



Mécanisme d'amendements de Tezos



Sommaire

Introduction	3
Définition des principaux concepts	5
Processus d'amendement	7
Première période - Proposition	9
Deuxième période - Exploration	11
Troisième période - Cooldown	17
Quatrième période - Promotion	19
Cinquième période - Adoption	21
Fin de processus	23
Historique des amendements	25
Gouvernance on-chain et hard fork	28
Comment voter?	30
Schéma récapitulatif du processus d'amendement	32

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 détail le mécanisme de gouvernance on-chain au travers du processus nécessaire à la prise en compte d'un amendement dans le protocole.

Définition des principaux concepts



Définition des principaux concepts

- **Baking** : Création de nouveaux blocs de la blockchain Tezos, par des "bakers", qui sont rémunérés en contrepartie pour chaque bloc "baké"
- **Endorsement** : Chaque bloc "baké" est validé par d'autres "bakers" qui n'ont pas "baké" le bloc. On dit qu'ils sont des "endorsers" du bloc et ils sont rémunérés en contrepartie pour cela.
- **Délégation** : Chaque détenteur de la crypto-monnaie tez peut déléguer son "droit à baker" et son "droit de vote associé" à un baker, tout en conservant le contrôle de ses fonds.
- **Roll** : Le baking s'effectue avec des droits à ajouter un bloc correspondants au nombre de "rolls" détenues et déléguées. Le droit de vote est également indexé sur ce nombre de rolls. Actuellement, une roll est égale à 8000tz.
- **Cycle** : unité de temps au cours duquel 4096 blocs ont été créés sur Tezos soit environ 2 jours, 20 heures et 16 minutes (1 minute par bloc si aucun baker n'a été défaillant)
- **Proposition** : demande d'ajout, de modification ou de suppression d'une fonctionnalité du protocole.

Processus d'amendement



Processus d'amendement

Sur Tezos, chacun peut soumettre une proposition pour modifier le protocole.

Le processus de proposition/vote se déroule par la suite entièrement on-chain et est nommé **processus d'amendement**.

Ce processus se déroule en 5 étapes :

1. **Proposition**
2. **Exploration**
3. **Cooldown**
4. **Promotion**
5. **Adoption**

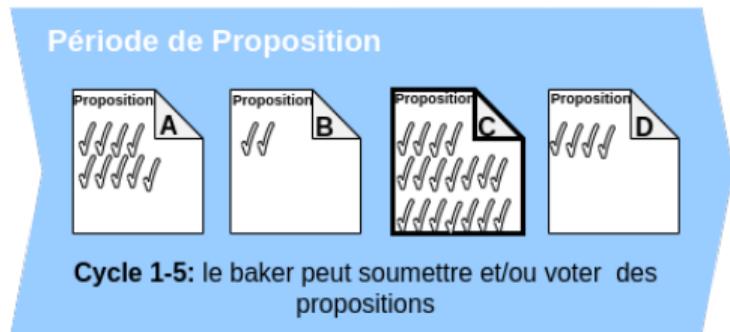


Chaque période a une durée de **5 cycles (≈ 14 jours)**, il faut compter **25 cycles** pour le déroulement d'un processus d'amendement soit environ **2 mois et 10 jours**.

Première période - Proposition



Première période - Proposition (Cycles 1-5)



Pendant cette période, chacun peut soumettre **jusqu'à 20 propositions d'amendement** qui seront soumises dans les étapes suivantes à des phases de votes et de tests.

Les propositions peuvent porter sur de nombreux aspects, notamment :

- La taille d'une roll,
- Le mécanisme de consommation du gas,
- Les fonctionnalités des langages informatiques utilisés
- etc.

Les acteurs du réseau vont ensuite procéder au vote (sous forme d'up-vote). Les propositions d'amendement les mieux classées passent à l'étape suivante d'**Exploration Vote**.

Deuxième période - Exploration



Deuxième période - Exploration (Cycles 6-10)

Période d' Exploration Vote



Règles

- Quorum
- Super majorité (80%)

Cycle 6-10: le baker peut voter pour tester la proposition la plus votée

Durant cette période, tous les votants doivent décider si les propositions passées à cette période passeront ou non à la période suivante : **la période de test**. Contrairement à la période précédente, pour décider de l'envoi ou non en période de test, Tezos utilise **le concept de Quorum et celui de super-majority vote** qui correspond à un vote à la majorité qualifiée.

Définissons les termes dédiés :

- **Quorum** : nombre de personnes requises pour qu'une délibération puisse avoir lieu.
- **Le super-majority vote** ou vote à la majorité qualifiée permet de définir un pourcentage minimal (80% pour Tezos) requis de votes positifs pour que la décision soit acceptée.

Pour passer à la phase suivante, une proposition doit donc recueillir un taux de participation supérieur au Quorum et un taux de votes positifs supérieur à la super majorité.

Vote de la période d'Exploration (Cycle 6-10) 1/2

Calcul du Quorum :

Au lancement du Mainnet de Tezos, le Quorum était à 80% et mis à jour à la fin de chaque vote réussi en fonction du taux de participation.

L'amendement Babylon a apporté deux changements majeurs dans le calcul du Quorum :

- Calcul à partir de la moyenne mobile exponentielle (MME) de la participation,
- Le Quorum est **borné** entre 30 et 70%

Le Quorum se calcule selon la formule suivante :

$$\text{Quorum} = 0.3 + \text{MME}_t * (0.7 - 0.3)$$

Ensuite, la moyenne mobile est mise à jour pour le prochain vote :

$$\text{MME}_{t+1} = 0.8 * \text{MME}_t + 0.2 * \text{Participation}_t$$

Vote de la période d'Exploration (Cycle 6-10) 2/2

Systeme de votes :

Il existe 3 types de votes possibles :

1. **Yays (Y) : Pour**
2. **Nays (N) : Contre**
3. **Abstains (A) : vote blanc**

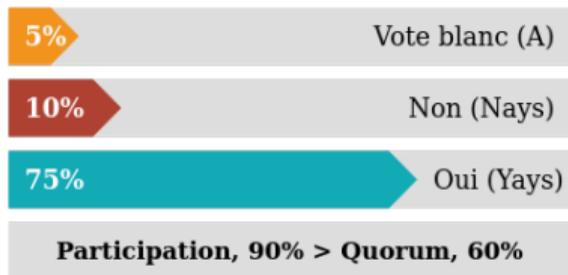
Pour voter chaque baker actif sur le réseau doit disposer **au minimum 1 roll** (8000tz). Chaque détenteur de la crypto-monnaie tez (atteignant ou non 1 roll) peut déléguer son "droit de vote associé" à un baker, tout en conservant le contrôle de ses fonds.

Dans la réalité, le poids d'une personne votant est défini au prorata du nombre de rolls qu'il possède. ***Plus une personne possède de tez, plus son vote a de poids.***

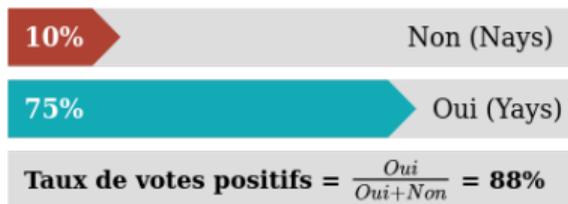
Exemples de votes 1/2

Pour illustrer ce mécanisme, prenons un exemple de 100 rolls actifs gérés par des bakers et une MME de participation de 75%. 90 votes correspondants (Yays, Nays et Abstaint) durant la période d'exploration vote. **Exemple 1 :**

1. Quorum = $0.3 + 75\% * (0.7 - 0.3) = 60\%$



3. Taux de votes positifs = 88%



2. Mise à jour de la moyenne mobile

$$MME_{t+1} = 0.8 * 75\% + 0.2 * 90\% = 78\%$$

Avec:

$$75\% = MME_t$$

90% = Taux de participation

4. Validation de la proposition



La proposition d'amendement peut passer à la période suivante de test

Avec:

88% = Taux de votes positifs

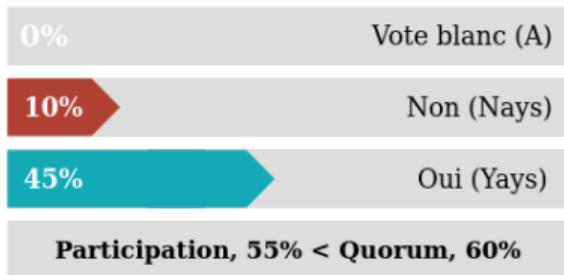
80% = Super majorité

Exemples de votes 2/2

Pour illustrer ce mécanisme, prenons un exemple de 100 rolls actifs gérés par des bakers et une MME de participation de 75%. 55 votes correspondants (Yays, Nays et Abstaint) durant la période d'exploration vote.

Exemple 2 :

1. $Quorum = 0.3 + 75\% * (0.7 - 0.3) = 60\%$



2. Mise à jour de la moyenne mobile

$$MME_{t+1} = 0.8 * 75\% + 0.2 * 55\% = 71\%$$

Avec:

75% = MME_t

55% = Taux de participation

3. Rejet de la proposition

Bien que le Oui ait remporté la super majorité, le Quorum n'étant pas atteint, **la proposition est rejetée**. On retourne à la première phase de propositions.

Troisième période – Cooldown



Troisième période – Cooldown (Cycles 11-15)

Période de Cooldown

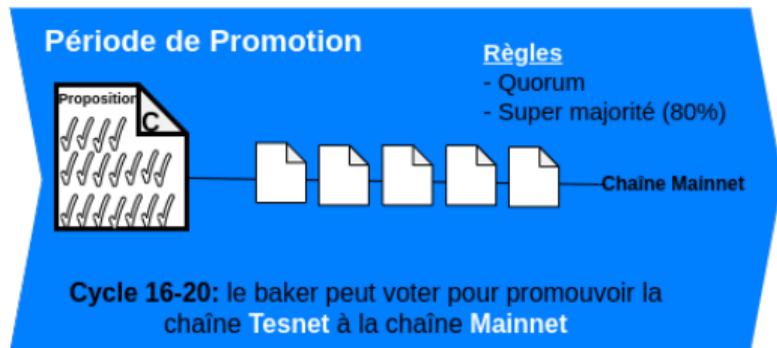
Cycle 11-15: le seul intérêt de cette période est d'accorder du temps avant la période de promotion

Si une proposition est acceptée par une super majorité au cours de la période d'Exploration Vote, la période de cooldown débute. Cette période remplace la précédente période de test qui était peu utilisée. En pratique, les tests sont effectués sur un testnet dédié.

Quatrième période – Promotion



Quatrième période – Promotion (Cycles 16-20)



À la fin de la période de test, le réseau décide ou non d'adopter la proposition d'amendement sur la base des discussions hors chaîne et de son comportement pendant la période de test.

Les mêmes principes de Quorum et super majorité sont appliqués.

Après le vote, la moyenne mobile de participation est encore mis à jour.

La version du protocole intégrant l'amendement est propagée par le réseau et transmise aux nœuds qui s'actualisent automatiquement de manière transparente.

Cinquième période – Adoption

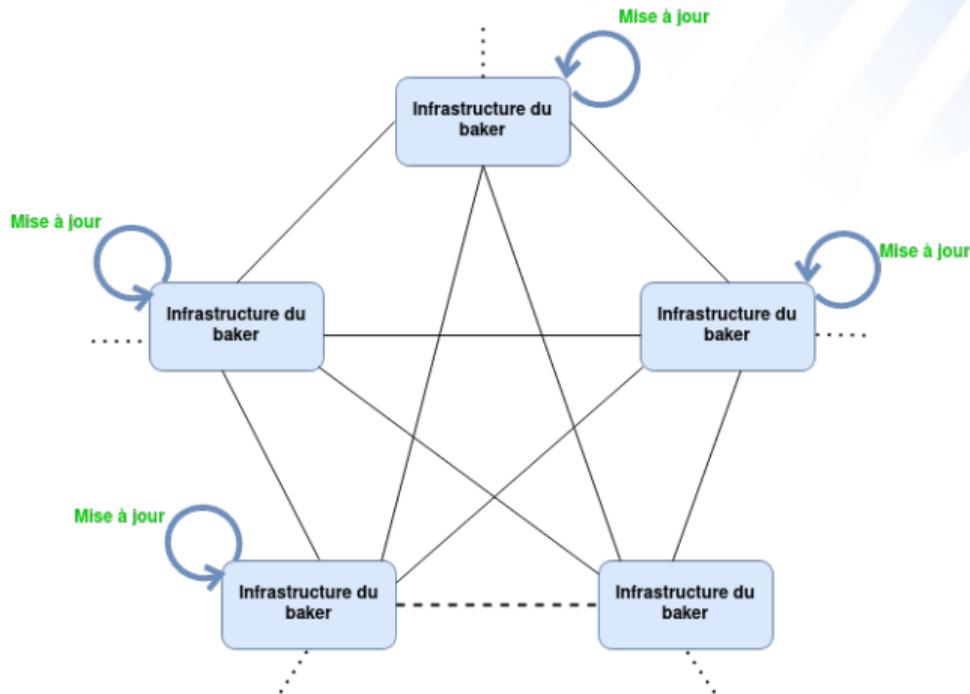


Cinquième période – Adoption (Cycles 21-25)

Période d'Adoption

Cycle 21-25 : Les bakers mettent à jour leur infrastructure

La période d'adoption est une période pendant laquelle les nœuds doivent être mis à jour. À l'issue de cette période le nouveau protocole sera adopté avec certitude, ce qui permet de mieux préparer la migration.



Fin de processus



Fin de processus

À la fin de la période d'adoption, on retourne à la période de proposition.

La personne dont la proposition a été adoptée comme amendement du protocole a le mérite d'avoir fait évoluer la blockchain Tezos et **est récompensée en $\text{t\$}$ d'un montant qu'elle a au préalable prédéfini dans le code source de sa proposition.**

Historique des amendements



Historique des amendements (1/2)

1. Mai 2019, amendement **Athènes** :
 - réduction de la taille d'une roll nécessaire pour un baker (10000 à 8000)
 - augmentation de la limite de gaz par opération et par bloc
2. Octobre 2019, amendement **Babylone** :
 - Modification de l'algorithme de consensus "emmy+"
 - Nouvelles features pour le langage de smart contract bas niveau (Michelson), modification du coût du gas
 - Modification de la formule de mise-à-jour du Quorum ($30\% \leq \text{Quorum} \leq 70\%$)
3. Mars 2020, amendement **Carthage** :
 - Augmentation de la limite de gas par opération et par bloc
 - Amélioration de la formule du calcul des récompenses de baking
4. Novembre 2020, amendement **Delphes** :
 - Réduction du coût du storage par 4
 - Recalcul généralisé du coût du gaz

Historique des amendements (2/2)

5. Février 2021, amendement **Edo** :

- Ajout du protocole Sapling
- Ajout des tickets
- Ajout de commandes Michelson dont les fonctions de hachage SHA3 et Keccak
- Mise à jour du protocole d'amendement :
 - ajout d'une cinquième période de vote (adoption)
 - réduction du temps des périodes de 8 à 5 cycles

6. Mai 2021, amendement **Florence** :

- Augmentation de la taille maximale des données d'une opération
- Ordre d'exécution suivant un parcours en profondeur
- Optimisation des performances
- Mise à jour du protocole d'amendement : la période de test est remplacée par une période de cooldown

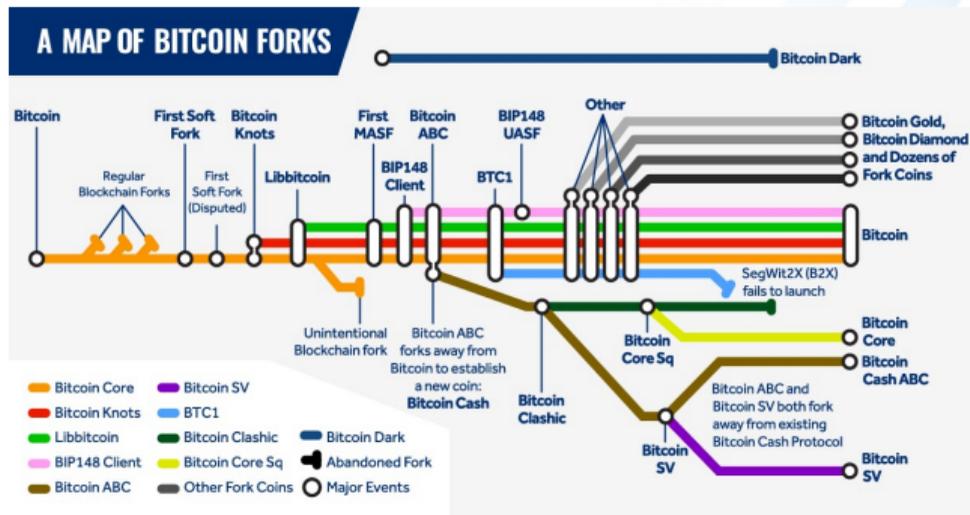
Gouvernance on-chain et hard fork



La gouvernance on-chain réduit les risques de hard fork

L'histoire de Bitcoin montre qu'il est nécessaire de passer par un hard fork afin d'apporter des changements à ce protocole.

C'est une opération risquée dans le sens où deux chaînes peuvent co-exister si un consensus n'est pas trouvé au sein de la communauté, conduisant à des risques opérationnels pour certains projets blockchain.



Cependant, quand des bugs critiques ont été identifiés, il est arrivé de mettre à jour le protocole en urgence, pour Bitcoin comme pour Tezos. Mais ce type de situation n'a jamais mené à des scissions en 2 chaînes différentes car ce type de changement fait consensus.

Comment voter ?



Comment voter ?

On peut voter directement en utilisant le client Tezos :

Pour connaître la période en cours :

```
$ tezos-client show voting period
```

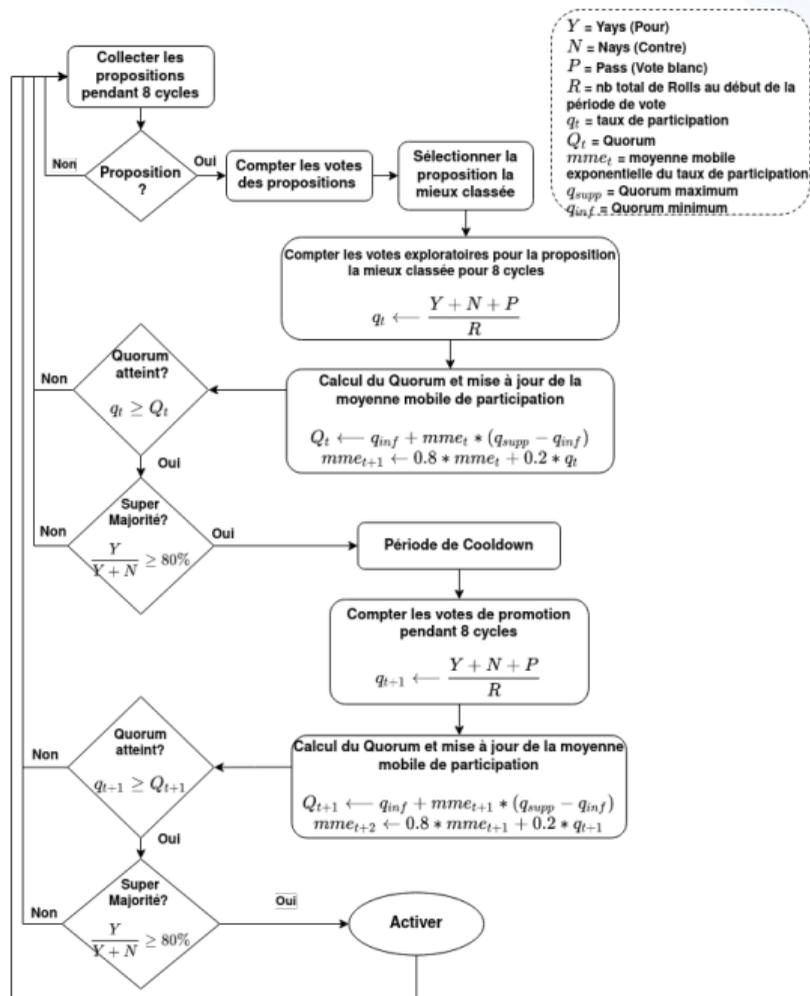
Pour voter pour la proposition dont le hash est <proposal> avec l'adresse <delegate> :

```
$ tezos-client submit ballot for <delegate> <proposal> <yay|nay|pass>
```

Kiln, un outil souvent utilisé par les bakers intègre une interface pour voter.

Schéma récapitulatif du processus d'amendement







nomadic labs

Continuons cet échange

<https://tezos.com>

<https://developers.tezos.com>

