PROJET SENTINEL

TOKEN : $DVPN

VALIDATOR : WWW.STAKELAB.FR

DELEGATION : SENTVALOPER1GWQT4JZHTVMS8U57GPL4TZXJXQQ8FSS2J3HX48

SENTINEL

1. Les 5 points clés de SENTINEL :
    a. **Provable Encryption -** Etablissement d'un cryptage de bout en bout entre l'utilisateur et le serveur auquel l'utilisateur a l'intention d'accéder aux données, grâce à des systèmes de transparence et de vérification de l'intégrité des applications à code source ouvert.
    b. **Proof of Bandwidth -** Avoir un système capable de fournir une bande passante suffisante du serveur en échange de la compensation convenue de l'utilisateur d'une manière fiable et prouvable.
    c. **Proof of No Logs -** Aucun journal relatif à l'historique de navigation ou de données de l'utilisateur n'est stocké de manière centralisée par les développeurs d'applications.
    d. **Distributed Exit Nodes -** Voir un réseau de "nœuds de sortie" (serveurs dVPN) dont la propriété est répartie entre de nombreux participants qui ne connaissent pas l'identité de l'utilisateur.
    e. **Distributed Relay Network -**Disposer d'un réseau d'interconnexion robuste ayant pour gouvernance forte la non tracabilité des hôtes des nœuds de sortie tout ne gardant une confidentialité.

2. Les parties prenantes impliquées dans le réseau Sentinel sont :
    a. Validateurs - Les participants au consensus dans le futur Sentinel - Cosmos Hub qui sont responsables de la sécurisation du réseau et participent à la gouvernance de l'écosystème Sentinel.
    b. Utilisateur - L'utilisateur final qui souhaite accéder à un dVPN construit sur le cadre Sentinel afin de sécuriser l'Internet d'une manière prouvable.
    c. Hôtes de nœuds dVPN - Membres de la communauté ayant l'intention de monétiser la fourniture de bande passante inutilisée aux dVPN construits sur le réseau Sentinel, en hébergeant soit un nœud de sortie, soit un nœud de relais (en respectant certains seuils de niveau de service requis).
    d. Créateur d'application dVPN - Le créateur d'un dVPN construit sur le cadre Sentinel tout en utilisant la zone dVPN Sentinel comme couche d'infrastructure. Le créateur de l'application est responsable de l'acquisition d'utilisateurs et du marketing afin de générer des revenus pour pouvoir payer les hôtes des nœuds dVPN.

3. Trois problèmes clés qui constituent des barrières à l'entrée pour les entreprises VPN nouvelles et existantes, atténués par l'écosystème Sentinel :
    a. Coût et processus de développement d'une application dVPN
    b. Gestion des nœuds et traitement des demandes DMCA
        i. Les principaux fournisseurs de services en nuage restreindraient inévitablement l'accès au serveur des hôtes de nœuds de sortie en raison de la diffusion en continu ou du téléchargement de contenu piraté à partir du nœud, ce qui attirerait sans aucun doute les demandes DMCA. Les organisations VPN centralisées doivent généralement s'appuyer sur des "services d'hébergement offshore" qui n'offrent pas nécessairement le même degré de fiabilité en termes de temps de fonctionnement et d'assistance client en temps réel que les fournisseurs mieux établis.

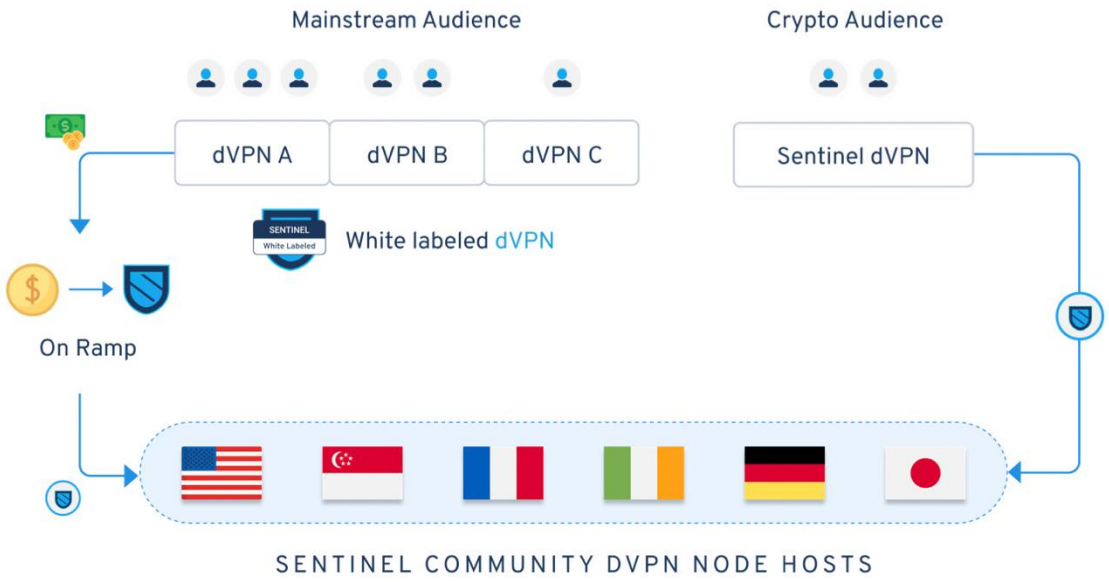
ii. L'écosystème Sentinel supprime la responsabilité de la gestion des nœuds de sortie pour les organisations qui créent des applications sur le cadre Sentinel grâce à l'intégration des hôtes de nœuds basés sur la communauté de Sentinel.
iii.
iv. Les propriétaires d'applications VPN auront la possibilité de créer des contrats de service et d'établir certaines normes de qualité avec les hôtes de nœuds dans l'écosystème Sentinel, sans avoir à gérer eux-mêmes la propriété de ces serveurs.

c. Menaces potentielles pour la sécurité et risques associés aux pirates informatiques
   i. Les solutions VPN centralisées et à code source fermé ne peuvent pas faire l'objet d'un examen par les pairs et ne peuvent donc pas être évaluées par des experts en sécurité impartiaux. Cela peut conduire à des vulnérabilités potentielles ou à des risques de sécurité qui ont la capacité de nuire ou de perturber sérieusement la réputation de l'entreprise qui fournit le service.
   ii. L'incidence d'une vulnérabilité de sécurité ne met pas seulement les utilisateurs en danger par l'exploitation potentielle de leurs données, mais crée également un énorme manque de crédibilité dans l'organisation VPN elle-même, ce qui peut affecter de manière drastique les revenus et la durabilité de l'organisation.
   iii. La structure open-source fournie par Sentinel réduit considérablement les risques de faille de sécurité. Un exemple de la force des logiciels libres est l'utilisation par les organisations militaires du monde entier de Linux comme système d'exploitation préféré pour la majorité de leurs systèmes. Linux est un logiciel entièrement libre et fait l'objet d'une révision constante par des tiers, contrairement à une suite logicielle telle que Windows, qui est fermée et connue pour ses problèmes de sécurité.
   iv. Bien que le cadre Sentinel offre les outils ainsi que l'infrastructure nécessaires pour construire et exploiter un service dVPN robuste, le propriétaire de l'application a la responsabilité d'acquérir des clients et de comprendre son marché cible spécifique afin de déployer des stratégies de marketing efficaces. Il est important de noter que le développement et l'exécution du produit ne sont qu'une partie de l'équation. L'autre partie est centrée sur l'intégration effective des utilisateurs et la mise en place d'un produit demandé par le marché.
   v.

Sentinel n'est pas une seule application dVPN, mais un réseau d'applications dVPN indépendantes construites sur le cadre du protocole dVPN de Sentinel.

L'objectif de l'écosystème Sentinel est de décentraliser l'industrie des VPN et d'introduire le "dVPN" auprès du grand public. Toutefois, cet objectif ne sera pas atteint par le lancement et la maintenance d'une seule application destinée aux consommateurs (le dVPN Sentinel), mais en établissant d'abord et en développant ensuite un cadre qui peut être utilisé pour créer un réseau de VPN décentralisés exploités indépendamment.

SENTINEL

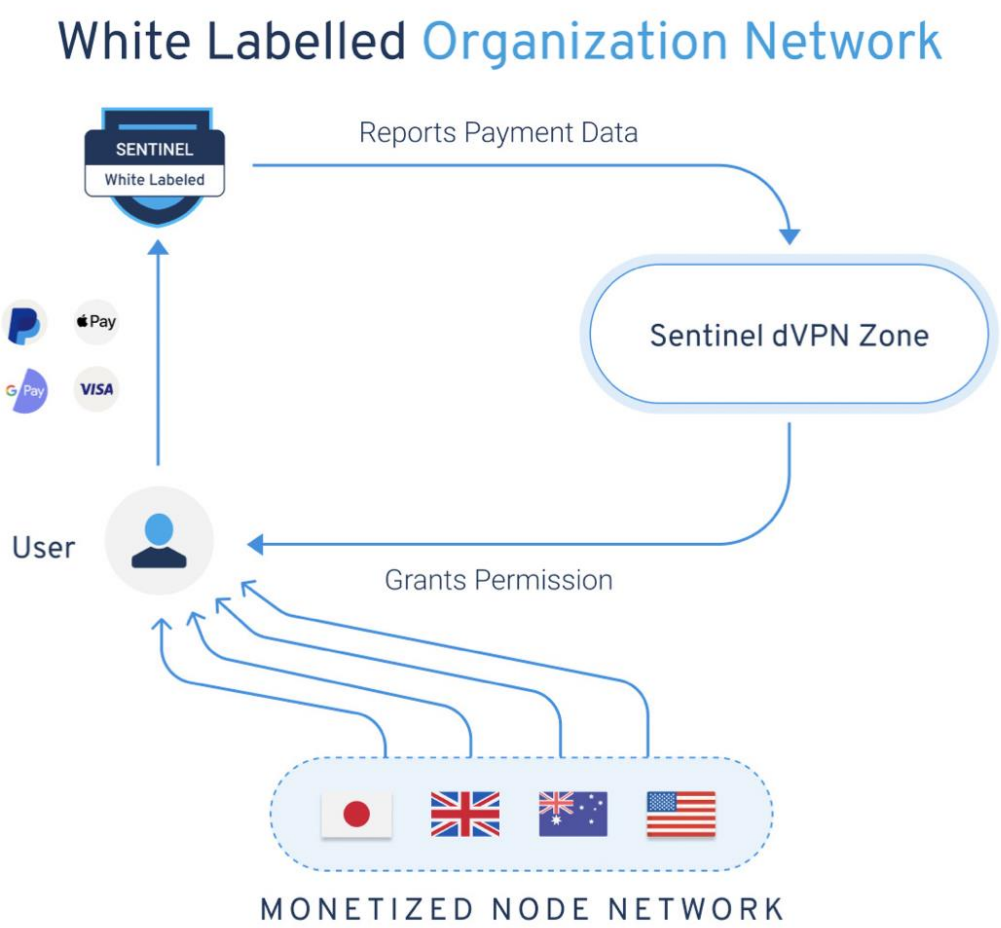


Les 4 principes clés pour le succès d'une application dVPN efficace sont les suivants :

a. **Strong UI/UX**
b. **Efficient Pricing Strategy**
c. **Integration of Mainstream Payment Gatewa**

Visa/Mastercard | Apple Pay | Google PlayStore | E-Wallets (e.g. Paypal, Skrill etc.)

Le fait de n'avoir qu'une option de paiement liée aux crypto-monnaies créerait une barrière massive à l'entrée ; empêchant le consommateur moyen de s'éloigner facilement d'un fournisseur de services VPN centralisé. Alors que les nœuds hébergés dans l'écosystème Sentinel doivent être payés en utilisant des actifs numériques basés sur la blockchain, les propriétaires d'applications dVPN ont la possibilité de monétiser leurs applications en utilisant des canaux de paiement en monnaie fiduciaire. Les monnaies fiduciaires collectées peuvent ensuite utiliser un service "on-ramp" pour convertir la monnaie fiduciaire en un actif numérique qui est ensuite utilisé pour payer les hôtes des nœuds.



d. **Diversity of Routing Protocols**

SENTINEL

Aperçu de l'architecture de la blockchain basée sur Sentinel Cosmos :

Les solutions d'interopérabilité qui facilitent l'échange d'actifs et de données entre divers réseaux décentralisés alimentés par des crypto-monnaies ont la capacité de réduire le tribalisme dans le secteur. Dans ce contexte, le "tribalisme" fait référence à la tendance agressive que manifestent les réseaux décentralisés lorsqu'ils tentent d'établir ou de montrer leur supériorité sur leurs homologues.
Le fait est que certains réseaux ont des propositions de services uniques, rendues possibles par leur architecture personnalisée et leur orientation de développement unique. L'interopérabilité permet aux participants de l'écosystème de profiter simultanément des mérites de chacun de ces réseaux sans avoir à établir de comparaison, ce qui permet une évolutivité/spécialisation horizontale.
Cosmos vise à réduire ce "tribalisme" dans l'écosystème en connectant ces chaînes concurrentes entre elles, réduisant ainsi efficacement une influence majeure qui les séparerait normalement. Le module IBC de Cosmos permettra à ces applications sur chaîne d'élargir leur marché cible en s'adressant à une base d'utilisateurs beaucoup plus large, ce qui facilitera l'acquisition de nouveaux clients en leur permettant d'accepter des paiements dynamiques inter-chaînes.
Actuellement, les initiatives d'interopérabilité les plus significatives entre Cosmos et d'autres réseaux de grande valeur et respectés comprennent les "ponts" interopérables construits entre Cosmos et ZCash et Polkadot.
L'écosystème Cosmos permet à Sentinel d'établir et de gérer sa propre chaîne native au niveau de la couche "Hub". Les applications dVPN construites sur le réseau Sentinel résident soit dans des zones partagées, soit dans leurs propres zones natives, en fonction des exigences de débit de chaque application.
Les chaînes construites à l'aide de Cosmos ont la possibilité de conserver leur autonomie en matière de gouvernance, tout en assurant l'interopérabilité entre les autres hubs et zones du réseau Cosmos.
Contrairement au modèle de jeton ERC20, les chaînes construites sur Cosmos n'auront pas à payer de frais dans le jeton natif de Cosmos "ATOM", mais pourront payer dans le jeton natif de la chaîne.

- **Hub and Zone Structure**
  - Sentinel utilise l'architecture Hub/Zone de Cosmos pour augmenter l'évolutivité des applications dVPN en faisant en sorte que toutes les transactions et les données spécifiques à l'application soient échangées sur la "Zone dVPN Sentinel" (ou sidechain), tout en faisant abstraction des transactions et de la gouvernance liées aux jetons sur le "Hub Sentinel" (ou main-chain). Les zones communiqueront avec la chaîne principale (hub) de Sentinel par le biais du protocole IBC (Inter-Blockchain Communication) de Cosmos. Une zone peut être comparée à un type de "canal d'état" qui est déployé pour une mise à l'échelle efficace.
  - La zone spécifique à l'application 'dVPN' aura sa propre gouvernance de consensus qui sera très probablement un sous-ensemble des participants au validateur de consensus du Hub. Bien qu'il n'y ait pas de valeur monétaire échangée au niveau de la zone, l'incitation et la désincitation des validateurs se feront au niveau du centre Sentinel.
  - Grâce à l'IBC, le centre du réseau Sentinel communique avec le centre Cosmos et les autres centres faisant partie du réseau Cosmos. Cela permettra non seulement aux services du réseau Sentinel de communiquer entre eux et d'accepter le jeton natif SENT

ou d'autres jetons de la liste blanche, mais aussi de les aider à se connecter à d'autres réseaux du réseau Cosmos.
    - La blockchain Sentinel - Tendermint peut accueillir des dApps et/ou des services qui fonctionnent dans leurs propres zones indépendantes en ayant une gouvernance spécifique construite sur le consensus Tendermint, permettant à leur propre ensemble de validateurs de vérifier les transactions
- **Throughput**
    - Tendermint utilise un système de consensus bPOS dans lequel les blockchains peuvent définir un nombre limité de validateurs afin d'obtenir un consensus plus rapide, tout en protégeant le réseau des "attaques byzantines".
    - Diverses solutions de communication P2P et de protection de la vie privée seront construites sur le réseau Sentinel et s'appuieront sur des modèles de revenus basés sur des microtransactions à fort volume. La blockchain Tendermint est donc parfaite pour soutenir le réseau Sentinel en raison de sa capacité à atteindre un TPS (transactions par seconde) élevé, surtout si on la compare aux "15 transactions par seconde" d'Ethereum, nettement inférieures.
    - Les transactions par seconde (TPS) pour les blockchains utilisant le consensus Proof-of-Work (POW) ont été relativement faibles.
    - Un cadre blockchain pour la création d'applications VPN décentralisées
    - 14
    - lentes et de nombreuses solutions de mise à l'échelle pour ces réseaux de consensus nécessitent un investissement élevé en matériel spécialisé.
    - Cosmos utilise un consensus unique de type Proof-of-Stake lié où les votes d'un nombre fixe de validateurs, avec un certain degré d'entropie, sont acceptés par le réseau à un moment précis. Cela augmente le débit global des transactions sur le réseau en raison d'un nombre fini de validateurs traitant les transactions.
    - Le système de consensus BFT de Tendermint permet au réseau Sentinel d'atteindre des vitesses de transaction plus rapides que celles de n'importe quel réseau PoW existant actuellement ; les réseaux PoW sont encombrés par un manque de finalité définie. Dans les systèmes basés sur les bPOS tels que Tendermint, la finalité quasi instantanée est obtenue par l'utilisation d'un système de vote à la ronde utilisant un nombre fini de validateurs, en permettant aux détenteurs de jetons de "lier" des jetons à des validateurs jugés dignes de confiance.
- **Interoperable**
    - La nature interopérable du protocole IBC de Cosmos permet la création d'une zone peg (adossée à une pièce stable). Cette fonctionnalité peut être développée pour les chaînes qui ne font pas partie de l'écosystème Tendermint ou Cosmos.
    - L'utilité de ces zones sera principalement pour les paiements inter-chaînes. Grâce à cette technologie, il est possible pour les nœuds hébergés par la communauté et fonctionnant sur le réseau dVPN Sentinel d'accepter des crypto-monnaies telles que Ethereum, BTC, PIVX, DASH, NEO, Dfinity, Cardano, etc. en échange de bande passante.
    - Toute crypto-monnaie peut être intégrée, indépendamment du fait qu'elle soit construite sur le SDK Cosmos. Cela est rendu possible par l'utilisation de "ponts", qui nécessitent l'établissement d'une connexion interopérable entre les deux réseaux. Le Hub Sentinel sera connecté à l'IBC Cosmos, ce qui permettra aux utilisateurs de dVPN d'effectuer

des paiements dans différentes devises ou pièces stables prises en charge par l'IBC Cosmos.

- Étant donné que le protocole IBC peut être utilisé efficacement pour la communication entre différents réseaux qui ont des mécanismes de consensus et des schémas structurels distincts (par exemple ZCash/Cosmos), Sentinel pense que le protocole IBC est extrêmement efficace pour l'extensibilité des transactions et l'efficacité liée au dAPP grâce à l'introduction du modèle Hub/Zone.
- La technologie fournie par le réseau Cosmos et Tendermint nous permet d'envisager une véritable économie de marché libre renforcée par des "intégrations de paiement inter-chaînes sans faille", ce qui n'a jusqu'à présent été possible avec aucune autre plateforme/réseau. Il s'agit de la première étape d'un long voyage vers la création d'applications blockchain qui seront adoptées dans le monde réel.

- **Governance**
  - Sur le réseau principal Sentinel basé sur Cosmos, la gouvernance du réseau sera entre les mains des validateurs. Ces validateurs seront déterminés démocratiquement sur le réseau principal Sentinel basé sur Cosmos par la délégation de jetons par les détenteurs. Le "pouvoir de vote" ou le poids des validateurs est déterminé non seulement par les performances historiques, mais aussi par la quantité de jetons qui leur est déléguée par les supporters de Sentinel.
  - Les propositions de gouvernance du réseau sont traitées par un ensemble de validateurs démocratiques, ce qui permet de contourner l'obligation de passer à une "nouvelle chaîne". Ces propositions peuvent inclure :
    - - l'acceptation de nouveaux validateurs ou le rejet de validateurs malveillants existants
    - - l'acceptation de nouvelles zones et de nouveaux ponts ou le rejet des zones et ponts existants
    - -des modifications de l'approvisionnement ou le verrouillage d'un compte malveillant ou piraté.

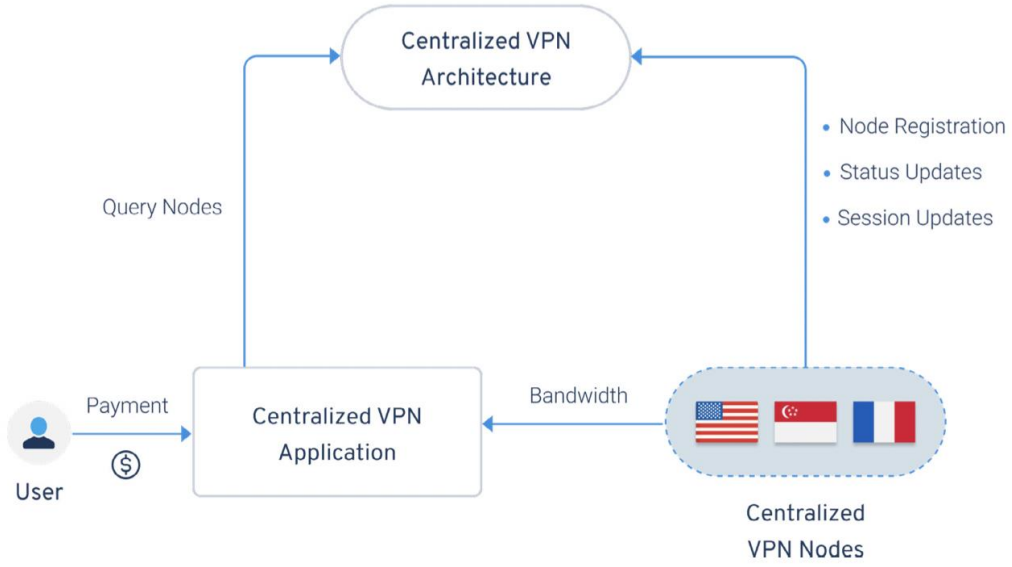
SENTINEL

Aperçu de l'architecture dVPN Sentinel :

L'architecture VPN centralisée est composée de plusieurs serveurs intermédiaires qui sont nécessaires pour la gouvernance des autorisations d'un utilisateur ainsi que pour l'établissement de la connectivité de l'utilisateur au nœud VPN. Cette architecture centralisée exige un degré élevé de dépendance à l'égard de ces serveurs intermédiaires, ce qui pose un risque pour la résilience des réseaux en raison des multiples points de défaillance et des multiples points d'attaque. Les temps d'arrêt des réseaux VPN centralisés peuvent être attribués au mauvais fonctionnement d'un ou plusieurs de ces composants et peuvent entraîner une diminution de l'expérience et de la satisfaction des utilisateurs.

Le cadre du dVPN Sentinel offre un degré incroyable de résilience et de sécurité par rapport à n'importe quel VPN de qualité grand public. L'architecture de Sentinel minimise le nombre de serveurs intermédiaires et de dépendances. En dehors du système de gestion et de création de compte qui se déroule entièrement sur la chaîne, le processus d'interrogation des serveurs disponibles se déroule sur la chaîne.

d'interrogation des serveurs disponibles se fait sur la chaîne. Comme la blockchain sur laquelle l'application est hébergée sera opérationnelle 24 heures sur 24, 7 jours sur 7, sans aucune interruption, et comme l'infrastructure de la communauté des validateurs est globalement décentralisée (elle n'est pas affectée par 1, 2 ou 3 pannes de centre de données), le temps de fonctionnement et l'expérience utilisateur d'une telle application dépasseront de loin les offres des concours centralisés.



L'un des principaux facteurs contribuant à la résilience architecturale de Sentinel est la distribution décentralisée de la puissance informatique qui sera nécessaire pour faire fonctionner le centre Sentinel et la zone Sentinel. La puissance de calcul dont l'écosystème dVPN Sentinel a besoin pour fonctionner n'est pas fournie par ou dépendante d'une organisation centralisée.

Elle est fournie par des organisations de "validation" expertes, réparties dans le monde entier et dotées de systèmes hautement redondants avec un débit de bande passante et un temps de fonctionnement importants.

Si l'architecture de Sentinel garantit que l'anonymat d'un utilisateur n'est pas compromis par l'application elle-même, l'utilisation du futur réseau de relais de Sentinel est nécessaire pour garantir l'anonymat complet d'un utilisateur du point de vue du nœud de sortie. Le réseau de relais de Sentinel permettra aux utilisateurs de faire passer leur connexion par une série de "nœuds relais" qui garantissent que l'utilisateur n'interagit pas directement avec le nœud de sortie.

Le protocole de "preuve de la largeur de bande", propre à Sentinel, garantit une mesure transparente et fiable de la fourniture de la largeur de bande du fournisseur de services (nœuds communautaires) à l'utilisateur final. Le protocole de "preuve de bande passante" s'intègre à la blockchain de Sentinel, fournissant un historique clair de la qualité du service de bande passante fourni et établissant un niveau de confiance entre tous les participants impliqués. Ces données sont ensuite utilisées pour déterminer si un nœud a respecté l'accord de niveau de service requis afin d'éviter toute pénalisation.

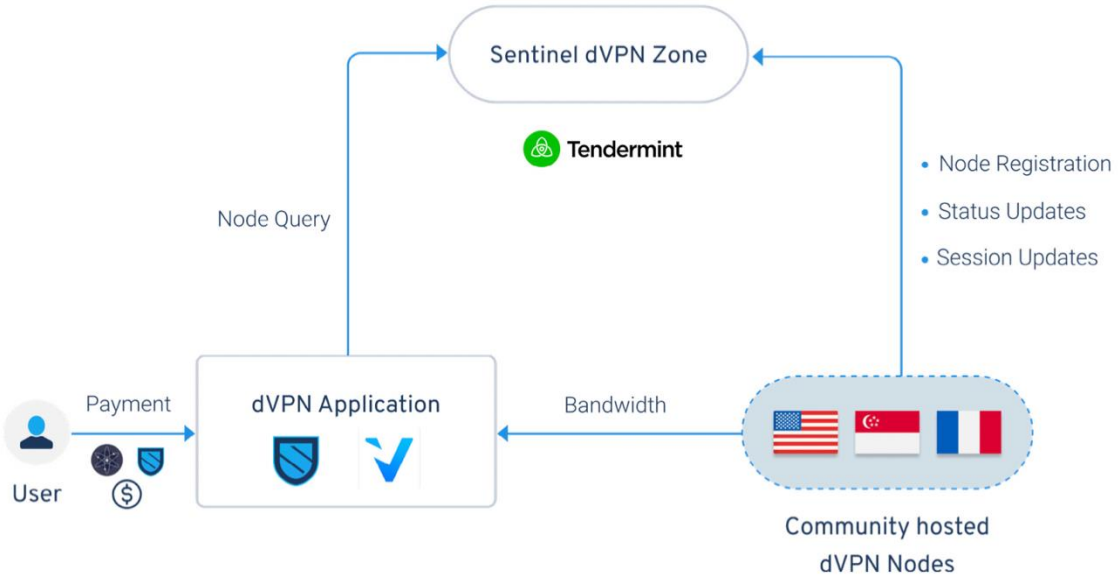
Requête sur la chaîne :

La mise en œuvre par Sentinel d'un système de requête "on-chain" est l'une des réalisations techniques les plus importantes de Sentinel et garantit une architecture hautement résiliente et décentralisée.

Grâce à l'architecture dVPN de Sentinel, une connexion entre l'utilisateur et le nœud de sortie peut être établie directement sans qu'il soit nécessaire de se connecter à un serveur intermédiaire (par exemple le masternode pour la découverte des nœuds) qui peut être contrôlé par le développeur de l'application ou un tiers. Pour ce faire, la blockchain est utilisée comme un registre pour "l'interrogation des nœuds", les nœuds ayant la capacité de s'interfacer avec les informations relatives aux propriétés des nœuds et aux instructions de connexion et de les stocker. L'application dVPN de l'utilisateur basée sur Sentinel interrogera simplement tous les nœuds dVPN disponibles en lisant les données des transactions sur la zone dVPN dédiée de Sentinel, alimentant une liste de serveurs disponibles.

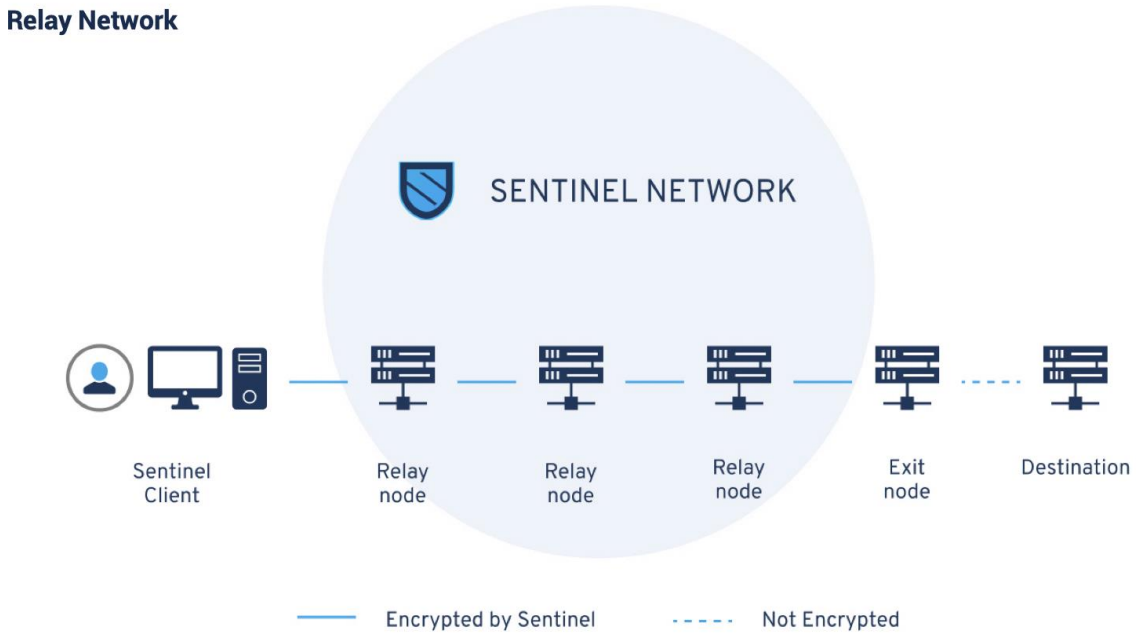
Des serveurs disponibles. Comme l'authentification et la gestion de l'identité s'effectuent déjà sur la chaîne, le seul point de défaillance de la structure d'application dVPN de Sentinel (autre que l'attaque de la sybil en réseau) devient théoriquement une défaillance potentielle de la sécurité du consensus au niveau de la chaîne. La seule façon de compromettre l'application Sentinel dVPN serait de compromettre le consensus piloté par le validateur.

SENTINEL



Les applications VPN classiques contrôlent généralement le nœud de sortie, tout en contrôlant et en utilisant les serveurs d'interrogation intermédiaires qui existent entre le nœud de sortie et l'utilisateur, ce qui rend l'objectif d'un réseau de relais redondant puisque l'IP de l'utilisateur original est facilement visible.

Cependant, une architecture de "requête sur la chaîne" signifie que l'utilisateur ne doit communiquer directement qu'avec la chaîne et non avec d'autres serveurs potentiellement centralisés qui pourraient enregistrer ses interactions.



STAKELAB

SENTINEL

Un solide réseau de relais est un aspect essentiel de toute solution dVPN de bout en bout qui respecte pleinement le droit à la vie privée de l'utilisateur. Bien que ni le créateur d'une application dVPN construite sur Sentinel ni aucun des participants à la blockchain Sentinel n'aient accès aux informations personnelles des utilisateurs (par exemple l'adresse IP), un nœud de sortie hébergé dans l'écosystème Sentinel aurait accès à l'adresse IP de l'utilisateur en l'absence d'un réseau de relais. Alors qu'une application dVPN est en mesure de prouver qu'aucun journal lié à la navigation de l'utilisateur et aux métadonnées n'est collecté/stocké de manière centralisée par les développeurs de l'application, il n'est actuellement pas possible de prouver que les journaux ne sont pas collectés ou stockés par un hôte de nœud de sortie sur son dispositif local.

Par analogie, pour décrire un réseau relais en termes plus simples, la connexion entre un utilisateur et le nœud de sortie pourrait être comparée à un appel cellulaire d'un utilisateur vers un tiers. Si l'intention de l'utilisateur est que la tierce partie ne puisse pas voir l'utilisateur.

ne puisse pas voir le numéro de l'utilisateur sur l'identification de l'appelant, l'utilisateur devra utiliser l'appareil de son ami comme relais pour masquer son numéro de téléphone. L'utilisateur doit ensuite appeler son ami, qui le met en attente et appelle le numéro de la tierce partie avant de fusionner les deux appels téléphoniques et de connecter ainsi l'utilisateur à la tierce partie sans exposer les données de l'utilisateur.

Comme dans l'exemple de l'appelant cellulaire intermédiaire, un réseau relais est constitué de "nœuds relais". Les nœuds relais diffèrent des nœuds de sortie par leur fonctionnement, car les nœuds de sortie communiquent directement avec les utilisateurs (en l'absence d'un réseau relais) tout en communiquant également avec les serveurs web sur l'internet. Alors que les nœuds relais ne communiquent qu'avec l'utilisateur, les autres nœuds relais ou le nœud de sortie.

Un réseau de relais fort est composé de :

- Un grand nombre de participants
- Une gouvernance forte
- Une intégration multi réseaux

L'utilisation d'un système de relais, basé sur Sentinel, s'adresse principalement aux utilisateurs soucieux du respect de la vie privée qui sont prêts à sacrifier la vitesse d'Internet pour améliorer la confidentialité.

Les avantages d'un réseau de relais ne se concrétisent que lorsqu'un grand nombre de participants uniques commencent à héberger des nœuds de relais ou de sortie sur le réseau. Si, à un moment donné, une entité prend le contrôle d'une proportion importante du réseau, il lui est possible de désanonymiser l'utilisateur par une attaque simple mais efficace de type "Man in the Middle" (MITM). L'un des principaux objectifs du réseau de relais est de s'assurer que les nœuds relais sont incapables de discerner s'ils sont en train d'établir un tunnel vers un utilisateur ou un autre nœud relais. Si un utilisateur achemine son trafic à travers les nœuds relais de l'attaquant ainsi qu'à travers le nœud de sortie, l'attaquant sera en mesure de corréler l'adresse IP de l'utilisateur et d'identifier que l'utilisateur est à l'origine de la demande de trafic et qu'il n'est pas simplement un autre participant au relais.

L'importance d'avoir un réseau distribué pour empêcher une attaque MITM dans un réseau de relais est partagée par l'écosystème Bitcoin, où l'intention de l'exploitation minière est d'empêcher une attaque à 51%. Si une seule entité prend le contrôle de 51 % du débit minier total du réseau Bitcoin, cette entité aurait la capacité d'endommager le réseau. L'intégrité en effectuant une attaque par double dépense. Bitcoin tente de combattre ces risques de monopolisation dans l'écosystème minier grâce à son mécanisme d'incitation. Ce mécanisme d'incitation fournit aux mineurs des récompenses en fonction de leur participation à la recherche et à la vérification des blocs nouvellement frappés sur le réseau. Si Bitcoin était un réseau basé sur le volontariat sans conception économique, sa sécurité serait très probablement compromise. Une entité puissante ayant accès à une infrastructure matérielle importante pourrait facilement prendre le contrôle majoritaire du réseau minier. Un exemple de réseau basé sur le volontariat est le réseau TOR. Dans le réseau TOR, les nœuds de relais et de sortie ne sont pas récompensés pour leur participation. Au contraire, ils sont encouragés à fournir leurs services simplement par respect partagé pour l'éthique de la décentralisation. Les experts de l'industrie craignent que le réseau TOR ait été compromis par des entités qui contrôlent un nombre important de nœuds de relais et de sortie TOR. À l'heure actuelle, il y a environ 6 000 nœuds de relais TOR sur le réseau, avec une moyenne de 6 millions d'utilisateurs actifs par jour. Cela montre clairement les limites et les risques d'un réseau basé sur le volontariat.

Le succès du réseau de relais Sentinel dépend entièrement du nombre de participants uniques. Attirer ces participants nécessite un certain niveau d'incitation par le biais de mécanismes sur le réseau.

Preuve de la bande passante :

La distribution de la bande passante dans un réseau réellement décentralisé partage un problème commun avec la génération de hachages par les mineurs dans un réseau Proof Work (PoW).
par les mineurs dans un réseau de preuve de travail (PoW). Ce problème tourne autour de la possibilité pour le fournisseur de services (ou le mineur dans le cas d'un PoW) de détourner ou de falsifier la quantité réelle de travail engagée. L'une des
responsabilités clés des mineurs sur la blockchain Bitcoin est de confirmer le travail réel (ou le nombre de hachages générés) par d'autres mineurs et de s'assurer que personne ne joue avec le système pour bloquer des récompenses. De même, il est nécessaire de disposer d'une architecture robuste dans le cas de la distribution de la bande passante sur un réseau P2P décentralisé afin d'éviter qu'un mauvais acteur n'ait l'intention d'usurper la quantité de bande passante fournie.
Une analogie qui peut être faite pour démontrer l'exigence de solutions de prouvabilité pour les réseaux de distribution de la bande passante est l'expérience frustrante que de nombreux utilisateurs de téléphones mobiles revendiquent avec leur opérateur de réseau en ce qui concerne leurs frais d'itinérance internationale. La plupart des plans d'itinérance proposés par les opérateurs de réseau imposent une restriction sur la quantité de bande passante pouvant être consommée, ou parfois même facturent en fonction de la quantité globale de bande passante consommée par l'utilisateur. Il n'est pas rare d'entendre des témoignages de personnes qui se méfient complètement de leur opérateur après une expérience où elles estiment avoir été surfacturées et ne comprennent pas comment a été calculée la consommation de bande passante pour la facture d'itinérance.
La possibilité de prouver la distribution de la bande passante n'est pas seulement importante pour les cas d'utilisation centrés sur les réseaux, mais également d'une importance capitale pour les cas d'utilisation centrés sur le stockage et l'informatique, qui impliquent également d'énormes quantités

d'utilisation de la bande passante. L'un des principaux objectifs de l'écosystème Sentinel est de développer et de mettre en œuvre le premier protocole de preuve de la bande passante, ou "preuve de la bande passante", afin de permettre un partage de la bande passante en toute confiance.

La portée de ce protocole s'étend au-delà des applications VPN décentralisées construites sur Sentinel, il a la capacité d'être intégré à d'autres réseaux distribués de partage de ressources p2p et même à des applications grand public.
Le premier prototype de mise en œuvre du protocole Proof of Bandwidth de Sentinel a été réalisé sur la chaîne Ethereum avec le soutien d'un réseau externe de masternodes distribués. Ces masternodes observent et mesurent la distribution de la bande passante entre le fournisseur de services et l'utilisateur, puis inscrivent certaines propriétés de la session, telles que la durée et la bande passante consommée, sur la blockchain Ethereum. Le mécanisme de facturation de l'application dVPN récupérerait ensuite ces données pour générer une facture qui devrait être payée par l'utilisateur. Ce prototype d'architecture a fonctionné comme prévu, mais n'a pas pu être qualifié de réellement décentralisé en raison de la nécessité d'un réseau de masternode supplémentaire.
L'implémentation actuelle du protocole de preuve de la largeur de bande, qui est en cours de construction sur le réseau Cosmos/Tendermint de Sentinel, implique la génération de "signatures de largeur de bande" de la part du fournisseur de services et de l'utilisateur. Ces signatures de bande passante sont essentiellement des messages qui se composent de la bande passante transmise dans la connexion P2P au cours d'une période de temps préconfigurée. Le fournisseur de services et l'utilisateur génèrent chacun leurs propres signatures qui sont signées avec leur clé privée respective, et ces signatures sont ensuite stockées sur la chaîne pour en assurer la provenance. En cas de divergence entre les déclarations d'échange de bande passante de l'utilisateur et du fournisseur de services (dans la période de temps préconfigurée), la connexion sera alors interrompue en raison de la présence d'au moins un acteur malveillant dans l'échange.

Variables de signature de bande passante déterminées par le développeur d'application dVPN :

- La période de temps pour la génération de chaque signature de bande passante
- Le seuil de pourcentage de divergence entre la signature de l'utilisateur et celle du fournisseur de services.

Modèles de paiement et dépôt fiduciaire :

La monétisation de la distribution de la bande passante en peer-to-peer permet l'utilisation de modèles de paiement plus dynamiques que ceux généralement utilisés dans le secteur des VPN conventionnels que ceux généralement observés dans le secteur des VPN conventionnels. En plus du système général de "prépaiement" dans lequel un utilisateur achète un abonnement pour une période de temps fixe, les fournisseurs de bande passante (hôtes de nœuds) ont la possibilité de fixer leur propre prix par unité (Go) de bande passante consommée.

Le paiement de l'utilisation des dVPN fonctionnant sur l'écosystème Sentinel sera possible à la fois avec des options conventionnelles basées sur des devises (par exemple, carte de crédit) et avec un grand nombre de crypto-monnaies qui seront prises en charge par l'IBC Cosmos. Cependant, la tarification de la bande passante via l'un ou l'autre des modèles sera principalement libellée en fiat.

Il est important de noter que si le paiement de la bande passante peut se faire en crypto-monnaies ou en fiat, le paiement du fournisseur de bande passante (hôtes du nœud) pour l'infrastructure d'hébergement du nœud sera presque toujours libellé en fiat. Ces coûts d'infrastructure comprennent les coûts de l'informatique en nuage ainsi que les coûts d'électricité et de matériel si l'hôte du nœud utilise une installation physique autonome.

Deux formes principales de modèles de paiement sont disponibles pour les utilisateurs de dVPN dans l'écosystème Sentinel :

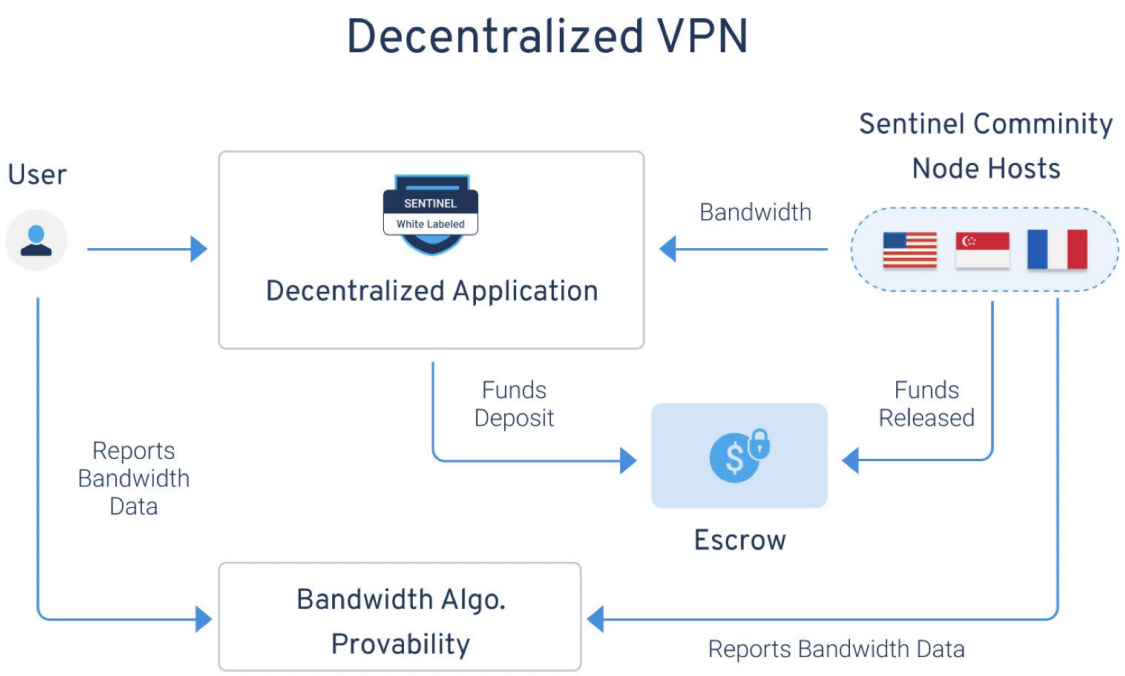
Temps réel - Un modèle de paiement en temps réel est utilisé par les hôtes de nœuds dVPN sur Sentinel qui ont l'intention de permettre aux utilisateurs de payer par "Go" de bande passante consommée. Dans ce modèle de paiement, les hôtes de nœuds ont également la possibilité de fixer leur propre prix pour leurs services.

Prépayé - Un modèle prépayé est un modèle de paiement plus conventionnel, semblable à ce que l'on voit couramment dans le secteur des VPN classiques, où les utilisateurs achètent un accès pour une période de temps spécifique. Il n'y a pas de restrictions sur la consommation de bande passante dans un modèle prépayé et l'utilisation est généralement illimitée.

Système de dépôt fiduciaire Sentinel dVPN - Un système de dépôt fiduciaire est utilisé dans le modèle de paiement en temps réel entre l'utilisateur et le fournisseur de services afin d'assurer la sécurité de l'utilisateur.

L’utilisateur et le fournisseur de services afin de garantir qu'aucune des parties impliquées ne puisse avoir un impact frauduleux sur la transaction. L'utilisateur doit bloquer un certain nombre de jetons dans le compte séquestre avant de pouvoir établir une connexion, et les jetons sont déduits de ce montant bloqué sur une base périodique en corrélation avec la bande passante consommée par l'utilisateur. La mesure précise de la bande passante fournie à l'utilisateur est assurée par le protocole Sentinel "Proof of Bandwidth" (preuve de bande passante), qui communique avec le séquestre pour établir une approche entièrement décentralisée de la libération des jetons du séquestre.

SENTINEL



Utilité des jetons :

L'utilité principale du jeton Sentinel s'articule autour de ses fonctions de :

- Jeton de gouvernance et de jalonnement

- Moyen de paiement pour les abonnements dVPN

- Moyen de paiement pour les services dVPN avancés

- Jeton de travail

Intégration du routeur matériel

L'intégration du protocole dVPN de Sentinel aux routeurs de réseau basés sur Open-WRT (firmware de routeur open-source populaire) permettrait aux propriétaires de routeurs de devenir des hôtes de nœuds en monétisant facilement leur bande passante. En outre, Sentinel vise à supporter et à s'intégrer à tout routeur open-source capable d'appliquer une connexion dVPN sur l'ensemble du réseau wi-fi. Un dVPN basé sur un routeur permettrait aux utilisateurs d'éviter d'installer une application VPN sur chacun de leurs appareils et l'utilisateur pourrait potentiellement créer un réseau domestique secondaire destiné uniquement à l'accès par le dVPN.

Caractéristiques générales d'un routeur :

1. Capacité d'établir un réseau sans fil

2. Possibilité d'appliquer des normes de cryptage aux données acheminées par le réseau sans fil

3. Capacité à permettre à un réseau sans fil de gérer plusieurs appareils avec équilibrage de charge

4. Augmentation de la couverture/portée du réseau

5. Capacité de double bande pour éviter le décalage

Quels sont les problèmes des routeurs standard de l'industrie ?

1. Les standards sont complètement fermés et n'offrent pas au public la possibilité d'effectuer des examens impartiaux du code.

2. Les routeurs standard n'offrent pas aux utilisateurs la possibilité de faire passer leur bande passante par un réseau dVPN éprouvé qui offre l'assurance de la sécurité et du cryptage.

3. Les routeurs standard n'offrent pas aux utilisateurs la possibilité de monétiser leur bande passante excédentaire non utilisée.

Qu'est-ce que cela signifie ?

1. Les routeurs standard peuvent être piratés et manipulés et il peut s'écouler des mois, voire plus, avant que les vulnérabilités soient découvertes et corrigées, car le code n'est pas ouvert au public (exemple : Linux vs Microsoft).

2. Les routeurs standard n'offrent pas actuellement aux utilisateurs la possibilité d'utiliser en toute sécurité une application VPN décentralisée et distribuée qui a la capacité de se connecter à un réseau local.Décentralisée et distribuée qui a la capacité de prouver de manière transparente l'intégrité de son back-end opérations.

3. Les routeurs standard ne permettent pas aux utilisateurs de monétiser l'excédent de bande passante inutilisée, ce qui entraîne un gaspillage de ressources payantes.