

Dynamique des jetons natifs d'Avalanche(\$AVAX)

Stephen Buttolph, Amani Moin, Kevin Sekniqi, et Emin Gün Sirer

Traduit par Christophe Nussbaumer

25/06/2020

Résumé

Cet article traite des détails clés d'implémentation du jeton natif d'Avalanche (appelé \$AVAX), et notamment de son économie (*tokenomics*). Le jeton natif sert à sécuriser le réseau et à payer les frais de transaction, et il fournit l'unité de compte de base entre les multiples blockchains déployées sur le réseau plus large d'Avalanche. Pour plus de détails sur Avalanche, plateforme polyvalente et universelle permettant à quiconque de lancer de nouvelles blockchains avec leurs propres règles, machines virtuelles et ensembles de validateurs, nous invitons le lecteur à lire le document d'architecture d'accompagnement [1] ou la documentation Avalanche [2].

Commit Git : 30d3aeb5863f5fcb033f9a34bcad5f21a79a4b7d

Déclaration : les informations décrites dans ce document sont préliminaires et sujettes à modification à tout moment. De plus, ce document peut contenir des déclarations prospectives. Celles-ci se rapportent généralement à des événements futurs ou à nos performances futures. Cela comprend, mais sans s'y limiter, les performances projetées d'Avalanche ; le développement attendu de ses affaires et projets ; l'exécution de sa vision et de sa stratégie de croissance ; ainsi que l'achèvement de projets actuellement en cours, en phase de développement ou à l'étude. Les déclarations prospectives représentent les convictions et hypothèses de notre direction uniquement à la date de cette présentation. Ces déclarations ne sont pas des garanties de performances futures et il ne faut pas s'y fier indûment. Ces déclarations prospectives impliquent nécessairement des risques connus et inconnus qui peuvent faire en sorte que le rendement réel et les résultats dans les périodes futures diffèrent sensiblement de toute projection explicite ou implicite dans ce texte. Avalanche n'assume aucune obligation de mettre à jour les déclarations prospectives. Bien que les déclarations prospectives constituent notre meilleure prédiction au moment où elles sont formulées, rien ne garantit qu'elles se révéleront exactes, dans le sens où les résultats réels et les événements futurs pourraient différer considérablement. Le lecteur est prié de ne pas se fier indûment aux déclarations prospectives.

1 Introduction

Le modèle économique d'une nouvelle monnaie ou d'un nouvel actif numérique est l'une des composantes les plus critiques de la plateforme sur laquelle ils résident. Cela est particulièrement vrai pour le jeton natif d'une plateforme auto-souveraine et sans permission comme **Avalanche**. Dans cet article, nous discutons de la conception du jeton natif appelé **\$AVAX**. La discussion est décomposée comme suit : propriétés de gouvernance du jeton, sa quantité totale (*supply*), la fonction de récompense (ou émission de nouveaux jetons) des personnes qui mettent en jeu leurs jetons (*stakers*), ainsi que d'autres détails économiques pertinents tels que l'économie transactionnelle.

1.1 Les propriétés clés de l'\$AVAX

Voici les principales propriétés clés à retenir de la conception du modèle économique de l'\$AVAX :

- les ressources dépensées par un validateur pour la mise en jeu (*staking*) sont proportionnelles à la mise en jeu totale de ce validateur ;
- les récompenses accumulées par un validateur pour la validation sont proportionnelles à la mise totale de ce validateur ;
- comme **Avalanche** n'a pas de leader, il n'y a pas d'effets cumulatifs du genre « les riches deviennent plus riches » ;
- les validateurs qui verrouillent leur mise plus longtemps sont davantage récompensés. Les validateurs sont incités à rester en ligne et à fonctionner correctement car leurs récompenses sont basées sur la preuve de disponibilité (*proof-of-uptime*) et la preuve d'exactitude (*proof-of-correctness*) ;
- **\$AVAX** est un jeton dont la quantité totale est plafonnée à 720 millions de jetons ;
- bien que plafonné, l'\$AVAX est toujours gouvernable. Le taux d'émission pour atteindre la quantité maximale dépend de la gouvernance. Les frais ne sont payés à aucun validateur spécifique. Au lieu de cela ils sont brûlés (*burned*), augmentant ainsi la rareté de l'\$AVAX.

2 Gouvernance

Nous débutons notre enquête sur la conception économique d'**Avalanche** en discutant d'abord de la gouvernance, celle-ci jouant un rôle essentiel à l'intérieur de futures composantes. Pour permettre au système de s'adapter aux conditions économiques changeantes, la plateforme **Avalanche** permet de modifier dynamiquement les paramètres clés du système en fonction des entrées (*inputs*) de l'utilisateur. Pour les systèmes décentralisés sans dépositaire, un processus viable est essentiel pour trouver des valeurs globalement acceptables concernant les paramètres système. **Avalanche** peut utiliser son mécanisme de consensus pour construire un système qui permet à quiconque de proposer des transactions spéciales qui sont, par essence, des sondages à l'échelle du système. Tout nœud participant peut émettre de telles propositions.

Le taux de récompense est un paramètre important qui affecte toute devise, qu'elle soit numérique ou fiat. Malheureusement, les crypto-monnaies qui corrigent ce paramètre peuvent rencontrer divers problèmes, dont la déflation ou l'hyperinflation. À cette fin, le taux de récompense sera soumis à la gouvernance dans des limites préétablies. Cela permettra aux détenteurs de jetons de choisir le taux auquel l'\$AVAX atteint le plafond de sa quantité totale.

Les frais de transaction, désignés par l'ensemble \mathcal{F} , seront aussi éventuellement soumis à la gouvernance. \mathcal{F} est en fait un n-uplet qui décrit les frais associés aux différentes instructions et transactions prises en charge dans les versions futures. Enfin, le temps et les montants de staking seront également soumis à la gouvernance. La liste de ces paramètres est définie en figure 1.

- Δ : montant du staking, libellé en \$AVAX. Cette valeur définit la mise minimale requise pour être placée en tant que caution avant de participer au système. La valeur d'origine par défaut sera de 2000 \$AVAX.
- δ_{\min} : durée minimale de staking d'un nœud pour participer au système. La valeur d'origine par défaut sera de 2 semaines.
- δ_{\max} : durée maximale de staking d'un nœud. La valeur d'origine par défaut sera de 52 semaines.
- γ, λ : les deux paramètres clés pour contrôler la fonction du taux d'émission des jetons.
- \mathcal{F} : la structure des frais, qui est un ensemble de paramètres de frais soumis à gouvernance définissant les coûts des diverses transactions.

FIGURE 1 – Paramètres de gouvernance clés utilisés dans **Avalanche**

En fin de compte, nous notons que la gouvernance dans l'\$AVAX a de l'hystérésis, ce qui signifie que les changements de paramètres dépendent fortement de leurs changements récents. Il existe deux limites associées à chaque paramètre soumis à gouvernance : le temps et la portée. Une fois qu'un paramètre est modifié à l'aide d'une transaction de gouvernance, il devient très difficile de la modifier immédiatement à nouveau et de manière importante. Ces contraintes de difficulté et de valeur s'assouplissent à mesure que le temps s'écoule depuis la dernière modification. Ces restrictions sont conformes à la philosophie de la conception de la prévisibilité : le système ne doit jamais changer radicalement sur une courte période de temps, permettant ainsi aux utilisateurs de prévoir en toute sécurité les paramètres du système à court terme, tout en conservant un contrôle et une flexibilité solides sur le long terme.

3 L'économie du jeton

La quantité plafonnée d'\$AVAX est de 720 000 000 (720 millions) de jetons. Le premier bloc (*genesis block*) aura 360 millions de jetons \$AVAX. Le reste des 360 millions de jetons sera émis selon l'équation ~1. La représentation graphique en figure 2 montre la courbe des émissions de jetons entre \$AVAX et BTC. Le principe de la fonction d'émission choisie pour **Avalanche** est simple : atteindre une quantité

plafonnée de manière similaire à la courbe d'émission du Bitcoin, tout en conservant la capacité de contrôler le taux auquel le système atteint cette limite.

95 3.1 Fonction d'émission

R_j est le nombre total de jetons à l'année j , avec $R_1 = 360$ millions, et R_l représentant la dernière année où les valeurs $\gamma, \lambda \in \mathbb{R}$ ont été modifiées ; c_j est l'offre encore non émise de pièces pour atteindre 720 millions à l'année j de sorte que $c_j \leq 360$ millions ; u représente un staker, avec le montant $u.s_{\text{montant}}$ représentant le montant total de la mise que u possède, et $u.s_{\text{temps}}$ la durée du staking pour u .

$$R_j = R_i + \sum_{\forall u} \rho(u.s_{\text{montant}}, u.s_{\text{temps}}) \times (c_j/L) \times \left(\sum_{i=0}^j \frac{1}{\left(\gamma + \frac{1}{1+i\lambda}\right)^i} \right), \quad (1)$$

où

$$L = \left(\sum_{i=0}^{\infty} \frac{1}{\left(\gamma + \frac{1}{1+i\lambda}\right)^i} \right). \quad (2)$$

A l'origine, $c_1 = 360$ millions. Les valeurs de γ et λ sont soumises à la gouvernance, et si elles sont changées, la fonction est recalculée avec la nouvelle valeur de c_* . Il se trouve que $\sum_* \rho(*) \leq 1$. $\rho(*)$ est une fonction linéaire qui peut être calculée comme suit ($u.s_{\text{temps}}$ est mesuré en semaines et $u.s_{\text{montant}}$ est mesuré en jetons \$AVAX) :

$$\rho(u.s_{\text{montant}}, u.s_{\text{temps}}) = (0.002 \times u.s_{\text{temps}} + 0.896) \times \frac{u.s_{\text{montant}}}{R_j}. \quad (3)$$

Si la totalité des jetons à l'année j est mise en jeu pour la durée maximale de temps de staking (une année, ou 52 semaines), alors $\sum_{\forall u} \rho(u.s_{\text{montant}}, u.s_{\text{temps}}) = 1$. Si, au contraire, tous les jetons sont mis en jeu continuellement pour la durée minimale de staking fixée à deux semaines, alors $\sum_{\forall u} \rho(u.s_{\text{montant}}, u.s_{\text{temps}}) = 0.9$. Dès lors, la mise en jeu pour la durée maximale engendre 11.11% supplémentaire de jetons émis. Comme la quantité totale est plafonnée, la fonction ci-dessus garantit que nous ne dépasserons jamais un total de 720 millions de jetons, quel que soit le nombre de changements de gouvernance.

$$\lim_{j \rightarrow \infty} R_j = 720 \text{ millions}. \quad (4)$$

4 Mécanisme d'émission du jeton

L'émission de jetons dans \$AVAX est conçue pour inciter les nœuds à se comporter d'une manière qui contribue positivement aux résultats globaux. Ceci est accompli par des transactions spéciales d'émission. Un nœud gagne le droit d'émission en hébergeant d'abord une mise, puis en participant activement au processus du consensus. Plus précisément, les récompenses des nœuds sont directement liées à leur disponibilité et leur temps de réponse. Chaque nœud conserve des informations locales sur

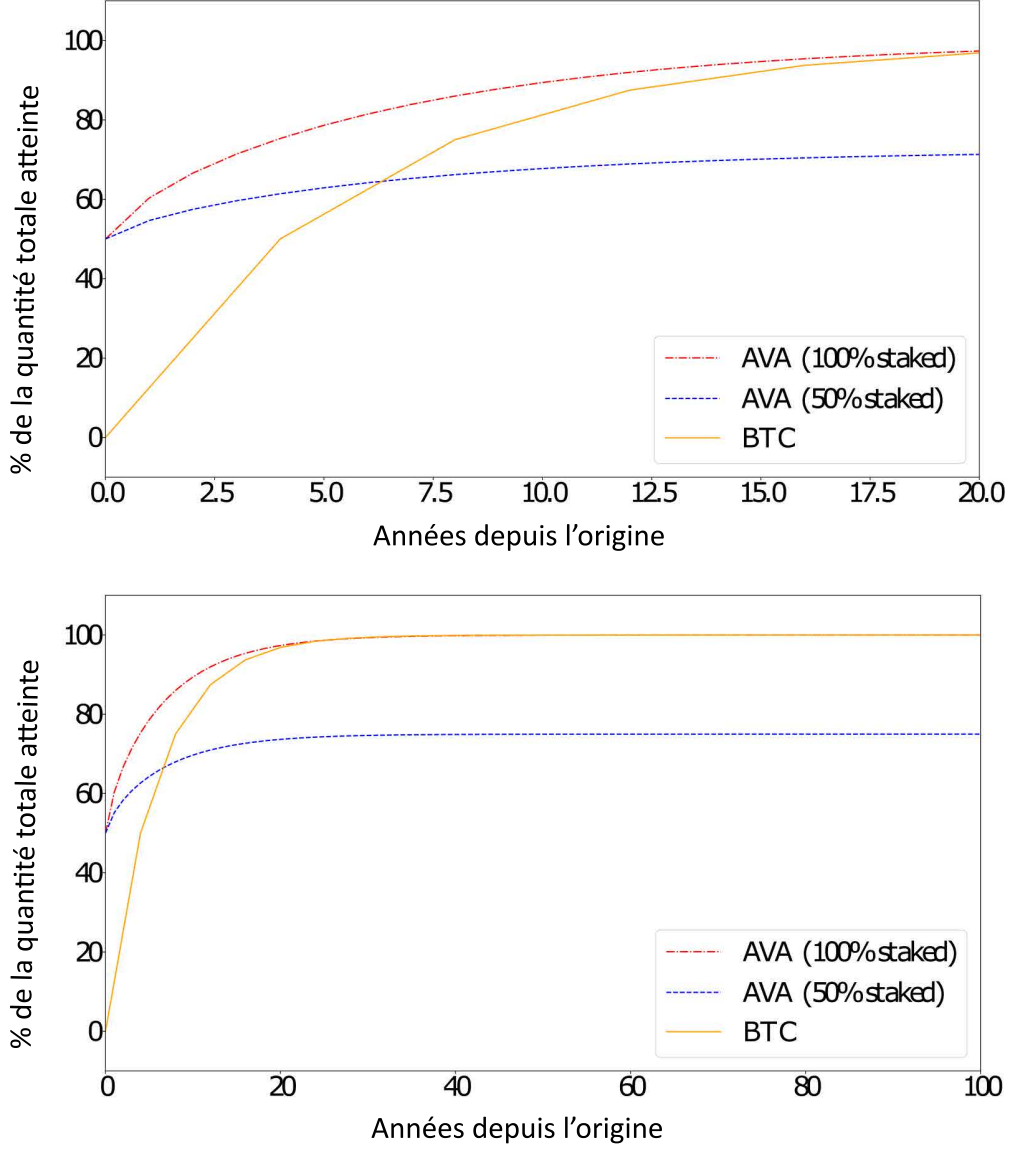


FIGURE 2 – Emissions de jetons entre \$AVAX et BTC, calculées sur un horizon de 20 et 100 ans, avec $\gamma = 1.15$ et $\lambda = 1.1$. La courbe pour « \$AVAX (100% staked) » représente le cas où chaque jeton est mis en jeu de façon répétée pour la durée de staking maximale d'un an, c'est-à-dire $\sum_{\forall u} \rho(u.s_{\text{montant}}, u.s_{\text{temps}}) = 1$. D'autre part, la courbe pour « \$AVAX (50% staked) » représente le cas où seulement 50% des jetons sont mis en jeu de façon répétée sur la durée de staking minimale de deux semaines, c'est-à-dire $\sum_{\forall u} \rho(u.s_{\text{montant}}, u.s_{\text{temps}}) = 0.45$. Nous notons que, par souci de simplicité, ces graphiques représentent le cas où γ et λ sont fixés à l'origine et ne sont jamais soumis à la gouvernance par la suite. En changeant γ et λ , le but est d'augmenter la quantité totale des jetons dans le cas où la quantité totale mise en jeu et observée empiriquement est trop basse.

la vitalité et le comportement de chaque autre nœud avec lequel il a interagi. A chaque fois qu'un nœud
120 v est échantillonné par u , ce dernier maintient un n -uplet (bit de réponse, horodatage). La première
entrée est un bit unique qui représente si v a répondu dans le délai d'expiration, et la seconde représente
l'horodatage de la réponse. En d'autres termes, l'émission dans **Avalanche** se fait via une preuve de
disponibilité (*proof-of-uptime*) et une preuve de réactivité (*proof-of-responsiveness*). Ce mécanisme a
des conséquences importantes. En particulier, comme il n'y a pas de « leader » qui accumule des
125 récompenses, il n'y a pas d'effets cumulatifs du genre « les riches deviennent plus riches ».

5 L'économie transactionnelle

5.1 Structure des frais

La structure des frais de la plateforme **Avalanche** comporte plusieurs caractéristiques de différenciation qui la distinguent des autres plateformes existantes et à venir.

130

Frais de stake. Contrairement à d'autres protocoles qui paient tous les frais au leader élu, comme dans Bitcoin, les frais d'**Avalanche** sont simplement brûlés. Par conséquent, le paiement est global et bénéficie à tout l'écosystème. La combustion des frais augmente la rareté des jetons dans le système. Le processus d'émission des jetons compense la combustion des frais de transaction. Le système ne
135 risque dès lors pas un arrêt total à long terme en raison de la destruction progressive des jetons.

Coûts de transaction. Dans **Avalanche**, les frais de transaction diffèrent selon le type de transaction. Les instanciations de nouveaux sous-réseaux entraînent les frais les plus élevés. Par contraste, d'autres types de transactions, comme de simples paiements d'**\$AVAX**, sont peu coûteux. Pour d'autres sous-
140 réseaux, les transactions paient des frais dans le jeton natif du sous-réseau en question ainsi qu'un certain montant dans le jeton **\$AVAX**. Une transaction native d'un sous-réseau peut spécifier sa propre structure de frais de transaction, et c'est au créateur du sous-réseau de choisir une structure de frais qui incite à la validation des sous-réseaux ouverts et sans permission.

145 *Fonction de coûts glissants.* Les frais de transaction ont une fonction de coûts glissants. Les frais ne sont pas fixés par l'émetteur de la transaction, mais plutôt par une fonction de frais vérifiable globalement. À mesure que la congestion du réseau augmente, les frais augmentent. À la fin d'une période de temps spécifique, la fonction est recalculée pour tenir compte des augmentations naturelles de volumes de transactions dans le réseau.

150

Niveaux de transaction. Contrairement à un modèle comme celui d'Ethereum, où chaque appel de transaction doit payer un certain montant, **Avalanche** adopte un modèle différent qui intègre deux types de mécanismes de traitement des transactions. Toutes les clés dont le solde de compte est positif pourront interagir immédiatement avec la plateforme, où les frais seront basés sur un mécanisme d'attribution, fonctionnellement similaire à un modèle de paiements échelonnés adopté dans les plateformes
155 de *cloud computing*. Chaque transaction comportera une adresse d'expéditeur (c'est-à-dire l'appelant),

qui sera vérifiée pour l'attribution actuelle des appels. S'il reste des invocations gratuites à l'adresse, la transaction ne doit pas comporter de frais pour l'expéditeur. Au-delà d'un certain nombre d'appels, l'expéditeur devra joindre certains frais en fonction des ressources utilisées pour calculer la transaction.

160 En outre, les utilisateurs peuvent choisir de payer leurs transactions par un calcul. À cette fin, les prochaines versions supporteront des transactions gratuites limitées en fréquence, qui ne nécessitent pas de frais en numéraire mais un calcul préliminaire. Chaque fois qu'une nouvelle transaction est générée, l'utilisateur calculera et joindra une preuve de travail valide à la transaction, qui pourra être vérifiée par toutes les parties.

165 5.2 Gestion du spam

Bien que les paiements simples entraînent des frais, la valeur en sera pratiquement nulle. Cependant, cela peut conduire à du spam sur le réseau. Dans les versions futures, pour éviter la congestion, chaque transaction comportera une preuve de travail (*PoW*) locale. La preuve de travail est initialement de faible difficulté, permettant donc à une transaction d'être émise immédiatement avec très peu de frais
170 généraux. Cependant, si une clé spécifique génère un grand nombre de transactions dans un court laps de temps, chaque transaction ultérieure entraînera une plus grande difficulté dans le puzzle de sa preuve de travail. Ce mécanisme fonctionne en conjonction avec la combustion des frais.

Références

- [1] AVA : Avalanche platform paper - architectural overview (2019),
175 <https://les.avalabs.org/papers/platform.pdf>
- [2] AVA : Avalanche platform documentation (2025),
<https://docs.avax.network>