LYRA Block Lattice

Feuille de route

Développeurs LYRA Block Lattice

Version 2.0

28 juin 2020

Basé sur la feuille de route originale rédigée le 7 janvier 2019 par Slava Gomzin

Objectifs principaux du LYRA Block Lattice

- Créez une plate-forme de paiement qui fournit des fonctionnalités de base « prêtes à l'emploi » des réseaux modernes de traitement des paiements, telles que la confidentialité, les autorisations en temps réel, la structure de frais conviviale, la prise en charge multidevise, les flux de transactions marchands spéciaux et les jetons marchands personnalisés Éliminez la dépendance à la Preuve de travail (POW)
- Fournit une scalabilité pratiquement illimitée pour permettre des taux TPS (transactions par seconde) compétitifs avec les réseaux de traitement de paiement « traditionnels » existants
- Éliminez un blocage prolongé des fonds dans les portefeuilles des utilisateurs (à la fois du payeur et du bénéficiaire) causé par l'attente de plusieurs « confirmations des blocs »
- Réduisez la latence du réseau qui affecte les délais d'autorisation des transactions aux niveaux acceptables par l'industrie du paiement
- Éliminez la dépendance à une seule, grande base de données blockchain en croissance continue
- Fournir des fonctionnalités bancaires ouvertes intégrées qui offriraient des avantages financiers à toutes les parties prenantes
- Découpler la plateforme de paiement de toute crypto-monnaie spécifique

Cas d'utilisation de base

Une fois qu'un utilisateur a créé un compte LYRA et déposé des fonds, il peut effectuer les actions suivantes:

Recevoir une part des revenus du traitement des transactions

Un utilisateur peut déléguer un vote pour le nœud d'autorisation de son choix et commencer à recevoir sa part des revenus de l'autorisateur payée à partir des frais de transaction traités par l'autorisateur.

Effectuer un paiement instantané et sans frais à un commerçant en ligne ou physique

Aucun frais n'est facturé à l'acheteur lors du paiement d'un marchand en utilisant le solde du compte LYRA. De plus, il n'y a pas de frais de réseau de crypto-monnaie car la crypto-monnaie est déjà déposée sur le compte LYRA.

Envoyer instantanément de la crypto ou de la monnaie fiduciaire à toute personne utilisant une adresse e-mail

Un code d'accès spécial à usage unique sera envoyé par e-mail à cette personne. Une fois le compte LYRA du destinataire créé, le transfert est terminé. Le destinataire peut utiliser le nouveau solde pour effectuer un paiement à un commerçant, ou transférer des fonds au sein du réseau LYRA, ou retirer de la crypto ou de la monnaie fiduciaire vers un portefeuille ou un compte externe.

Envoyez instantanément de la crypto ou de la monnaie fiduciaire à toute personne sans frais ou frais symboliques minimes

Les frais de transfert LYRA sont nettement inférieurs aux frais de réseau des principales crypto-monnaies. Les premières transactions sur les comptes LYRA peuvent ne nécessiter aucuns frais. Étant donné que la crypto ou la monnaie fiduciaire est déjà déposée sur le compte LYRA, il n'y a pas de frais de réseau de blockchain externe. Contrairement à une transaction blockchain typique, il n'est pas nécessaire d'attendre plusieurs minutes à plusieurs heures pour plusieurs confirmations car les fonds sont déjà déposés sur le compte LYRA et le transfert est effectué à l'intérieur du réseau LYRA.

Hébergez un nœud d'autorisation et gagnez des frais de traitement des transactions

Tout le monde peut devenir autorisateur en créant un nœud d'autorisation. L'autorisateur commence à recevoir des revenus après avoir reçu suffisamment de votes de la part des titulaires de compte LYRA pour passer en haut de la liste des autorisateurs.

Échangez instantanément des devises cryptographiques ou fiduciaires contre d'autres actifs numériques

Un utilisateur peut échanger son solde contre d'autres actifs numériques (pièces, jetons, « stablecoins », fiat) pris en charge par LYRA. Par exemple, un commerçant peut mettre en place un échange automatique des paiements reçus en Bitcoin ou autre crypto en monnaie fiduciaire (« stablecoins » représentant les devises fiduciaires déposées sur le compte LYRA) pour toujours obtenir des paiements en fiducie et éliminer tout effet de la volatilité cryptographique sur son entreprise.

Retirer le solde d’un portefeuille externe

Le solde du compte LYRA peut être retiré et envoyé à n'importe quel portefeuille externe, à tout moment. Ainsi, l'utilisateur peut utiliser son dépôt pour percevoir des revenus, mais le même dépôt peut être utilisé pour payer n'importe qui, à tout moment.

Recevez des paiements instantanés des clients

Un commerçant peut utiliser le point de vente LYRA pour recevoir des paiements instantanés en ligne ou dans des magasins physiques dans diverses devises fiat et crypto. Les paiements peuvent être convertis en une autre crypto de monnaie fiduciaire et stockés sur le compte marchand LYRA ou retirés à tout moment.

Créer un jeton personnalisé

Le jeton personnalisé LYRA peut être facilement créé par n'importe quel utilisateur en ajoutant un nouveau type de devise et en générant un bloc de genèse - aucun contrat intelligent n'est requis car divers types de jetons prédéfinis ont déjà des propriétés et des comportements adaptés à des fonctions particulières.

Principes

L'objectif principal de LYRA est de créer un système capable de transférer rapidement de l'argent de l'entité A vers l'entité B sans autorité centrale au milieu, c'est-à-dire d'effectuer des paiements instantanés inconditionnels et sans permission. Pour éliminer les fausses attentes dès le départ: un tel transfert n'est possible qu'avec de l'argent numérisé comme la crypto. Lorsqu'il s'agit d'un mode de paiement « traditionnel » (espèces, carte plastique, compte bancaire), il doit être numérisé (pour A) et dé-numérisé (pour B) à l'aide d'entités semi-centralisées ou décentralisées telles que les bourses ou les courtiers. À première vue, il s'agit d'une limitation sérieuse. Mais d'un point de vue historique, en supposant que la cryptographie remplacera les formes traditionnelles de gestion de l'argent, un tel système finira par devenir entièrement décentralisé.

Devises vs systèmes de paiement

Les gens confondent souvent monnaie et système de paiement. La monnaie est l'argent. Le système de paiement est un mécanisme qui permet à la devise de changer de propriétaire (transaction). Le dollar américain est la monnaie. L'euro est la monnaie. Les billets et pièces en dollars américains (espèces, billets de banque) sont un système de paiement qui permet des transactions en face à face. Visa et Mastercard sont des systèmes de paiement qui permettent des transactions électroniques sans espèces. PayPal est un système de paiement qui permet d'effectuer des transactions en ligne en toute sécurité. Bitcoin est une monnaie en ligne native (crypto-monnaie, ou simplement crypto), avec un système de paiement de base « intégré » qui permet de traiter les transactions Bitcoin en ligne. Il existe de nombreuses autres crypto-monnaies. Le monde n'a pas besoin d'une autre devise, mais il a besoin d'un système de paiement sans

autorisation, sécurisé, privé, rapide et pratique, capable de traiter les paiements et les transferts à la fois en ligne et dans les magasins physiques, dans diverses devises et crypto-monnaies. Seuls les systèmes de paiement décentralisés peuvent offrir une confidentialité absolue, une sécurité maximale et un accès sans discrimination aux acheteurs et aux commerçants. Sans parler du fait que seuls les systèmes de paiement décentralisés peuvent faire fonctionner des crypto-monnaies décentralisées sans réduire la valeur de leurs propriétés fondamentales.

Systèmes de paiement traditionnels vs crypto-monnaies

Les systèmes de paiement traditionnels fonctionnent avec les devises existantes et établies, ce qui leur permet de se concentrer uniquement sur le domaine du traitement des paiements. Les systèmes de paiement crypto, en plus des systèmes de paiement, ont le fardeau de prendre soin de leur propre devise sous-jacente - quelque chose qui est généralement pris en charge par les gouvernements nationaux, les banques ou d'énormes communautés telles que les Bitcoins et les sociétés financières. En conséquence - système de paiement peu pratique, lent et non sécurisé, ou monnaie illiquide et volatile, ou les deux.

Lyra vs systèmes de paiement traditionnels et crypto

Contrairement à d'autres crypto-monnaies, Lyra est un système de paiement pur qui n'a pas de devise ou de jeton sous-jacent « intégré ». Le jeton de démarrage spécial Lyra est créé et utilisé pour financer le développement initial et lancer les mécanismes de vote et d'autorisation de preuve de participation délégués lors de la phase initiale du projet. Comme les systèmes de paiement traditionnels, Lyra fonctionne avec les devises existantes, il est donc totalement exempt de politiques monétaires, de volatilité et d'autres problèmes non liés au domaine du traitement des paiements. En conséquence, Lyra présente des caractéristiques difficiles ou impossibles à atteindre avec des systèmes mono-crypto-monnaie: vitesse élevée, évolutivité pratiquement illimitée et polyvalence des méthodes de paiement. Ce qui le différencie des systèmes de paiement traditionnels, cependant, c'est la décentralisation, qui ouvre une boîte pandora de fonctionnalités inestimables: accès sans autorisation sans discrimination, sécurité, confidentialité, frais bas, économie participative ouverte, et plus encore.

PoW vs DPoS

L'émission continue et l'offre en croissance rapide de pièces « minables » contribuent à une forte volatilité de ces pièces. Une émission continue est nécessaire pour les blockchains de preuve de travail afin de les maintenir. Les mineurs reçoivent des incitations importantes sous forme de récompenses globales, même si le volume des transactions est insignifiant. Par conséquent, une blockchain exploitable devient «

rentable » même si elle n'assure pas une fonction de paiement significative. En l'absence de mineurs voraces, les systèmes de preuve d'enjeu peuvent être durables avec un approvisionnement constant. Les récompenses des autorisateurs devraient plutôt provenir des frais de transaction.

Concepts de conception

Nano a été la première crypto-monnaie à implémenter un système block lattice, où les transactions sont enregistrées dans des comptes individuels (blockchains) au lieu d'une seule blockchain centrale. [1] LYRA introduit un concept similaire où les transactions sont également enregistrées sur des chaînes individuelles mais les blocs d'envoi et de réception ne sont pas directement liés pour préserver la confidentialité.

Registre (Ledger)

Contrairement à la blockchain traditionnelle de type bitcoin, où toutes les transactions sont compilées en blocs dans une seule blockchain, le block lattice (introduit par Nano) est une collection de plusieurs blockchains. C'est pourquoi nous l'appelons également blocklist car c'est à quoi ressemble exactement la base de données des nœuds Lyra - une grande liste (collection en termes de base de données nosql) de blocs. Chaque compte utilisateur ajoute des transactions à sa propre blockchain. Une telle conception permet une évolutivité extrêmement élevée, une autorisation et des règlements instantanés, des clients ultra légers et de nombreuses autres fonctionnalités.

Transactions

Chaque utilisateur Lyra gère sa propre blockchain appelée compte. Chaque bloc contient une seule transaction. Le réseau ne maintient pas une seule chaîne de blocs, ce qui lui permet de traiter les transactions plus rapidement. La transaction Lyra consiste en des blocs d'envoi et de réception. L'application de portefeuille de l'expéditeur génère un bloc d'envoi et l'envoie aux nœuds d'autorisation pour autorisation. Une fois qu'un bloc d'envoi est autorisé par le quorum des autorisateurs, il est ajouté à la blockchain du compte de l'expéditeur. Lorsqu'un destinataire reçoit le bloc d'envoi autorisé diffusé, il génère le bloc de réception et l'envoie aux autorisateurs pour autorisation. Une fois autorisé, le bloc de réception est ajouté à la blockchain du compte destinataire (qui fait également partie de la chaîne de collecte). Par rapport au flux de traitement de paiement traditionnel, le traitement du bloc d'envoi est similaire à la phase d'autorisation, tandis que le bloc de réception correspond à la phase de règlement du traitement de la transaction de paiement. Cependant, une fois qu'un bloc d'envoi est accepté par le réseau, la transaction Lyra est considérée comme irréversible, avant même que le bloc de réception ne soit créé par le destinataire.

Consensus

Lyra sécurise son grand livre à l'aide d'un algorithme de consensus propriétaire basé sur les concepts de réseau de blocs (block lattice), de preuve d'enjeu déléguée et de tolérance aux pannes byzantine. Chaque concept contribue à la sécurité et aux performances du système. Chaque transaction Lyra est approuvée par un groupe de nœuds d'autorisation élus par un processus de vote. La transaction est considérée comme approuvée et définitive lorsqu'elle recueille les signatures de la très grande majorité (2⁄3 + 1) des principaux autorisateurs. Chaque transaction est située dans son propre bloc, les blocs étant enchaînés dans les chaînes de blocs de comptes individuels. Les nœuds d'autorisation communiquent de la manière la plus efficace car ils se « connaissent ». La combinaison de ces facteurs crée un processus d'autorisation hautement sécurisé et ultra rapide.

Preuve d'enjeu déléguée (Delegated Proof-of-Stake)

Plusieurs tentatives fructueuses ont été faites pour éliminer la preuve de travail et la remplacer entièrement par une preuve de participation. Plusieurs projets cryptographiques «de haut rang» (EOS, Tezos, Lisk, BitShares, Nano, Ark) ont mis en place une preuve de participation déléguée (DPOS), ou ont basé leur mécanisme de consensus sur les principes DPOS (Cardano). Dans DPOS, tous les participants peuvent voter pour quelques nœuds en déléguant leurs soldes de pièces aux nœuds en qui ils ont confiance. Plus le nœud reçoit de votes (plus le solde de mise) est élevé, plus sa position est élevée et plus la possibilité d'être élu comme nœud d'autorisation. Il est préférable que la monnaie de vote ait une offre limitée et soit équitablement répartie entre les participants au réseau. Les jetons Lyra seront utilisés comme jetons de vote. Les titulaires de compte peuvent voter pour un autorisateur en fonction du solde de leur compte. Chaque compte de vote est lié à un autorisateur particulier. Les dividendes proviennent des frais de transaction que l'autorisateur perçoit en participant au processus d'autorisation. De cette façon, tous les utilisateurs sont motivés à voter lorsqu'ils participent au partage de récompenses Lyra, i. e. les titulaires de comptes deviennent parties prenantes du système Lyra. Dans les systèmes de paiement centralisés traditionnels tels que Visa ou PayPal, les revenus sont reçus par la société propriétaire du réseau et une partie est distribuée aux actionnaires. Dans LYRA, tous les revenus sont partagés directement entre les autorisateurs et les titulaires de comptes de vote, sans bureaucratie d'entreprise au milieu.

Nœuds d'autorisation

Un nœud candidat qui reçoit plus de votes que n'importe quel nœud d'autorisation devient un autorisateur, tandis que l'autorisation avec le moins de votes revient au groupe de candidats. L'autorisation et les nœuds candidats reçoivent des récompenses (frais Tx). Nous suggérons de limiter le nombre de nœuds d'autorisation à 21 autorisateurs principaux. Les nœuds restants avec un solde de vote minimum deviennent des autorisateurs de sauvegarde.

Solution au verrouillage des fonds

La plupart des crypto-monnaies ont une période appelée « solde verrouillé », lorsque tout ou partie des fonds d'un portefeuille ne peuvent pas être utilisés pour de nouvelles transactions. Cela se produit après chaque transaction, que vous receviez un nouveau transfert ou que vous envoyiez des fonds à quelqu'un. De cette façon, la plupart des blockchains empêchent de dépenser des fonds situés dans des blocs qui ne sont pas encore « confirmés » par le réseau. Les blockchains de preuve de travail sont particulièrement sujets à ce problème car les blocs récents peuvent être « réécrits » par quelqu'un qui a plus de puissance de calcul. Une telle « fourchette » rend les transactions dans plusieurs blocs récents invalides quelques minutes voire quelques heures après avoir été initialement « acceptées » par le réseau et même ajoutées à une blockchain. Le problème d'équilibre bloqué est très gênant et empêche l'adoption par le grand public. Imaginez une situation où vous avez 1000 $ dans votre carte de paiement et que vous avez acheté quelque chose pour seulement 1 $ mais que vous ne pouvez pas utiliser la carte pendant une heure supplémentaire car le solde de la carte est verrouillé par votre banque. Lyra résout le problème de solde verrouillé, grâce à l'architecture en treillis de blocs (block lattice). Étant donné que chaque transaction est écrite dans son propre bloc et que chaque bloc de transaction est individuellement et instantanément autorisé par le réseau, il n'est pas nécessaire de verrouiller un solde pour éviter une double dépense. Une fois qu'un bloc de transaction est signé par les nœuds d'autorisation, il devient la partie d'une blockchain de compte immuable qui ne peut pas être modifiée. Le solde du compte devient utilisable juste après la réception de la réponse d'autorisation (pour toute transaction) du réseau.

Taille

Les blocs d'envoi et de réception contiennent le solde du compte mis à jour (pour le compte de l'expéditeur et du destinataire respectivement), ce qui permet l'élagage, c'est-à-dire que tous les nœuds n'ont pas à stocker toutes les chaînes, mais ne peuvent stocker que les derniers blocs. Ainsi, les portefeuilles et autres applications n'ont pas besoin de scanner l'ensemble de la blockchain pour récupérer le solde du compte actuel, ce qui permet des transactions financières en temps réel et réduit considérablement les exigences système en matière de processeur, de mémoire et d'espace disque. Cette fonctionnalité résout également le problème rencontré par la plupart des crypto-monnaies avec une seule blockchain - des bases de données de transactions en croissance continue, ce qui augmente continuellement le coût de fonctionnement de chaque nœud du réseau.

Scalabilité

Une grande Scalabilité est obtenue en utilisant une collection en chaîne de comptes individuels, où les transactions appartenant à différents comptes peuvent être ajoutées simultanément, sans qu'il soit nécessaire de les accumuler en blocs et de maintenir une seule chaîne continue de blocs. Ainsi, LYRA a

une Scalabilité pratiquement illimitée, qui n'est limitée que par les performances des nœuds d'autorisation, et peut atteindre des nombres de TPS (transactions par seconde) compétitifs avec les réseaux de traitement de paiement traditionnels.

Confidentialité

Les blocs d'envoi et de réception sont protégés à l'aide des méthodes définies dans la Feuille de route CryptoNote et ses améliorations ultérieures, telles que les paiements dissociables (également appelés adresses furtives) et les transactions confidentielles de « ring ». [2, 3] Les montants des transactions et les adresses du portefeuille sont masqués, c'est-à-dire qu'un observateur ne peut pas établir de lien entre l'expéditeur et le destinataire, ni déterminer les soldes des transactions et des comptes.

Transférer et payer les transactions

Bien que le transfert et le paiement soient tous deux des transactions de dépenses qui utilisent le même mécanisme décrit ci-dessus (blocs d'envoi / réception), ils sont traités d'une manière légèrement différente. Étant donné qu'une transaction Payante est destinée aux commerçants pour collecter les paiements de leurs clients en temps réel, elle est priorisée par rapport aux virements réguliers lorsqu'elle est traitée par le réseau.

Jetons personnalisés

Il y aura des codes réservés pour les jetons créés par les développeurs pour les principales devises crypto et fiat. D'autres codes peuvent être utilisés par n'importe quel utilisateur pour créer des jetons personnalisés tels que des chèques-cadeaux marchands ou des points de fidélité. Tous les jetons sont traités par les autorisateurs de la même manière, mais seules les notes réservées peuvent participer au processus de vote.

Les jetons LYRA peuvent être créés comme indiscernables (fongibles) ou uniques (non fongibles, personnalisés). En fait, il existe des utilisations pour les deux dans la plupart des applications, avec le passage de fongible à non fongible au moment de la rédemption. Exemple: jetons de récompense fongibles (en tant que points de fidélité accumulés) et jetons de réduction / cadeau non fongibles (en tant que mécanisme d'échange de récompenses de fidélité).

Applications de paiement spéciales

Transactions annulées, préautorisées et terminées

Le fait que chaque transaction LYRA se compose de deux blocs (envoyer et recevoir) permet des fonctionnalités très importantes qui ne sont pas disponibles sur la blockchain classique alors qu'elles sont largement utilisées par l'industrie des cartes de paiement depuis des années. Les transactions de paiement peuvent être acceptées par le destinataire (en générant un bloc de réception complémentaire) ou rejetées (en générant une transaction d'annulation spéciale).

LYRA peut également facilement mettre en œuvre des mécanismes de pré-autorisation et d'achèvement qui sont absolument nécessaires pour l'hôtellerie, les stations-service et d'autres segments de l'industrie du traitement des paiements.

Pre-auth / Complete est essentiellement un contrat intelligent codé en dur. La transaction de préautorisation est un bloc d'envoi de transaction de paiement avec un indicateur spécial. La préautorisation doit être suivie de Terminé, qui est une autre transaction émise par le commerçant avec le montant de la modification qui ne peut pas dépasser le montant initial de la préautorisation. Complete peut être émis avec un montant nul, ce qui signifie que le montant total de la préautorisation est facturé par le commerçant. Si Complete n'est pas émis par le marchand dans un intervalle de temps prédéfini (7 à 30 jours), le portefeuille de l'expéditeur peut émettre une transaction inversée annulant la préautorisation.

Cartes de paiement en plastique et portefeuille froid LYRA

Le fait que LYRA mette à jour le solde du compte courant pour chaque bloc / transaction permet une mise en œuvre très légère des cartes de dépenses. La carte à puce ne doit stocker qu'une seule transaction récente afin de pouvoir créer une nouvelle transaction de dépenses et suivre correctement le solde du compte. La carte n'a pas besoin d'utiliser une «aide» externe pour être en mesure de construire la transaction de dépenses car il n'y a toujours qu'une seule entrée (le solde récent) utilisée dans la transaction. En outre, la transaction entrante la plus récente (blocage de réception), si la carte est «bidirectionnelle», peut être facilement demandée via le terminal de paiement sans aucune violation de la confidentialité car tous les blocs / transactions du compte sont cryptés.

Conclusion

LYRA combine les meilleures idées et technologies actuellement disponibles dans l'industrie de l'espace cryptographique et du paiement, et les applique à l'espace du réseau de paiement financier. Compte tenu des limites du PoW et de la blockchain, DPoS et block lattice fournissent en fin de compte les meilleures fonctionnalités qui sont cruciales pour la plate-forme de paiement moderne.

Références

1. Nano: A Feeless Distributed Cryptocurrency Network. Colin LeMahieu. https://nano.org/en/whitepaper
2. CryptoNote V2.0. Nicolas van Saberhagen. https://cryptonote.org/whitepaper.pdf
3. Ring Confidential Transactions. Shen Noether, Adam Mackenzie and Monero Core Team. https://lab.getmonero.org/pubs/MRL-0005.pdf