Nervos Network - Prise de position

1. Objectif de ce document

Le réseau Nervos est composé de plusieurs protocoles et innovations. Il est important d'avoir une documentation claire et des spécifications techniques sur la conception et la mise en œuvre clés du protocole - pour lesquelles nous utilisons un processus de RFC (Request For Comment ou demande de commentaire en Français). Cependant, nous estimons qu'il est tout aussi important d'aider nos communautés à comprendre ce que nous essayons d'accomplir, les compromis que nous avons faits et comment nous sommes parvenus à nos décisions de conception actuelles.

Nous commençons ce document par un examen détaillé des problèmes auxquels sont confrontées les blockchains publiques sans permission aujourd'hui ainsi que des solutions existantes qui tentent de les résoudre. Nous espérons que cela fournira le contexte nécessaire à nos lecteurs pour comprendre notre propre raisonnement sur la meilleure façon d'aborder ces défis et nos décisions de conception sous-jacentes. Nous fournissons ensuite une description générale de toutes les parties du réseau Nervos, en mettant l'accent sur la façon dont elles fonctionnent ensemble pour soutenir la vision globale du réseau.

2. Contexte

La scalabilité, la durabilité et l'interopérabilité figurent parmi les plus grands défis auxquels sont confrontées les blockchains publiques sans permission aujourd'hui. Bien que de nombreux projets prétendent avoir des solutions à ces problèmes, il est important de comprendre d'où viennent ces problèmes et de mettre les solutions dans le contexte des compromis possibles.

2.1 Scalabilité

Bitcoin[1] a été la première blockchain publique sans permission, conçue pour être utilisée comme une monnaie électronique pair-à-pair. Ethereum[2] a créé plus de cas d'utilisation possibles et a créé une plate-forme de calcul décentralisée à usage général. Cependant, ces deux plateformes imposent des limites à leurs capacités de transaction - Bitcoin limite la taille de ses blocs et Ethereum limite son plafond de gaz de bloc. Ce sont des étapes nécessaires pour assurer la décentralisation à long terme, mais elles limitent également les capacités des deux plateformes.

La communauté de la blockchain a proposé de nombreuses solutions de scalabilité ces dernières années. En général, nous pouvons diviser ces solutions en deux catégories: la scalabilité on-chain (sur la chaîne) et la scalabilité off-chain (hors de la chaîne).

Les solutions de scalabilité on-chain visent à étendre le débit du processus de consensus et à créer des blockchains avec une capacité native qui rivalise avec les systèmes centralisés. Les solutions de scalabilité off-chain n'utilisent que la blockchain comme plateforme d'actifs et de règlement sécurisé, tout en déplaçant presque toutes les transactions vers des couches supérieures.

2.1.1 Scalabilité on-chain avec une seule blockchain

Le moyen le plus simple d'augmenter le débit d'une blockchain est d'augmenter son offre d'espace de blocs. Avec plus d'espace de blocs, plus de transactions peuvent circuler à travers le réseau et être traitées. L'augmentation de l'offre d'espace de blocs en réponse à une demande de transactions accrue permet également aux frais de transaction de rester bas.

Bitcoin Cash (BCH) adopte cette approche pour mettre à l'échelle son réseau de paiement pair-à-pair. Le protocole Bitcoin Cash a commencé avec une taille de bloc maximale de 8 MB, qui a été augmentée ultérieurement à 32 MB, et qui continuera à être augmentée indéfiniment à mesure que la demande de transactions augmente. Pour référence, après la mise en œuvre de Segregated Witness de Bitcoin en août 2017, le protocole Bitcoin permet maintenant une taille de bloc moyenne d'environ 2 MB.

Dans le cadre d'un centre de données, les maths fonctionnent. Si 7.5 milliards de personnes créent chacune 2 transactions on-chain par jour, le réseau aura besoin de la production de blocs de 26 GB toutes les 10 minutes, entraînant un taux de croissance de la blockchain de 3.75 TB par jour ou 1.37 PB par an[3]. Ces exigences de stockage et de bande passante sont raisonnables pour tout service cloud aujourd'hui.

Cependant, la limitation de l'opération des nœuds à un environnement de centre de données conduit à une seule topologie de réseau viable et force des compromis en matière de sécurité (le taux de fork de la blockchain augmentera à mesure que les exigences de transmission de données à travers le réseau augmenteront), ainsi qu'en matière de décentralisation (le nombre de noeuds complets sera réduit à mesure que le coût de la participation au consensus augmente).

Du point de vue économique, une taille de bloc en constante augmentation allège la pression des frais ressentie par les utilisateurs. L'analyse du réseau Bitcoin a montré que les frais restent stables jusqu'à ce qu'un bloc soit rempli à environ 80 %, puis augmentent de manière exponentielle[4].

Bien que le fait de faire reposer le coût de croissance d'un réseau sur ses opérateurs puisse sembler être une décision raisonnable, cela pourrait être à court terme pour deux raisons :

- La suppression des frais de transaction force les mineurs à se fier principalement à la compensation de la nouvelle émission de pièces (récompenses de bloc). À moins que l'inflation ne soit une partie permanente du protocole, la nouvelle émission de pièces s'arrêtera finalement (lorsque le plafond du total des pièces sera atteint), et les mineurs ne recevront ni récompenses de bloc ni frais de transaction significatifs. L'impact économique de cela compromet gravement le modèle de sécurité du réseau.

- Le coût d'exécution d'un nœud complet devient prohibitif. Cela supprime la capacité des utilisateurs réguliers à vérifier indépendamment l'historique et les transactions d'une blockchain, obligeant à s'appuyer sur des prestataires de services tels que les échanges et les processeurs de paiement pour garantir l'intégrité de la blockchain. Cette exigence de confiance annule la proposition de valeur fondamentale des blockchains publiques sans permission en tant que systèmes distribués sans confiance entre pairs.

Les plates-formes d'optimisation des coûts de transaction telles que Bitcoin Cash sont confrontées à une concurrence importante d'autres blockchains (avec et sans permissions), ainsi que de systèmes de paiement traditionnels. Les décisions de conception qui améliorent la sécurité ou la résistance à la censure entraîneront des coûts associés et augmenteront à leur tour le coût d'utilisation de la plate-forme. En tenant compte de la concurrence, ainsi que des objectifs déclarés du réseau, il est probable que des coûts plus bas seront l'objectif principal du réseau, au détriment de toute autre considération.

Cet objectif est cohérent avec nos observations sur l'utilisation des réseaux transactionnels. Les utilisateurs de ces systèmes sont indifférents aux compromis significatifs à long terme car ils n'utiliseront le réseau que pendant une courte période. Une fois que leurs biens ou services ont été reçus et que leur paiement a été réglé, ces utilisateurs n'ont plus aucune préoccupation pour le fonctionnement efficace du réseau. L'acceptation de ces compromis est apparente dans l'utilisation répandue des échanges de crypto-actifs centralisés, ainsi que de blockchains plus centralisées. Ces systèmes sont populaires principalement pour leur commodité et leur efficacité transactionnelle.

Certaines plates-formes de contrats intelligents ont adopté des approches similaires pour augmenter le débit de la blockchain, en ne permettant qu'à un ensemble limité de validateurs de « super ordinateurs » de participer au processus de consensus et de valider indépendamment la blockchain.

Bien que les compromis en matière de décentralisation et de sécurité du réseau permettent des transactions moins chères et puissent être pratiques pour un ensemble d'utilisateurs, le modèle de sécurité à long terme compromis, la barrière de coût pour vérifier indépendamment les transactions et la concentration et l'enracinement probables des opérateurs de nœuds nous amènent à penser que ce n'est pas une approche appropriée pour mettre à l'échelle les blockchains publiques.

2.1.2 Scalabilité on-chain avec plusieurs chaînes

La scalabilité on-chain avec plusieurs chaînes peut être réalisée via le “sharding” (partitionnement), comme on le voit sur Ethereum 2.0, ou les chaînes d'application, comme on le voit sur Polkadot. Ces conceptions divisent efficacement l'état et les transactions globaux du réseau en plusieurs blockchains, permettant à chaque blockchain d'atteindre rapidement un consensus local, puis à l'ensemble du réseau d'atteindre un consensus global via le consensus de la "Beacon Chain" ou de la "Relay Chain".

Ces conceptions permettent à plusieurs chaînes d'utiliser un modèle de sécurité partagé, tout en permettant un débit élevé et des transactions rapides à l'intérieur des shards (Ethereum) ou des para-chains (Polkadot). Bien que chacun de ces systèmes soit un réseau

de blockchains interconnectées, ils diffèrent en ce qui concerne les protocoles fonctionnant sur chaque chaîne. Dans Ethereum 2.0, chaque shard exécute le même protocole, tandis que dans Polkadot, chaque para-chain peut exécuter un protocole personnalisé, créé via le framework Substrate.

Dans ces architectures multi-chaînes, chaque dApp (application décentralisée ou instance d'un dApp) ne réside que sur une seule chaîne. Bien que les développeurs d'aujourd'hui soient habitués à la capacité de construire des dApps qui interagissent parfaitement avec n'importe quel autre dApp sur la blockchain, les modèles de conception devront s'adapter aux nouvelles architectures multi-chaînes. Si une application décentralisée est divisée entre différents shards, des mécanismes seront nécessaires pour maintenir l'état synchronisé entre différentes instances du dApp (résidant sur différents shards). De plus, bien que les mécanismes de couche de niveau 2 puissent être déployés pour une communication inter-shard rapide, les transactions inter-shard nécessiteront un consensus global et introduiront une latence de confirmation.

Avec ces transactions asynchrones, le fameux problème du “train et de l'hôtel” se pose. Lorsque deux transactions doivent être atomiques (par exemple, la réservation d'un billet de train et d'une chambre d'hôtel sur deux shards différents), de nouvelles solutions sont nécessaires. Ethereum introduit le "yanking" de contrat, dans lequel un contrat dépendant est supprimé sur un shard, créé sur un deuxième shard (qui contient l'autre contrat dépendant), et les deux transactions sont ensuite exécutées sur le deuxième shard. Cependant, le contrat “yanked” ne serait alors plus disponible sur le shard d'origine, introduisant des problèmes d'utilisabilité et nécessitant à nouveau de nouveaux modèles de conception.

Le sharding a ses propres avantages et défis. Si les shards peuvent être vraiment indépendants et que les besoins de cross-shard sont minimes, une blockchain peut augmenter linéairement son débit en augmentant le nombre de shards. Cela convient le mieux aux applications autonomes qui ne nécessitent pas d'état extérieur ou de collaboration avec d'autres applications.

Une architecture utilisant les shards peut poser des problèmes pour les applications développées en composant des applications "bloc de construction" les unes avec les autres (c'est ce qu'on appelle le "problème de la compositionnalité"). La compositionnalité est particulièrement pertinente dans la finance décentralisée (DeFi), où les produits les plus avancés ont tendance à être construits sur d'autres produits de blocs de construction.

Sur une note plus technique, le sharding nécessite généralement une topologie "1 + N", dans laquelle N blockchains se connectent à une méta chaîne, introduisant une limite supérieure au nombre de shards qu'une méta chaîne peut prendre en charge sans rencontrer elle-même des problèmes de scalabilité.

Nous observons une valeur significative dans un état global unifié, permettant l'émergence d'un écosystème d'applications interdépendantes et aux développeurs d'innover sur les bords, de manière similaire à l'utilisation par les développeurs Web de bibliothèques pour les préoccupations de bas niveau et d'API ouvertes pour l'intégration de services. Une expérience de développement beaucoup plus simple est activée lorsque les développeurs n'ont pas à considérer la synchronicité (dans le transfert d'actifs cross-shard ou le passage

de messages), ainsi qu'une expérience utilisateur supérieure, résultant de la cohérence dans les préoccupations architecturales des interactions de blockchain.

Nous reconnaissons que le sharding est une solution de scalabilité prometteuse (en particulier pour les applications moins interdépendantes), mais nous pensons qu'il est bénéfique d'avoir une conception qui concentre l'état le plus précieux sur une seule blockchain, permettant la compositionnalité. Avec cette conception, des approches de mise à l'échelle off-chain sont utilisées pour permettre un débit plus élevé.

2.1.3 Scalabilité off-chain grâce à la couche de niveau 2

Dans les protocoles de couche de niveau 2, la blockchain de base agit comme une couche d’accord (ou d'engagement), tandis que la deuxième couche achemine des preuves cryptographiques qui permettent aux participants de "prendre livraison" de la crypto-monnaie. Toutes les activités de la deuxième couche sont cryptographiquement sécurisées par la blockchain sous-jacente et la couche de base n'est utilisée que pour régler les montants entrant/sortant du réseau de deuxième couche, ainsi que pour la résolution des litiges. Ces conceptions fonctionnent sans délégation de garde (ou risque de perte) de fonds et permettent des transactions instantanées et presque gratuites.

Ces technologies montrent comment un réseau de réserve de valeur tel que Bitcoin pourrait être utilisé pour des paiements quotidiens. L'exemple le plus typique d'une solution de couche de niveau 2 en pratique est un canal de paiement entre un client et un café. Supposons qu'Alice visite le café Bitcoin chaque matin. Au début du mois, elle dépose des fonds dans un canal de paiement Lightning qu'elle a ouvert avec le café. À chaque visite, elle signe cryptographiquement le droit du café à prendre une partie des fonds, en échange de son café. Ces transactions se produisent instantanément et sont complètement pair-à-pair, off-chain, permettant une expérience client fluide. Le canal Lightning est sans confiance, Alice ou le café peuvent fermer le canal à tout moment, en prenant les fonds qui leur sont dus à ce moment-là.

Les technologies de canal de paiement telles que Lightning ne sont qu'un exemple d'une technique de scalabilité off-chain ; il existe de nombreuses technologies matures qui peuvent augmenter en toute sécurité le débit de la blockchain de cette manière. Bien que les canaux de paiement incluent des accords off-chain pour les soldes de canal entre deux parties, les canaux d'état incluent des accords off-chain pour un état arbitraire entre les participants du canal. Cette généralisation peut être la base d'applications décentralisées, évolutives et sans confiance. Un seul canal d'état peut même être utilisé par plusieurs applications, permettant une efficacité encore plus grande. Lorsqu'une partie est prête à sortir du canal, elle peut soumettre la preuve cryptographique convenue à la blockchain, qui exécutera ensuite les transitions d'état convenues.

Une side-chain est une autre construction qui permet d'augmenter le débit, mais via des opérateurs de blockchain tiers de confiance. Avec une liaison bidirectionnelle vers une blockchain avec un consensus fiable et sans confiance, les fonds peuvent être déplacés d'avant en arrière entre la chaîne principale et la side-chain. Cela permet un grand volume de transactions de confiance sur la side-chain, avec un règlement net ultérieur sur la chaîne principale. Les transactions de side-chain ont des frais minimaux, une confirmation rapide et

un débit élevé. Bien que les side-chains offrent une expérience supérieure à bien des égards, elles compromettent la sécurité. Cependant, il existe de nombreuses recherches sur les side-chains sans confiance, qui peuvent offrir les mêmes améliorations de performance sans compromettre la sécurité.

Un exemple de technologie de side-chain sans confiance est Plasma (abordé en 5.4), une architecture de side-chain qui utilise une racine de confiance sur une blockchain avec un consensus mondial plus large. Les chaînes Plasma offrent les mêmes améliorations de performances que les side-chains centralisées, mais offrent des garanties de sécurité. En cas de comportement malveillant ou défaillant d'un opérateur de chaîne Plasma, les utilisateurs disposent d'un mécanisme qui leur permet de retirer en toute sécurité leurs actifs de side-chain vers la chaîne principale. Cela se fait sans la coopération de l'opérateur de la chaîne Plasma, offrant aux utilisateurs la commodité des transactions de side-chain, ainsi que la sécurité d'une blockchain de couche 1.

La mise à l'échelle off-chain permet la décentralisation, la sécurité et la scalabilité. En déplaçant tout sauf les transactions de règlement et les litiges off-chain, le consensus mondial limité d'une blockchain publique est utilisé de manière efficace. Des protocoles de couche de niveau 2 divers peuvent être mis en œuvre en fonction des exigences de l'application, offrant une flexibilité aux développeurs et aux utilisateurs. À mesure que de plus en plus de participants rejoignent le réseau, les performances ne sont pas impactées et toutes les parties peuvent partager les garanties de sécurité offertes par le consensus de la couche de niveau 1.

2.2 Durabilité

Assurer le fonctionnement à long terme d'une blockchain publique autonome et sans propriétaire présente un défi considérable. Les incitations doivent être équilibrées entre les parties prenantes diverses et le système doit être conçu de manière à permettre une opération complète des nœuds et une vérifiabilité publique étendue. Les exigences matérielles doivent rester raisonnables tout en soutenant un réseau ouvert et mondial.

De plus, une fois qu'une blockchain publique est en opération, il est très difficile de modifier les règles sous-jacentes qui régissent le protocole. Dès le départ, le système doit être conçu pour être durable. Dans cet intérêt, nous avons effectué un inventaire complet des défis liés à la construction de blockchains publiques et sans permission durables.

2.2.1 Décentralisation

L'un des plus grands défis à long terme auxquels les blockchains publiques font face est une barrière croissante à la participation indépendante et à la vérification des transactions, reflétée dans le coût de l'opération d'un nœud complet. Les nœuds complets permettent aux participants de la blockchain de vérifier indépendamment l'état / l'historique on-chain et de tenir les mineurs ou les validateurs du réseau responsables en refusant de router les blocs invalides. À mesure que le coût des nœuds complets augmente et que leur nombre diminue, les participants au réseau sont de plus en plus obligés de s'appuyer sur des opérateurs de services professionnels pour fournir à la fois l'historique et l'état actuel, érodant le modèle de confiance fondamental des blockchains ouvertes et sans permission.

Pour qu'un nœud complet suive la progression de la blockchain, il doit avoir une capacité de calcul adéquate pour valider les transactions, une capacité de bande passante pour recevoir les transactions et une capacité de stockage pour stocker l'état global entier. Pour contrôler le coût d'exploitation d'un nœud complet, le protocole doit prendre des mesures pour limiter la croissance de la capacité de toutes ces trois ressources. La plupart des protocoles de blockchain limitent leur débit de calcul ou de bande passante, mais très peu limitent la croissance de l'état global. À mesure que ces chaînes augmentent en taille et en durée d'exploitation, les coûts d'exploitation des nœuds complets augmenteront de manière irréversible.

2.2.2 Modèles économiques

Bien qu'il y ait eu beaucoup de recherches sur les protocoles de consensus ces dernières années, nous pensons que l'économie de la cryptographie est un domaine sous-étudié. En général, les modèles économiques actuels pour les protocoles de couche de niveau 1 se concentrent principalement sur les mesures incitatives et les sanctions pour assurer le consensus du réseau, et les jetons natifs sont principalement utilisés pour payer les frais de transaction ou pour satisfaire les exigences de “staking” qui fournissent une résistance Sybil.

Nous pensons qu'un modèle économique bien conçu doit aller au-delà du processus de consensus et garantir la durabilité à long terme du protocole également. En particulier, le modèle économique devrait être conçu avec les objectifs suivants:

- Le réseau doit avoir un moyen durable de compenser les fournisseurs de services (typiquement les mineurs ou les validateurs), assurant que le réseau reste durablement sécurisé
- Le réseau doit avoir un moyen durable de maintenir une faible barrière à la participation, assurant que le réseau reste décentralisé dans le temps
- Les ressources du réseau public doivent être allouées efficacement et équitablement
- Le jeton natif de la blockchain doit avoir une valeur intrinsèque

2.2.3 Analyse du modèle économique de Bitcoin

Le protocole Bitcoin limite la taille des blocs et impose un temps de bloc fixe. Cela rend la bande passante du réseau, un bien rare que les utilisateurs doivent payer via des frais de transaction. Le langage de script de Bitcoin n'autorise pas les boucles, ce qui rend la longueur du script une bonne approximation de sa complexité de calcul. En général, une demande accrue d'espace de bloc se traduit par des frais de transaction plus élevés pour les utilisateurs. De plus, plus il y a d'entrées, de sorties ou d'étapes de calcul impliquées dans une transaction, plus un utilisateur devra payer de frais de transaction.

La valeur intrinsèque de Bitcoin provient presque entièrement de sa prime monétaire (la volonté de la société de le considérer comme de l'argent) et en particulier, la volonté de le conserver comme réserve de valeur. Comme le revenu des mineurs est libellé en BTC, cette perception doit être maintenue pour que le modèle économique de Bitcoin soit durable. En d'autres termes, le modèle de sécurité de Bitcoin est circulaire - il dépend de la croyance collective selon laquelle le réseau est durablement sécurisé et peut donc être utilisé comme réserve de valeur monétaire.

Le plafond de la taille des blocs de Bitcoin fixe effectivement la barrière à la participation au réseau - plus le plafond de la taille des blocs est bas, plus il est facile pour les non-professionnels de faire fonctionner des nœuds complets. L'état global de Bitcoin est son ensemble de sorties non dépensées (UTXO), dont le taux de croissance est également effectivement limité par la limite de la taille des blocs. Les utilisateurs sont incités à créer et à utiliser des UTXO de manière efficace ; créer plus d'UTXO se traduit par des frais de transaction plus élevés. Cependant, aucune incitation n'est fournie pour encourager la combinaison des UTXO et la réduction de la taille de l'état global ; une fois qu'un UTXO est créé, il occupera l'état global gratuitement jusqu'à ce qu'il soit dépensé.

Le modèle économique de Bitcoin basé sur les frais de transaction est un modèle équitable pour allouer la bande passante du réseau, une ressource rare imposée par le protocole. C'est un modèle économique approprié pour un système de paiement pair-à-pair, mais un choix médiocre pour une plate-forme de réserve de valeur véritable. Les utilisateurs de Bitcoin qui utilisent la blockchain pour stocker de la valeur ne paient des frais de transaction qu'une seule fois, mais peuvent ensuite occuper l'état pour toujours, bénéficiant d'une sécurité continue fournie par les mineurs, qui sont tenus de faire des investissements continus en ressources.

Bitcoin a une limite d'approvisionnement totale et sa nouvelle émission via des récompenses de bloc finira par tomber à zéro. Cela pourrait poser deux problèmes :

Premièrement, si Bitcoin continue de réussir en tant que réserve de valeur, la valeur unitaire du BTC continuera d'augmenter, et la valeur totale que le réseau sécurise augmentera également (à mesure que plus de valeur monétaire passe sur le réseau). Une plate-forme de réserve de valeur doit être capable d'augmenter son budget de sécurité à mesure que la valeur qu'elle protège augmente au fil du temps, sinon, elle invite les attaquants à doubler les dépenses et à voler les actifs du réseau.

Lorsque le coût pour briser la sécurité du protocole est inférieur au bénéfice qu'ils peuvent gagner en agissant honnêtement, les attaquants attaqueront toujours. Cela est analogue à une ville qui doit augmenter ses dépenses militaires à mesure que la richesse à l'intérieur de la ville augmente. Sans cet investissement, tôt ou tard, la ville sera attaquée et pillée.

Avec l'existence des récompenses de bloc, Bitcoin est capable de mettre à l'échelle la sécurité à la valeur agrégée qu'il stocke - si le prix de Bitcoin double, le revenu que les mineurs reçoivent des récompenses de bloc doublera également, ils peuvent donc se permettre de produire deux fois le taux de hachage, rendant le réseau deux fois plus cher à attaquer.

Cependant, cela change lorsque les récompenses de bloc prévisibles tombent à zéro. Les mineurs devront compter entièrement sur les frais de transaction ; leur revenu ne sera plus lié à la valeur de l'actif Bitcoin, mais sera déterminé par la demande de transaction du réseau. Si la demande de transaction n'est pas assez élevée pour remplir l'espace de bloc disponible, les frais de transaction totaux seront minuscules. Étant donné que les frais de transaction sont strictement une fonction de la demande d'espace de bloc et indépendants du prix d'un Bitcoin, cela aura un impact profond sur le modèle de sécurité de Bitcoin. Pour que Bitcoin reste sécurisé, il faudrait supposer une demande de transaction constante et en

surcapacité, qui évolue également avec le prix du Bitcoin. Ce sont des hypothèses très fortes.

Deuxièmement, lorsque les récompenses de bloc prévisibles s'arrêtent, la variance des revenus par bloc pour les mineurs augmente et fournit des incitations aux mineurs à “forker”, au lieu d'avancer la blockchain. Dans le cas extrême, lorsque le mempool d'un mineur est vide et qu'il reçoit un bloc chargé de frais, son incitation est de “forker” la blockchain et de voler les frais, au lieu d'avancer la blockchain et de produire un bloc avec potentiellement aucun revenu[5]. Cela est connu sous le nom de défi de "fee sniping" dans la communauté Bitcoin, pour lequel aucune solution satisfaisante n'a encore été trouvée, sans enlever le plafond absolu de Bitcoin.

2.2.4 Analyse du modèle économique des plateformes de contrats intelligents

Le modèle économique typique des plateformes de contrats intelligents est confronté à encore plus de défis. Prenons Ethereum comme exemple. Le script Ethereum permet des boucles, donc la longueur d'un script ne reflète pas la complexité de calcul du script. C'est la raison pour laquelle Ethereum ne limite pas la taille des blocs ou le débit de bande passante, mais le débit de calcul (exprimé dans la limite de gaz de bloc).

Pour que leurs transactions soient enregistrées sur la blockchain Ethereum, les utilisateurs enchérissent sur le coût par calcul qu'ils sont prêts à payer en frais de transaction. Ethereum utilise le concept de "gaz" comme mesure du coût de calcul tarifé en ETH, et le contrôle des tarifs "prix du gaz" garantit que le coût par étape de calcul est indépendant des mouvements de prix du jeton natif. La valeur intrinsèque du jeton ETH provient de sa position en tant que jeton de paiement de la plate-forme de calcul décentralisée ; c'est la seule devise qui peut être utilisée pour payer le calcul sur Ethereum.

L'état global d'Ethereum est représenté avec le trie d'état de l'EVM, la structure de données qui contient les soldes et l'état interne de tous les comptes. Lorsque de nouveaux comptes ou valeurs de contrat sont créés, la taille de l'état global se dilate. Ethereum facture des montants fixes de gaz pour l'insertion de nouvelles valeurs dans son stockage d'état et offre une "allocation de gaz" fixe qui compense les coûts de gaz d'une transaction lorsque les valeurs sont supprimées.

Un modèle de stockage "payer une fois, occuper pour toujours" ne correspond pas à la structure de coûts permanents des mineurs et des nœuds complets, et le modèle ne fournit aucune incitation pour les utilisateurs de supprimer volontairement l'état ou de supprimer l'état plus tôt. Par conséquent, Ethereum a connu une croissance rapide de sa taille d'état. Une taille d'état plus grande ralentit le traitement des transactions et augmente le coût d'exploitation des nœuds complets. Sans incitations fortes pour effacer l'état, c'est une tendance qui est destinée à continuer.

De même que Bitcoin, la tarification du gaz axée sur la demande d'Ethereum est un modèle équitable pour allouer son débit de calcul, la ressource rare de la plate-forme. Le modèle sert également le but d'Ethereum en tant que système de calcul décentralisé. Cependant, son modèle de frais de stockage d'état ne correspond pas à sa proposition potentielle en tant que plate-forme de stockage d'état ou d'actifs décentralisée. Sans coût pour le stockage d'état à long terme, il sera toujours dans l'intérêt des utilisateurs d'occuper l'état pour

toujours gratuitement. Sans rareté de la capacité de stockage d'état, ni marché, ni dynamique de l'offre et de la demande ne peuvent être établis.

Contrairement à Bitcoin, qui spécifie la limite de taille de bloc dans son protocole central, Ethereum permet aux mineurs d'ajuster dynamiquement la limite de gaz de bloc lorsqu'ils produisent des blocs. Les mineurs disposant d'un matériel avancé et d'une bande passante importante sont en mesure de produire plus de blocs, dominant ainsi ce processus de vote. Leur intérêt est d'ajuster la limite de gaz de bloc vers le haut, d'élever la barre de participation et de forcer les plus petits mineurs à sortir de la compétition. C'est un autre facteur qui contribue à la rapide augmentation du coût de l'exploitation du nœud complet.

Les plates-formes de contrats intelligents comme Ethereum sont des plates-formes multi-actifs. Elles prennent en charge l'émission et les transactions de tous les types de crypto-actifs, généralement représentés sous forme de "jetons". Elles offrent également une sécurité non seulement à leurs propres jetons natifs, mais également à la valeur de tous les crypto-actifs sur la plate-forme. "Réserve de valeur" dans un contexte multi-actifs se réfère donc à la propriété de préservation de valeur qui profite à la fois aux jetons natifs de la plate-forme et aux crypto-actifs stockés sur la plate-forme.

Avec ses récompenses de bloc, Bitcoin dispose d'un excellent modèle économique de "réserve de valeur". Les mineurs sont payés en récompenses de bloc fixes libellées en BTC, et donc leurs revenus augmentent avec le prix du BTC. Par conséquent, la plate-forme a la capacité de générer des revenus pour les mineurs afin d'augmenter la sécurité (mesurée par le coût de l'attaque) tout en maintenant un modèle économique durable.

Pour les plates-formes multi-actifs, il devient beaucoup plus difficile de remplir cette exigence, car "la valeur" peut être exprimée avec des crypto-actifs au-delà du jeton natif. Si la valeur des crypto-actifs sécurisés par la plate-forme augmente, mais que la sécurité du réseau ne le fait pas, il devient plus rentable d'attaquer le processus de consensus de la plate-forme pour doubler les dépenses de crypto-actifs stockés sur la plate-forme.

Pour qu'une plate-forme de contrat intelligent multi-actif fonctionne comme une réserve de valeur, il est nécessaire de mettre en place des mesures incitatives appropriées pour aligner la croissance de la valeur des actifs d'un réseau avec sa sécurité sous-jacente. Ou, pour le dire autrement, le jeton natif de la plate-forme doit être un bon indicateur de la valeur agrégée des actifs de la plate-forme. Si la valeur intrinsèque du jeton natif d'une plate-forme est limitée au paiement des frais de transaction, sa valeur sera déterminée uniquement par la demande de transaction, plutôt que par la demande de stockage d'actifs.

Les plates-formes de contrats intelligents qui ne sont pas conçues pour fonctionner comme des réserves de valeur doivent s'appuyer sur la prime monétaire du jeton natif (la volonté des gens de détenir les jetons au-delà de leur valeur intrinsèque) pour soutenir leur sécurité en cours. Cela n'est possible que si une plate-forme domine avec des fonctionnalités uniques qui ne peuvent être trouvées ailleurs, ou si elle surpasse les autres en proposant le coût le plus bas possible des transactions.

Ethereum jouit actuellement d'une telle domination et peut donc maintenir sa prime monétaire. Cependant, avec la montée de plates-formes concurrentes, nombre d'entre elles conçues pour des transactions par seconde (TPS) plus élevées et fournissant des

fonctionnalités similaires, il est bon de savoir si la dépendance à une prime monétaire seule peut soutenir la sécurité d'une blockchain, en particulier si les jetons natifs ne sont pas explicitement conçus ou crus pour être de l'argent. De plus, même si une plate-forme peut fournir des fonctionnalités uniques, sa prime monétaire peut être abstraite par l'interface utilisateur grâce à des échanges efficaces (très probable lorsque l'adoption de la blockchain sera enfin de masse). Les utilisateurs détiendraient les actifs avec lesquels ils sont les plus familiers, tels que Bitcoin ou des stables coins, et acquerraient des jetons de plateforme juste à temps pour payer les frais de transaction. Dans les deux cas, les fondements de la cryptographie-économie d'une plate-forme s'effondreraient.

2.2.5 Financement du développement du protocole de base

Les blockchains publiques et sans permission sont des infrastructures publiques. Le développement initial de ces systèmes nécessite un financement important, et une fois en fonctionnement, nécessitent une maintenance et des mises à niveau continues. Sans des personnes dédiées à la maintenance de ces systèmes, ils risquent de subir des bugs catastrophiques et un fonctionnement sous-optimal. Les protocoles Bitcoin et Ethereum ne fournissent pas de mécanisme natif pour assurer le financement du développement continu, et donc s'appuient sur l'engagement continu des entreprises ayant des intérêts alignés et des communautés altruistes de code source ouvert.

Dash a été le premier projet à utiliser une trésorerie pour garantir que le développement continu était financé dans le protocole. Tout en soutenant de manière durable le développement du protocole, cette conception fait un compromis en ce qui concerne la durabilité de la valeur de la crypto-monnaie. Comme la plupart des trésors de blockchain, ce modèle repose sur un financement basé sur l'inflation, qui érode la valeur des avoirs à long terme.

Le réseau Nervos utilise un modèle de trésorerie qui fournit un financement durable pour le développement central. Les fonds de la trésorerie proviennent de l'inflation ciblée des détenteurs de jetons à court terme, tandis que les effets de cette inflation sont atténués pour les détenteurs à long terme. Plus d'informations sur ce mécanisme sont décrites dans (4.6).

2.3 Interopérabilité

L'interopérabilité entre les blockchains est un sujet souvent discuté, et de nombreux projets ont été proposés spécifiquement pour relever ce défi. Avec des transactions fiables entre les blockchains, de véritables effets de réseau peuvent être réalisés dans l'économie décentralisée.

Le premier exemple d'interopérabilité de blockchain était les échanges atomiques entre Bitcoin et Litecoin. L'échange sans confiance de Bitcoin contre Litecoin et vice versa est rendu possible non pas par des mécanismes en protocole, mais par une norme cryptographique partagée (en particulier l'utilisation de la fonction de hachage SHA2-256).

De même, la conception d'Ethereum 2.0 permet l'interconnexion de nombreuses chaînes de shards (grappes en Francais), toutes utilisant le même protocole et les mêmes primitives cryptographiques. Cette uniformité sera précieuse lors de la personnalisation du protocole

pour la communication inter-shards, mais Ethereum 2.0 ne sera pas interopérable avec d'autres blockchains qui n'utilisent pas les mêmes primitives cryptographiques.

Les réseaux de blockchains tels que Polkadot ou Cosmos vont un peu plus loin, permettant aux blockchains construites avec le même framework (Cosmos SDK pour Cosmos et Substrate pour Polkadot) de communiquer et d'interagir les unes avec les autres. Ces frameworks offrent aux développeurs une certaine flexibilité dans la construction de leurs propres protocoles, et assurent la disponibilité de primitives cryptographiques identiques, permettant à chaque chaîne de lire les blocs des autres et de valider les transactions. Cependant, les deux protocoles reposent sur des ponts ou des "zones d'ancrage" pour se connecter à des blockchains qui ne sont pas construites avec leurs propres frameworks, introduisant une couche de confiance supplémentaire. Pour illustrer : bien que Cosmos et Polkadot permettent des "réseaux de blockchains", les réseaux Cosmos et Polkadot ne sont pas conçus pour être interopérables l'un avec l'autre.

L'économie de la cryptographie des réseaux inter-chaînes (cross-chain en Anglais) nécessite peut-être une étude plus approfondie. Pour Cosmos et Polkadot, des jetons natifs sont utilisés pour le “staking”, la gouvernance et les frais de transaction. En mettant de côté la dynamique crypto-économique introduite par le jalonnement, qui ne peut pas donner seule une valeur intrinsèque à un jeton natif (discuté dans la section 4.2.4), la dépendance à l'égard des transactions inter-chaînes pour capturer la valeur de l'écosystème peut être un modèle faible. En particulier, les transactions inter-chaînes sont une faiblesse, pas une force des réseaux multi-chaînes, tout comme les transactions inter-shard sont une faiblesse des bases de données partitionnées. Ils introduisent de la latence, ainsi que la perte d'atomicité et de compositionnalité. Il y a une tendance naturelle pour les applications qui ont besoin d'interagir les unes avec les autres de finir par résider sur la même blockchain pour réduire les frais généraux des transactions inter-chaînes, réduisant ainsi la demande de transactions inter-chaînes et donc la demande pour le jeton natif.

Les réseaux inter-chaînes bénéficient d'effets de réseau - plus il y a de chaînes interconnectées dans un réseau, plus le réseau est précieux et plus il est attractif pour les nouveaux participants potentiels dans le réseau. Idéalement, une telle valeur serait capturée par le jeton natif et utilisée pour encourager davantage la croissance du réseau. Cependant, dans un réseau de sécurité regroupé tel que Polkadot, un coût plus élevé de participation au réseau devient un obstacle à l'accumulation de valeur supplémentaire pour le réseau. Dans un réseau peu connecté comme Cosmos, si l'on suppose une même demande et des frais de transaction inter-chaînes, un coût plus élevé de participation au “staking” réduit le rendement attendu pour les validateurs, décourageant une participation au “staking” supplémentaire.

Avec son approche en couches, le réseau Nervos est également un réseau multi-chaînes. Architecturalement, Nervos utilise le modèle de cellule et une machine virtuelle de bas niveau pour prendre en charge une véritable personnalisation et des primitives cryptographiques créées par l'utilisateur, permettant l'interopérabilité entre les blockchains hétérogènes (couvert dans 4.4.1). Crypto-économiquement, le réseau Nervos concentre la valeur (au lieu du passage de messages) sur sa chaîne racine. Ce mécanisme augmente le budget de sécurité du réseau à mesure que la valeur agrégée sécurisée par le réseau augmente. Cela est détaillé dans la section (4.4).

3. Principes fondamentaux du réseau Nervos

Nervos est un réseau en couches conçu pour répondre aux besoins de l'économie décentralisée. Il existe plusieurs raisons pour lesquelles nous croyons qu'une approche en couches est la bonne méthode pour construire un réseau blockchain. Il existe de nombreux compromis bien connus dans la construction de systèmes blockchain, tels que la décentralisation par rapport à la scalabilité, la neutralité par rapport à la conformité, la confidentialité par rapport à l'ouverture, la réserve de valeur par rapport au coût des transactions et la solidité cryptographique par rapport à l'expérience utilisateur. Nous croyons que tous ces conflits découlent des tentatives de répondre à des préoccupations complètement opposées avec une seule blockchain.

Nous croyons que la meilleure façon de construire un système n'est pas de construire une couche unique qui englobe tout, mais plutôt de dissocier les préoccupations et de les aborder à différents niveaux. En faisant cela, la blockchain de la couche de niveau 1 peut se concentrer sur la sécurité, la neutralité, la décentralisation et l'infrastructure publique et ouverte, tandis que des réseaux plus petits de la couche de niveau 2 peuvent être spécialement conçus pour répondre au mieux au contexte de leur utilisation.

Dans le réseau Nervos, le protocole de la couche de niveau 1 (Common Knowledge Base - *La base de connaissance commune en* Français) est la couche de préservation de valeur de l'ensemble du réseau. Il est philosophiquement inspiré par Bitcoin et est une blockchain ouverte, publique et basée sur la preuve de travail, conçue pour être la plus sûre et la plus résistante possible à la censure, pour servir de gardien décentralisé de la valeur et des crypto-actifs. Les protocoles de la couche de niveau 2 tirent parti de la sécurité de la blockchain de la couche de niveau 1 pour offrir une scalabilité illimitée, des coûts de transaction minimaux et permettent également des compromis spécifiques aux applications en ce qui concerne les modèles de confiance, la confidentialité et la finalité.

Voici les principes fondamentaux qui ont conduit à la conception du réseau Nervos :

- Une blockchain de la couche de niveau 1 durable et multi-actifs doit être conçue cryptographiquement pour être une réserve de valeur.
- La couche de niveau 2 offre les meilleures options de scalabilité, offrant des capacités transactionnelles presque illimitées, des coûts de transaction minimaux et une expérience utilisateur améliorée. Les blockchains de la couche de niveau 1 doivent être conçues pour compléter, et non pour concurrencer avec les solutions de la couche 2.
- La preuve de travail en tant que méthode de résistance à Sybil est essentielle pour les blockchains de la couche de niveau 1.
- La blockchain de la couche de niveau 1 doit fournir un modèle de programmation générique pour les protocoles interactifs et l'interopérabilité blockchain, et permettre au protocole d'être maximale personnalisable et facile à mettre à niveau.
- Pour mieux allouer les ressources et éviter la "tragédie des biens communs", le stockage de l'état doit avoir un modèle de propriété clair et finement granulé. Pour offrir des récompenses à long terme cohérentes aux mineurs (indépendamment de la demande de transaction), l'occupation de l'état doit avoir un coût continu.

4. Le Common Knowledge Base de Nervos

4.1 Aperçu

"La connaissance commune” est définie comme la connaissance que tout le monde ou presque connaît, généralement en référence à la communauté dans laquelle le terme est utilisé. Dans le contexte des blockchains en général, et du réseau Nervos en particulier, "la connaissance commune" se réfère à l'état vérifié par un consensus mondial et accepté par tous dans le réseau.

Les propriétés de la connaissance commune nous permettent de traiter collectivement la cryptomonnaie stockée sur les blockchains publiques comme de la monnaie. Par exemple, les soldes et l'historique de toutes les adresses sur Bitcoin sont une connaissance commune pour les utilisateurs de Bitcoin, car ils sont capables de répliquer indépendamment le grand livre partagé, de vérifier l'état mondial depuis le bloc de genèse, et de savoir que n'importe qui d'autre peut faire de même. Cette connaissance commune permet aux gens de transiger complètement de pair à pair sans faire confiance à un tiers.

Le “Common Knowledge Base” (CKB) de Nervos est conçu pour stocker toutes sortes de connaissances communes, sans se limiter à la monnaie. Par exemple, le CKB pourrait stocker des actifs cryptographiques définis par l'utilisateur, tels que des jetons fongibles et non fongibles, ainsi que des preuves cryptographiques précieuses qui offrent une sécurité pour les protocoles de couche supérieure, tels que les canaux de paiement (5.2) et les chaînes d'engagement (5.4).

Bitcoin et le CKB de Nervos sont des systèmes de stockage et de vérification de connaissances communes. Bitcoin stocke son état mondial sous forme de l'ensemble des UTXO, et vérifie les transitions d'état à travers des règles codées en dur et des scripts intégrés dans les transactions. Le CKB de Nervos généralise la structure de données et les capacités de scriptage de Bitcoin, stocke l'état mondial sous forme de l'ensemble des cellules programmables actives, et vérifie les transitions d'état au moyen de scripts “Turing-complets” définis par l'utilisateur, qui s'exécutent dans une machine virtuelle.

Alors que le CKB de Nervos possède des capacités de contrat intelligent complètes comme celles d'Ethereum et d'autres plateformes, son modèle économique est conçu pour la préservation de la connaissance commune, plutôt que pour le paiement de la computation décentralisée.

4.2 Consensus

Le consensus de Nakamoto (NC) de Bitcoin est bien reçu en raison de sa simplicité et de sa faible surcharge de communication. Cependant, NC souffre de deux inconvénients : 1) son débit de traitement des transactions est loin d'être satisfaisant, et 2) il est vulnérable aux

attaques de minage égoïstes, dans lesquelles les attaquants peuvent gagner des récompenses de bloc supplémentaires en s'écartant du comportement prescrit par le protocole.

Le protocole de consensus de CKB est une variante de NC qui élève sa limite de performance et sa résistance au minage égoïste tout en conservant ses mérites. En identifiant et en éliminant le goulot d'étranglement dans la latence de propagation de bloc de NC, notre protocole prend en charge des intervalles de bloc très courts sans sacrifier la sécurité. Un intervalle de bloc raccourci augmente non seulement le débit, mais réduit également la latence de confirmation des transactions. En incorporant tous les blocs valides dans le calcul d'ajustement de difficulté, le minage égoïste n'est plus rentable dans notre protocole.

4.2.1 Augmentation du débit

Nervos CKB augmente le débit du consensus de preuve de travail avec un algorithme de consensus dérivé du consensus de Nakamoto. L'algorithme utilise le taux d'orphelins de la blockchain (le pourcentage de blocs valides qui ne font pas partie de la chaîne canonique) comme mesure de la connectivité à travers le réseau.

Le protocole vise un taux d'orphelins fixe. En réponse à un faible taux d'orphelins, la difficulté cible est abaissée (augmentant le taux de production de blocs) et lorsque le taux d'orphelins dépasse un seuil défini, la difficulté cible est augmentée (diminuant le taux de production de blocs).

Cela permet d'utiliser toutes les capacités de bande passante du réseau. Un faible taux d'orphelins indique que le réseau est bien connecté et peut gérer une plus grande transmission de données; le protocole augmente ensuite le débit dans ces conditions.

4.2.2 Elimination du goulot d'étranglement de la propagation de blocs

Le goulot d'étranglement de tout réseau de blockchain est la propagation de blocs. Le protocole de consensus de Nervos CKB élimine le goulot d'étranglement de la propagation de blocs en modifiant la confirmation des transactions en un processus en deux étapes : 1) proposer et 2) valider.

Une transaction doit d'abord être proposée dans la "zone de proposition" d'un bloc (ou l'un de ses oncles). La transaction sera ensuite validée si elle apparaît dans la "zone de validation" d'un bloc dans une fenêtre de temps définie après sa proposition. Cette conception élimine le goulot d'étranglement de la propagation de blocs, car les transactions validées d'un nouveau bloc ont déjà été reçues et vérifiées par tous les nœuds lors de leur proposition.

4.2.3 Atténuation des attaques de minage égoïstes

L'une des attaques les plus fondamentales contre le consensus de Nakamoto est le minage égoïste. Dans cette attaque, des mineurs malveillants gagnent des récompenses de bloc injustes en rendant délibérément les blocs orphelins extraits par d'autres.

Les chercheurs observent que l'opportunité de profit injuste est enracinée dans le mécanisme d'ajustement de difficulté du consensus de Nakamoto, qui néglige les blocs orphelins lors de l'estimation de la puissance de calcul du réseau. Cela conduit à une difficulté d'extraction plus faible et à des récompenses de blocs plus élevées.

Le protocole de consensus du CKB de Nervos intègre des blocs oncles dans le calcul d'ajustement de difficulté, rendant le minage égoïste non rentable. Cela est valable indépendamment de la stratégie ou de la durée de l'attaque ; un mineur ne peut pas obtenir de récompenses injustes grâce à une combinaison d'extraction honnête et égoïste.

Notre analyse montre qu'avec un processus de confirmation de transaction en deux étapes, le minage égoïste de facto est également éliminé via une fenêtre de temps d'attaque limitée.

Pour une compréhension détaillée de notre protocole de consensus, veuillez lire ici.

4.2.4 Preuve de travail ou Preuve d'enjeu

Les systèmes de Preuve de travail (PoW) et de Preuve d'enjeu (PoS) sont tous deux vulnérables aux concentrations de pouvoir. Cependant, les qualités des systèmes offrent des réalités opérationnelles très différentes pour ceux qui sont au pouvoir.

Le minage en PoW entraîne des dépenses réelles qui peuvent dépasser les recettes de minage sans une surveillance rigoureuse des coûts. Ceux qui sont au pouvoir sont tenus de rester innovants, de poursuivre des stratégies commerciales judicieuses et de continuer à investir dans l'infrastructure pour rester dominants. L'équipement de minage, les opérations de pool d'extraction et l'accès à l'énergie bon marché sont tous soumis à des changements dus à l'innovation technologique. Il est difficile de maintenir la monopolisation des trois pendant de longues périodes.

En revanche, les créateurs de blocs dans les systèmes PoS sont récompensés de manière déterministe, en fonction du montant “staked”, avec des exigences en capital opérationnel très faibles. À mesure que le système se développe, l'impact des avantages naturels fournis aux entreprises et aux particuliers qui se déplacent en premier se renforcera. Dans un système PoS, il est possible que le pouvoir se concentre entre les mains de quelques détenteurs d'enjeux. Bien que les systèmes PoW aient un problème similaire avec la concentration de minage, le coût pour rester au pouvoir dans un système PoS est significativement inférieur.

De plus, les validateurs PoS ont un pouvoir unique : le contrôle de l'ensemble des validateurs. L'acceptation d'une transaction qui permet à un validateur de rejoindre le groupe de consensus est entre les mains des validateurs existants. Les efforts de collusion visant à influencer l'ensemble des validateurs par la censure des transactions et la manipulation de l'ordre seraient difficiles à détecter, ainsi qu'à punir. En revanche, la participation au consensus dans les systèmes PoW est vraiment ouverte et n'est pas soumise à la structure de pouvoir actuelle. Les avantages ne sont pas donnés aux premiers participants du système.

En ce qui concerne l'économie des jetons, bien qu'il soit admis que le “staking” peut attirer des capitaux cherchant à gagner un rendement (et donc augmenter la demande pour le

jeton natif), ce n'est pas tout à fait exact. Tous les projets PoS verront éventuellement leur taux de “staking” se stabiliser, et le capital entrant et sortant du pool de capital “staked” serait alors à peu près le même. Le mécanisme de “staking” en lui-même ne stimulera pas la demande pour le jeton natif. En d'autres termes, bien que l'introduction du “staking” fournisse une demande pour le jeton natif dans la phase initiale d'un projet (à mesure que le taux de “staking” augmente), le staking seul ne peut pas fournir une demande à long terme pour le jeton natif et ne peut donc pas être la seule valeur intrinsèque du jeton natif.

Les détenteurs de jetons à long terme dans un système PoS ont trois options : ils peuvent 1) gérer l'infrastructure et exécuter un nœud de validation par eux-mêmes pour recevoir une nouvelle émission, 2) déléguer leurs jetons à un tiers et faire confiance à leur intégrité et à leur infrastructure, ou 3) voir la valeur de leurs jetons diluée par une émission continue. Aucune de ces options n'est particulièrement attrayante pour les détenteurs de jetons orientés vers la conservation de la valeur à long terme.

Nous croyons que la participation sans permission en PoW est une exigence pour l'infrastructure à la base de l'activité économique mondiale. L'objectif principal de la couche de niveau 1 est de s'assurer que la blockchain est aussi décentralisée, sécurisée et neutre que possible. Bien que les systèmes PoS aient un rôle à jouer dans l'économie décentralisée, à notre avis, ils ne répondent pas aux exigences d'une couche de niveau 1 véritablement ouverte et décentralisée.

4.2.5 Fonction de la preuve de travail

Les blocs Nervos CKB peuvent être proposés par n'importe quel nœud, à condition que 1) le bloc soit valide ; et 2) le proposant ait résolu une énigme computationnelle difficile appelée preuve de travail. L'énigme de preuve de travail est définie en termes du bloc qui est proposé ; cela garantit que la solution de l'énigme identifie de manière unique un bloc.

La preuve de travail de Bitcoin exige de trouver un nonce valide de sorte que le résultat de l'application d'une fonction de hachage sur l'en-tête de bloc satisfasse un certain niveau de difficulté. Pour Bitcoin, la fonction de hachage est SHA2-256 itéré deux fois. Bien que SHA2 était un bon choix pour Bitcoin, cela n'est pas vrai pour les crypto-monnaies qui viennent après. Une grande quantité de matériel dédié a été développée pour miner Bitcoin, dont une grande partie est inutilisée, ayant été rendue obsolète par des améliorations d'efficacité.

Une nouvelle crypto monnaie utilisant la même énigme de preuve de travail rendrait ce matériel périmé à nouveau utile. Même le matériel à jour peut être loué et réutilisé pour miner une nouvelle crypto monnaie. La distribution de la puissance de minage pour une monnaie basée sur SHA2 serait très difficile à prévoir et susceptible de changements soudains et importants. Cet argument s'applique également aux optimisations algorithmiques adaptées à SHA2, qui ont été développées pour rendre le calcul logiciel de la fonction moins cher également.

Pour une nouvelle crypto monnaie, il est logique de définir l'énigme de preuve de travail en termes d'une fonction qui n'a pas encore été utilisée par d'autres crypto monnaies. Pour Nervos CKB, nous sommes allés plus loin et avons choisi de la définir en termes d'une fonction de preuve de travail qui n'aurait pas pu faire l'objet d'une optimisation prématurée, car elle est nouvelle.

Cependant, l'indisponibilité prévue du matériel de minage n'est le cas qu'initialement. À long terme, le déploiement de matériel de minage dédié est bénéfique, augmentant considérablement les défis d'attaque du réseau. Par conséquent, en plus d'être nouveau, une fonction de preuve de travail idéale pour une nouvelle crypto monnaie est également simple, abaissant considérablement la barrière au développement de matériel.

La sécurité est le troisième objectif de conception évident. Bien qu'une vulnérabilité connue puisse être exploitée par tous les mineurs de manière égale, et ne conduirait qu'à une difficulté plus élevée, une vulnérabilité non divulguée pourrait entraîner une optimisation de minage qui offre au ou aux découvreurs un avantage supérieur à leur part de puissance de minage contribuée. La meilleure façon d'éviter cette situation est de faire une forte argumentation pour l'invulnérabilité.

4.2.6 Eaglesong

Eaglesong est une nouvelle fonction de hachage développée spécifiquement pour la preuve de travail de Nervos CKB, mais elle convient également à d'autres cas d'utilisation dans lesquels une fonction de hachage sécurisée est nécessaire. Les critères de conception étaient exactement ceux énumérés ci-dessus : la nouveauté, la simplicité et la sécurité. Nous voulions une conception qui soit à la fois suffisamment nouvelle pour constituer un petit pas en avant pour la science, tout en étant suffisamment proche des conceptions existantes pour faire une forte argumentation en faveur de sa sécurité.

À cette fin, nous avons choisi d'instancier la construction en éponge (comme utilisée dans Keccak/SHA3) avec une permutation construite à partir d'opérations ARX (addition, rotation et xor) ; l'argument pour sa sécurité repose sur la stratégie de large trajectoire (le même argument sous-jacent à AES).

À notre connaissance, Eaglesong est la première fonction de hachage (ou fonction, d'ailleurs) qui combine avec succès les trois principes de conception.

Vous pouvez en savoir plus sur Eaglesong ici.

4.3 Modèle de Cellule

Nervos CKB utilise le Modèle de Cellule, une nouvelle construction qui peut offrir de nombreux avantages du modèle de compte (utilisé dans Ethereum), tout en préservant la propriété des actifs et les propriétés de vérification basées sur la preuve du modèle de sortie (UTXO, utilisé dans Bitcoin).

Le modèle de cellule se concentre sur l'état. Les cellules contiennent des données arbitraires, qui peuvent être simples, telles qu'un montant de jeton et un propriétaire, ou plus complexes, telles que du code spécifiant des conditions de vérification pour un transfert de jeton. La machine à états de CKB exécute des scripts associés aux cellules pour garantir l'intégrité d'une transition d'état.

En plus de stocker leurs propres données, les cellules peuvent référencer des données dans d'autres cellules. Cela permet aux actifs appartenant aux utilisateurs et à la logique qui les régit d'être séparés. Cela contraste avec les plateformes de contrat intelligent basées sur

des comptes, dans lesquelles l'état est une propriété interne d'un contrat intelligent et doit être accédé via des interfaces de contrat intelligent. Sur Nervos CKB, les cellules sont des objets d'état indépendants qui sont possédés, peuvent être référencés et passés directement. Les cellules peuvent exprimer de vrais "actifs supportables", appartenant à leurs propriétaires (tout comme les UTXOs sont des actifs supportables pour les propriétaires de Bitcoin), tout en référençant une cellule qui détient la logique assurant l'intégrité des transitions d'état.

Les transactions de modèle de cellule sont également des preuves de transition d'état. Les cellules d'entrée d'une transaction sont supprimées de l'ensemble des cellules actives et les cellules de sortie sont ajoutées à l'ensemble. Les cellules actives constituent l'état global de Nervos CKB, et sont immuables : une fois que les cellules ont été créées, elles ne peuvent pas être modifiées.

Le modèle de cellule est conçu pour être adaptable, durable et flexible. Il peut être décrit comme un modèle de sortie généralisé et peut prendre en charge des jetons définis par l'utilisateur, des contrats intelligents et des protocoles de couche de niveau 2 divers.

Pour une compréhension plus approfondie du Modèle de Cellule, veuillez voir ici.

4.4 Machine Virtuelle

Alors que de nombreux projets blockchain de prochaine génération utilisent WebAssembly comme base d'une machine virtuelle blockchain, Nervos CKB inclut le choix de conception unique d'une machine virtuelle (CKB-VM) basée sur l'ensemble d'instructions RISC-V.

RISC-V est une architecture d'ensemble d'instructions RISC open source créée en 2010 pour faciliter le développement de nouveaux matériels et logiciels, et est un ensemble d'instructions libre de redevances, largement compris et largement audité.

Nous avons trouvé de nombreux avantages à utiliser RISC-V dans un contexte blockchain :

- Stabilité : L'ensemble d'instructions de base de RISC-V a été finalisé et gelé, ainsi que largement mis en œuvre et testé. L'ensemble d'instructions de base de RISC-V est fixe et ne nécessitera jamais de mise à jour.
- Ouvert et pris en charge : RISC-V est fourni sous licence BSD et pris en charge par des compilateurs tels que GCC et LLVM, avec des implémentations de langage Rust et Go en cours de développement. La fondation RISC-V comprend plus de 235 organisations membres qui favorisent le développement et le soutien de l'ensemble d'instructions.
- Simplicité et extensibilité : L'ensemble d'instructions RISC-V est simple. Avec le support des entiers 64 bits, l'ensemble ne contient que 102 instructions. RISC-V fournit également un mécanisme modulaire pour les ensembles d'instructions étendus, permettant la possibilité de calcul vectoriel ou d'entiers 256 bits pour les algorithmes cryptographiques à haute performance.
- Tarification précise des ressources : L'ensemble d'instructions RISC-V peut être exécuté sur un CPU physique, fournissant une estimation précise des cycles de

machine requis pour l'exécution de chaque instruction et informant la tarification des ressources de la machine virtuelle.

CKB-VM est une machine virtuelle RISC-V de bas niveau qui permet une computation flexible et complète. Grâce à l'utilisation du format ELF largement mis en œuvre, les scripts CKB-VM peuvent être développés avec n'importe quel langage qui peut être compilé en instructions RISC-V.

4.4.1 CKB-VM et le Modèle de Cellule

Une fois déployées, les blockchains publiques existantes sont plus ou moins fixes. La mise à niveau d'éléments fondamentaux, tels que les primitives cryptographiques, nécessite des engagements pluriannuels ou ne sont tout simplement pas possibles.

CKB-VM prend du recul et déplace des primitives précédemment intégrées dans des VM personnalisées vers des cellules sur le dessus de la machine virtuelle. Bien que les scripts CKB soient plus bas niveau que les contrats intelligents dans Ethereum, ils apportent l'avantage significatif de la flexibilité, permettant une plateforme réactive et une base pour l'économie décentralisée en progression.

Les cellules peuvent stocker du code exécutable et référencer d'autres cellules en tant que dépendances. Presque tous les algorithmes et les structures de données sont implémentés sous forme de scripts CKB stockés dans des cellules. En gardant la VM aussi simple que possible et en déchargeant le stockage du programme sur les cellules, la mise à jour des algorithmes clés est aussi simple que de charger l'algorithme dans une nouvelle cellule et de mettre à jour les références existantes.

4.4.2 Exécution d'autres machines virtuelles sur la CKB-VM

Grâce à la nature de bas niveau de la CKB-VM et à la disponibilité d'outils dans la communauté RISC-V, il est facile de compiler d'autres VM (comme l'EVM d'Ethereum) directement dans la CKB-VM. Cela présente plusieurs avantages :

- Les contrats intelligents écrits dans des langages spécialisés fonctionnant sur d'autres machines virtuelles peuvent être facilement portés pour fonctionner sur la CKB-VM. (Strictement parlant, ils fonctionneraient sur leur propre VM qui est compilée pour fonctionner à l'intérieur de la CKB-VM.)
- Le CKB peut vérifier les transitions d'état de résolution de litige des transactions de couche de niveau 2, même si les règles des transitions d'état sont écrites pour fonctionner dans une machine virtuelle autre que la CKB-VM. C'est l'une des exigences clés pour prendre en charge des chaînes latérales de couche de niveau 2 à usage général sans confiance.

Pour un guide technique de la CKB-VM, veuillez consulter ici.

4.5 Modèle économique

Le jeton natif de Nervos CKB est le "Common Knowledge Byte", ou CKByte pour faire court. Les CKBytes donnent au détenteur du jeton le droit d'occuper une partie de l'espace de

stockage total de l'état de la blockchain. Par exemple, en détenant 1000 CKBytes, un utilisateur peut créer une cellule de 1000 bytes de capacité ou plusieurs cellules dont la somme est équivalente à 1000 bytes.

L'utilisation des CKBytes pour stocker des données sur la CKB crée un coût d'opportunité pour les propriétaires de CKBytes; ils ne pourront pas déposer des CKBytes occupés dans le NervosDAO pour recevoir une partie de l'émission secondaire. Les CKBytes ont un prix de marché, et donc une incitation économique est fournie aux utilisateurs pour libérer volontairement l'espace de stockage de l'état afin de répondre à la forte demande d'expansion de l'état. Après qu'un utilisateur a libéré de l'espace de stockage, il recevra une quantité de CKBytes équivalente à la taille de l'état (en octets) que leurs données occupaient.

Le modèle économique de la CKB permet l'émission du jeton natif pour limiter la croissance de l'état, maintenir une faible barrière de participation et assurer la décentralisation. À mesure que les CKBytes deviennent une ressource rare, ils peuvent être évalués et alloués de manière optimale.

Le bloc de genèse du réseau Nervos contiendra 33,6 milliards de CKBytes, dont 8,4 milliards seront immédiatement brûlés. La nouvelle émission de CKBytes comprend deux parties - l'émission de base et l'émission secondaire. L'émission de base est limitée à une offre totale finie (33,6 milliards de CKBytes), avec un calendrier d'émission similaire à celui de Bitcoin. La récompense de bloc est divisée par deux environ tous les 4 ans, jusqu'à atteindre 0 nouvelle émission. Toute l'émission de base est attribuée aux mineurs comme incitation à protéger le réseau. L'émission secondaire a un taux d'émission constant de 1,344 milliard de CKBytes par an et est conçue pour imposer un coût d'opportunité pour l'occupation de l'espace de stockage de l'état. Après l'arrêt de l'émission de base, il n'y aura plus que l'émission secondaire.

Nervos CKB inclut un contrat intelligent spécial appelé NervosDAO, qui sert de "refuge contre l'inflation" contre les effets de l'émission secondaire. Les propriétaires de CKByte peuvent déposer leurs jetons dans le NervosDAO et recevoir une partie de l'émission secondaire qui compense exactement les effets inflationnistes de l'émission secondaire. Pour les détenteurs de jetons à long terme, tant qu'ils bloquent leurs jetons dans le NervosDAO, l'effet inflationniste de l'émission secondaire est seulement nominal. Avec les effets de l'émission secondaire atténués, ces utilisateurs détiennent effectivement des jetons à offre limitée comme Bitcoin.

Bien que les CKBytes soient utilisés pour stocker l'état, ils ne peuvent pas être utilisés pour gagner des récompenses d'émission secondaire via le NervosDAO. Cela fait de l'émission secondaire une taxe d'inflation constante, ou "loyer d'état" sur l'occupation du stockage d'état. Ce modèle économique impose des frais de stockage d'état proportionnels à l'espace et au temps d'occupation. Il est plus durable que le modèle "payer une fois, occuper pour toujours" utilisé par d'autres plateformes, et est plus réalisable et convivial que d'autres solutions de location d'état qui nécessitent des paiements explicites.

Les mineurs sont rémunérés à la fois par les récompenses de bloc et les frais de transaction. Pour les récompenses de bloc, lorsqu'un mineur extrait un bloc, il reçoit la récompense d'émission de base complète du bloc, ainsi qu'une partie de l'émission

secondaire. La partie est basée sur l'occupation de l'état, par exemple : si la moitié de tous les tokens natifs sont utilisés pour stocker l'état, un mineur recevrait la moitié de la récompense d'émission secondaire pour le bloc. Des informations supplémentaires sur la distribution de l'émission secondaire sont incluses dans la section suivante (4.6). À long terme, lorsque l'émission de base s'arrête, les mineurs recevront toujours un revenu de "location d'état" indépendant des transactions, mais lié à l'adoption du “Common Knowledge Base” de Nervos.

Dans une analogie, les CKBytes peuvent être considérés comme des terrains, tandis que les crypto-actifs stockés sur le CKB peuvent être considérés comme des maisons. Le terrain est nécessaire pour construire une maison, et les CKBytes sont nécessaires pour stocker des actifs sur le CKB. Avec la demande croissante de stockage d'actifs sur CKB, la demande de CKBytes augmente également. Avec l'augmentation de la valeur des actifs stockés, la valeur des CKBytes augmente également.

Le CKB est conçu pour traduire la demande d'une multitude d'actifs en demande d'un seul actif, et l'utiliser pour rémunérer les mineurs pour sécuriser le réseau.

Pour une explication plus détaillée du modèle économique, veuillez consulter ici.

4.6 Trésorerie

La partie de l'émission secondaire qui ne va ni aux mineurs ni aux détenteurs à long terme avec des jetons bloqués dans le NervosDAO ira vers un fonds de trésorerie. Pour illustrer : si 60 % des CKBytes émis sont utilisés pour stocker l'état et 30 % des CKBytes sont déposés dans le NervosDAO, les mineurs recevront 60 % de l'émission secondaire, le NervosDAO (détenteurs à long terme) recevra 30 % de l'émission secondaire, et 10 % de l'émission secondaire ira à la trésorerie.

Le fonds de trésorerie sera utilisé pour financer la recherche et le développement continu du protocole, ainsi que pour construire l'écosystème du réseau Nervos. L'utilisation des fonds de la trésorerie sera transparente et enregistrée sur la chaîne pour que tout le monde puisse la voir. Par rapport à un modèle de financement de trésorerie basé sur l'inflation, ce modèle ne dilue pas les détenteurs de jetons à long terme (qui ont déposé leurs jetons dans le NervosDAO). Le financement du développement de protocoles est strictement dérivé du coût d'opportunité pour les détenteurs de jetons à court terme.

La trésorerie ne sera pas activée immédiatement après le lancement du réseau principal du “Common Knowledge Base” de Nervos. Avec l'approbation de la communauté, elle sera activée avec un hard fork ultérieur, seulement après que la Fondation Nervos aura épuisé le Fonds d'Écosystème, inclus dans le bloc de genèse. Avant l'activation de la trésorerie, cette partie de l'émission secondaire sera brûlée.

4.7 Gouvernance

La gouvernance est la façon dont la société ou les groupes au sein de celle-ci s'organisent pour prendre des décisions. Toute partie concernée par le système devrait être impliquée dans ce processus. En ce qui concerne une blockchain, cela devrait inclure non seulement

les utilisateurs, les détenteurs, les mineurs, les chercheurs et les développeurs, mais également les fournisseurs de services tels que les portefeuilles, les échanges et les pools miniers. Les différents groupes d'intéressés ont des intérêts divers et il est presque impossible d'aligner les incitations de tout le monde. C'est pourquoi la gouvernance des blockchains est un sujet complexe et controversé. Si nous considérons une blockchain comme une grande expérience sociale, la gouvernance nécessite une conception plus sophistiquée que toute autre partie du système. Après dix ans d'évolution, nous n'avons toujours pas identifié les meilleures pratiques générales ou les processus durables pour la gouvernance des blockchains.

Certains projets effectuent la gouvernance via un "dictateur bienveillant à vie" (comme Linus Torvalds à Linux). Nous reconnaissons que cela rend un projet hautement efficace, cohérent et également charmant : les gens adorent les héros ; cependant, cela est contradictoire avec la décentralisation, la valeur fondamentale de la blockchain.

Certains projets confient à un comité hors chaîne distingué un pouvoir de prise de décision étendu, tel que l'ECAF (EOSIO Core Arbitration Forum) sur EOS. Cependant, ces comités manquent du pouvoir essentiel pour garantir que les participants respectent leurs décisions, ce qui aurait pu jouer un rôle dans la décision de fermer l'ECAF plus tôt cette année.

Certains projets, tels que Tezos, vont plus loin et mettent en œuvre une gouvernance on-chain pour garantir que tous les participants respectent les décisions votées. Cela évite également tout impact de discorde entre les développeurs et les mineurs (ou les utilisateurs de nœuds complets). Notez que la gouvernance on-chain est différente d'un simple vote on-chain, si une fonctionnalité ou un correctif proposé a acquis suffisamment de votes grâce à la gouvernance on-chain, le code de la chaîne sera mis à jour automatiquement, les mineurs ou les nœuds complets n'ont aucun moyen de contrôler ce changement. Polkadot adopte une approche encore plus sophistiquée de la gouvernance on-chain, en utilisant un conseil élu, un processus de référendum pour le vote pondéré par les enjeux et des mécanismes de biais positif/négatif pour tenir compte du taux de participation des électeurs.

Cependant, malgré sa simplicité, la gouvernance on-chain en pratique n'est pas aussi élégante qu'elle n'y paraît. Tout d'abord, les votes ne reflètent que l'intérêt des détenteurs de jetons, en ignorant simplement toutes les autres parties. Deuxièmement, un faible taux de participation aux votes est un problème de longue date dans le monde de la blockchain et dans le monde réel. Comment les résultats peuvent-ils être dans le meilleur intérêt de la majorité si seule une minorité vote? Enfin et surtout, une bifurcation dure devrait toujours être considérée comme un recours final pour toutes les parties prenantes. Étant donné l'excellente disponibilité des données fournie par la large réplication d'une blockchain sans permission, la bifurcation à partir de la chaîne existante avec une préservation complète des données et sans interruption devrait toujours être une option. Une bifurcation dure ne pourrait jamais être mise en œuvre via une gouvernance on-chain.

Il n'y a pas encore de réponses viables aux questions de gouvernance, donc pour Nervos Network, nous adopterons une approche évolutive. Nous nous attendons à ce que la communauté se développe de manière organique dans les premiers jours et au fil du temps, à mesure que plus de jetons sont extraits, que l'exploitation minière devient plus distribuée et que plus de développeurs sont engagés, les responsabilités de gouvernance deviendront

progressivement plus décentralisées. À long terme, la gouvernance basée sur la communauté gérera le processus de mise à niveau du protocole et l'allocation des ressources du trésor.

Nervos CKB est conçu pour être une infrastructure autonome décentralisée qui pourrait durer des centaines d'années, ce qui signifie qu'il y a certaines choses qui demandent notre meilleur effort en tant que communauté pour être vraies, peu importe comment ce réseau évolue. Les 3 invariants principaux sont les suivants :

- Le calendrier d'émission est entièrement fixé, il ne doit donc jamais être modifié.
- L'état/les données stockées dans les cellules ne doivent pas être altérés.
- La sémantique des scripts existants ne doit pas être modifiée.

La gouvernance basée sur la communauté pour les blockchains est un domaine très nouveau et il y a de nombreuses expériences en cours qui valent la peine d'être étudiées. Nous reconnaissons que ce n'est pas un sujet trivial et que du temps est nécessaire pour étudier, observer et itérer pour arriver à une approche optimale. Nous adoptons une approche conservatrice de la gouvernance basée sur la communauté à court terme, tout en restant pleinement engagés dans cette direction à long terme.

5. Aperçu des solutions de couche de niveau 2

5.1 Qu'est-ce que la couche de niveau 2?

La couche de niveau 1 d'un réseau blockchain est définie par des contraintes. Une blockchain idéale en couche de niveau 1 ne fait aucun compromis en matière de sécurité, de décentralisation et de durabilité, mais cela crée des défis liés à la scalabilité et aux coûts de transaction. Les solutions de couche de niveau 2 sont construites sur les protocoles de couche de niveau 1, permettant à la computation d'être déplacée off-chain avec des mécanismes pour se régler de manière sécurisée sur la blockchain de couche de niveau 1.

Ceci est similaire au règlement net dans le système bancaire actuel ou aux dépôts réglementaires mandatés par la SEC. En réduisant la quantité de données nécessitant un consensus global, le réseau peut servir plus de participants et faciliter plus d'activités économiques qu'il ne le pourrait autrement, tout en maintenant les propriétés de la décentralisation.

Les utilisateurs de la couche de niveau 2 dépendent de la sécurité fournie par la blockchain de couche de niveau 1, et utilisent cette sécurité lorsqu'ils déplacent des actifs entre les couches ou règlent un différend. Cette fonction est similaire à un système judiciaire : le tribunal n'a pas à surveiller et valider toutes les transactions, mais sert uniquement de lieu pour enregistrer les preuves clés et régler les différends. De même, dans un contexte de blockchain, la blockchain de couche de niveau 1 permet aux participants de transiger off-chain, et en cas de désaccord leur offre la possibilité de fournir des preuves cryptographiques à la blockchain et de pénaliser la malhonnêteté.

5.2 Canaux de paiement et d'état

Les canaux de paiement sont créés entre deux parties qui effectuent souvent des transactions. Ils offrent une expérience de paiement immédiat à faible latence que les transactions effectuées directement sur une blockchain globale ne pourraient jamais fournir. Les canaux de paiement fonctionnent de manière similaire à une note de bar - vous pouvez ouvrir une note avec un barman et continuer à commander des boissons, mais ne régler la note et payer le montant final que lorsque vous êtes prêt à quitter le bar. Dans l'exploitation d'un canal de paiement, les participants échangent des messages contenant des engagements cryptographiques sur leurs soldes et peuvent mettre à jour ces soldes un nombre illimité de fois hors chaîne, avant d'être prêts à fermer le canal et à régler les soldes de retour sur la blockchain.

Les canaux de paiement peuvent être unidirectionnels ou bidirectionnels. Les canaux de paiement unidirectionnels vont de la partie A à la partie B, de manière similaire à l'exemple de la note de bar ci-dessus. La partie A dépose le montant maximum qu'elle peut dépenser avec la partie B, puis signe lentement les fonds au fur et à mesure qu'elle reçoit des biens ou des services.

Les canaux de paiement bidirectionnels sont plus compliqués, mais commencent à montrer l'étendue des possibilités pour les technologies de la couche de niveau 2. Dans ces canaux de paiement, les fonds circulent d'avant en arrière entre les parties. Cela permet le "rééquilibrage" des canaux de paiement et ouvre la possibilité de paiements entre les canaux par l'intermédiaire d'une contrepartie partagée. Cela permet les réseaux de canaux de paiement, tels que le Lightning Network de Bitcoin. Les fonds peuvent être transférés de la partie A à la partie B sans qu'il y ait un canal direct entre eux, tant que la partie A peut trouver un chemin à travers un intermédiaire avec des connexions ouvertes aux deux parties.

Tout comme les canaux de paiement peuvent mettre à l'échelle les paiements on-chain, les canaux d'état peuvent mettre à l'échelle toutes les transactions on-chain. Alors qu'un canal de paiement est limité à la gestion des soldes entre deux parties, un canal d'état est un accord sur un état arbitraire, permettant tout, d'un jeu d'échecs sans confiance à des applications décentralisées évolutives.

De manière similaire à un canal de paiement, les parties ouvrent un canal, échangent des signatures cryptographiques au fil du temps et soumettent un état final (ou un résultat) à un contrat intelligent on-chain. Le contrat intelligent exécutera alors en fonction de cette entrée, réglant la transaction en fonction des règles encodées dans le contrat.

Un "canaux d'état généralisés" est une construction de canal d'état puissante, permettant à un seul canal d'état de prendre en charge des transitions d'état sur plusieurs contrats intelligents. Cela réduit l'encombrement de l'état inhérent à une architecture de "un canal par application" et permet également une intégration facile en utilisant les canaux d'état que les utilisateurs ont déjà ouverts.

5.3 Side-chains

Une side-chain est une blockchain séparée qui est attachée à une blockchain sans confiance (main-chain) avec un peg bidirectionnel. Pour utiliser la side-chain, un utilisateur envoie des fonds à une adresse spécifiée sur la main-chain, verrouillant ces fonds sous le contrôle des opérateurs de la side-chain. Une fois que cette transaction est confirmée et qu'une période de sécurité a été respectée, une preuve peut être communiquée aux opérateurs de la side-chain détaillant le dépôt de fonds. Les opérateurs créeront ensuite une transaction sur la side-chain, distribuant les fonds appropriés. Ces fonds peuvent ensuite être dépensés sur la side-chain avec des frais peu élevés, une confirmation rapide et un débit élevé.

Le principal inconvénient des side-chains est qu'elles nécessitent des mécanismes de sécurité supplémentaires et des hypothèses de sécurité. La construction de side-chain la plus simple, une side-chain fédérée, place la confiance dans un groupe de plusieurs signatures d'opérateurs. Sur les plateformes de contrat intelligent, les modèles de sécurité peuvent être affinés avec des incitations en jetons ou des jeux économiques de mise en fonds/défi/sanction.

Comparées à d'autres solutions de mise à l'échelle générales hors chaîne, les side-chains sont plus faciles à comprendre et à mettre en œuvre. Pour les types d'applications qui permettent la création d'un modèle de confiance acceptable pour leurs utilisateurs, les side-chains peuvent être une solution pratique.

5.4 Commit-chains

Sur les commit-chains[6], telles que Plasma[7], une chaîne de couche de niveau 2 est construite qui tire parti d'une racine de confiance sur une blockchain de couche de niveau 1 (root-chain) avec un consensus mondial général. Ces commit-chains sont sécurisées; en cas de comportement malveillant ou dysfonctionnel de l'opérateur de la chaîne, les utilisateurs peuvent toujours retirer leurs actifs via un mécanisme sur la root-chain.

Un opérateur de commit-chain est chargé d'exécuter correctement les transactions et de publier des mises à jour périodiques sur la root-chain. Dans toutes les conditions, sauf en cas d'attaque prolongée de censure sur la root-chain, les actifs sur les commit-chains resteront en sécurité. De manière similaire aux side-chains fédérées, les designs de commit-chain offrent une expérience utilisateur supérieure par rapport aux blockchains sans confiance. Cependant, ils le font tout en maintenant des garanties de sécurité plus solides.

Le commit-chain est sécurisé par un ensemble de contrats intelligents fonctionnant sur la root-chain. Les utilisateurs déposent des actifs dans ce contrat et l'opérateur de commit-chain leur fournit ensuite des actifs sur la commit-chain. L'opérateur publiera périodiquement des engagements sur la root-chain, que les utilisateurs pourront ultérieurement utiliser pour prouver la propriété d'actifs grâce à des preuves de Merkle, une "sortie", dans laquelle les actifs de la commit-chain sont retirés vers la root-chain.

Cela décrit la notion générale de designs commit-chain, la base d'une famille émergente de protocoles, y compris Plasma. Le livre blanc Plasma[7] publié par Vitalik Buterin et Joseph

Poon en 2017 expose une vision ambitieuse. Bien que toutes les chaînes Plasma soient actuellement basées sur des actifs, et ne peuvent stocker que la propriété (et les transferts) de jetons fongibles et non fongibles, l'exécution de code sans confiance (ou smart contracts) est un domaine de recherche actif.

5.5 Calculs vérifiables hors chaîne

La cryptographie fournit un outil apparemment adapté à la dynamique de la vérification coûteuse sur chaîne et de la computation peu coûteuse hors chaîne : les systèmes de preuve interactive. Un système de preuve interactive est un protocole à deux participants, le prouveur et le vérificateur. En envoyant des messages aller-retour, le prouveur fournira des informations pour convaincre le vérificateur qu'une certaine affirmation est vraie, tandis que le vérificateur examinera ce qui est fourni et rejettera les fausses affirmations. Les affirmations que le vérificateur ne peut pas rejeter sont acceptées comme vraies.

La principale raison pour laquelle le vérificateur ne vérifie pas simplement l'affirmation naïvement de son côté est l'efficacité - en interagissant avec un prouveur, le vérificateur peut vérifier des affirmations qui seraient prohibitives à vérifier autrement. Cette différence de complexité peut venir de diverses sources : 1) le vérificateur peut exécuter du matériel léger qui ne peut prendre en charge que des calculs bornés en espace ou en temps (ou les deux), 2) la vérification naïve peut nécessiter l'accès à une longue séquence de choix non déterministes, 3) la vérification naïve peut être impossible car le vérificateur ne possède pas certaines informations secrètes.

Bien que la confidentialité des informations importantes soit certainement un facteur de contrainte pertinent dans le contexte des crypto-monnaies, un facteur de contrainte plus pertinent dans le contexte de la scalabilité est le coût de la vérification sur chaîne, en particulier par rapport à la computation relativement peu coûteuse hors chaîne.

Dans le contexte des crypto-monnaies, une attention significative a été portée aux zk-SNARKs (arguments de connaissance succincts non interactifs à zéro connaissance). Cette famille de systèmes de preuves non interactifs tourne autour du circuit arithmétique, qui encode un calcul arbitraire sous la forme d'un circuit d'additions et de multiplications sur un champ fini. Par exemple, le circuit arithmétique peut encoder "Je connais une feuille dans cet arbre de Merkle".

Les preuves zk-SNARK ont une taille constante (de l'ordre de centaines d'octets) et sont vérifiables en temps constant, bien que cette efficacité de vérification se fasse au prix d'une configuration de confiance et d'une chaîne de référence structurée, en plus de l'arithmétique basée sur des paires (dont la difficulté cryptographique concrète reste un sujet de préoccupation).

Les systèmes de preuve alternatifs offrent des compromis différents. Par exemple, Bulletproofs ne nécessitent pas de configuration de confiance et reposent sur l'hypothèse logarithmique de discrétion, mais ont des preuves de taille logarithmique (bien que toujours assez petites) et des vérificateurs en temps linéaire. Les zk-STARKs offrent une alternative aux zk-SNARKs en termes de scalabilité, sans configuration de confiance et ne reposent

que sur des hypothèses cryptographiques solides, bien que la preuve produite soit de taille logarithmique (et assez grande : des centaines de kilo-octets).

Dans le contexte d'un écosystème de crypto monnaies multi-couches tel que le réseau Nervos, les preuves interactives offrent la possibilité de décharger les calculs coûteux du côté prouveur vers la couche de niveau 2 tout en ne nécessitant qu'un travail modeste du côté Vérificateur de la couche de niveau 1. Cette intuition est capturée, par exemple, dans le protocole ZK Rollup de Vitalik Buterin[8] : un relai sans permission rassemble les transactions hors chaîne et met périodiquement à jour une racine Merkle stockée sur la chaîne. Chaque mise à jour de la racine est accompagnée d'un zk-SNARK qui montre que seules des transactions valides ont été accumulées dans le nouvel arbre Merkle. Un contrat intelligent vérifie la preuve et permet la mise à jour de la racine Merkle uniquement si la preuve est valide.

La construction décrite ci-dessus devrait être capable de prendre en charge des transitions d'état plus complexes au-delà des transactions simples, y compris les DEX, les jetons multiples et le calcul préservant la vie privée.

5.6 Modèle économique des solutions de couche de niveau 2

Bien que les solutions de couche de niveau 2 offrent une scalabilité impressionnante, les modèles économiques des jetons de ces systèmes peuvent poser des défis de conception.

Les économies de jetons de couche de niveau 2 peuvent impliquer une compensation pour l'infrastructure critique (telle que les validateurs et les watchtowers), ainsi que la conception d'incitation spécifique à l'application. L'infrastructure critique de la couche de niveau 2 tend à mieux fonctionner avec un modèle de durée, basé sur l'abonnement. Dans le réseau Nervos, cette structure de prix peut être facilement mise en œuvre grâce à la méthode de paiement basée sur le coût d'opportunité du CKB. Les fournisseurs de services peuvent collecter des frais sur les "dépôts" de leurs utilisateurs via le NervosDAO. Les développeurs de la couche de niveau 2 peuvent ensuite se concentrer sur les modèles économiques de jetons pour les incitations spécifiques à leurs applications.

De cette manière, ce modèle de tarification est exactement la façon dont les utilisateurs paient pour le stockage d'état sur le CKB. Ils paient essentiellement des frais d'abonnement aux mineurs avec la distribution de leurs récompenses d'inflation émises par le NervosDAO.

6. Le Réseau Nervos

6.1 La couche de niveau 1 en tant que plateforme de réserve de valeur multi-actifs

Nous croyons qu'un réseau blockchain de couche de niveau 1 doit être construit comme une réserve de valeur. Pour maximiser la décentralisation à long terme, il doit être basé sur un consensus de preuve de travail avec un modèle économique conçu autour de l'occupation de stockage d'état, plutôt que des frais de transaction. Le Common Knowledge Base (CKB)

est une blockchain multi-actifs de réserve de valeur basée sur la preuve de travail, avec à la fois des modèles de programmation et économiques conçus autour de l'état.

Le CKB est la couche de base du réseau Nervos, avec le plus haut niveau de sécurité et le plus haut degré de décentralisation. Posséder et effectuer des transactions d'actifs sur le CKB implique le coût le plus élevé, mais fournit le stockage d'actifs le plus sûr et le plus accessible du réseau et permet une composabilité maximale. Le CKB convient le mieux aux actifs de grande valeur et à la préservation à long terme des actifs.

Le Common Knowledge Base est la première blockchain de couche de niveau 1 construite spécifiquement pour prendre en charge les protocoles de couche de niveau 2:

- Le CKB est conçu pour compléter les protocoles de couche de niveau 2, en se concentrant sur la sécurité et la décentralisation, plutôt que sur les priorités de couche niveau 2 telles que la scalabilité.
- Le CKB modélise son registre autour de l'état, plutôt que des comptes. Les cellules sont essentiellement des objets d'état autonomes qui peuvent être référencés par des transactions et circuler entre les couches. Cela est idéal pour une architecture en couches, où les objets référencés et circulant entre les couches sont des morceaux d'état, plutôt que des comptes.
- Le CKB est conçu comme une machine de vérification généralisée, plutôt qu'un moteur de calcul. Cela permet au CKB de servir de tribunal cryptographique, qui vérifie les transitions d'état hors chaîne.
- Le CKB permet aux développeurs d'ajouter facilement des primitives cryptographiques personnalisées. Cela permet de préparer l'avenir du CKB, en permettant la vérification de preuves générées par une variété de solutions de couche de niveau 2.

Le Common Knowledge Base vise à être l'infrastructure pour stocker les connaissances communes les plus précieuses du monde, avec l'écosystème de couche de niveau 2 de classe mondiale offrant les transactions blockchain les plus évolutives et efficaces.

6.2 Scalabilité avec les solutions de couche de niveau 2

Avec son architecture en couches, le réseau Nervos peut évoluer à la couche de niveau 2 pour un nombre quelconque de participants, tout en maintenant les propriétés essentielles de la décentralisation et de la préservation des actifs. Les protocoles de couche de niveau 2 peuvent utiliser n'importe quel type d'engagement de couche de niveau 1 ou de primitive cryptographique, offrant ainsi une grande flexibilité et créativité dans la conception de systèmes transactionnels pour prendre en charge une base d'utilisateurs de couche de niveau 2 en croissance. Les développeurs de la couche de niveau 2 peuvent choisir leurs propres compromis en matière de débit, de finalité, de confidentialité et de modèles de confiance qui fonctionnent le mieux dans le contexte de leurs applications et de leurs utilisateurs.

Dans le réseau Nervos, la couche de niveau 1 (CKB) est utilisée pour la vérification de l'état, tandis que la couche de niveau 2 est responsable de la génération de l'état. Les canaux d'état et les side-chains sont des exemples de génération d'état, mais tout type de modèle

de génération-vérification est pris en charge, comme un cluster de génération de preuves à connaissance nulle. Les portefeuilles fonctionnent également à la couche de niveau 2, exécutant une logique arbitraire, générant un nouvel état et soumettant des transitions d'état au CKB pour validation. Les portefeuilles dans le réseau Nervos sont très puissants car ils sont des générateurs d'état, avec un contrôle total sur les transitions d'état.

Les side-chains sont conviviales pour les développeurs et offrent une bonne expérience utilisateur. Cependant, elles dépendent de l'honnêteté de leurs validateurs. Si les validateurs se comportent de manière malveillante, les utilisateurs risquent de perdre leurs actifs. Nervos Network fournit une pile de side-chain open-source et facile à utiliser pour lancer des side-chains sur le CKB, composée d'un framework blockchain Preuve d'enjeu (PoS) appelé "Muta" et d'une solution de side-chain basée sur celle-ci appelée "Axon".

Muta est un framework blockchain hautement personnalisable et haute performance conçu pour prendre en charge la preuve de participation, le consensus BFT et les contrats intelligents. Il dispose d'un consensus BFT haute capacité et faible latence appelé "Overlord", et prend en charge diverses machines virtuelles, notamment CKB-VM, EVM et WASM. Différentes machines virtuelles peuvent être utilisées simultanément dans une seule blockchain Muta, avec une interopérabilité entre les machines virtuelles. Muta réduit considérablement les barrières pour les développeurs pour construire des blockchains haute performance, tout en permettant une flexibilité maximale pour personnaliser leurs protocoles.

Axon est une solution complète construite avec Muta pour fournir aux développeurs une chaîne latérale clé en main sur le dessus de Nervos CKB, avec un modèle de sécurité pratique et économique basé sur un jeton. Les solutions d'Axon utilisent CKB pour la garde sécurisée des actifs, et utilisent un mécanisme de gouvernance basé sur un jeton pour gérer les validateurs de chaîne latérale. Des protocoles de chaîne croisée pour les interactions entre une chaîne latérale Axon et CKB, ainsi qu'entre les chaînes latérales Axon, seront également intégrés. Avec Axon, les développeurs peuvent se concentrer sur la construction d'applications, au lieu de construire des infrastructures et des protocoles de chaîne croisée.

Muta et Axon sont actuellement en cours de développement. Nous ouvrirons bientôt les frameworks, et les RFC pour Muta et Axon sont également en route.

Les protocoles de couche de niveau 2 sont un domaine florissant de recherche et de développement. Nous prévoyons un avenir dans lequel tous les protocoles de couche de niveau 2 sont normalisés et inter opèrent de manière transparente. Cependant, nous reconnaissons que les solutions de couche de niveau 2 sont encore en cours de maturation, et que nous repoussons souvent les limites de ce qu'elles peuvent faire, ainsi que de trouver leurs compromis acceptables. Nous avons vu des solutions prometteuses, mais il reste encore beaucoup de recherches à mener sur des sujets tels que l'interopérabilité, la sécurité et les modèles économiques dans les conceptions de la couche de niveau 2.

6.3 Durabilité

Dans l'intérêt de la durabilité à long terme, le “Common Knowledge Base” de Nervos limite l'état, impose un coût de stockage on-chain et offre des incitations aux utilisateurs pour qu'ils

effacent leur stockage d'état. Un état limité maintient les exigences de participation des nœuds complets faibles, garantissant que les nœuds peuvent fonctionner sur du matériel peu coûteux. Une participation robuste des nœuds complets accroît la décentralisation et, par conséquent, la sécurité.

En imposant un coût de "location d'état" proportionnel au temps sur le stockage d'état, le “Common Knowledge Base” de Nervos atténue la tragédie des communs à laquelle sont confrontées de nombreuses blockchains dans un paradigme "payer une fois, stocker pour toujours". Mis en œuvre via "l'inflation ciblée", ce mécanisme de location d'état offre une expérience utilisateur fluide tout en imposant un coût sur le stockage d'état.

Ce coût d'inflation peut être ciblé car les utilisateurs possèdent l'espace de consensus occupé par leurs données. Ce modèle comprend également un mécanisme natif permettant aux utilisateurs de supprimer leur état de l'espace de consensus. Associé aux incitations économiques de la location d'état, cela garantit que la taille de l'état se rapprochera toujours de la quantité minimale de données requises par les participants du réseau.

L'état individuellement possédé réduit également considérablement les coûts des développeurs. Au lieu d'être obligés d'acheter des CKBytes pour les besoins d'état de tous leurs utilisateurs, les développeurs n'ont à acheter que suffisamment de CKBytes pour stocker le code de vérification requis par leur application. Chaque utilisateur utiliserait ses propres cellules pour stocker ses jetons et serait entièrement responsable de ses actifs.

Enfin, la location d'état offre une récompense continue aux mineurs grâce à l'émission de nouveaux jetons. Ce revenu prévisible incite les mineurs à faire avancer la blockchain, plutôt que de créer des forks de blocs rentables pour prendre les frais de transaction.

6.4 Des mesures d'incitation alignées

Le modèle économique du “Common Knowledge Base” est conçu pour aligner les incitations de tous les participants de l'écosystème.

Le “Common Knowledge Base” de Nervos est construit explicitement pour la préservation sécurisée de la valeur, plutôt que pour les frais de transaction bon marché. Cette position critique attirera les utilisateurs de la réserve de valeur, semblables à la communauté d'utilisateurs de Bitcoin, plutôt que les utilisateurs de moyen d'échange.

Les cas d'utilisation de moyen d'échange ont tendance à toujours pousser un réseau blockchain vers la centralisation, à la poursuite d'une plus grande efficacité et de frais bas. Sans revenus significatifs des frais pour les opérateurs d'infrastructure qui sécurisent le réseau (mineurs ou validateurs), la sécurité doit être financée par l'inflation monétaire, ou est simplement sous-financée. L'inflation monétaire est préjudiciable aux détenteurs à long terme, et une sécurité sous-financée est préjudiciable à tous les parties prenantes du réseau.

Les utilisateurs de réserve de valeur ont cependant de fortes demandes en matière de résistance à la censure et de sécurité des actifs. Ils comptent sur les mineurs pour fournir cela, et en retour les compensent pour leur rôle. Dans un réseau de réserve de valeur, ces parties ont des intérêts alignés.

En alignant les incitations de tous les participants, une communauté Nervos unie peut croître, et le système économique aligné du réseau est également censé être résistant aux “hard-forks”.

6.5 Capture et génération de valeur

Pour qu'une blockchain reste sécurisée à mesure que la valeur des actifs sécurisés par la plateforme augmente, le système doit avoir un mécanisme pour capturer la valeur à mesure que la valeur des actifs sécurisés croît. En limitant l'état, le CKB fait de l'espace d'état une ressource rare et tarifée sur le marché. À mesure que la demande de stockage d'actifs sur le réseau augmente, le système devrait mieux rémunérer les mineurs pour sécuriser de tels actifs.

En tant que plateforme de préservation de valeur, la valeur intrinsèque du CKB en tant que plateforme est déterminée par la quantité de sécurité qu'il fournit aux actifs qu'il préserve. À mesure que la valeur des actifs sécurisés augmente, le mécanisme de capture de valeur du modèle économique du CKB est capable d'augmenter automatiquement le budget de sécurité du CKB pour attirer davantage de ressources minières, rendant la plateforme plus sûre. Non seulement cela est important pour rendre la plateforme durable, mais cela offre également un chemin de croissance pour la valeur intrinsèque de la plateforme - à mesure que la plateforme devient plus sûre, elle devient également plus attrayante pour les actifs de valeur supérieure, générant plus de demande. Évidemment, cela est limité par la valeur globale agrégée qui finira par se déplacer vers l'espace blockchain.

Au fil du temps, nous prévoyons que la densité économique du CKB augmentera. Les CKBytes seront utilisés pour le stockage d'actifs de grande valeur et les actifs de faible valeur se déplaceront vers des blockchains connectées au CKB, telles que des chaînes latérales de couche de niveau 2. Au lieu de sécuriser directement des actifs, le CKB peut être utilisé comme racine de confiance pour sécuriser l'écosystème entier d'une chaîne latérale, par exemple, à travers quelques centaines d'octets de preuves cryptographiques. La densité économique de telles preuves est extrêmement élevée, renforçant davantage la courbe de demande d'espace de stockage : analogue à une petite parcelle de terrain augmentant considérablement sa densité économique en soutenant un gratte-ciel.

Enfin, grâce à la conception de la NervosDAO et à sa fonction "refuge d'inflation", les détenteurs de jetons à long terme conserveront toujours un pourcentage fixe de l'émission totale, faisant du jeton natif lui-même une solide réserve de valeur.

6.6 Combler l'écart réglementaire

Les blockchains publiques sans permission permettent une décentralisation totale dans l'émission et la transaction d'actifs. C'est ce qui les rend précieuses, mais c'est aussi la raison pour laquelle elles ne sont pas compatibles avec les systèmes financiers et judiciaires du monde réel.

L'émergence d'une architecture en couche offre la possibilité de créer des parties conformes à la réglementation d'une blockchain sans permission ni réglementation. Par exemple, les utilisateurs peuvent stocker leurs actifs décentralisés sur la couche de niveau 1, bénéficier

d'une propriété absolue de ces actifs, et peuvent également traiter des affaires du monde réel sur la couche de niveau 2, où ils sont soumis à des contraintes réglementaires et juridiques.

Prenons l'exemple des échanges de crypto-monnaies - des pays comme le Japon et Singapour ont délivré des licences aux échanges et créé des exigences réglementaires. Un échange conforme ou une succursale d'un échange mondial pourrait construire une chaîne de trading de couche de niveau 2, importer des identités et des actifs d'utilisateurs et ensuite mener des affaires légales conformément aux exigences réglementaires locales.

L'émission et la transaction d'actifs du monde réel deviennent possibles dans une construction en couches de blockchain. Les actifs du monde réel peuvent affluer vers l'écosystème de la blockchain via une side-chain réglementée de couche de niveau 2 vers la blockchain de couche de niveau 1 sans permission, permettant à ces actifs d'accéder au plus grand écosystème de services financiers décentralisés composites.

À l'avenir, il est prévu que le réseau Nervos utilisera également des side-chains et des applications de couche de niveau 2 comme base pour l'adoption à grande échelle des utilisateurs, en coopération avec les principales entreprises de ce secteur.

Référence

[1] Satoshi Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System". 31 Oct 2008, https://bitcoin.org/bitcoin.pdf

[2] Vitalik Buterin. "Ethereum White Paper: A Next Generation Smart Contract & Decentralized Application Platform". Nov 2013 http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

[3] Avec une taille moyenne de transaction Bitcoin de 250 bytes : (2 * 250 * 7,500,000,000) / (24 * 6) = 26,041,666,666 blocs de byte (toutes les 10 minutes); 26,041,666,666 * (24 * 6) = 3,750,000,000,000 byte (croissance de la blockchain chaque jour); 3,750,000,000,000 * 365.25 = 1,369,687,500,000,000 byte (croissance de la blockchain chaque année)

[4] Gur Huberman, Jacob Leshno, Ciamac C. Moallemi. "Monopoly Without a Monopolist: An Economic Analysis of the Bitcoin Payment System". Bank of Finland Research Discussion Paper No. 27/2017. 6 Sep 2017, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3032375

[5] Miles Carlsten, Harry Kalodner, S. Matthew Weinberg, Arvind Narayanan. "On the Instabiliity of Bitcoin Without the Block Reward". Oct 2016, https://www.cs.princeton.edu/~smattw/CKWN-CCS16.pdf

[6] Lewis Gudgeon, Perdo Moreno-Sanchez, Stefanie Roos, Patrick McCorry, Arthur Gervais. "SoK: Off The Chain Transactions". 17 Apr 2019, https://eprint.iacr.org/2019/360.pdf

[7] Joseph Poon, Vitalik Buterin. "Plasma: Scalable Autonomous Smart Contracts". 11 Aug 2017, https://plasma.io/plasma.pdf

[8] Vitalik Buterin. "On-chain scaling to potentially ~500 tx/sec through mass tx validation". 22 Sep 2018, https://ethresear.ch/t/on-chain-scaling-to-potentially-500-tx-sec-through-mass-tx-validation/3477