Baking - Création de blocs sur Tezos

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 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

L'objectif de ce document est de présenter en détails l'algorithme de consensus et le mécanisme de création de blocs appelé ``baking'' sur Tezos.

Définition des concepts principaux

Définition des concepts principaux 1/3

- **Bloc :** Un regroupement de plusieurs opérations devant être validées. Un bloc contient en particulier des informations comme le numéro du bloc en cours, des informations concernant le bloc précédent, mais également l'heure à laquelle il a été validé.
- **Baking :** Création de nouveaux blocs de la blockchain Tezos, par des ``**bakers**'', qui sont rémunérés en contrepartie pour chaque bloc ``baké''. Un baker est aussi appelé délégué.
- **Endorsement :** En plus de créer des nouveaux blocs, les bakers peuvent approuver les blocs d'autres bakers. On dit qu'ils sont des ``**endorsers**'' du bloc et ils sont rémunérés en contrepartie de cela.
- **Délégation :** Chaque détenteur de tez (XTZ ou ꜩ) peut transférer les ``droits de baking'' et ``droits de vote'' associés à ses tez à un baker. Le détenteur conserve toujours le contrôle de ses fonds et peut changer de délégué à tout moment.

Définition des concepts principaux 2/3

- **Roll :** 1 roll est égal à 8000ꜩ. Pour avoir le droit d'être reconnu comme un baker au sein du réseau, un détenteur de tez doit avoir au moins un roll dans sa balance de staking. Les droits de vote sont également indexés sur ce nombre de rolls (1 roll = 1 vote).

- **Cycle :** Unité de temps au cours de laquelle 4096 blocs sont créés sur la blockchain Tezos. Cela correspond à environ 2 jours, 20 heures et 16 minutes (en considérant 1 minute par bloc créé si aucun baker n'a été défaillant).

- **Fitness :** Score représentant la qualité de la chaîne jusqu'à un bloc donné. Dans le protocole actuel, la fitness est égale à la hauteur de la chaîne.

- **Le double baking** et **le double endorsing** sont définis en slide 35.

- **Slot :** Un slot est un emplacement disponible pour un bloc ou un endorsement. Chaque cycle contient 4096 slots de baking et 131 072 slots d'endorsement. Au début de chaque cycle le protocole attribue à chaque slot une liste de bakers selon une loi uniforme pondérée par le nombre de rolls. Le premier baker de la liste sera chargé de baker ou d'endorser selon le cas, s'il ne le fait pas, le baker suivant sera chargé de le faire et ainsi de suite.

Définition des concepts principaux 3/3

- **Nœud** [1] **:** Un nœud Tezos est un pair (une machine) dans le réseau pair à pair. Il maintient une copie de l'état courant et propage les blocs créés et les opérations réalisées aux autres pairs. Un nœud n'est pas nécessairement un baker mais un baker est toujours associé à un ou plusieurs nœuds. Les nœuds sont généralement implémentés selon un des 3 modes suivants :
  - En mode **archive** et contenir tout l'historique de la chaîne, en fin 2020, un nœud archive mesure environ 80 Go.
  - En mode **rolling** et contenir le minimum d'informations nécessaires au fonctionnement actuel de la chaîne, en supprimant périodiquement les informations les plus anciennes.
  - En mode **full** (mode par défaut). Le mode full est un mode intermédiaire qui contient toutes les informations d'un nœud rolling plus le minimum d'informations pour pouvoir reconstruire toute la chaîne depuis le bloc genesis.

  En théorie il peut exister d'autres types de nœuds.

1. Pour plus d'informations sur les nœuds (en)

Contenu d’un bloc

Contenu d'un bloc

La blockchain est composée d'une succession de blocs. Chaque bloc est composé lui même d'une en-tête et d'une liste d'opérations. L'en-tête contient des informations essentielles pour la validité du bloc, notamment :

- Le niveau du bloc, c'est-à-dire la hauteur de la chaîne
- Le hash du bloc précédent permettant de chaîner les blocs entre eux
- La date de création du bloc
- La signature du baker qui a produit le bloc
- La ``fitness'' du bloc, attribuant un score à la chaîne jusqu'à ce bloc

Le corps du bloc contient ensuite une liste d'opérations diverses (transfert de tez, déploiement de smart contracts, ...) dans la limite de la taille maximale autorisée par le protocole (actuellement 512kB par bloc).

Liquid Proof of Stake et délégation

Liquid proof of stake - Délégation

Concernant Tezos, les droits de baking sont distribués aléatoirement selon le nombre de rolls détenus (1 roll = 8000ꜩ).

Un détenteur de tez peut :

- *Devenir baker* si il possède en fonds propres ou en délégation au moins 1 roll.
- *Déléguer ses tez à un baker*, afin de participer au consensus.

En pratique, certains bakers distribuent une partie des récompenses perçues aux personnes leur ayant délégué leurs tez. Cette distribution peut inciter d'autres personnes à déléguer leurs tez, augmentant donc le nombre de rolls de ces bakers et par conséquent leur chance de baker/endorser.

Le **Liquid proof-of-stake** se caractérise par la possibilité pour un détenteur de tez de rester propriétaire de ses fonds tout en pouvant déléguer ses droits (votes, baking) associés à un baker. Ce principe est différent du delegated proof-of-stake (DPOS) suivi par d'autres blockchains où les participants votent pour élire un nombre limité de validateur de blocs.

Baking

Baking

Concernant Tezos, les participants au processus de validation des blocs sont appelés des **délégués**. Ces délégués peuvent jouer deux rôles :

- Le rôle du baker, qui crée les blocs et les signe.
- Le rôle de l'endorser qui approuve les blocs en émettant une opération d'endorsement (les endorsements visibles au bloc de niveau $n+1$ concernent donc le bloc de niveau n).

Les droits de baking et d'endorsement sont déterminés aléatoirement plusieurs cycles en avance. Pour décourager les comportements non souhaitables (ex : le double baking ou le double endorsement), **chaque délégué doit mettre une quantité fixe de tez sous séquestre pendant une durée limitée** (5 cycles) qui seront confisqués en cas de tentative de compromission de la chaîne (double baking/endorsement).

Les conditions nécessaires pour devenir baker sont les suivantes :

- Avoir un serveur disponible 24h/24 et une connexion à internet stable
- Posséder au moins 8GB de RAM
- Posséder un disque SSD (de plus de 100 GO de préférence)
- Posséder au moins 1 Roll ($8000\frac{1}{3}$)

Endorsement

Endorsement

Pour chaque bloc, une liste d'endorsers est déterminée. Leur rôle est de vérifier l'intégrité et d'approuver le bloc créé par le baker.

Tout comme les bakers, les endorsers sont choisis aléatoirement, parmi les délégués existants.

Pour approuver un bloc au niveau n, les endorsers émettent chacun une opération de signature qui sera incluse dans le bloc au niveau $n+1$. Après le baking du bloc $n+1$, plus aucune opération d'endorsement n'est acceptée pour le bloc n.

Chaque bloc possède 32 slots d'endorsement. Rien n'oblige un baker d'inclure 32 endorsements mais sa récompense est proportionnelle au nombre d'endorsements inclus.

Un endorser peut, pour un bloc donné, obtenir plusieurs slots d'endorsement, il sera alors rémunéré pour chaque endorsement réalisé (correspondant à chaque slot validé).

Enfin, comme pour les bakers, les endorsers déposent une garantie pour limiter les risques de comportement compromettant la chaîne (ex : double endorsement).

Alternatives pour baker

Alternatives pour baker

En pratique, baker et endorser des blocs se fait de manière automatique. Il existe plusieurs façons de baker, chacune possédant des avantages et inconvénients. Voici quelques alternatives pour baker avec des liens les décrivant plus en détail :

- KILN et Ledger Nano S : `https://gitlab.com/tezos-kiln/kiln`. Il s'agit d'un ``plug & use'' très intuitif pour lancer son nœud et son baker.
- Remote Signer et Ledger Nano S : `https://github.com/obsidiansystems/ledger-app-tezos`.
- Remote Signer par Cloud : `https://www.ecadlabs.com/signatory`.

Les liens suivants peuvent aider à lancer un baker :

- `https://github.com/tzConnectBerlin/baking-support`
- Tezos Node Setup & Maintenance by BakingBenjamins

Remote signing

Remote signing 1/2

L'une des façons de baker en réduisant l'exposition des clés privées est d'utiliser **un logiciel de remote signing**. Dans le processus de validation des blocs (baking/endorsement), le logiciel interagit avec un système de gestion de clé privées (ex : Ledger Nano S, machine distante communicant par un canal sécurisé).

Le remote signing consiste à dissocier physiquement les requêtes de baking/endorsement provenant du réseau et destinées à un délégué donné, et l'opération de signature de ce même délégué. Il existe des schémas de signature préalablement implémentés par le client tezos (unix, tcp, http et https) permettant d'envoyer des requêtes de signature à travers le canal de communication choisi par le baker.

Remote signing 2/2

Lors d'une opération de remote signing, plusieurs évènements se produisent :

1. Le réseau envoie une requête de signature au logiciel de remote signing qui interagit avec le système de gestion de clés privées.

2. Le logiciel de remote signing vérifie en quoi consiste l'opération : création de bloc ou endorsement, puis l'envoie au système de gestion de clés qui procédera à la signature de l'opération.

3. La signature est ensuite validée par le logiciel de remote signing, et renvoyée au nœud Tezos qui propagera l'opération au réseau.

La clé doit être de préférence **conservée sur un module hardware** pour ne jamais être directement accessible sur le réseau. Il est cependant plus sécurisé de s'assurer que le module hardware autorise uniquement la signature de bloc et non la signature d'une transaction quelconque (c'est à dire ne pas créer un mécanisme de signature aveugle).
À titre d'exemple, le Ledger Nano S associé à Kiln respecte ces deux conditions.

Sélection du baker

Sélection du baker

À chaque cycle, une graine aléatoire est générée, basée sur un certain nombre d'informations contenues dans les blocs précédents.

La graine du cycle n permet d'abord de sélectionner un ``roll snapshot'' (photo de l'état des rolls des participants au réseau) du cycle $n - 2$.
La graine permet ensuite de sélectionner les rolls (parmi ceux du snapshot) auxquels seront attribués des droits de baking/endorsement pour le cycle $n + 5$.

Les droits sont répartis selon le mécanisme suivant :

- Pour chaque bloc, une liste infinie est établie définissant un ordre de priorité pour les bakers et endorsers

Une fois inscrit, un baker doit donc attendre au moins 7 cycles avant d'être sélectionnable.

Récompenses des bakers et endorsers

Récompenses des bakers et endorsers

Le rôle des bakers est primordial puisqu'ils font fonctionner la chaîne en créant les blocs et en veillant à l'intégrité des informations contenues. Pour les motiver à effectuer ce travail, chaque bloc créé entraîne l'émission de nouveaux tez pour rémunérer le baker et endorsers.

La récompense du baker dépend de son niveau de priorité et du nombre d'endorsements réunis pour le bloc qu'il bake suivant la formule :

$$\text{récompense de baking} = \begin{cases} e * 1.25 & \text{si priorité} = 0 \\ e * 0.1875 & \text{sinon} \end{cases} \quad \text{avec } e = \text{nombre d'endorsements}$$

Soit 40ꜩ maximum pour le baker, sans compter les frais des transactions incluses dans son bloc.
Pour l'endorser, sa récompense dépend aussi de son niveau de priorité suivant la formule :

$$\text{récompense d'endorsing} = \begin{cases} e * 1.25 & \text{si priorité} = 0 \\ e * 0.833333 & \text{sinon} \end{cases} \quad \text{avec } e = \text{nombre de slots de l'endorser}$$

Un endorser peut avoir plusieurs slots parmi les 32 disponibles pour un bloc donné.

Émission de nouveaux tez

Émission de nouveaux tez 1/2

Chaque création et validation de bloc est accompagnée de la création de tez.

La formule de récompense par bloc permet d'estimer qu'un bloc produit au maximum 80ꜩ. Ramené au nombre de blocs créés par an correspondant à un bloc créé par minute soit 52 560 par an (hors années bissextiles), en supposant que tous les rolls sont actifs (19 077 au bloc 0) on atteint une augmentation du nombre de tez d'au plus 5,51% la première année (soit en 2018). Les récompenses étant fixes, ce pourcentage va décroître au fil des années.

L'augmentation de la ``masse monétaire'' ne concerne pas uniquement les bakers. En effet, si un détenteur de tez les délègue à un baker redistribuant une partie de ses récompenses, il profitera lui aussi de la création monétaire.

Émission de nouveaux tez 2/2

Plusieurs phénomènes indépendants du baker font varier son rendement :

- Tous les rolls ne sont pas actifs dans le processus de baking, ce qui peut augmenter le rendement annuel
- L'intervalle de temps entre deux blocs est légèrement supérieur à une minute, ce qui peut diminuer le rendement annuel
- Les 32 endorsements ne sont toujours réunis, ce qui peut également diminuer le rendement annuel

Un détenteur qui délègue ses tez peut souhaiter choisir un baker fiable qui lui verse des intérêts. Il est possible d'observer le rendement estimé en fonction du montant de tez que l'on décide de déléguer :

- `https://www.stakingrewards.com/earn/tezos`

Modélisation des gains d’un baker

Modélisation des gains d'un baker 1/2

Les hypothèses suivantes sont considérées :

1. Nombre de rolls actifs la première année = 84 156 (valeur en septembre 2020)
2. Un bloc est baké toutes les minutes
3. 32 endorsements pour tous les blocs

Sous ces hypothèses, un baker possédant 1 roll, créera en moyenne 1 bloc tous les deux mois environ, et endorsera environ 16 blocs par mois, ce qui revient à une moyenne de près de 480 ꜩ gagnés par an, soit un rendement approximatif de 6%. Cette valeur est légèrement supérieure au chiffre de 5,51% mentionné précédemment car on fait l'hypothèse ici qu'il y a des rolls inactifs, ce qui permet aux rolls actifs d'avoir plus de revenus que dans le contexte où tous les rolls sont actifs.

Un baker reçoit, en plus de sa récompense pour avoir créé un bloc, un certain montant lié à des frais payés par les transactions incluses dans son bloc. Ces derniers dépendent de l'offre et de la demande, mais les gains qu'ils représentent actuellement sont très inférieurs à la récompense de création du bloc (≈ 0.1% des gains du baker en 2019).

Modélisation des gains d'un baker 2/2

Suivant les hypothèses du slide 30, voici un exemple de ce qu'un baker qui conserve ses récompenses pour baker peut gagner par an, selon son nombre de tez :

Année	Total de kꜩ en circulation	Alice				Bob			
		ꜩ	rolls	R.O.I	C.R.O.I	ꜩ	rolls	R.O.I	C.R.O.I
1	673248	8 000,00ꜩ	1	6,25%	6,25%	80 000,00ꜩ	10	6,25%	6,25%
2	715296	8 499,64ꜩ	1,06	5,53%	12,12%	84 996,44ꜩ	10,62	5,53%	12,12%
3	757344	8 969,92ꜩ	1,12	4,95%	17,68%	89 699,16ꜩ	11,21	5,45%	18,23%
4	799392	9 414,08ꜩ	1,18	4,47%	22,94%	94 584,95ꜩ	11,82	4,89%	24,02%
5	841440	9 834,88ꜩ	1,23	4,06%	27,93%	99 213,75ꜩ	12,4	4,84%	30,01%
6	883488	10 234,65ꜩ	1,28	3,72%	32,69%	104 011,01ꜩ	13	4,76%	36,2%
7	925536	10 615,40ꜩ	1,33	3,42%	37,24%	108 960,70ꜩ	13,62	4,34%	42,11%
8	967584	10 978,84ꜩ	1,37	3,17%	41,58%	113 685,52ꜩ	14,21	4,28%	48,19%
9	1009632	11 326,50ꜩ	1,42	2,94%	45,75%	118 552,67ꜩ	14,82	3,93%	54,02%
10	1051680	11 659,67ꜩ	1,46	2,74%	49,74%	123 217,12ꜩ	15.4	3,89%	60,01%

Alice n'a initialement qu'un roll et Bob en a 10. Après 10 ans, Alice bake encore avec un seul roll alors que Bob en possède 5 de plus. Ceci révèle un **effet de seuil** entre les bakers. Contrairement aux ``petits'' bakers, les ``gros'' voient leur nombre de rolls augmenter de façon linéaire au cours du temps.

Ces résultats sont des simulations basées sur des hypothèses, le revenu effectif d'un baker peut donc être différent des chiffres mentionnés dans ce tableau.

Dépôt de garantie et accusation

Dépôt de garantie et accusation

Pour éviter le double baking/endorsement [1], **un dépôt de garantie est nécessaire** :

- 512ꜩ par bloc baké
- 64ꜩ par slot d'endorsement

Le dépôt de garantie reste physiquement sur le compte mais est bloqué pour une période de 5 cycles (environ 2 semaines), les tez correspondants seront toujours pris en compte pour calculer les slots, mais ils ne pourront ni être dépensés, ni servir pour un nouveau dépôt de garantie tant qu'ils n'auront pas été libérés.
Il est conseillé à un baker de posséder au moins 10% du montant total de tez qui lui servent à baker. En effet cela lui permettra de réaliser sans problème les dépôts de garantie demandés pour chaque baking/endorsement. Dans le cas contraire, il peut se trouver dans l'impossibilité de déposer la garantie et donc manquer ses opérations de baking ou d'endorsement. Cela représente un manque à gagner mais n'engendre aucune pénalité.
Si un double baking/endorsement est constaté, un baker peut en apporter la preuve dans un bloc, et ce pendant une période de 5 cycles à partir de l'opération fallacieuse. La moitié de la garantie du baker coupable revient alors à l'accusateur, l'autre moitié est détruite.

1. Le double baking (resp. endorsement) consiste à baker (endorser) deux blocs différents d'un même niveau avec la même clef, ce qui peut temporairement, conduire à une séparation de la chaîne.

Actions préjudiciables au réseau

Actions préjudiciables au réseau

Les actions pénalisées par une saisie du dépôt de garantie sont les suivantes :

- **Le double baking** : un baker malhonnête pourrait essayer de baker deux blocs à la même hauteur de chaîne. Cependant cela implique d'être tiré au sort et ensuite de réaliser un dépôt de 512ꜩ par bloc baké.

- **Le double endorsement** : un endorser malhonnête pourrait essayer d'endorser deux blocs à la même hauteur de chaîne, pour se faire, il doit être tiré au sort et ensuite réaliser un dépôt de 64ꜩ par slot d'endorsement.

- **La non révélation de graine ((en) seed slash)** : un baker est invité à fournir des graines d'aléatoire pour nourrir l'algorithme de sélection des bakers. Pour éviter que l'algorithme soit déterministe, les graines sont données sous forme hachée. Le baker s'engage à livrer au cycle suivant les graines correspondantes aux hashs envoyés. S'il ne le fait pas, il ne gagne pas de récompense, mais pourra tout de même récupérer le dépôt associé.

Le protocole permet à un ``accusateur'' qui sur une durée de 5 cycles, pourra montrer (plusieurs fois s'il le faut) la preuve du double baking ou double endorsing. Ainsi, le baker malhonnête se verra confisqué son ou ses dépôts, depuis l'opération fallacieuse, jusqu'au cycle actuel (cela peut être très coûteux, surtout si le baker a ``beaucoup'' baké/endorsé sur la période).

Délai minimum pour baker un bloc

Délai minimum pour baker un bloc

Le délai minimum entre deux blocs est d'une minute. Le baker à la priorité 0 pourra donc baker au minimum 60 secondes après le dernier bloc. Le baker à la priorité 1 devra attendre au moins 40 secondes supplémentaires, puis encore 40 secondes pour celui de priorité 2, etc.

Pour baker le plus rapidement possible, le baker doit réunir assez d'endorsements (au moins 24 sur 32), sinon il doit encore attendre plusieurs secondes de ``pénalité'' par endorsement manquant selon la formule suivante :

$$\text{Délai} = 60 + 40 * p + 8 * \max(0,\ 24 - e) \text{ secondes} \quad \text{avec} \quad \begin{array}{l} p = \text{priorité du baker} \\ e = \text{nombre d'endorsements} \end{array}$$

Tout bloc baké avant la durée minimale sera automatiquement rejeté suivant les règles du protocole.

Over délégation

Over délégation

À chaque baking/endorsement d'un bloc, un dépôt de garantie est nécessaire. Cette somme est bloquée durant 5 cycles. De plus, un baker ne peut ni dépenser les tez qui lui sont délégués, ni les utiliser pour réaliser les dépôts garantie. Par conséquent, un baker doit posséder suffisamment de fonds propres pour baker/endorser des blocs.

Si un baker ne possède pas assez de fonds propres par rapport à son nombre de rolls, il est dit ``over délégué''. Il ne pourra donc pas déposer la garantie nécessaire pour tous les blocs qui lui sont attribués. Il sera donc indisponible pour certains blocs entraînant un ralentissement de la chaîne puisqu'il faudra attendre un baker avec une plus faible priorité.

Des mesures sont étudiées pour permettre aux bakers de refuser la délégation et éviter de se retrouver dans une situation d'over délégation. Cela pourrait être possible à l'avenir si un amendement intégrant ces mesures était voté.

Inactivité

Inactivité

Un baker refusant de baker et d'endorser (ou présentant une incapacité technique) pendant 5 cycles, sera considéré comme inactif par la chaîne et ne pourra plus être sélectionné comme baker/endorser.

Un baker considéré comme inactif devra attendre 7 cycles après avoir procédé à la réactivation de son compte pour pouvoir baker à nouveau.

Ce mécanisme est avant tout là pour éviter qu'un baker ayant cessé son activité ne ralentisse la chaîne.

Attaques

Attaques

Voici une liste non exhaustive d'attaques dont un baker peut être la cible :

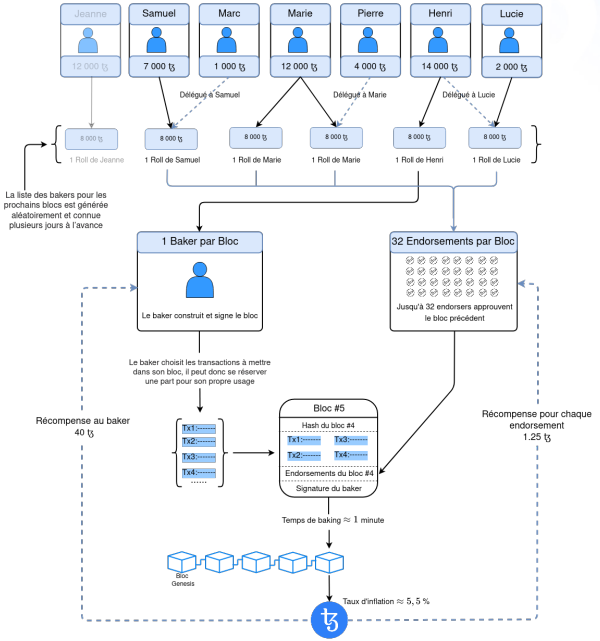
- **DoS (attaque par déni de service)** : Sachant qu'Alice va bientôt baker un bloc avec priorité 0, Bob peut tenter une attaque DoS pour empêcher Alice de diffuser correctement son bloc. Bob peut ainsi porter atteinte à la réputation d'Alice. Si l'attaque dure assez longtemps, Bob peut aussi voler le bloc d'Alice s'il est bien placé dans la liste des potentiels bakers (en particulier s'il a la priorité 1).

- **Vol ou perte de la clé privée** : posséder la clé privée est la seule façon d'avoir accès aux tez qui lui sont associés, ainsi que pour signer les différentes opérations. Il est donc primordial de bien la sécuriser (par exemple à l'aide d'un hardware wallet).

- **Attaque par éclipse** : l'attaquant peut essayer de couper (ou prendre contrôle de) la connexion entre le baker et les nœuds du réseau auxquels il est connecté. Le résultat est proche d'une attaque DoS mais l'attaquant peut en plus envoyer au baker ``isolé'' des blocs qui ne font pas consensus.

Schéma récapitulatif

nomadic labs
Schéma récapitulatif



nomadic labs

Continuons cet échange

https://tezos.com
https://developers.tezos.com
https://tezos-baking.slack.com