MEMBRES DU GROUPE :

- BARRO TIOMOKO
- DERA MAMOUNATA
- SANOGO MOUNIR S.

THEME DE PRESENTATION : BITCOIN TAPROOT

SOMMAIRE

Introduction

L'un des plus grands mythes du Bitcoin est qu'il s'agit d'une « vieille technologie » qui ne change jamais. Ce n'est évidemment pas vrai et l'un des exemples les plus récents de ces changements constants est l'énorme soft fork Bitcoin Taproot. Il faut des années pour planifier, construire et exécuter, c'est quelque chose dont tous les investisseurs devraient être conscients étant donné les impacts à long terme que cela aura sur le réseau. En effet, Taproot est une technologie qui vise à améliorer la confidentialité et la capacité de Bitcoin à créer des contrats intelligents complexes. Ceci afin d'améliorer ses bénéfices et de contribuer à l'évolution de son écosystème en pleine croissance. Sa fonction est de chercher à améliorer la confidentialité et la mise en œuvre de Scripts Bitcoin, éliminant le besoin de révéler des informations importantes ou des données contenues dans des scripts complets. Par conséquent, il n'affiche que la condition activée au moment de la transaction.

I- La mise à niveau de la racine pivotante

La mise à niveau Taproot est un projet d'amélioration du Bitcoin (BTC) avec un nouveau schéma de signature connu sous le nom de Schnorr. Cet ajustement du protocole ouvre de nouvelles possibilités en matière de confidentialité, de portefeuilles multi signatures et de sécurité. Taproot est largement considérée comme l'une des améliorations les plus importantes du protocole Bitcoin. La mise à niveau a été activée lorsque la chaîne a atteint le bloc 709 632 à 6h15 le dimanche 14 novembre. Cela a définitivement activé la première mise à niveau majeure du BTC depuis l'introduction du Segregated Witness (SegWit) en 2017. Taproot est une fusion de diverses innovations techniques de l'histoire du Bitcoin en une seule mise à niveau. Elle a été proposée pour la première fois par Greg Maxwell en 2018. Depuis lors, les 3 propositions d'amélioration de Bitcoin (BIP) qui ont été rédigées par Pieter Wuille, Tim Ruffing, A.J. Townes et Jonas Nick

Précédemment, Bitcoin utilisait l'algorithme de signature ECDSA où un utilisateur signe une transaction avec sa clé privée afin d'approuver l'opération.

Taproot passe à un protocole de signature différent baptisé « Schnorr ». Chaque transaction utilisera désormais ce nouveau schema de signature.

- BIP340

Introduit l'algorithme de signature de Schnorr (SSA), un schéma cryptographique qui rend les transactions complexes en bitcoins plus simples et plus sûres.

Voici un exemple de ce que le SSA apportera :

Si 10 utilisateurs différents envoyaient des BTC à une seule adresse de portefeuille (clé publique) dans le cadre de la configuration actuelle, cela apparaîtrait sur le registre de bitcoin comme 10 transactions distinctes. Mais en utilisant le SSA, le réseau bitcoin sera capable de regrouper ces 10 transactions en une seule transaction avec une clé unique.

- BIP341

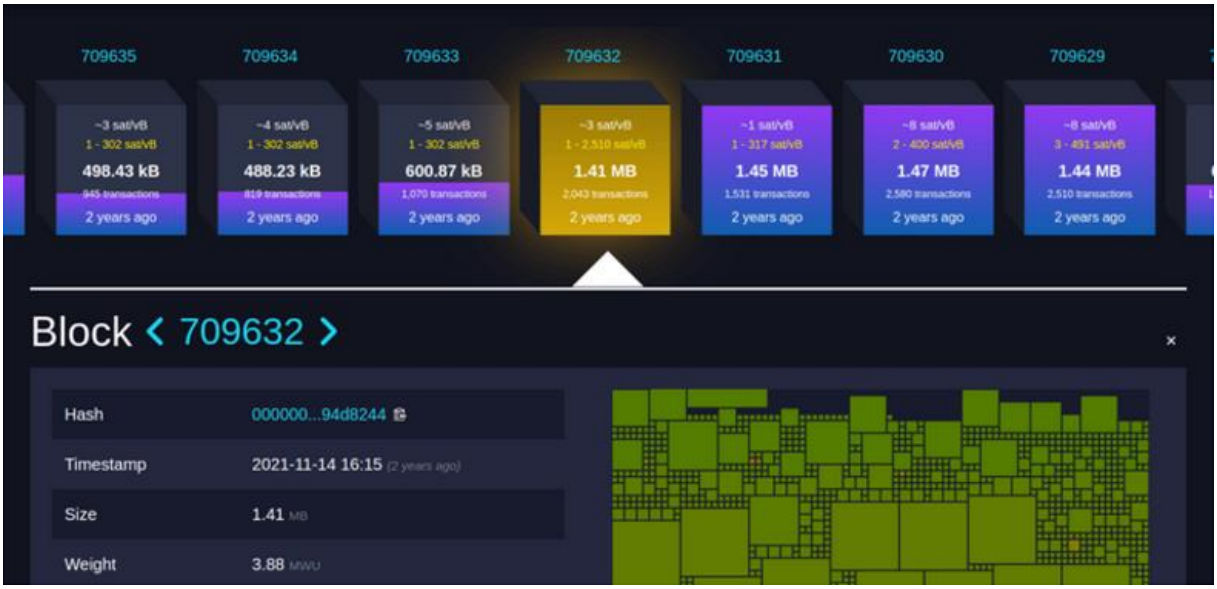
Il s'appuie sur la mise à niveau SegWit de 2017 et améliore la confidentialité des bitcoins tout en réduisant les frais de transaction. Elle introduit également MAST, qui permet aux utilisateurs de verrouiller les sorties à plusieurs scripts.

Dans le cadre de MAST, les conditions complexes requises pour les transactions seront compressées en une seule ligne de données, réduisant ainsi la quantité de données à stocker et à transférer sur la Blockchain. L'efficacité s'en trouvera renforcée.

- BIP342

Réforme le langage de script de bitcoin en introduisant un langage de script différent appelé "Tapscript" qui modifie la façon dont les signatures sont évaluées.

Les changements apportés par Taproot sont importants car les transactions et les conditions de leur exécution sont stockées dans la Blockchain.



II- Les avantages de Taproot

Comme Déjà évoqué, Taproot a apporté des améliorations majeures à la vie privée du Bitcoin et a amélioré ses cas d'utilisation. Il a d'autres avantages potentiels qui sont :

- L'amélioration de la scalabilité du réseau en réduisant la quantité de données à transférer et à stocker sur la Blockchain, l'augmentation du nombre de transactions par bloc (taux TPS plus élevé) et la réduction des frais de transaction.
- Un autre avantage de Taproot est le fait que les signatures ne seront plus malléables, ce qui est un risque de sécurité connu dans le réseau Bitcoin. En termes simples, la malléabilité des signatures signifie qu'il est techniquement possible de modifier la signature d'une transaction avant qu'elle ne soit confirmée. En faisant cela, l'attaque s'affichera comme si la transaction n'avait jamais eu lieu. Cela expose le Bitcoin au triste célèbre problème de double dépense, qui pourrait ruiner l'intégrité du registre distribué.
- La réduction du coût des transactions, grâce à la mise à jour Taproot, les frais seront réduits pour les transactions complexes. À l'heure actuelle, le réseau Bitcoin est capable de traiter environ quatre à cinq transactions par seconde. Les frais de transaction peuvent dépasser les 75 dollars. Cette mise à jour va aussi améliorer la capacité du Bitcoin pour le Scripting. Ainsi, le BTC pourra enfin rivaliser avec d'autres Blockchains comme l'Ethereum sur ce terrain. Cette cryptomonnaie dispose déjà des « smart contracts » programmables. La précédente mise à jour majeure du Bitcoin remonte au mois de juillet 2017. Il s'agissait de l'introduction du Segregated Witness (SegWit), qui a permis de régler les problèmes d'extensibilité.

Cette nouvelle amélioration pourrait rendre le Bitcoin plus compétitif, et faire grimper sa valeur.

III- Comment Taproot affecte-t-il le bitcoin ?

Comme mentionné, Taproot était une mise à niveau majeure de l'ensemble du réseau Bitcoin. Il a introduit un nouveau type d'adresse, rendu les transactions plus efficaces, plus petites, plus rapides à traiter et amélioré la confidentialité et la sécurité. Cela a également eu pour impact majeur de rendre les contrats intelligents Bitcoin beaucoup plus utilisables grâce à la capacité des signatures Schnorr à regrouper plusieurs signatures en une seule.

Cela a mieux positionné Bitcoin dans le monde de la finance décentralisée (DeFi) et a également permis des mises à niveau de script plus faciles à l'avenir. Taproot a également permis d'autres améliorations importantes du réseau Lightning et a rendu possible le protocole Taro.

IV- Comment la mise à niveau Taproot aide-t-elle les mineurs de bitcoin ?

La plupart des mineurs de Bitcoin se concentrent principalement sur leur retour sur investissement ou ROI. L'essentiel est de savoir combien de transactions peuvent tenir dans chaque bloc, car plus il y a de transactions dans chaque bloc, plus elles doivent percevoir de frais. Comme Taproot réduit la taille en kilo-octets des transactions P2TR, cela signifie qu'un plus grand nombre d'entre elles peuvent tenir dans un bloc de même taille. Plus de transactions signifie plus de frais, ce qui signifie plus d'argent pour les mineurs. Comme Taproot améliore considérablement la convivialité des contrats intelligents Bitcoin et d'autres transactions plus complexes, cela encourage davantage de transactions de ce type et donc des frais plus élevés. Dans l'ensemble, Taproot a été une mise à niveau très positive pour les mineurs, c'est pourquoi la mise à niveau a bénéficié d'un soutien si large et unanime.

Conclusion

Taproot promet une amélioration conséquente de la Blockchain Bitcoin en introduisant des procédés indispensables à la mise à l'échelle du réseau. Ce soft fork de Bitcoin apporte deux grandes innovations techniques : L'introduction des signatures Schnorr et l'implémentation du MAST. Les bénéfices de ces nouveautés s'annoncent immenses et doivent permettre d'offrir plus de sécurité, de confidentialité et de scalabilité à Bitcoin. La mise à jour Taproot constitue une étape indispensable sans laquelle de nombreuses évolutions futures du protocole ne sauraient avoir lieu.