LYRA Block Lattice

- ***Laporan Resmi***
- Pengembang LYRA Block Lattice
- Versi 2.0
- 28 Juni 2020
- Berdasarkan white paper asli yang ditulis pada 7 Januari 2019 oleh Slava Gomzin

Tujuan Utama dari LYRA Block Lattice

- Menciptakan platform pembayaran yang menyediakan fitur dasar "di luar kotak" dari jaringan pemrosesan pembayaran modern seperti privasi, otorisasi waktu nyata, struktur biaya yang ramah pembeli, dukungan multi-mata uang, aliran transaksi pedagang khusus, dan token pedagang khusus
- Menghilangkan ketergantungan pada Proof of Work
- Menyediakan skalabilitas yang hampir tidak terbatas untuk memungkinkan tarif TPS (transaksi per detik) bersaing dengan jaringan pemrosesan pembayaran "tradisional" yang ada
- Menghilangkan penguncian dana yang berkepanjangan di dompet pengguna (baik pembayar maupun penerima pembayaran) yang disebabkan oleh menunggu beberapa "konfirmasi blokir"
- Mengurangi latensi jaringan yang memengaruhi waktu otorisasi transaksi ke tingkat yang dapat diterima oleh industri pembayaran
- Menghilangkan ketergantungan pada database blockchain tunggal, besar, dan terus berkembang
- Menyediakan fitur perbankan terbuka bawaan yang akan memberikan keuntungan finansial bagi semua pemangku kepentingan
- Memisahkan platform pembayaran dari cryptocurrency tertentu

Permasalahan Penggunaan Dasar

Setelah pengguna membuat akun LYRA dan menyimpan dana, mereka dapat melakukan tindakan berikut:

Menerima pembagian hasil dari pemrosesan transaksi

Pengguna dapat mendelegasikan pemungutan suara untuk node pemberi otorisasi pilihan mereka dan mulai menerima bagi hasil mereka dari pendapatan pemberi otorisasi yang dibayar dari biaya transaksi yang diproses oleh pemberi otorisasi.

Melakukan pembayaran instan tanpa biaya ke pedagang online atau fisik

Tidak ada biaya yang dibebankan kepada pembeli saat membayar pedagang menggunakan saldo akun LYRA. Juga, tidak ada biaya jaringan cryptocurrency karena cryptocurrency sudah disimpan ke akun LYRA.

Kirim mata uang kripto atau fiat secara instan ke siapa pun yang menggunakan alamat email

Kode akses satu kali khusus akan dikirim ke email orang tersebut. Setelah akun LYRA penerima dibuat, transfer selesai. Penerima dapat menggunakan saldo baru untuk melakukan pembayaran ke pedagang, atau mentransfer dana dalam jaringan LYRA, atau menarik mata uang kripto atau fiat ke dompet atau akun eksternal.

Kirim mata uang kripto atau fiat secara instan kepada siapa pun dengan biaya nol atau biaya simbolis kecil

Biaya transfer LYRA secara signifikan lebih rendah daripada biaya jaringan cryptocurrency utama. Transaksi pertama di akun LYRA mungkin memerlukan biaya nol. Karena mata uang kripto atau fiat sudah disimpan ke akun LYRA, tidak ada biaya jaringan blockchain eksternal. Tidak seperti transaksi blockchain pada umumnya, tidak perlu menunggu beberapa menit hingga beberapa jam untuk beberapa konfirmasi karena dana sudah disimpan ke akun LYRA, dan transfer dilakukan di dalam jaringan LYRA.

Otorisasi node host dan dapatkan biaya pemrosesan transaksi

Siapa pun dapat menjadi pemberi otorisasi dengan menyiapkan node otorisasi. Pemberi otorisasi mulai menerima pendapatan setelah menerima cukup suara dari pemegang akun LYRA untuk pindah ke bagian atas daftar pemberi otorisasi.

Tukarkan mata uang kripto atau fiat secara instan ke aset digital lainnya

Seorang pengguna dapat menukar saldo mereka dengan aset digital lainnya (koin, token, stablecoin, fiat) yang didukung oleh LYRA. Misalnya, pedagang dapat mengatur pertukaran pembayaran otomatis yang diterima dalam Bitcoin atau kripto lainnya ke dalam mata uang fiat (stablecoin mewakili mata uang fiat yang disimpan ke akun LYRA) untuk selalu mendapatkan pembayaran dalam bentuk fiat dan menghilangkan efek volatilitas kripto pada bisnisnya.

Tarik saldo ke dompet eksternal

Saldo di akun LYRA dapat ditarik dan dikirim ke dompet eksternal mana saja, kapan saja. Dengan demikian, pengguna dapat menggunakan deposit mereka untuk mengumpulkan pendapatan, tetapi deposit yang sama dapat digunakan untuk membayar siapa saja, kapan saja.

Terima pembayaran instan dari pelanggan

Pedagang dapat menggunakan tempat penjualan LYRA untuk menerima pembayaran instan online atau di toko fisik dalam berbagai mata uang fiat dan kripto. Pembayaran dapat dikonversi ke kripto mata uang fiat lain dan disimpan di akun pedagang LYRA atau ditarik kapan saja.

Membuat token khusus

Token khusus LYRA dapat dengan mudah dibuat oleh pengguna mana pun dengan menambahkan jenis mata uang baru dan menghasilkan blok genesis - tidak diperlukan kontrak pintar karena berbagai jenis token yang telah ditentukan sebelumnya sudah memiliki properti dan perilaku yang disesuaikan untuk fungsi tertentu.

Prinsip

Tujuan utama LYRA adalah menciptakan sistem yang mampu mentransfer uang dengan cepat dari entitas A ke entitas B tanpa otoritas pusat di tengah, yaitu melakukan pembayaran instan tanpa syarat, tanpa izin. Untuk menghilangkan ekspektasi palsu dari awal: transfer seperti itu hanya mungkin dilakukan dengan uang digital seperti crypto. Kapan pun bentuk pembayaran "tradisional" terlibat (tunai, kartu plastik, rekening bank), itu harus didigitalkan (untuk A) dan dide-digitalisasi (untuk B) menggunakan entitas semi-tersentralisasi atau desentralisasi seperti bursa atau pialang. Sekilas, ini adalah batasan yang serius. Tetapi melihat dari perspektif historis, dengan asumsi krypto akan menggantikan bentuk penanganan uang tradisional, sistem seperti itu pada akhirnya akan menjadi sepenuhnya terdesentralisasi.

Mata Uang vs Sistem Pembayaran

Sebagian orang merasa bingung untuk membedakan antara mata uang dan sistem pembayaran. Mata uang adalah Uang. Sistem Pembayaran adalah mekanisme yang memungkinkan mata uang untuk berganti pemilik (bertransaksi). Dolar AS adalah mata uang. Euro adalah mata uang. Uang kertas dan koin dolar AS (uang tunai, uang kertas) adalah sistem pembayaran yang memungkinkan transaksi tatap muka. Visa dan Mastercard adalah sistem pembayaran yang memungkinkan transaksi elektronik non tunai. PayPal adalah sistem pembayaran yang memungkinkan untuk bertransaksi online dengan aman. Bitcoin adalah mata uang online asli (cryptocurrency, atau hanya crypto), dengan sistem pembayaran "built-in" dasar yang memungkinkan untuk memproses transaksi Bitcoin secara online. Ada banyak kripto lain yang ada. Dunia tidak membutuhkan mata uang lain, tetapi ia membutuhkan sistem pembayaran tanpa izin, aman, pribadi, cepat, dan nyaman yang akan dapat memproses pembayaran dan transfer baik secara online maupun di toko fisik, dalam berbagai mata uang dan cryptocurrency. Hanya sistem pembayaran terdesentralisasi yang dapat memberikan privasi mutlak, keamanan tertinggi, dan akses tanpa pandang bulu ke pembeli dan pedagang. Belum lagi fakta bahwa hanya sistem pembayaran terdesentralisasi yang dapat mengoperasikan cryptocurrency terdesentralisasi tanpa mengurangi nilai properti fundamentalnya.

Sistem Pembayaran Tradisional vs Cryptocurrency

Sistem pembayaran tradisional beroperasi dengan mata uang yang sudah ada dan mapan, yang memungkinkan mereka untuk fokus hanya pada domain pemrosesan pembayaran. Sistem pembayaran Crypto, selain sistem pembayaran, memiliki beban untuk menjaga mata uang mereka sendiri - sesuatu yang biasanya diurus oleh pemerintah nasional, bank, atau komunitas

besar seperti Bitcoin dan perusahaan keuangan. Akibatnya - sistem pembayaran yang tidak nyaman, lambat, tidak aman, atau tidak likuid, mata uang yang tidak stabil, atau keduanya.

Lyra vs Sistem Pembayaran Tradisional dan Crypto

Tidak seperti crypto lainnya, Lyra adalah sistem pembayaran murni yang tidak memiliki mata uang atau token yang mendasari "built-in". Token Pemula Lyra Khusus dibuat dan digunakan untuk mendanai pengembangan awal dan memulai pemungutan suara dan mekanisme otorisasi bukti kepemilikan yang didelegasikan pada tahap awal proyek. Seperti sistem pembayaran tradisional, Lyra beroperasi dengan mata uang yang ada, jadi Lyra benar-benar bebas dari kebijakan moneter, volatilitas, dan masalah lain yang tidak terkait dengan domain pemrosesan pembayaran. Hasilnya, Lyra memiliki karakteristik yang sulit atau tidak mungkin dicapai menggunakan sistem mono-cryptocurrency: kecepatan tinggi, skalabilitas yang hampir tidak terbatas, dan keserbagunaan metode pembayaran. Apa yang membedakannya dari sistem pembayaran tradisional, bagaimanapun, adalah desentralisasi, yang membuka kotak pandora fitur tak ternilai: akses tanpa izin tanpa pandang bulu, keamanan, privasi, biaya rendah, partisipasi ekonomi terbuka, dan banyak lagi.

PoW vs DPoS

Emisi yang terus-menerus dan pasokan koin "yang dapat ditambang" yang berkembang pesat berkontribusi pada volatilitas yang tinggi dari koin-koin tersebut. Emisi berkelanjutan diperlukan untuk blockchain proof-of-work agar tetap berjalan. Para penambang menerima insentif yang signifikan dalam bentuk hadiah blok, meskipun volume transaksi tidak signifikan. Oleh karena itu, blockchain yang dapat ditambang menjadi "menguntungkan" meskipun tidak memiliki fungsi pembayaran yang signifikan. Dengan tidak adanya penambang yang rakus, sistem bukti kepemilikan dapat berkelanjutan dengan pasokan yang konstan. Hadiah dari pengotorisasi seharusnya diterima dari biaya transaksi.

Konsep Desain

Nano adalah mata uang kripto pertama yang menerapkan kisi blok, di mana transaksi dicatat dalam akun individu (blockchain), bukan di blockchain pusat tunggal. [1] LYRA memperkenalkan konsep serupa di mana transaksi juga dicatat pada rantai individu tetapi blok kirim dan terima tidak ditautkan secara langsung untuk menjaga privasi.

Ledger

Tidak seperti blockchain seperti bitcoin tradisional, di mana semua transaksi dikompilasi dalam blok dalam satu blockchain, kisi blok (diperkenalkan oleh Nano) adalah kumpulan dari banyak blockchain. Itulah mengapa kami juga menyebutnya daftar blokir karena seperti itulah tepatnya database node Lyra - daftar besar (kumpulan dalam istilah database nosql) blok. Setiap akun pengguna menambahkan transaksi ke blockchain mereka sendiri. Desain seperti itu memungkinkan skalabilitas yang sangat tinggi, otorisasi dan penyelesaian instan, klien super ringan, dan banyak fitur lainnya.

Transaksi

Setiap pengguna Lyra memiliki blockchain sendiri yang disebut akun. Setiap blok berisi satu transaksi. Jaringan tidak memelihara satu rantai blok, yang memungkinkannya memproses transaksi lebih cepat. Transaksi Lyra terdiri dari blok kirim dan terima. Aplikasi dompet pengirim menghasilkan blok pengiriman dan mengirimkannya ke node otorisasi untuk otorisasi. Setelah blok pengiriman diotorisasi oleh kuorum pemberi otorisasi, blok tersebut ditambahkan ke blockchain akun pengirim. Ketika penerima menerima blok kirim resmi yang disiarkan, itu menghasilkan blok terima dan mengirimkannya ke otorisasi untuk otorisasi. Setelah diotorisasi, blok penerima ditambahkan ke blockchain akun penerima (yang juga merupakan bagian dari koleksi rantai). Dibandingkan dengan aliran pemrosesan pembayaran tradisional, pemrosesan blok kirim mirip dengan fase otorisasi, sedangkan blok terima sesuai dengan fase penyelesaian dari pemrosesan transaksi pembayaran. Namun, setelah blok kirim diterima oleh jaringan, transaksi Lyra dianggap tidak dapat diubah, bahkan sebelum blok terima dibuat oleh penerima.

Konsensus

Lyra mengamankan ledger menggunakan algoritme konsensus berpemilik berdasarkan konsep kisi blok, Bukti Pasak yang Didelegasikan, dan Toleransi Kesalahan Bizantium. Setiap konsep berkontribusi pada keamanan dan kinerja sistem. Setiap transaksi Lyra disetujui oleh sekelompok node otorisasi yang dipilih melalui proses pemungutan suara. Transaksi dianggap disetujui dan final ketika mengumpulkan tanda tangan dari supermajority (2⁄3 + 1) dari pemberi otorisasi utama. Setiap transaksi terletak di bloknya sendiri, dengan blok yang dirangkai ke dalam blokir akun individu. Node authorizer berkomunikasi dengan cara yang paling efisien

karena mereka “mengenal” satu sama lain. Kombinasi dari faktor-faktor ini menciptakan proses otorisasi yang sangat aman dan super cepat.

Proof-of-Stake yang Didelegasikan

Beberapa upaya yang berhasil telah dilakukan untuk menghilangkan proof-of-work dan menggantinya sepenuhnya dengan proof-of-stake. Beberapa proyek crypto “peringkat tinggi” (EOS, Tezos, Lisk, BitShares, Nano, Ark) telah menerapkan bukti kepemilikan yang didelegasikan (DPOS), atau mendasarkan mekanisme konsensus mereka pada prinsip DPOS (Cardano). Di DPOS semua peserta dapat memilih beberapa node dengan mendelegasikan saldo koin mereka ke node yang mereka percaya. Semakin banyak suara (semakin besar saldo saham) yang diterima node, semakin tinggi posisinya dan kemungkinan untuk dipilih sebagai node yang berwenang. Lebih disukai bahwa mata uang pemungutan suara memiliki persediaan yang terbatas dan didistribusikan secara adil di antara peserta jaringan. Token Lyra akan digunakan sebagai token pemungutan suara. Pemegang akun dapat memilih pemberi otorisasi berdasarkan saldo akun mereka. Setiap akun pemungutan suara ditautkan ke otorisasi tertentu. Dividen berasal dari biaya transaksi yang diperoleh otorisasi dengan berpartisipasi dalam proses otorisasi. Dengan cara ini, semua pengguna termotivasi untuk memilih saat mereka berpartisipasi dalam berbagi hadiah Lyra, i. e. pemegang akun menjadi pemangku kepentingan sistem Lyra. Dalam sistem pembayaran terpusat tradisional seperti Visa atau PayPal, pendapatan diterima oleh perusahaan yang memiliki jaringan, dan sebagian didistribusikan ke pemegang saham. Di LYRA, semua pendapatan dibagikan langsung antara pemberi otorisasi dan pemegang akun pemungutan suara, tanpa birokrasi perusahaan di tengahnya.

Node Otorisasi

Node kandidat yang menerima suara lebih banyak daripada node pemberi otorisasi menjadi pemberi otorisasi, sedangkan pemberi otorisasi dengan suara paling sedikit kembali ke grup kandidat. Node otorisasi dan kandidat menerima hadiah (biaya Tx). Kami menyarankan untuk membatasi jumlah node pemberi otorisasi menjadi 21 pemberi otorisasi utama. Node yang tersisa dengan saldo voting minimum menjadi otorisasi cadangan.

Locked Balance Solution

Sebagian besar cryptocurrency memiliki periode waktu yang disebut "locked balance", ketika sebagian atau seluruh dana di dompet tidak dapat digunakan untuk transaksi baru. Itu terjadi

setelah setiap transaksi tidak peduli apakah Anda menerima transfer baru atau mengirim dana ke seseorang. Dengan cara ini sebagian besar blockchain mencegah pengeluaran dana yang terletak di blok yang belum "dikonfirmasi" oleh jaringan. Blockchain bukti kerja sangat rentan terhadap masalah ini karena blok terbaru dapat "ditulis ulang" oleh seseorang yang memiliki lebih banyak daya komputasi. "Fork" seperti itu membuat transaksi di beberapa blok baru-baru ini menjadi tidak valid, beberapa menit atau bahkan beberapa jam setelah awalnya "diterima" oleh jaringan dan bahkan ditambahkan ke blockchain. Masalah keseimbangan terkunci sangat merepotkan dan mencegah adopsi oleh arus utama. Bayangkan sebuah situasi ketika Anda memiliki $ 1000 di kartu pembayaran Anda dan Anda membeli sesuatu hanya dengan $ 1 tetapi tidak dapat menggunakan kartu tersebut selama satu jam lagi karena seluruh saldo kartu dikunci oleh bank Anda. Lyra memecahkan masalah keseimbangan terkunci, berkat arsitektur blok kisi. Karena setiap transaksi ditulis ke dalam bloknya sendiri, dan setiap blok transaksi secara individual dan langsung diotorisasi oleh jaringan, tidak perlu mengunci saldo untuk mencegah pembelanjaan ganda. Setelah blok transaksi ditandatangani oleh node otorisasi, itu menjadi bagian dari blockchain akun yang tidak dapat diubah yang tidak dapat dimodifikasi. Saldo akun menjadi dapat dihabiskan segera setelah respons otorisasi (untuk setiap transaksi) diterima dari jaringan.

Pemangkasan

Blok kirim dan terima berisi saldo akun yang diperbarui (masing-masing untuk akun pengirim dan penerima), yang memungkinkan pemangkasan, yaitu semua node tidak harus menyimpan seluruh rantai tetapi hanya dapat menyimpan blok terakhir. Karenanya, dompet dan aplikasi lain tidak perlu memindai seluruh blockchain untuk mengambil saldo akun saat ini, yang memungkinkan transaksi keuangan waktu nyata dan secara dramatis mengurangi persyaratan sistem untuk CPU, memori, dan ruang disk. Fitur ini juga memecahkan masalah yang dialami oleh sebagian besar crypto dengan blockchain tunggal - database transaksi yang terus berkembang, yang terus meningkatkan biaya operasi setiap node jaringan.

Skalabilitas

Skalabilitas tinggi dicapai dengan menggunakan kumpulan berantai dari akun individu, di mana transaksi milik akun yang berbeda dapat ditambahkan secara bersamaan, tanpa perlu mengakumulasikannya dalam blok dan mempertahankan rantai blok tunggal yang berkelanjutan. Dengan demikian, LYRA memiliki skalabilitas yang hampir tidak terbatas, yang hanya dibatasi oleh kinerja node otorisasi, dan dapat mencapai angka TPS (transaksi per detik) yang bersaing dengan jaringan pemrosesan pembayaran tradisional.

Privasi

Blok kirim dan terima dilindungi dengan menggunakan metode yang ditentukan dalam kertas putih CryptoNote dan peningkatan berikutnya, seperti pembayaran yang tidak dapat ditautkan (alias alamat tersembunyi) dan transaksi rahasia cincin. [2, 3] Jumlah transaksi dan alamat dompet dikaburkan, yaitu pengamat tidak dapat membuat hubungan antara pengirim dan penerima, atau menentukan transaksi dan saldo rekening.

Transfer dan membayar Transaksi

Meskipun Transfer dan Pembayaran adalah transaksi pengeluaran yang menggunakan mekanisme yang sama seperti yang dijelaskan di atas (kirim / terima blok), keduanya diproses dengan cara yang sedikit berbeda. Karena transaksi Bayar dimaksudkan agar pedagang mengumpulkan pembayaran dari pelanggan mereka secara real time, itu diprioritaskan daripada transfer biasa saat diproses oleh jaringan.

Custom Tokens

Akan ada kode yang dipesan untuk token yang dibuat oleh pengembang untuk mata uang kripto dan fiat utama. Kode lain dapat digunakan oleh pengguna mana pun untuk membuat token khusus seperti sertifikat hadiah pedagang atau poin hadiah loyalitas. Semua token diproses oleh otorisasi dengan cara yang sama, tetapi hanya catatan yang dipesan yang dapat berpartisipasi dalam proses pemungutan suara.

Token LYRA dapat dibuat sebagai tidak dapat dibedakan (sepadan) atau unik (tidak dapat dipertukarkan, dipersonalisasi). Faktanya, ada kegunaan untuk keduanya di dalam sebagian besar aplikasi, dengan transisi dari yang dapat dipertukarkan menjadi tidak dapat dipertukarkan pada saat penukaran. Contoh: token hadiah yang dapat dipertukarkan (sebagai poin loyalitas yang terkumpul) dan token diskon / hadiah yang tidak dapat dipertukarkan (sebagai mekanisme penebusan hadiah loyalitas).

Aplikasi Pembayaran Khusus

Membatalkan, Pre-Auth, dan Menyelesaikan Transaksi

Fakta bahwa setiap transaksi LYRA terdiri dari dua blok (kirim dan terima) memungkinkan fungsionalitas yang sangat penting yang tidak tersedia di blockchain biasa sementara banyak digunakan oleh industri kartu pembayaran selama bertahun-tahun. Transaksi pembayaran dapat diterima oleh penerima (dengan menghasilkan blok Penerimaan tambahan) atau ditolak (dengan membuat transaksi Void khusus).

LYRA juga dapat dengan mudah menerapkan mekanisme pra-otorisasi dan penyelesaian yang mutlak diperlukan untuk perhotelan, pompa bensin, dan segmen lain dari industri pemrosesan pembayaran.

Pra-autentikasi / Selesai pada dasarnya adalah kontrak pintar dengan kode keras. Transaksi pra-auth adalah blok kirim transaksi Pay dengan bendera khusus. Pra-otorisasi harus diikuti dengan Selesai, yang merupakan transaksi lain yang dikeluarkan oleh pedagang dengan jumlah perubahan yang tidak boleh melebihi jumlah pra-otorisasi awal. Selesai dapat diterbitkan dengan jumlah nol yang berarti bahwa seluruh jumlah pra-otorisasi ditagih oleh pedagang. Jika Selesai tidak dikeluarkan oleh pedagang dalam interval waktu yang telah ditentukan (7-30 hari), dompet pengirim dapat mengeluarkan transaksi terbalik yang membatalkan pra-otorisasi.

LYRA Plastic Payment dan Cold Wallet Cards

Fakta bahwa LYRA memperbarui saldo akun saat ini untuk setiap blok / transaksi memungkinkan penerapan kartu pengeluaran yang sangat ringan. Kartu pintar harus menyimpan hanya satu transaksi terakhir untuk dapat membuat transaksi pengeluaran baru dan melacak saldo akun dengan benar. Kartu tidak perlu menggunakan "bantuan" eksternal untuk dapat membangun transaksi pengeluaran karena selalu hanya ada satu input (saldo terkini) yang digunakan dalam transaksi. Selain itu, transaksi masuk terbaru (blok penerimaan), jika kartunya "dua arah", dapat dengan mudah diminta melalui terminal pembayaran tanpa pelanggaran privasi karena semua blok / transaksi akun dienkripsi.

Kesimpulan

LYRA menggabungkan ide dan teknologi terbaik yang saat ini tersedia di ruang crypto dan industri pembayaran, dan menerapkannya ke ruang jaringan pembayaran keuangan. Mengingat

keterbatasan PoW dan blockchain, DPoS dan block lattice pada akhirnya memberikan fitur terbaik yang sangat penting untuk platform pembayaran modern.

Referensi

Nano: Jaringan Cryptocurrency Terdistribusi Feeless. Colin LeMahieu. https://nano.org/en/whitepaper

CryptoNote V2.0. Nicolas van Saberhagen. https://cryptonote.org/whitepaper.pdf

Deringkan Transaksi Rahasia. Shen Noether, Adam Mackenzie dan Monero Core Team. https://lab.getmonero.org/pubs/MRL-0005.pdf