur pour l'importation de certificats SSL personnalisés et ne peut pas implémenter nativement des schémas multi-cryptage bien plus puissants.
   — En utilisant les navigateurs Web existants, il n'existe aucun moyen de masquer les adresses IP du client et de l'hôte. Ceci est essentiel pour garantir que Force Network reste privé et résistant à la censure.

   Afin de rendre le réseau essentiellement privé, Force opte pour le développement d'un navigateur personnalisé, livré au sein d'un portefeuille. Cela permet au réseau Force d'utiliser ses propres protocoles de résolution de nom et de cryptage, assurant que le trafic sur le réseau reste secret et résistant à la censure.

   Tout en considérant ce qui précède, les pages publiques non chiffrées seront toutefois toujours disponibles à l'affichage avec les navigateurs Web réguliers. Ceci permettra à tout le monde d'afficher des informations publiques telles que les services, les prix et les adresses de portefeuille des noeuds de paiement de la manière la plus facile possible .Les pages publiques non

chiffrées fournissent également un point d'entrée familier aux services contractuels sur Force Network.

3. Force est un réseau multi-protocolaire, qui permet une large gamme de services de réseau décentralisés et évolutifs. En plus des caractéristiques garantissant le respect de la vie privée des utilisateurs, nous visons à être beaucoup plus qu'une simple solution Web. Nous prévoyons de livrer toute une gamme de services de réseaux et protocoles privés, se basant sur le protocole de base du réseau Force comme décrit dans la section III.

   Ceci est le point qui distingue fortement Force Network vis-à-vis d'autres technologies similaires. En étant plus qu'une solution limitée non-extensible et se basant sur le seul Internet, le réseau Force vise à être un cadre "protocol agnostic" (ouvert à tous protocoles) et extensible. Force Network peut soutenir une multitude de services de natures diverses, fournissant par ceci une alternative complète et efficace aux réseaux traditionnels à grande échelle existant jusqu'ici.

4. Un modèle de paiement granulaire et spécifique au service. Force Network utilise pleinement l'excédent économique, en faisant appel à un mécanisme de tarification intelligente (DSP) ainsi qu'à la base de données sur les informations de santé des noeuds. Le réseau veille en permanence, à la recherche de zones de service (DSHs) sous ou sur-desservies, et ajuste la tarification en conséquence à l'échelle du réseau, pour s'assurer que les participants s'efforcent constamment d'équilibrer la qualité et la disponibilité à travers la gamme de services fournis par le réseau.

   Il s'agit d'une approche radicalement différente par rapport aux mécanismes traditionnels d'équilibrage de charge qui existent dans les services à tâche unique. La charge n'est plus considérée comme des ressources du réseau n'étant utilisées de manière optimale pour fournir un service. Au contraire, il s'agirait plutôt d'une valeur économique inexploitée, tandis que zones de service entières sont équilibrées les unes contre les autres pour parvenir à une harmonie entre l'offre et la demande.

5. Force Network utilise un modèle fournisseur de services, basé sur un Plug-and-Play dynamique, similaire à celui d'Uber. Étant le contrepoint au paragraphe numéro 4 ci-dessus, et permettant la mise en place de la tarification intelligente, les nœuds sont en mesure de se détacher dynamiquement et de s'attacher à tout DSH, en fonction de leurs préférences, sans avoir besoin d'installer de matériel supplémentaire. Il s'agit d'une transition transparente qui permet au réseau, dans son ensemble, de faire face à très peu de temps d'arrêt, de fournir un service et une expérience utilisateur de qualité supérieure, tout en compensant pleinement les fournisseurs de services en même temps. Le retrait du réseau en tant que fournisseur de services entraînera un coût, mais il sera sensiblement plus bas que celui appliqué d'habitude dans une situation similaire. Ceci ne s'applique que lorsque le processus de fourniture de services est actif et sera gratuit si le noeud est inactif.

   Ce modèle de répartition des coûts permet de niveler les règles du jeu et d'accroître la responsabilisation de tous les participants. À l'heure actuelle, les coûts associés au changement de service pèsent lourdement sur les consommateurs, tandis que les fournisseurs de services encourent des frais d'annulation de minimaux (par exemple, des frais d'annulation pour toute cessation de service récurrente).

   Force Network prévoit également que des outils de gestion avancés d'administration de netnodes soient développés pour assister intelligemment les fournisseurs de netnodes à maximiser l'utilisation de leurs noeuds (et ainsi donc le revenu qu'ils en tirent), tels que des services internes qui surveillent automatiquement le marché et effectuent des transitions douces (et sans frais) de services à faible demande vers des services à forte demande.

III Vue d'ensemble de l'infrastructure réseau

III. A La superposition de réseaux

Nous proposons un modèle de réseau à trois couches pour fournir les services du réseau Force. Ces trois couches interagissent les unes avec les autres pour s'assurer que le service Force est opérationnel.

— **La couche 1** sera le protocole de consensus de base proof-of-stake, attaché à une blockchain privée. C'est ici que les transactions sur Force Network auront lieu et utiliseront la validation proof-of-stake. Les clés de cryptage ainsi que le point d'entrée IPs seront également transférés à l'aide de la couche 1

— **La couche 2** présentera des masternodes qui agiront comme le premier point de connexion au

sein du réseau. Les masternodes hébergeront du contenu tel que les pages d'index du service réseau, les informations sur la santé des nœuds et les itinéraires cryptés des hopnodes.
Les pages d'index incluront des informations telles que des descriptions de service réseau, leurs prix et les adresses de portefeuille des nœuds de paiement. Ces pages permettront également d'être vues en utilisant l'Internet traditionnel. Les pages d'index de service réseau ne peuvent être mises à jour qu'avec la clé privée correcte, générée par le nœud de paiement lors de la création du service.
Les masternodes accumuleront et stockeront également les informations de santé réseau (INSA) concernant les nœuds de paiement à surveiller. Bien que toutes les informations personnelles d'identification seront cryptées afin d'éviter toute violation de la vie privée, l'INSA sera publiquement visible comme un moyen de fournir aux consommateurs la transparence nécessaire afin de faciliter le processus de sélection de leurs futurs fournisseurs de services .Les masternodes ne connaîtront pas l'adresse IP directe de tous les nœuds. Au lieu de cela, le nœud de paiement générera des itinéraires uniques à partir du moment où la confirmation de paiement concernant un service a été établie (pour plus de détails veuillez voir la section III D.). Les masternodes hachent régulièrement leurs bases de données et s'assurent qu'elles sont synchronisées avec le reste du réseau de masternodes.

— **La couche 3** sera le service d'hébergement et la couche de livraison, composée d'une variété de nœuds différents. Ce sont ces nœuds qui fournissent tout les services de bas niveau du protocole réseau (voir la liste des exemples de protocoles réseaux pris en charge dans la section Introduction).Chaque nœud peut, à un moment donné, entrer ou sortir volontairement et dynamiquement d'une ruche de services distribués (DSH). Une DSH est une collection de netnodes exécutant simultanément un protocole spécifique au service pour former un réseau distribué qui héberge et fournit le service. Par exemple, le service DVPN sera son propre DSH où un nombre quelconque de nœuds pourraient simultanément rejoindre ou quitter cette ruche, et chaque ruche fournira son service à l'aide de ses nœuds constitutifs. Un nœud peut également être exploité en tant que noeud de paiement, aussi connu sous le nom d' « oracles de service escrow » (Service Escrow Oracles - SEO). La fonction des SEOs est de :

  — Servir d'intermédiaires entre les fournisseurs de services et les consommateurs ;
  — S'assurer que le service est livré en toute sécurité après son paiement ;
  — Contracter les nœuds ;
  — Générer des chaînes de hopnodes (voir section III. D) ;
  — Multi-crypter la chaîne les adresses IP des chaînes hop ;
  — Transférer les clés de cryptage pour chaque étape de la chaîne de hopnodes au client ;

  Les SEOs seront appelés «nœuds de paiement». Plus d'informations sur la fonction des nœuds de paiement seront décrites ci-dessous.

III. B Routage de chaînes ad-hoc et architectures de réseau à grande échelle canalisé

Force Network utilise le mécanisme de routage de chaînes ad-hoc (Ad-hoc Chain Routing - AHCR), ce qui signifie que les demandes ne sont pas diffusées sur l'ensemble du réseau. Au lieu de cela, les demandes voyagent seulement le long de la chaîne de hopnodes, avec chaque hopnode connaissant seulement l'adresse d'IP du nœud l'ayant précédé, et celui vers lequel la transaction est dirigée selon le type de service requis. Les réponses reviennent le long de la même chaîne jusqu'à ce qu'ils atteignent la personne ayant fait la demande (demandeur d'origine). Même le premier nœud, contacté directement après la requête du demandeur d'origine ne sait pas qui celui-ci est, car ce dernier ressemble à n'importe quel autre hopnode.

Dans le cadre du réseau Force, des adresses publiques hachées uniques (Unique Hashed Public Addresses - UHPA) sont utilisées pour identifier les nœuds. Les UHPAs sont stockés par les masternodes aux côtés d'autres données de service vitales pour produire une base de données dynamique à laquelle les nœuds de paiement peuvent se référer pour déterminer les nœuds optimaux à inclure dans les chaînes ad-hoc pour chaque demande de service. Les UHPAs sont utilisés pour corréler les informations publiques avec les nœuds, tandis que les adresses IP traditionnelles sont utilisées uniquement par les nœuds de paiement pendant le processus de génération du hopnode et par les hopnodes eux-mêmes (voir section III D pour plus de détails).Les adresses IP ne sont utilisées que lorsque nécessaire, pour activer la communication TCP/IP de base entre les nœuds.

Pour compléter le mécanisme AHCR, et former une solution de cartographie et de routage efficace et complète, Force Network utilisera une architecture de réseau à grande échelle canalisé (LargeScale Tunneled Network - LSTN), où un UHPA connu de

l'éventail des masternodes sera automatiquement assigné à chaque nœud participant. L'utilisation d'un LSTN obfusque complètement toutes les adresses IP vis-à-vis du réseau de masternodes publiquement accessibles. L'adresse IP de chaque nœud contracté est envoyée uniquement au nœud de paiement après réception du paiement du contrat.

Un nœud peut opter pour la fourniture simultanée de plusieurs services et ensuite rejoindre plus d'un DSH en même temps. Avant que le nœud ne joigne un nouveau DSH, il génère un nouveau UHPA et le télécharge vers les masternodes. Cela réduit les vecteurs d'attaque vu que les identités de service sont plus difficiles à corréler. Même les DSHs ne contiendront aucune information de routage et constitueront seulement de simples et efficaces constructions de regroupement de service pour les nœuds participants.

III. C Communication avec le réseau

L'établissement de services pour la première fois nécessite un délicat va-et-vient afin de garantir le respect de la vie privée et la protection contre la censure. Dans cette section, nous décrivons le processus que Force Network entreprendra pour utiliser un service à partir du moment où le client se connecte à un masternode, jusqu'au moment où le client reçoit les données demandées.

1. Le client demande la liste des services hébergés par le masternode le plus proche et choisit un service. Sont énumérés le prix minimum requis, une adresse de portefeuille et le type de service fourni.
2. Le client envoie un montant de FOR à l'adresse spécifiée avec les éléments suivants attachés à la transaction :
   — La clé publique d'une paire de clés unique générées pour décrypter les données
   — L'emplacement approximatif du client pour l'optimisation des itinéraires (optionnel)
   — Toute autre information requise pour le type de service offert.
3. Un nœud de paiement associé à l'adresse de portefeuille est averti par le paiement et génère une chaîne de hopnodes. Ce processus met en place une connexion cryptée et anonyme entre le client et le fournisseur de services. (les étapes sont décrites ci-dessous dans ≪Comment les chaînes de hopnodes sont créées≫).
4. Le nœud de paiement crypte l'adresse IP du point d'entrée avec la clé publique du client et envoie une micro-transaction au client avec ces données attachées.
5. Le client décrypte l'IP du hopnode d'entrée en utilisant la clé privée qu'il a généré à l'étape 2 et bénéficie maintenant d'un point d'entrée sur Force Network, et de toutes les clés de cryptage nécessaires au multi-cryptage de la demande de données pour chaque saut (hop). (voir la section cryptage de l'IP du hopnode pour plus de détails).
6. Le client peut maintenant multi-crypter et envoyer/recevoir des données comme d'habitude pour le service à/de l'IP point d'entrée de la chaîne hop. Le hopnode d'entrée transmet les données à l'IP du hopnode suivant défini par le nœud de paiement, et les données seront acheminées de cette façon jusqu'à ce qu'elles atteignent le nœud d'hébergement final.

III. D Comment les chaînes de hopnodes sont créées (processus de genération de chaînes de hopnodes)

Une fois que le client envoie le paiement à l'adresse de portefeuille des nœuds de paiement, le nœud de paiement générera une chaîne hop pour que le client se connecte au nœud de service demandé. Pour que le réseau fonctionne rapidement et sans accroc, les nœuds de paiement doivent être très économiques sur la façon dont ils génèrent des chaînes de hopnodes. Chaque chaîne peut être générée dynamiquement, de manière unique et singulière par rapport à la demande du client. Les chaînes doivent également être résilientes et disposer d'une bonne longévité. Par conséquent, le processus de génération de chaîne prend place aussi rarement que possible.

Les masternodes fournissent une liste de chaque hopnode par UHPA, celle-ci incluant l'adresse de portefeuille, la clé publique de cryptage, la géolocalisation approximative, le rapport de disponibilité, et le coût lié à ces services. Un seul nœud exécutant un seul portefeuille peut avoir plusieurs UHPAs pour différents services rendus. Les nœuds de paiement utilisent cette liste afin de contracter dynamiquement les meilleurs nœuds pour fournir le service au client. Dans le cas de notre service initial similaire à l'Internet, le mieux signifierait que les nœuds situés les plus près du client seraient contractés, afin de minimiser la latence.

Lorsqu'un nœud de paiement localise des hopnodes appropriés, il envoie le paiement avec un paquet de contrat attaché et chiffré avec la clé publique du nœud. Le paquet de contrat inclut :

— Un identifiant de service pour identifier ce contrat ;

— Une clé mot de passe pour identifier et authentifier l'utilisateur final ;
— Une clé privée pour décrypter les données multi-cryptées via une étape pour rendre le pistage de données à travers les nœuds impossible ;
— L'adresse IP du nœud suivant dans la chaîne vers lequel acheminer les données ;
— Les adresses IP de hopnodes supplémentaires si le nœud principal échoue (service optionnel) ;

Si un service souhaite réduire au minimum la génération de hopnodes supplémentaires dans le cas où l'un échoue, d'autres IPs de saut suivant peuvent être fournis lors de la première génération de la chaîne. Si le point principal échoue, un point alternatif peut être tenté sans qu'il ne soit nécessaire de générer une nouvelle chaîne hop.

S'il n'y a aucun moyen pour un hopnode de transmettre les données, un signal d'échec est renvoyé le long de la chaîne vers le client, entrainant un remboursement du service payé sans les frais de transaction.

Le client enverra ensuite une autre transaction au portefeuille des nœuds de paiement pour générer une nouvelle chaîne. Ces transactions pourraient être des micro-paiements pour la solution la moins coûteuse ou englober une plus grande rémunération pour des services achetés à l'avance.

Ce mécanisme de téléchargement/récupération concernant la chaîne hop a de multiples avantages :

— L'adresse IP des nœuds de paiement et d'hébergement de contenu n'est jamais révélée au client.
— L'adresse IP du client n'est jamais révélée aux nœuds de paiement ou d'hébergement de contenu.
— Les nœuds de paiement ont la possibilité de surveiller préventivement l'état du nœud et d'envoyer de nouvelles adresses IP de hopnodes si nécessaire.
— Les hopnodes ne connaissent que l'adresse IP les précédant, que celle les suivant dans la chaîne. Ils ne savent pas à quelle étape de la chaîne ils sont, de sorte qu'ils ne peuvent pas savoir si l'adresse IP précédente est un client, ou si la prochaine IP est la destination finale.

Toutes les communications effectuées sur Force Network seront cryptées à l'aide d'algorithmes de cryptage supportés par le matériel. Cela les différencie des certificats SSL traditionnels, qui nécessitent des noms de domaine connus et centralisés comme bénéficiaire de la fiducie. Comme les navigateurs traditionnels tels que Chrome, Firefox et Safari sont conçus pour exiger une telle certification SSL afin d'informer de manière fiable l'utilisateur que leur communication est cryptée, Force Network utilisera navigateur embarqué personnalisé, dans le portefeuille et basé sur Chromium, tout en maintenant le même niveau d'utilisabilité et de convivialité à laquelle les utilisateurs sont habitués. Le navigateur et le portefeuille seront Open-source pour permettre des audits de sécurité indépendants.

Une fois que l'ensemble de la technologie ci-dessus sera entièrement développé et sécurisé, la prochaine étape sera de transposer certains de ces services sur les navigateurs traditionnels de bureau et mobile en utilisant une extension personnalisée et/ou une application mobile comme pont entre le les nécessités de design du navigateur et l'architecture du réseau Force. Cela permettra à Force d'étendre ses services offerts à un marché beaucoup plus vaste.

Chaque DSH définira le nombre de hops requis pour son service. Cette autonomie permettra à certains services d'être plus privés que d'autres, en échange d'un coût accru. Certaines données, comme les pages d'index, peuvent être répertoriées comme non privées et peuvent être servies directement à partir des masternodes en utilisant l'Internet traditionnel.

Les chaînes de hopnodes sont créées par le nœud de paiement quand le paiement est reçu de la part du client. Le nœud de paiement peut prendre en compte plusieurs facteurs lors de la conception de la chaîne de hopnodes demandée en fonction du service, de la largeur de bande requise, de l'emplacement approximatif, etc.

III. E Comment le nœud de paiement génère la chaîne à l'envers pour restreindre l'identification d'adresses IP

Les adresses IP sont de puissants outils. Une adresse IP est la méthode par laquelle les hôtes de contenu peuvent être identifiés et le contenu supprimé. Puisque nous construisons un réseau de pages anti-censure, nous devons être très prudents concernant le protocole pour la gestion de la sécurité des adresses IP, tout particulièrement en ce qui concerne l'IP du nœud d'hébergement final. Pour protéger ces informations sensibles, nous utiliserons un système de connaissances restreintes, de façon à ce que seul le nœud précédent au sein d'une chaîne connaisse l'adresse IP suivante dans la chaîne et qu'aucun des nœuds de service ne soit au courant de la destination finale.

1. Le nœud de paiement obtient l'IP du nœud d'hébergement soit après en avoir contracté un, soit en en utilisant un que les fournisseurs de services déterminent.
2. Le nœud de paiement contracte le hopnode final dans la chaîne et lui envoie l'adresse IP du nœud d'hébergement comme le prochain hop. Ce hopnode envoie son IP au nœud de paiement (à l'aide d'une autre micro transaction).
3. Éventuellement le nœud de paiement atteint le premier hopnode dans la chaîne et envoie cette adresse IP au client comme point d'entrée.

IV Caractéristiques avancées supportrices du réseau

IV. A Une vérification de l'état de santé du réseau et de la disponibilité des nœuds à partir du hachage (Hash-based Node Uptime Verification - HNUV)

Dans le cas où un nœud souhaite interrompre ses services (de manière permanente ou temporaire, et indépendamment de la raison), il doit passer par la procédure de retrait appropriée. Cela implique l'envoi d'une notification de retrait au masternode, qui peut mettre à jour la base de données des nœuds. Cette base de données est périodiquement contrôlée par les nœuds de paiement afin de déterminer la disponibilité des nœuds concernés par la génération de chaînes hop ainsi que les pénalités de temps d'interruption.

Si un nœud est déconnecté sans suivre les procédures de retrait, il y aura un mécanisme de nouvelle tentative de connexion intégré dans la chaîne de hopnode. Le nœud qui est situé en amont du nœud défaillant enverra l'adresse IP de ce dernier au nœud de paiement à l'aide d'une micro transaction. Le nœud de paiement enverra alors ou bien une nouvelle adresse IP à suivre à ce hopnode ou bien générera une toute nouvelle chaîne et l'enverra au client. En fonction du régime de paiement contractuel, le nœud de paiement prend note du nœud défaillant, le pénalise et envoie un rapport à la base de données d'informations sur la santé des masternodes.

Pour ce faire, chaque nœud doit avoir un portefeuille Force ouvert et en cours d'exécution. Le portefeuille enverra régulièrement des données chiffrées au réseau de masternodes, incluant l'UHPA, les types de services offerts, la localisation approximative pour un routage efficace, le temps de disponibilité et le statut. Cela permettra aux nouveaux nœuds de paiement de choisir le meilleur itinéraire pour chaque demandeur. Avec suffisamment de rapports concernant un nœud défaillant, le masternode mettra à jour l'état des nœuds ainsi que leur ratio de disponibilité dans la base de données, puis propagera la mise à jour aux autres masternodes. Lorsque le nœud est de nouveau en ligne, il doit renvoyer son entrée de service au masternode pour obtenir l'autorisation d'être répertorié. Comme il est impossible pour les hopnodes d'envoyer des données aux nœuds de paiement sans transaction, ils transmettent périodiquement des informations de santé au réseau de masternodes afin qu'ils puissent être contactés par de nouveaux nœuds de paiement.

Pour encore protéger davantage le réseau contre les acteurs malveillants et assurer la QoS, le mécanisme HNUV sera mis en place. Tout comme les systèmes de consensus blockchain peuvent choisir d'accepter ou de rejeter un nœud du réseau basé sur l'intégrité des données qu'il diffuse via la simple vérification de son hachage, toute tentative malveillante de la part d'un nœud de conserver son statut actif pour le paiement en altérant son client afin d'envoyer de fausses données de disponibilité sans rendre le service offert par le DSH dont il est membre, se traduira par son rejet du réseau suivi d'une période punitive temporaire de blocage s'il veut être réintégré. Cela se fera en vérifiant le hachage du code client, ainsi que les paramètres clés qu'il diffuse périodiquement à l'aide d'un algorithme unique de hachage et de vérification, le HNUV.

IV. B Niveaux de confidentialité personnalisables

Différents types de contenu peuvent être soumis à différents niveaux de sécurité en fonction de la façon dont le nœud de paiement est établi pour le service en question. Nous décrivons les niveaux les plus élevés de sécurité dans ce article de documentation technique, parce que ceux-ci sont les plus difficiles à mettre en œuvre. Des niveaux et mesures de sécurité moindres (moins de hops, pas hops, moins de cryptage, etc.) sera disponible pour les services qui désirent privilégier la vitesse par rapport à la confidentialité absolue ou la résilience de contenu.

IV. C Hébergement de contenu et/ou de services sur Force Network

Les fournisseurs de contenu et de services ont de nombreuses possibilités de rendre disponible leur contenu sur Force Network. Par exemple, partons du principe que vous souhaitez héberger une page Web résistante à la censure sur Force Network. Il vous faut pour cela :

1. Paramétrer (ou contracter) un nœud de paiement et instaurer un prix pour votre contenu. En cas de contenu gratuit, celui ci est facilement distribué par le biais d'un réseau existant, mais doit être accessible à tous. Les contenus ou services qui utilisent le système d'autorisation pour restreindre l'accès, doivent facturer un prix d'accès.
2. Paramétrer (ou contracter) un réseau de hopnodes à utiliser. Le nœud de paiement peut également être désigné pour utiliser la base de données de masternodes pour contracter des hopnodes dynamiquement pour chaque utilisateur disposant de nœuds qui répondent à sa liste de critères.
3. Configurer (ou contracter) un netnode qui se connecte au site Web DSH pour stocker et héberger votre contenu.
4. Mettre en ligne une page d'index de service sur le réseau de masternodes et permettre votre nœud de paiement d'accepter la rémunération de la part des clients. Il peut maintenant générer des chaînes de hopnodes pour les clients vers le netnode pour la livraison de contenu.

Par la suite, les développeurs vont créer des services qui automatisent les tâches communes sur Force Network et fournissent des matrices type. Ils bâtiront également des suites complètes de gestion de contenu qui surplomberont Force Network. Un réseau de service ou un netnode peut en contracter un autre pour agréger le contenu en un seul emplacement, au bénéfice de l'utilisateur final en termes de confort.

IV. D Modèle de contrôle d'accès au réseau

La sécurité et la confidentialité sont au cœur du réseau de la force. Conformément à notre volonté de mettre l'accent sur la sécurité et la protection de la vie privée, nous développerons un vaste mécanisme de contrôle d'accès à base d'autorisations au niveau du réseau. Les acteurs malveillants n'auront aucun moyen de se connecter directement aux netnodes de prestation de service. Ils devront passer par le schéma d'autorisation complet mis en place par les nœuds de paiement pour afficher ne soit ce que l'adresse IP du premier hopnode. De plus, ils doivent également posséder la clé de service correcte avant que le nœud d'entrée puisse acheminer correctement leur demande.

Pour illustrer la puissance de cet accès limité au réseau, comparons-la au modèle actuel. Avec l'Internet existant, il n'y a pas de restrictions intégrées à l'accès au contenu. Chaque page Web doit avoir ses propres fonctionnalités de gestion de compte pour cacher son contenu aux yeux du public. N'importe qui a accès aux champs « nom d'utilisateur » et « mot de passe ». Sans restrictions en place, l'Internet traditionnel est constamment vulnérable aux injections de code malicieux et aux attaques de « force brute ». En outre, l'adresse IP du serveur est directement à la disposition des attaquants, ce qui rend le site vulnérable aux attaques de déni de service (DDoS) et autres attaques de serveur.

En revanche, Force Network requiert d'un utilisateur potentiel de passer par plusieurs couches de sécurité. À moins que l'accès soit explicitement accordé au préalable, le nœud de paiement ne vous permettra pas l'obtention de l'adresse IP du premier hopnode. Même si cela était le cas, les nœuds de service ne propageraient pas votre demande, ou ne fourniraient pas quelconque autre service sans la clé de service requise. À partir de la clé de service, les demandes peuvent même être acheminées vers des netnodes différents, en fonction du niveau d'accès établi. Cet accès, contrôlé au niveau du réseau, réduit considérablement les vecteurs d'attaque de la part d'un hacker.

Chaque page, fichier ou service peut avoir sa propre liste de permissions, avec des options telles que : autoriser l'accès à tout le monde, restreindre l'accès en lecture, restreindre l'accès en écriture, etc. Étant donné que les nœuds sont distribués, il n'est pas nécessaire d'héberger des informations privées sur le même nœud que les informations publiques. Cela signifie qu'un site Web peut avoir une page d'index accessible au public visible pour tous et hébergé sur le réseau de nœuds gratuits. La page d'index public pourrait indiquer ce que le site offre, la tarification, ainsi qu'une adresse de portefeuille de nœud de paiement. Le reste du site/service ne serait alors qu'accessible après avoir rempli la liste d'exigences du nœud de paiement en question.

V Modèle utilitaire et économique du jeton

V. A Cas d'utilisation du jeton FOR

1. **Paiement des services.** Ceux-ci sont remis directement par les consommateurs aux nœuds de paiement escrow, qui à leur tour les relaient aux noeuds fournissant le service, moins les frais de transaction. Le nœud de paiement peut regrouper des paiements en fonction du schéma de paiement des nœuds pour réduire la charge sur le réseau et les frais de transaction.

2. **Gestion de l'échange des clés d'authentification.** Les clients paient l'adresse du portefeuille associé à un service, répertorié dans la base de données des masternodes. Un nœud de paiement surveille le portefeuille et envoie les clés d'accès au client après avoir généré la chaîne réseau.
3. **≪Staking≫ des jetons pour la mise en place d'un nœud (master, paiement, hop, net, etc) pour assurer de bons comportements**
4. **Rémunération des masternodes et de ≪ stakeurs ≫ de jetons pour leur services permettant l'établissement du consensus, améliorer des services et la sécurisation du réseau Force.**

V. B ≪Staker≫ les jetons FOR

N'importe qui peut transformer son appareil en n'importe quel type de nœud Force de son choix, en fonction des ressources qu'il possède et souhaite allouer au réseau. Un certain type de nœud ne peut être activé que si les critères en ressources spécifiques aux nœuds sont remplis (tels que la caution en jetons et la configuration matérielle requise).

Par conception, plus un type de nœud est essentiel au bon fonctionnement du réseau, plus la caution en jetons qu'il exige pour qu'un utilisateur puisse l'activer est élevée. Par conséquent, plus un nœud devient essentiel, et moins les utilisateurs sont susceptibles de vouloir lancer une attaque malicieuse sur le réseau en utilisant ledit nœud, car ils risquent une part encore plus grande de leur propre investissement (caution). Ceci est la prémisse fondamentale qui conduit à la sécurité du consensus proof-of-stake appliquée au réseau Force.

V. C Rémunération des services

Force Network fonctionne en masquant autant d'informations concernant la connexion que possible. Cette section décrira comment les services sont rémunérés à l'aide de la crypto-monnaie FOR.

Le nœud de service conserve le suivi de l'utilisation en fonction de la clé de service générée lors de la génération de la chaîne réseau. Si nécessaire, il peut informer le client lors de l'envoi de données que des fonds supplémentaires sont nécessaires et peut arrêter l'accès au contenu. Le client peut ensuite envoyer des fonds supplémentaires au nœud de paiement, lequel met à jour l'état du paiement dans le nœud de service. Le nœud de paiement utilisera ces fonds pour payer les hopnodes en utilisant le schéma de service convenu auparavant.

Les hopnodes peuvent suivre les données d'utilisation en fonction de la clé de service. Différents nœuds auront des différentes exigences de paiement, ces dernières étant basées sur les préférences des opérateurs de nœud. Par exemple, certains hopnodes peuvent limiter le nombre total de fois qu'une clé de service peut être utilisée, ou la bande passante utilisée par cette clé. Si la paiement n'est pas conforme avec ce qui est attendu, le hopnode peut signaler les nœuds de paiement n'agissant pas conformément à ce qui était prévu au réseau de masternodes. Les nœuds malveillants seront condamnés à une amende à partir des pièces qu'ils stakent.

V. D Tarification dynamique du service (Dynamic Service Pricing - DSP)

Étant donné que le réseau sera distribué et que la participation des fournisseurs de services sera volontaire, l'architecture du réseau doit être en mesure d'assurer un niveau élevé de disponibilité des services pour s'aligner avec la demande. Une façon relativement simple d'assurer une disponibilité de service inégalée serait d'inciter économiquement les fournisseurs de services en créant un mécanisme de tarification intelligente, équitable et dynamique, pour les services qu'ils proposent. Pour répondre à cela, nous suggérons le mécanisme de tarification dynamique du service (DSP). Le DSP est une fonction calculée et vérifiée par le réseau, dont le but est de déterminer le point de prix le plus économique pour les fournisseurs de services, autant que possible en temps réel, à base d'une combinaison de facteurs :

1. **Score composite de spécification du réseau de service (Composite Service Network Requirement Score - CSNRS) :** Le réseau évaluera le niveau général des ressources nécessaires à chaque service pour fournir une qualité de service suffisamment élevée, créera un score composite pour servir de multiplicateur, et, tous les autres étant égaux, plus les exigences du service seront élevées, plus le niveau du prix sera élevé afin d'assurer une compensation adéquate.
2. Le ratio du nombre d'utilisateurs actifs consommant chaque service (demande de service) N_u par rapport au nombre de netnodes participant activement au DHS (offre de services) N_{noeud}.
3. (Facultatif) Valeur fiat du jeton FOR, basé sur la moyenne pondérée en fonction du volume récupérée à partir de données fournies par les échanges.

Les DSPs spécifiques au service calculeront et normaliseront leurs données pour créer un classement des prix de service. Chaque score DSP normalisé sera multiplié par l'indice des prix du réseau (IPR), lequel est calculé via le calcul décrit dans le paragraphe 2 ci-dessus, à la fois en tant que ratio et en tant que nombres absolus.

Chaque nœud recevra également un rang de base déterminé par ses performances réseau et la fiabilité de ses services. Ceci créera un élément de concurrence entre les nœuds les incitant à devenir le nœud le plus fiable pour chaque service. Un nœud qui à passe continuellement d'un service à l'autre et génère de fait des interruptions sera noté bien plus négativement qu'un nœud qui persiste même si la tarification à l'échelle du service diminue.

Les informations concernant les prix seront propagées par le réseau et seront accessibles à tous les participants. À partir des données DSP, les clients seront en mesure de prendre des décisions instruites par rapport à leur consommation de services et les fournisseurs de services seront en mesure de déterminer à quelles ruches leurs nœuds doivent se connecter à un moment donné dans le temps. Cette mesure servira également à réguler la demande. Trop de nœuds ne prendront pas prendre en charge les services sous-demandés, et inversement, trop peu de nœuds ne pourront pas prendre en charge les services surdemandés.

VI Conclusion

Dans cet article, nous avons présenté un aperçu de haut niveau d'une nouvelle infrastructure de réseau décentralisée qui alimente les services réseau évolutifs décentralisés (Decentralized Scalable Network Services - DSNS). Dans ce nouveau paradigme, les clients seront en mesure de consommer des services de réseau ad-hoc proposés par les fournisseurs de services, avec très peu de besoins en connaissances antérieures ou de ressources. Cela se fera via un mécanisme de jumelage client-fournisseur agnostique concernant les services, impartial, autonome et digne de confiance, tout en garantissant l'obfuscation de l'identité des participants. Le protocole comporte deux types d'architectures révolutionnaires : le routage de chaîne ad-hoc (Ad-hoc Chain Routing - AHCR) et le réseau à grande échelle canalisé (Large-Scale Tunneled Network - LSTN). Celles-ci sont désignées de manière à permettre aux communications et au contenu gérés par le réseau d'être résistants à la censure en utilisant du cryptage de bout en bout.

Les fournisseurs de services peuvent joindre et/ou migrer entre les services ou se retirer du réseau de manière simple et fluide, et sont incités économiquement à maintenir la qualité de leur service pour empêcher la dégradation de celui-ci, en utilisant des algorithmes de classement et de tarification en temps réel maintenus par un consensus inter-réseau. Les acteurs responsables de la sécurité et de la résilience de l'infrastructure sous-jacente sont régulièrement indemnisés par le réseau pour leurs services en utilisant son jeton économique, le jeton FOR, tandis que les fournisseurs de services de réseau sont en concurrence directe au niveau de la qualité et de l'expérience des services qu'ils offrent afin d'être rémunérés directement par les utilisateurs finaux avec ledit jeton.

Les services de réseau traditionnels sont intrinsèquement désavantagés en raison de leur nature centralisée ; Ils exigent la confiance sur plusieurs niveaux afin de maintenir l'intégrité du service. Par exemple, les initiatives mondiales qui cherchent à saper la neutralité du net pour les participants honnêtes prennent de l'élan, et peuvent être facilement mises en place par les autorités centrales et les prestataires de services, tant que le consensus est concentré entre les mains de quelques acteurs. Comme Force Network repose sur un consensus de réseau sans confiance en utilisant un mécanisme proof-of-stake, il devient économiquement impossible de tenter de créer une brèche dans n'importe quel aspect de son fonctionnement.

Force Network vise non seulement à protéger la liberté d'information contre la censure indésirable à l'échelle mondiale, mais aussi à perturber le paysage commercial établi grâce à son architecture robuste et résiliente. Avec des applications de marché très larges, telles que la communication cryptée, la livraison de contenu, les médias streaming, le Pay-Per-View et le Cloud Computing, ainsi que des services de stockage, et à un moment où les entreprises démontrent une intérêt de plus en plus prononcé pour les services entièrement gérés, l'automatisation des tâches, le matériel délocalisé et sous-traité, le déploiement rapide des services et le stockage de données de grande taille, l'éventail d'opportunités pour Force Network est vaste avec son profil commercial à bas coûts, entretien, sans frictions et ne nécessitant pas de confiance comme dans les systèmes réseaux traditionnels.

Avec tout un ensemble de protocoles Internet, cette architecture de réseau ouvrira la voie à un nouveau type d'Internet. Ce document servira de référence pour les développements et sera corrigé et amélioré au fil du temps, en abordant les failles et les vecteurs d'attaque potentiels et en décrivant en détail

les implémentations de niveau inférieur au fur et à mesure qu'elles seront déployées.

Remerciements particuliers

Les auteurs voudraient remercier tout particulièrement ihackcoinz et PDQ pour leurs idées et leur contribution à la rédaction de ce document.