nomadic labs

Les Nœuds dans la blockchain Tezos

Sommaire

Introduction

Introduction

La blockchain Tezos se distingue des autres blockchains par ces éléments caractéristiques :

1. La gouvernance on-chain permettant l'auto-évolution du protocole par des amendements [1] successifs
2. Le consensus LPOS (Liquid Proof Of Stake)
3. Le langage Michelson, langage de développement des smart contracts, permettant la vérification par preuve formelle

La blockchain est un réseau pair à pair. Chaque pair est un nœud qui assure diverses fonctions dans le logiciel distribué.

Dans ce document nous aborderons en détail le concept de nœud dans la blockchain Tezos, son rôle et ses limites.

1. Document sur les amendements

Définition

Définition

Dans une blockchain, les nœuds sont des acteurs indispensables pour maintenir la décentralisation du réseau. Un nœud est une machine physique sur laquelle est stockée une copie de l'état actuel de la blockchain et qui met à jour sa copie avec les informations qu'elle reçoit de la part des autres nœuds avec lesquels elle est connectée au moyen du réseau pair à pair.

Un nœud communique systématiquement les informations qu'il reçoit aux autres nœuds avec qui il est connecté, pour que ceux-ci transmettent à leur tour ces informations à leurs pairs. Ainsi tous les nœuds du réseau disposent des mêmes informations.

La particularité d'une blockchain publique est que n'importe qui peut lancer un nœud. Il est donc attendu que la chaîne possède un grand nombre de nœuds, ce qui réduit les risques liés à une défaillance potentielle d'un acteur critique pour le réseau.
Une fois lancé, un nœud se connecte à d'autres pairs (une quarantaine en moyenne) du réseau en établissant un canal de communication permettant aux parties concernées de s'échanger des informations.

La blockchain Tezos compte, à la mi-année 2020, plus de 1000 nœuds actifs sur le réseau.[1]

1. Inspecting Tezos decentralization, analyse par Baking Bad

Réseau pair à pair

Réseau pair à pair

Le réseau Tezos implémente un protocole de bavardage [1] dont les principales opérations sont :

- Un mécanisme de planification des lectures/écritures pour contrôler l'usage de la bande passante,
- Un service de communication chiffrée,
- Un service de liste noire, grise et blanche pour établir ou refuser des connexions provenant de certains pairs.

1. *gossip protocol* en anglais

Différences entre nœuds et baker

Différences entre nœuds et baker

Sur la blockchain Tezos, les bakers sont ceux assurant le rôle de créateurs des nouveaux blocs (équivalent des mineurs sur Bitcoin). Un nœud n'est donc pas nécessairement rattaché à un baker. Par contre, un baker doit forcément se connecter à un nœud pour suivre l'arrivée de nouveaux blocs, récupérer les transactions en attente et diffuser ses propres blocs si il est sélectionné.

Beaucoup de bakers possèdent leur propre nœud, cependant les concepts de baker et de nœud sont distincts. Ainsi, un nœud peut être indépendant des bakers alors qu'un baker a besoin d'interagir avec au moins un nœud.

Les différents types de nœud

Les différents types de nœud

Lorsqu'on lance un nœud Tezos, il existe plusieurs configurations permettant à ce nœud de se synchroniser avec les autres nœuds de la blockchain. Chaque type de nœud mène à une synchronisation plus ou moins rapide du nœud et permet d'assurer différentes fonctions. Voici les 3 principaux modes de configurations des nœuds :

- **Mode archive** : nœud stockant l'intégralité de la blockchain. Un nœud lancé sur la blockchain Tezos en mode archive téléchargera l'intégralité de la chaîne de blocs [1] depuis le lancement du réseau. Début 2021, l'intégralité de la blockchain occupe environ $145 Go$.
- **Mode full** (mode par défaut) : nœud stockant l'intégralité de la chaîne de blocs, sans le contexte (état de la blockchain contenant des informations du type : ``Le compte d'Alice [2] contient 5ℏ'') en dessous d'un certain niveau appelé **savepoint**. Il est possible de reconstruire un nœud archive à partir d'un snapshot full.
- **Mode rolling** : nœud le plus léger existant. Il stocke un fragment minimal de la chaîne et supprime tout ce qui se situe avant ce fragment. (blocs, opérations, contextes archivés).

Il est possible d'utiliser un *snapshot*, représentant une copie de l'état de la blockchain à un moment donné pour permettre à un nœud de se synchroniser plus rapidement. Les snapshots peuvent être utilisés pour initialiser les nœuds full et rolling. Il est également possible de switcher entre les différents types de nœud. [3].

1. Les nœuds archive conservent les contextes et les "tickets de caisse" de tous les blocs
2. En pratique, Alice est désignée sous pseudonymat par le hash de sa clé publique.
3. Voir les différents modes

Configuration d'un nœud

Configuration d'un nœud

Les différents types de nœud présentés précédemment permettent aux utilisateurs de choisir celui qui leur est le plus adapté en fonction de la quantité d'informations dont ils ont besoin. Un explorer [1] par exemple aura tendance à avoir un nœud archive, tandis qu'un utilisateur voulant expérimenter le déploiement d'un nœud peut se contenter d'un nœud rolling.

Pour lancer un nœud dans un des différents modes :

- `$ tezos-node run --history-mode (archive, full, experimental-rolling)`

Pour importer un snapshot full/rolling [2] :

- `$ tezos-node import snapshot path/to/snapshot`

Les liens suivants permettent d'obtenir des snapshots :

- https://snapshots.tulip.tools/#/
- https://snapshots-tezos.giganode.io/
- https://xtz-shots.io/

1. Outil permettant d'oberserver les blocs créés, les transactions réalisées, ...
2. Un snapshot avec l'extension correspondante (*.roll* ou *.full*) est nécessaire.

Les actions possibles avec un nœud

Les actions possibles avec un nœud

Dans une blockchain, un nœud sert d'interface entre l'utilisateur et le réseau pair à pair. On compte deux utilisations principales :

- **Stockage de l'information** : étant donné qu'un nœud conserve une copie de l'état courant de la blockchain, il permet de s'informer sur ce qui se passe en temps réel. Cet usage permet par exemple d'alimenter des indexers, lesquels récupérent les informations du nœud et les traitent pour les rendre plus expressives pour un humain.
- **Transmission de l'information** : les transactions initiées par les utilisateurs transitent par les nœuds avant de faire partie de la blockchain. Ils sont un point d'entrée des opérations destinées à être validées par les bakers.

Généralement, ces usages sont complémentaires. Par exemple, un client aura souvent besoin de consulter le contenu de la chaîne afin de vérifier que ce qu'il envoie n'est pas immédiatement rejeté.
Un baker utilisera les deux aspects susmentionnés pour fonctionner. Il devra lire les transactions en attente de validation, puis lire le contexte [1] pour s'assurer que les transactions sont applicables avant de les valider en les incluant dans un bloc qui sera transmis au reste du réseau.

1. État courant de la blockchain

Comment communiquer avec un nœud ?

Comment communiquer avec un nœud ?

Comme nous l'avons vu à la slide 16, communiquer avec un nœud permet d'accéder au réseau pair à pair. Les bakers communiquent automatiquement avec le nœud mis à leur disposition [1], mais il peut être utile pour un utilisateur de pouvoir interagir directement avec son nœud lorsqu'il veut s'informer sur l'état de la chaîne ou publier lui même des transactions.

La communication directe avec un nœud se fait par l'utilisation d'appels RPC (Remote Processing Call) [2].

On peut également, selon le besoin, utiliser une interface utilisateur dédiée comme un client [3], un indexer [4] ou un wallet [5].

Néanmoins, en pratique, les indexers sont l'outil le plus pratique pour un humain afin d'obtenir des informations sur la chaîne.

1. Pour plus d'informations consultez notre document sur le baking
2. Guide des appels RPC
3. Guide d'utilisation du client tezos
4. Indexers de tezos
5. Wallets tezos

Les avantages offerts par un nœud

Les avantages offerts par un nœud

Une entité pourrait souhaiter avoir le contrôle de son propre nœud Tezos pour des raisons opérationnelles. Un tel contrôle permet d'éviter la dépendance à un nœud tiers qui pourrait être défaillant. Premièrement, cela implique de ne pas être dépendant d'un nœud de la blockchain qui pourrait être sujet à une panne. De plus, posséder son propre nœud permet d'ajouter de la sécurité en contribuant au réseau pair à pair.

Posséder son propre nœud signifie qu'il est possible de gérer ses propres transactions et de s'assurer que celles-ci sont bien diffusées au réseau.

Faire tourner son nœud permet de contribuer au réseau Tezos et ainsi accroître sa sécurité et sa décentralisation. Une blockchain est d'autant plus décentralisée et robuste qu'elle possède de nœuds.

Devenir baker sur la blockchain Tezos implique généralement de contrôler son propre nœud, mais confère aussi des avantages. En effet, tout baker du réseau reçoit des récompenses en contrepartie de son travail de validation des blocs et de sécurisation de la chaîne. Il peut notamment inclure ses propres transactions sans payer de frais. À cela s'ajoute l'obtention des droits de vote concernant les amendements [1] proposés par la chaîne.

1. Document sur les amendements

Les attaques possibles sur un nœud

Les attaques possibles sur un nœud (1/2)

Il existe différentes attaques que peut subir un nœud de la blockchain, celles-ci sont inhérentes à tous les logiciels basés sur un réseau pair à pair. Il est recommandé à tout nœud de sécuriser ses canaux de communication et stocker (si il en a) ses clés privées en cold wallet [1].

Déployer un nœud sur une blockchain peut comporter quelques risques. En effet, un détenteur de nœud pourrait être pris pour cible par un attaquant qui chercherait à compromettre sa connexion avec les autres pairs de la blockchain, ou encore tenter de lui envoyer des informations erronées.

Attaque par déni de service :
L'attaque par déni de service (ou encore DoS) est une attaque informatique rendant indisponible un service. Sur Tezos, certaines requêtes pouvant être adressées à un nœud sont parfois très gourmandes en ressources (le calcul des droits de baking jusqu'à des niveaux arbitrairement élevés par exemple). Le but étant pour l'attaquant de rendre le nœud donné indisponible, par manque de ressources nécessaires pour répondre à ladite requête.

Pour parer cette attaque, il est préférable de limiter l'accès à ces requêtes, surtout sur un nœud qui est directement utilisé par un baker. Il s'agit d'une attaque très classique sur Internet, les préventions habituelles s'appliquent [2].

1. Technique de stockage des clés privées qui utilise un matériel non connecté au réseau internet (exemples : les produits Ledger et Trezor).
2. https://fr.wikipedia.org/wiki/Mitigation_de_DDoS

Les attaques possibles sur un nœud (2/2)

Attaque Sybil :
Il s'agit d'une attaque consistant à créer un grand nombre d'identités sur un réseau pair à pair pour isoler un pair du reste du réseau et de lui communiquer des informations erronées. Dans le cas de Tezos, il s'agit de générer une grande quantité de nœuds, afin d'isoler un nœud cible à qui l'attaquant communiquerait des blocs erronés ou bloquerait l'accès à certaines informations.

Pour prévenir ce genre d'attaques, une des fonctionnalités de la blockchain Tezos permet à tout nœud de changer de pairs régulièrement et de façon automatisée, ainsi l'attaquant ne peut pas avoir la certitude de maintenir son emprise suffisamment longtemps pour que la chaîne modifiée soit considérée valide par le nœud cible.

De plus, créer une identité de nœud coûte un certain de temps calcul [1]. Ainsi, générer un nœud prend quelques secondes mais en générer suffisamment pour diviser le réseau prendrait beaucoup de temps, même avec une machine puissante.

Enfin, en cas d'attaques observées sur le réseau, il serait possible d'augmenter le niveau de travail exigé par ses pairs et régénérer toutes les identités pour se prémunir de l'attaque, et l'endiguer totalement si tous les pairs le font.

1. Pour créer une adresse, il faut lui donner un certain niveau de "travail" allant de 0 à 255. Ce niveau correspond au nombre de zéro devant le hash de son identité. Lors de la création d'une identité, le programme génère des versions différentes jusqu'à ce qu'il en trouve dont le niveau soit suffisant. On peut alors choisir de refuser de se connecter à des pairs dont l'identité est inférieure à une certaine valeur. Par défaut cette valeur est fixée à 26.

Services d'accès à un nœud

Services d'accès à un nœud

Certains nœuds sont publiquement accessibles, comme celui de SmartPy :

- `https://mainnet.smartpy.io`

Il existe aussi des services de nœuds, notamment :

- `https://tezoslink.io/`
- `https://tezos.giganode.io/`

nomadic labs

Continuons cet échange

https://tezos.com
https://developers.tezos.com