LIGHTNING vs COVENANTS vs ROLLUPS: UNE GRILLE DE LECTURE

Introduction :

Depuis quelque temps, certains influenceurs ou membres de la communauté Bitcoin **réclament l'introduction urgente de nouvelles fonctionnalités** permettant de mettre en place des « **covenants** ». Pour le Bitcoineur moyen, il n'est pas toujours facile de s'y retrouver, d'autant plus que ce sont souvent des sociétés (avec leurs intérêts financiers) qui soutiennent ces propositions et que différents cas d'usages se cachent derrière. Voici quelques réflexions personnelles pour faire le point sur ces « covenants » et mieux comprendre l'état actuel des choses.

TL,DR : Pour les plus pressés, rendez-vous directement au tableau récapitulatif

Le problème.à résoudre : la scalabilité des transactions

On entend souvent dire que « Bitcoin est lent » et qu'il ne « scale » pas suffisamment, d'où la nécessité de recourir aux couches de type Layer2. En effet, **comment accueillir 8 milliards d'utilisateurs** si chacun veut réaliser plusieurs transactions on-chain chaque année, alors que l'espace dans les blocs est limité ? C'est précisément ce défi que les propositions de Layer2 cherchent à résoudre.

Lightning est déjà une excellente solution de seconde couche : elle est rapide, sécurisée, relativement mature, et permet de diminuer l'empreint sur la chaîne principale en déplaçant de nombreuses transactions off-chain. Cependant, l'ouverture et la fermeture de canaux Lightning exigent au moins deux transactions on-chain. Bien que cela fonctionne très bien actuellement (en période de faibles frais), la question se pose de savoir si ce modèle pourrait tenir l'épreuve de milliards d'utilisateurs. En pratique, rien n'est urgent pour le moment, car le nombre d'utilisateurs actifs de Bitcoin reste limité. Mais cela pose la question : pourquoi vouloir introduire si rapidement une nouvelle fonctionnalité sur Bitcoin ? Et surtout, comment être sûr que cela n'apportera pas des usages indésirables ou un impact négatif ? Bitcoin doit préserver sa décentralisation et sa sécurité : si l'on prend le risque d'y ajouter des changements profonds, mieux vaut avoir la certitude qu'ils soient indispensables et sans conséquences néfastes.

Les **covenants** forment une famille de propositions techniques visant à réaliser certains calculs directement sur la chaîne principale, afin de valider des transactions ou de gérer des règles plus complexes. L'idée centrale est d'exécuter un grand nombre d'opérations off-chain (sur une Layer2) et d'ancrer les preuves de validité de ces opérations sur la blockchain. Il existe plusieurs

approches techniques, dont les détails sont souvent complexes et encore en cours de recherche.

Les **rollups** : les rollups sont une catégorie spécifique de Layer2 (issue principalement des développements historiques sur Ethereum) permettant de traiter un grand nombre de transactions hors de la chaîne principale (plus économique et efficace) et d'y ancrer régulièrement des preuves condensées de validité.Les rollups fonctionnent généralement sur un état global unique partagé par tous les utilisateurs. Cette centralisation leur permet certaines optimisations mais pose également des défis spécifiques en termes de sécurité, de résistance à la censure et d'utilisation de l'espace des blocs. Pour implémenter les rollups sur Bitcoin, diverses propositions existent et font appel, ou non, au besoin que Bitcoin supporte une technologie de covenants.

Premier point intermédiaire dans cette discussion : tous les covenants ne sont pas nécessairement à destination d'un usage de rollups, et tous les rollups ne nécessitent pas tous – théoriquement - des covenants. Toutefois, il est important de préciser :

1. Tous les covenants ne sont pas égaux. Par exemple, certains covenants non récursifs pourraient être introduits via une softfork afin de faciliter des Layer2 comme Ark (proche de Lightning), en sacrifiant légèrement de la décentralisation pour réduire les contraintes de liquidité, sans pour autant ouvrir facilement la porte aux rollups plus centralisés
2. Par ailleurs, il est possible techniquement de faire des rollups aujourd'hui sur Bitcoin sans covenants (par exemple via BitVM), mais leur complexité et leur manque de compatibilité naturelle avec le modèle UTXO de Bitcoin les rendraient très consommateurs d'espace de bloc, notamment lorsqu'il faudrait challenger les séquenceurs via des « fraud proofs ».

Conférence de Charles Guillemet, CTO de @Ledger à Surfin Bitcoin 2024

Lors de cette conférence, Charles Guillemet a fait la promotion des **rollups** basés sur les covenants, tout en soulignant leur potentiel et leurs limites. Son intervention offre un bon aperçu de l'état actuel de ces projets et des dangers potentiels. Vous pouvez la consulter directement pour vous faire votre propre opinion:

Petit retour sur les détails croustillants qu'on y apprend…

Voici quelques points relevés lors de cette conférence faisant la promotion des « rollups » qui sont des layers2 qui iraient s'ancrer sur Bitcoin grâce aux covenants

- *Les rollups sont centralisés car il n'y a qu'un seul « état » du Layer2 qui doit être partagé*. Commentaire: c'est ce qui s'appelle le « single shared state ». En étant taquin on pourrait dire que, dans l'état actuel, ces rollups ne sont pas très scalables : ce sont des « **scale-up »**.. Il faut bien comprendre la différence avec Lightning ! Lightning est un système **« scale-out »** (on ajoute autant de nœuds que nécessaire, sans état global unique), tandis que les rollups relèvent plutôt d'un « scale-up » (il existe un état partagé unique, et le gain de capacité passe par l'agrégation et l'optimisation des transactions sur une même couche). Autrement dit, pour Lightning, lorsqu'on multiplie les noeuds et les canaux on répartit la charge, alors que pour les rollups, on concentre les opérations dans un même environnement (une seule "machine virtuelle" partagée) et on y applique des mécanismes de compression/batching afin d'augmenter le débit transactionnel. La **différence est fondamentale**.
- *L'ancrage sur chaine des rollups est indispensable et avec une certaine fréquence*. Commentaire: la ou un canal Lightning peut rester ouvert indéfiniment, les rollups vont venir

bouffer de l'espace de block en permanence. Il faudrait créer une métrique qui puisse **comparer l'espace de block** pris par utilisateur sur une vie entière pour comparer adéquatement ces technos. En effet si le rollup vient s'ancrer toutes les heures, les utilisateurs seront chacun indirectement « responsables » d'une infime empreinte x 24h x 365jrs x 70 ans.

- *Les types de Rollup appelés Optimistics Rollups requièrent de* ***supposer que l'autorité centrale est de confiance*** *! De plus l'utilisateur doit de son côté faire une « fraude proof » ce qui n'est pas simple, et en réalité peu implémentée sur les Optimistic Rollups sur Ethereum*. Commentaire: c'est marrant de critiquer le besoin de watchtower sur Lightning (efficace et simple) sans la comparer à la complexité de la Fraud Proof. De plus que penser du commentaire de pouvoir faire le « *roll back de l'état du Layer2* » ? C'est du grand n'importe quoi et ne semble pas distribué/décentralisé. Cela fait penser au « can dev do something » pour ceux qui ont la ref. Pour conclure sur le fait que les « *Optimistics Rollup ca ne marche pas vraiment notamment à cause du modele de sécurité, et que 90% des L2 sur ETH n'ont pas de fraude proof ; « le modèle est complètement trusted »*.
- *Les types de Rollup appelés Validity Rollups (techno ZK Rollups ,BitVM etc) reposent sur une autorité centrale qui doit générer et ancrer les preuves de validité (séquenceur centralisé). Sur Ethereum cela repose sur un « smart contract »*. Commentaire: le coût de génération de la preuve est très élevé (besoin de machines), ce qui exclu de facto la plèbe de ce genre d'activités. Le coût et les modalités de la vérification de la preuve (fraud proof) par l'utilisateur ne sont précisés.
- *Il y a le* ***problème de la résistance à la censure*** *: impossible sauf à décentraliser le séquenceur (quelqu'un sait comment?); ou bien à avoir un mécanisme de « force quit » mais sans en expliquer l'empreinte sur la chaine principale, ni les modalités comme la rapidité et les corner cases. (on suppose que personne ne sait pour l'instant!)*. Commentaire : il semble que le niveau de maturité de ce genre de solution, par rapport à ce que fait Bitcoin aujourd'hui, frise le ridicule. Ce ne semble pas mûr. Comment accepter une fonctionnalité de covenant sans qu'il y ait un système en production sur un testnet Bitcoin dédié, à l'échelle (c-a-d avec des milliers d'utilisateurs) et avec du recul (débuggage).
- *Les ZK rollup ne sont* ***pas confidentiels*** *car il y a besoin avoir les états du réseau pour pouvoir l'auditer*. Commentaire: de quoi faire sauter le bitcoineur moyen au plafond ?.
- *Il existe un risque économique des Layers2 de type Rollup pour les plèbes, car ils seront opérés par des grosses entreprises qui auront les moyen de payer l'espace de block on-chain dont ils ont besoin en permanence*. Commentaire: en gros avec les rollups, tel qu'envisagés aujourd'hui, les plèbes pourraient être priced-out pour leur transactions Bitcoin ! Et si ces Layer2 rollups ne sont pas là pour faire des transactions Bitcoin par millions, mais pour faire du Shitcoin sur Bitcoin, alors cela serait catastrophique. Une fois la boite de pandore du covenant+rollup ouverte comment prévenir les Shitcoin sur Bitcoins ? Cela sera impossible. Enfin le problème du risque économique impacte aussi indirectement la résistance à la censure: la petite transaction ne sera plus intéressante pour les mineurs.

Résumé synthétique : Lightning vs Rollups

	Lightning	Rollups basés sur Covenants
Scale out (on ajoute des noeuds et la scalabilité augmente)	Oui, chaque node étend d'autant le réseau, pas d'état à partager en permanence	Non, il y un « état du L2 » centralisé. C'est le « shared single state ».
Scalabité additionelle apportée à BTC L1 (gain final)	Enorme surtout si bcp de transactions Besoin d'un UTXO par utilisateur (mais auj pas un pb car les frais sont faibles)	Footprint sur la chaine par *user* /*lifetime* n'est pas calculée ! Ces L2 vont bouffer du block space en permanence (même si ils sont vides) donc on ne sait pas si meilleur que LN. Le block space addtl avec l'arrivée des shitcoin sur BTC personne ne l'a calculé non plus
Scalabilité sociale, (tout le monde peut il faire tourner ce layer)	Oui, tout le monde peut avoir son noeud. Pas de barrière économique. Cout de la watchtower faible	Non pour le séquenceur centraliser Optimistic rollup : coût de vérifier la preuve élevé ZK rollup : cout de la verification de la preuve par le pleb (fraud proof) pas précisé.
Décentralisé (resistance censure)	Très élévée	Problématique. Pour l'instant la décentralisation du sequenceur inexistante. Problème économique : si seules les L2 ont la puissance éco pour s'ancrer les pleb sont priced out donc possiblement censurés
Confidentialité	Très élévée	ZK rollup pas confidentiel car besoin avoir les états du reseau pour pouvoir l'auditer
Risque pour BTC	Dérisqué, bénefice net	Shitcoin sur Bitcoin ! perte de blockspace ! censure économique !

Conclusions

Notre principal point d'interrogation porte sur l'usage des covenants pour faire des rollups sur Bitcoin, plus que sur la technologie des covenants elle-même. Une nuance importante à apporter est qu'une softfork ciblée introduisant des covenants non récursifs pourrait permettre à des solutions telles que Ark d'être moins contraignantes, tout en évitant les dérives potentielles liées à des rollups centralisés. Le tableau précédent propose une grille d'analyse critique pour peser le bénéfice/risque de l'introduction des rollups basés sur les covenants, au regard des propositions actuelles.

Il est fort probable que l'on aura besoin d'une techno de type covenant un jour pour passer Bitcoin à une échelle supérieure. Mais il faudra bien comprendre les cas d'usages associés :

- Bitcoin only (c-a-d la monnaie), ou Shitcoin/RWA ? Ou autres besoins d'ancrage?
- Gain nets en scalabilité par rapport à LN
- Gain ou perte en scalabilité sociale
- Gain ou perte en décentralisation ?
- Gain ou perte en résistance à la censure ?
- Footprint on-chain ou bien un layer sur Lightning (c-a-d un Layer3)

Tant que ces questions ne trouveront pas de réponse satisfaisante, il semble prématuré de risquer la stabilité de Bitcoin pour une technologie encore incertaine. Mieux vaut développer et tester ces systèmes sur des environnements dédiés, tirer des enseignements concrets, et n'envisager ensuite d'intégrer des modifications au protocole qu'avec une extrême prudence.

Si notre hypothèse que Bitcoin n'est pas simplement un réseau monétaire, mais plutôt un réseau de confiance (de preuves) dont la monnaie n'est que la première application, alors il faudra trouver un moyen de préserver l'intégrité du cas d'usage de la monnaie. C-est-à-dire qu'introduire les covenants doit être un net positif pour la monnaie sans perdre en décentralisation, accessibilité et sécurité. Seulement ensuite les autres types d'ancrage seront dé-risqués et l'on en verra de nombreux types: identité (?), preuves, RWA, shitcoins etc.

Avril 2025

Merci @Pantamis pour la relecture.