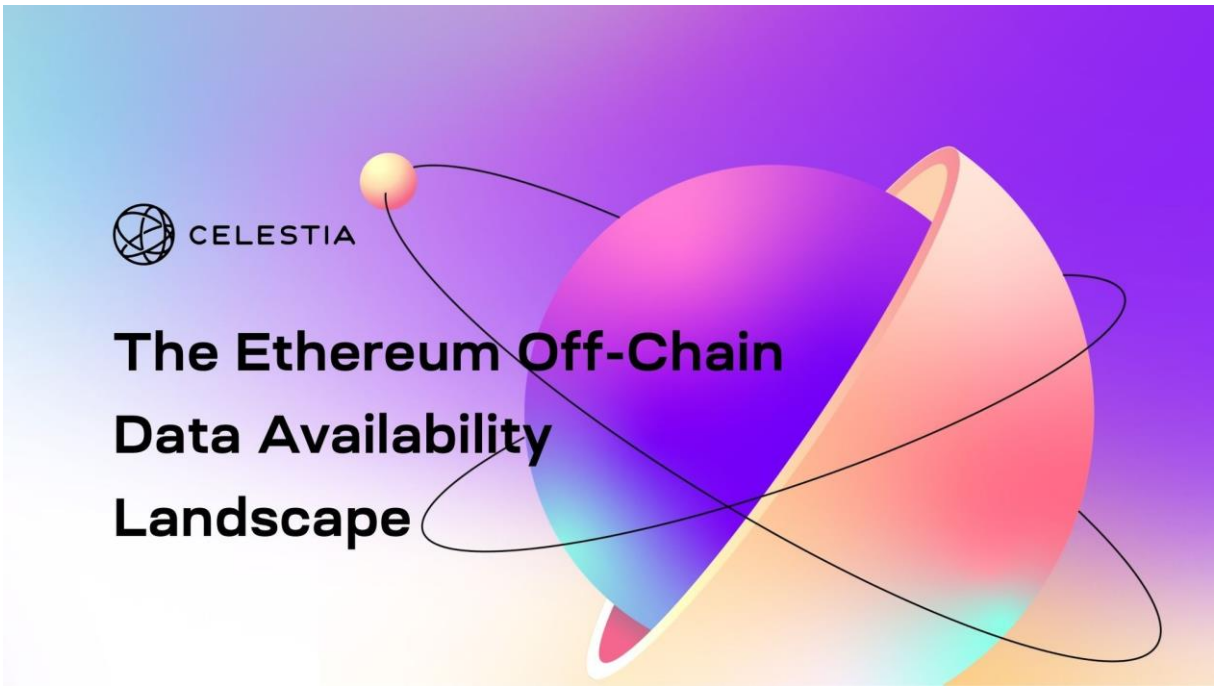
Le paysage de la disponibilité des données hors chaîne d'Ethereum

14/02/2022

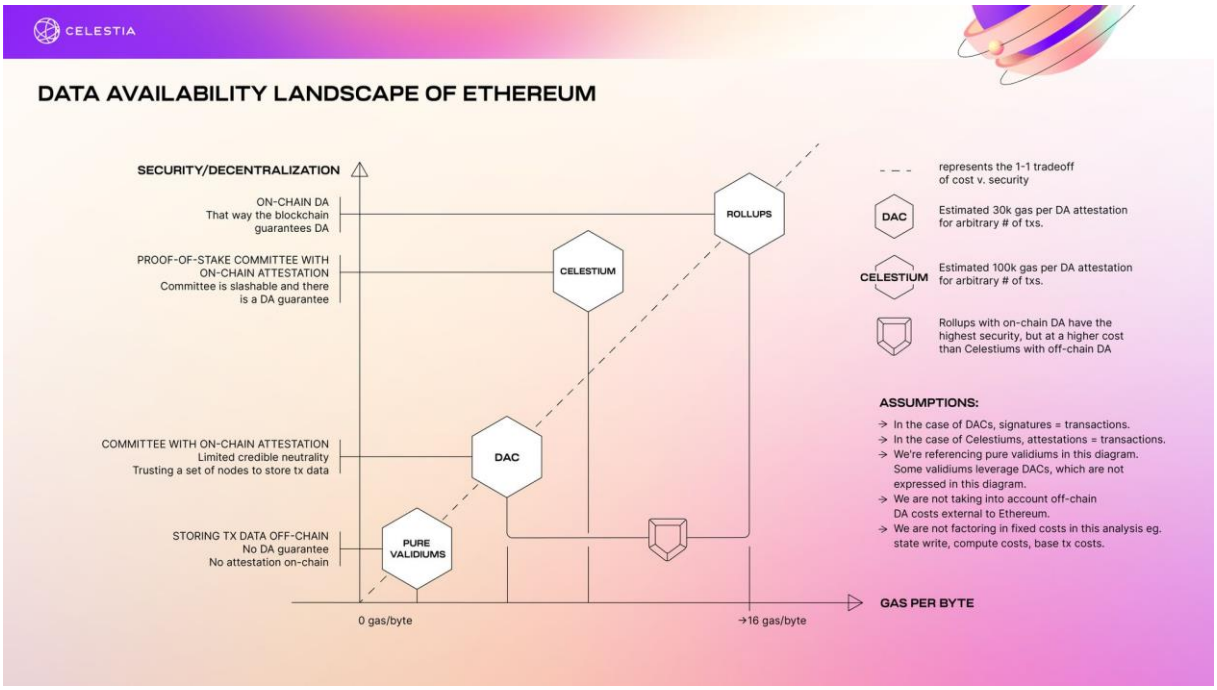
Source : https://blog.celestia.org/ethereum-off-chain-data-availability-landscape/



Les blockchains doivent garantir la disponibilité des données (DA), notamment les chaînes rollup et de couche 2 (L2). Le problème de la disponibilité des données blockchains est le suivant : les participants aux réseaux peuvent être dans l'incapacité d'interpréter son état ou de le mettre à jour lorsque les créateurs de blocs transmettent l'état du système mais retiennent les données des transactions sous-jacentes.

Les solutions de disponibilité des données pour les L2 d'Ethereum se sont rapidement développées, allant des solutions exploitant les couches DA hors chaîne et sur chaîne. Il peut être complexe de s'y retrouver, c'est pourquoi nous sommes ici. Dans cet article, nous allons examiner spécifiquement la disponibilité des données hors chaîne pour l'écosystème L2 d'Ethereum.

Toutes les solutions DA pour les L2 d'Ethereum sont confrontées à un dilemme de choix. Elles doivent faire un compromis entre le coût et la sécurité. Le coût, dans ce cas, fait référence à la capacité des solutions DA hors chaîne à se développer sans faire augmenter les frais de gas. La sécurité fait référence à la capacité de garantir la disponibilité des données.



Le paysage de la disponibilité des données d'Ethereum.

Nous allons aborder le paysage de la disponibilité des données hors chaîne en partant de gauche à droite depuis l'image ci-dessus. Notez que cette analyse a été réalisée en tenant compte de plusieurs hypothèses :

- Dans le cas des DACs, nous considérons que signatures = transactions. Dans le cas des Celestiums, les attestations = transactions.
- Nous ne faisons référence qu'aux validiums purs dans ce post. Il peut y avoir des validiums qui tirent parti des DACs mais ils ne seront pas évoqués dans l'analyse ci-dessous.
- Seuls les frais de gas Ethereum sont pris en compte, le coût d'inclusion des données sur les couches off-chain ne sont pas compris dans l'analyse. Dans le cas des Celestiums, il y aura effectivement des frais sur Celestia, cependant, le débit de données maximum sera beaucoup plus important, et donc pour les besoins de cette analyse, il est supposé que les frais de données sur Celestia on-chain sont insignifiants par rapport à Ethereum.
- Les coûts fixes ne sont pas pris en compte dans cette analyse, en particulier :
    - Coûts d'écriture d'état - coûts associés à la mise à jour de l'état dans les smart contracts rollup (~20 000 gas).
    - Coût de calcul - coûts associés à la transmission d'en-tête, le hachage, les boucles, etc (~10,000 gas).

    - Coût de transaction de base - coût sur Ethereum pour la transmission d'une tx (21 000 gas).
- Nous ne tenons pas compte des coûts de mise à jour de l'ensemble des validateurs dans le cas des Celestiums. Étant donné que les grands changements dans le pouvoir de vote ne se produisent que très occasionnellement, il s'agit d'une meilleure estimation.

Validiums

Les validiums purs sont représentés au plus bas du graphique DA ci-dessus. Un validium utilise des preuves de connaissance zéro pour la validité des transactions et stocke les données de transaction hors chaîne à l'aide d'un fournisseur de données centralisé. Comme on peut le voir sur le graphique, les validiums représentent la solution la moins cher en termes de frais de données.

Pour accéder au dernier état d'un validium, il faut que les données hors chaîne soient disponibles. C'est très bien, sauf dans les cas où le fournisseur de données se comporte mal ou est hors ligne. Par conséquent, il n'y a pas de garantie de DA et la sécurité est faible.

Les conceptions actuelles de validium utilisent un comité (voir la section suivante) plutôt qu'un fournisseur unique en raison de ces problèmes de sécurité.

Comités de disponibilité des données (DAC)

Les comités de disponibilité des données (DACs) peuvent être considérés comme des validiums comportant plusieurs nœuds.

Les nœuds ou les membres des DAC sont des parties de confiance qui conservent des copies des données hors chaîne et les renvoient dans le cas où les opérateurs de rollup agissent de manière malveillante.Ces nœuds attestent que les données de la L2 sont disponibles en publiant des signatures on-chaîne.

Les coûts d'exploitation des DACs sont modérément bas. L'installation d'un nœud dans un DAC est relativement bon marché et les comités sont généralement composés de 7 à 10 membres.

En supposant qu'un DAC compte 10 membres et que la vérification d'une signature coûte 3 000 gas, le coût de la vérification d'une attestation de DA est d'environ 30 000 gaz. Aucune donnée de transaction n'est activement postée sur la chaîne en dehors de l'attestation de la disponibilité des données, le coût est donc relativement faible et fixe, quel que soit le volume des transactions (en supposant un nombre fixe de nœuds dans le DAC).

D'un point de vue sécurité, certains choix ont été faits. Un comité restreint qui peut ne pas être crédiblement neutre exige que les utilisateurs finaux fassent confiance à ce groupe fixe d'acteurs pour stocker les données de transaction. Si un nombre minimum de membres du comité devait agir de manière malveillante, ils pourraient geler (dans le cas d'un zk rollup) ou voler (dans le cas d'un optimistic rollup) tous les fonds et détruire entièrement la vivacité de la chaîne, ce qui représente un risque considérable.

DACs : des projets comme DeversiFi et ImmutableX utilisent des DACs.

Celestiums

Un Celestium est une chaîne L2 qui s'appuie sur Celestia pour la disponibilité des données, mais utilise Ethereum pour la partie paiement et la résolution des conflits. Un Celestium peut être considéré comme un DACs sans permission avec des garanties supplémentaires concernant la disponibilité des données car le comité peut être révoqué s'il se comporte mal. Cela est rendu possible par les nœuds légers du réseau Celestia qui peuvent détecter les blocs indisponibles grâce à l'échantillonnage des données, et donc, de manière similaire à un nœud complet, peuvent s'arrêter automatiquement si l'ensemble des validateurs devient malveillant.

En effet, Celestia est plus crédible en tant que couche DA qu'en tant que DAC, car elle existe en tant que chaîne indépendante à part entière, en tant que couche DA à usage universel, plutôt qu'en tant que couche DA dédiée à une L2 spécifique d'Ethereum.

Les Celestiums coûtent environ 100 000 gas par attestation DA pour un nombre arbitraire de transactions. Environ 30 signatures sont nécessaires par attestation à 3 000 gas par signature = 90 000 gas (signatures provenant de >⅔ du pouvoir de vote de l'ensemble des validateurs). Cette estimation est basée sur les chaînes reposant sur Tendermint. Actuellement, ⅔ du pouvoir de vote sur le Cosmos Hub est délégué à 22 validateurs.

Couches DA : Celestia, Polygon Avail.

Rollups Ethereum

Les rollups traditionnels d'Ethereum constituent le dernier groupe du diagramme. Les rollups exploitent la disponibilité des données sur la chaîne, ce qui les rend très sûrs. Le coût, cependant, est également élevé, étant donné que les données de transaction sont postées sur Ethereum.

La plupart des rollups sur Ethereum se heurtent au problème des coûts élevés des calldata, qui dépassent les autres frais. Bien qu'il existe des idées pour réduire drastiquement le coût des calldata, ce n'est pas encore fait et cela prendra du temps et un effort communautaire significatif de la part des développeurs et des équipes travaillant sur les rollups.

À l'heure actuelle, les calldata coûtent environ 16 gas par octet pour l'envoi vers Ethereum, ce qui constitue le principal obstacle à l'évolutivité des rollups Ethereum.

Les rollups Ethereum : Optimism, Arbitrum, Aztec, zkSync, StarkNet, etc.