Radiant: Sistem Aset Digital Peer-to-Peer

11 Agustus 2022
radianblockchain.org
Translated By Chris45

Abstrak. Jaringan Radiant adalah sistem aset digital peer-to-peer yang memungkinkan pertukaran nilai secara langsung tanpa melalui pihak pusat. Protokol asli Bitcoin[1] menyediakan apa yang diperlukan untuk membuat sistem kas elektronik peer-to-peer, tetapi tidak memiliki kemampuan untuk memverifikasi riwayat transaksi dan oleh karena itu, tidak dapat digunakan untuk memvalidasi aset digital. Tanda tangan digital dan batasan keluaran memberikan bagian dari solusi, tetapi manfaat utama hilang jika pihak ketiga yang tepercaya masih diperlukan untuk memvalidasi aset digital. Mirip dengan Bitcoin, jaringan Radiant membutuhkan struktur minimal, dan mencatat waktu transaksi ke dalam rantai bukti kerja berbasis hash yang sedang berlangsung. Kami memperkenalkan dua teknik untuk memvalidasi aset digital: referensi unik dan sistem bukti induksi tujuan umum yang keduanya beroperasi dalam ruang dan waktu O(1) konstan. Dimungkinkan untuk menyusun output dengan cara apa pun, tanpa mengorbankan karakteristik paralelisme dan kinerja yang melekat dari arsitektur berbasis output transaksi yang tidak terpakai (UTXO). Oleh karena itu, pengguna dapat keluar dan bergabung kembali dengan jaringan Radiant sesuka hati dan yakin akan integritas dan keaslian aset digital mereka.

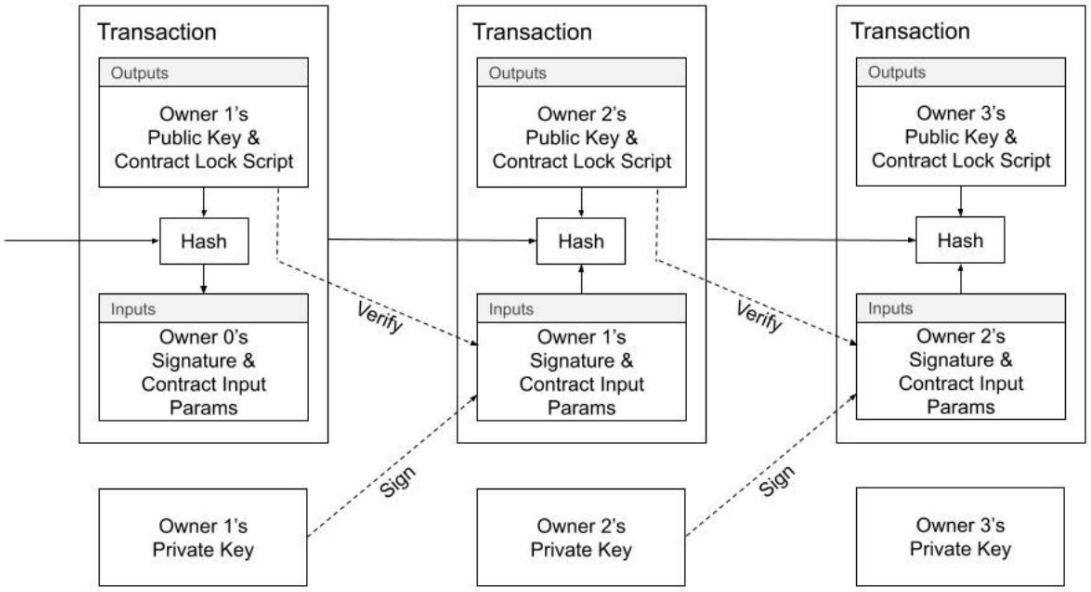
1. Perkenalan

Perdagangan dengan blockchain, atau teknologi buku besar digital (DLT), dalam banyak kasus bergantung pada penerbit dan kustodian yang berfungsi sebagai pihak tepercaya untuk mengautentikasi aset digital. Sementara sistem tersebut bekerja cukup baik untuk transaksi seperti pembayaran elektronik, mereka masih menderita kelemahan yang melekat pada model berbasis kepercayaan untuk tingkat lanjut menggunakan. Blockchain berbasis Ethereum Virtual Machine (EVM) [2] sangat fleksibel untuk semua jenis program, tetapi biaya tinggi membuat penggunaan aplikasi pembayaran mikro menjadi tidak praktis.

Yang dibutuhkan adalah sistem pembayaran elektronik yang dapat digunakan untuk sistem manajemen aset digital dengan biaya rendah, kinerja tinggi, dan kemampuan pemrograman tingkat lanjut. Dalam makalah ini, kami mengusulkan solusi untuk masalah penskalaan dan kontrak blockchain menggunakan dua teknik baru yang memberikan referensi unik dan sistem bukti induksi umum, yang membuat program Turing Complete [3] melintasi batas transaksi menjadi mungkin. Sistem yang diusulkan terdesentralisasi, menggunakan mekanisme konsensus proof-of-work seperti Bitcoin, tetapi dengan tingkat throughput yang jauh lebih tinggi, sambil memberikan fleksibilitas yang sama dari blockchain berbasis EVM, dengan biaya yang sangat rendah.

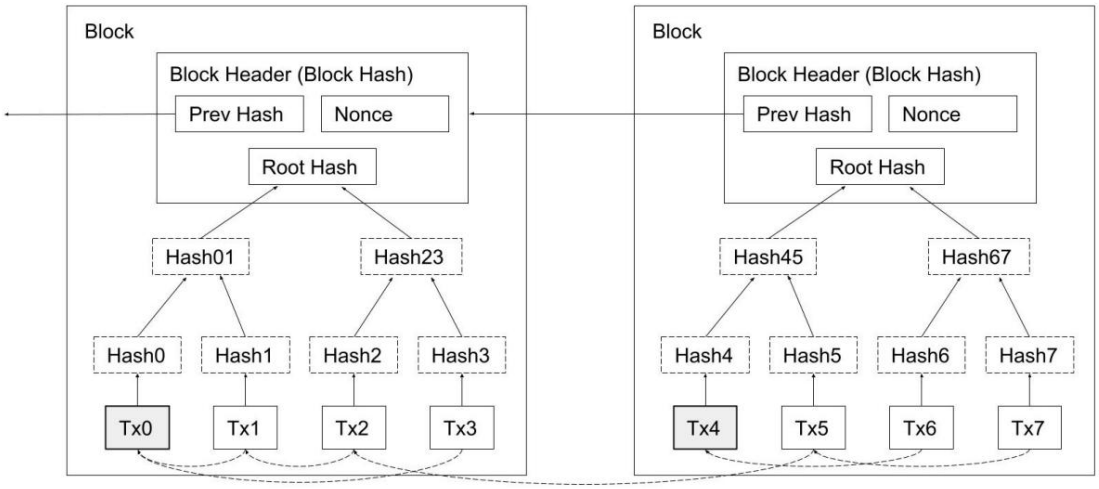
2. Transaksi

Mirip dengan Bitcoin, kami mendefinisikan koin elektronik sebagai rangkaian tanda tangan digital. Di mana transaksi di Radiant berbeda adalah bahwa setiap pemilik mentransfer koin ke yang berikutnya dengan menandatangani hash secara digital dari transaksi sebelumnya selain parameter input yang diperlukan untuk membuka kunci koin. Sebuah transaksi juga menciptakan kendala penguncian keluaran baru, yang mungkin termasuk kunci publik dari pemilik berikutnya, di antara aturan lain yang ditentukan oleh pengguna.



> Diagram 1. Transaksi Radiant.

Untuk memverifikasi bahwa pembelanjaan ganda tidak terjadi, kami menggunakan server timestamp terdistribusi, menggunakan sistem proof-of-work berbasis hash untuk mengatur riwayat kanonis guna menentukan transaksi mana yang tiba lebih dulu. Transaksi diatur ke dalam blok. Sesuai kesepakatan, transaksi pertama, yang disebut "transaksi berbasis koin", dalam sebuah blok adalah transaksi khusus yang memulai koin baru yang dimiliki oleh pembuat blok. Blok dirantai bersama dan mengatur transaksi menjadi Pohon Merkle [4]. Semua transaksi, kecuali yang pertama, harus mengacu pada transaksi sebelumnya yang membentuk grafik asiklik terarah (DAG) di mana semua koin pada akhirnya terhubung kembali ke setidaknya satu transaksi khusus di awal blok.



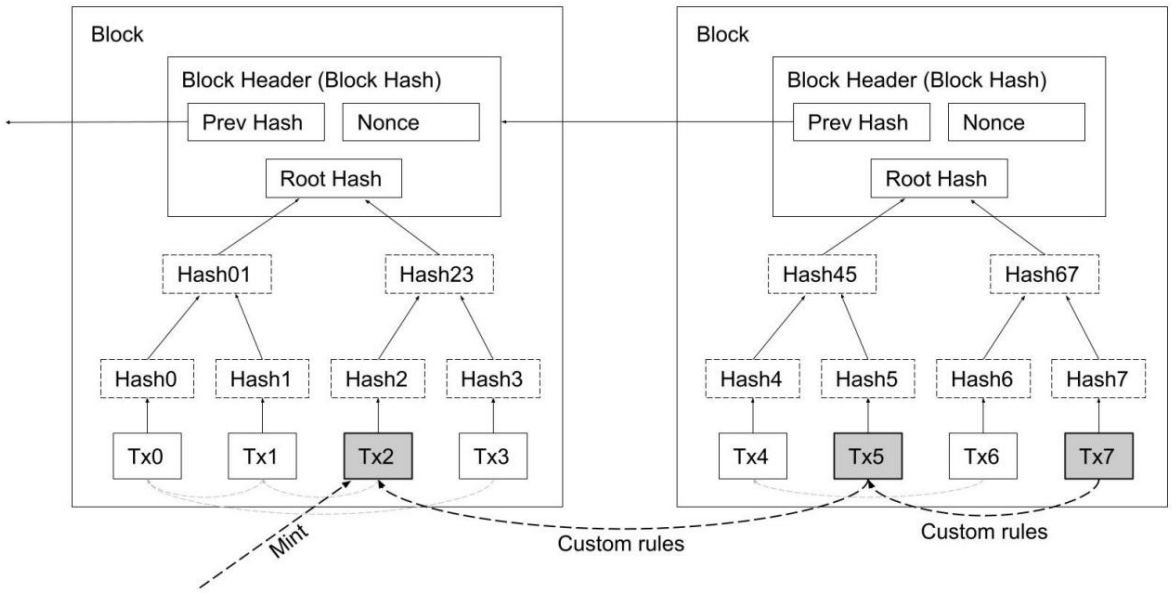
> Diagram 2. Struktur Blok; transaksi diatur ke dalam Pohon Merkle.

Masalah dengan desain ini, dalam konteks aset digital, adalah hanya ada satu jenis koin, atau aset digital, dan tidak ada konsep koin yang ditentukan pengguna (atau jenis aset digital). Desainnya berfungsi cukup baik untuk transaksi seperti pembayaran elektronik di unit akun asli, namun tidak langsung cocok untuk digunakan untuk jenis koin atau aset digital lainnya. Solusi umum adalah dengan memperkenalkan layanan seperti pengindeks transaksi yang memantau transaksi untuk urutan data khusus untuk menandai pembuatan aset digital. Masalah dengan solusi ini adalah bergantung pada perusahaan yang menjalankan layanan, dengan keaslian aset digital yang perlu dipercaya, sama seperti layanan lain di web.

Kami membutuhkan cara bagi pengguna untuk menunjukkan pembuatan jenis koin khusus, tetapi tidak bergantung pada layanan tepercaya yang akan digunakan untuk presentasi data.

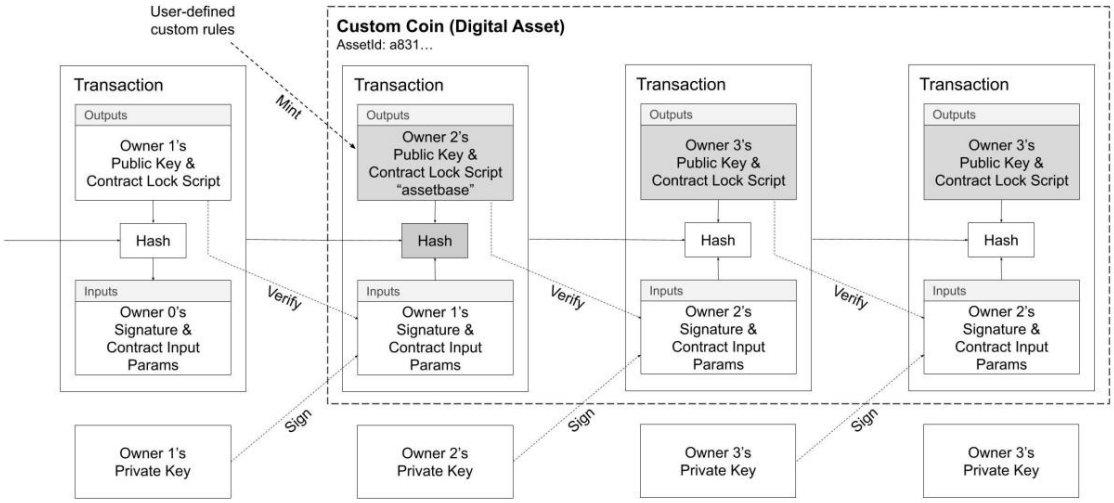
3. Aset Digital

Kami mendefinisikan koin elektronik khusus, atau aset digital, sebagai rangkaian tanda tangan digital. Aset digital adalah jenis koin yang ditentukan pengguna menggunakan penanda transaksi khusus, yang disebut "transaksi basis aset", untuk membuat atau mencetak aset digital. Mirip dengan transaksi coinbase, yang menyuntikkan koin baru ke dalam sistem, transaksi assetbase mewarnai atau menandai koin elektronik dengan pengidentifikasi 36-byte unik untuk seumur hidup. Koin elektronik kustom dilapisi di atas jenis koin dasar dan berfungsi dengan cara yang sama. Transaksi basis aset dapat muncul di mana saja di blok dan dapat memberlakukan aturan dan batasan khusus apa pun yang diputuskan di muka.



> Diagram 3. Transaksi yang mewakili jenis koin yang ditentukan pengguna — atau digital aktiva.

Untuk melakukannya, kita perlu membuat pengidentifikasi unik yang stabil dan mekanisme transaksi untuk melacak keaslian jenis koin (aset digital). Pengguna sistem perlu memiliki bukti bahwa jenis koin khusus bukan pemalsuan dan secara akurat mewakili aset digital.

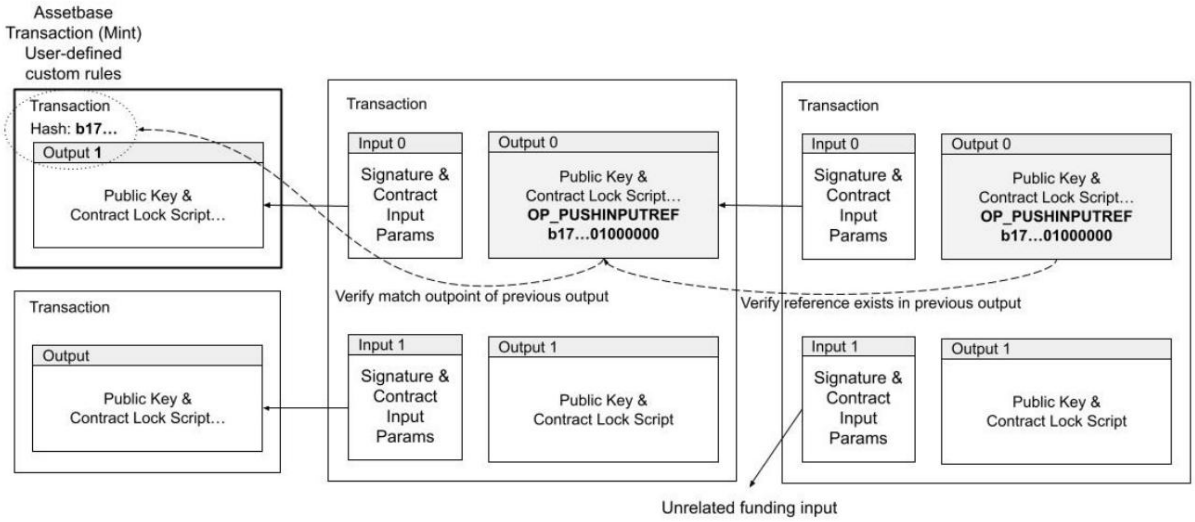


> Diagram 4. Jenis koin khusus yang ditentukan pengguna ditentukan dari transaksi mint khusus. Pengidentifikasi unik digunakan untuk mengklasifikasikan jenis koin.

4. Pengidentifikasi Unik

Untuk menerapkan pengidentifikasi unik untuk jenis koin, kami menggunakan transaksi penanda khusus, yang disebut "transaksi basis aset", yang bertindak sebagai awal (mint) rantai tanda tangan digital. Daripada memerlukan struktur data baru untuk pengenal unik, kami menggunakan kembali pengenal transaksi dan indeks keluaran, yang disebut "outpoint", sebagai pengenal unik untuk jenis koin. Dipastikan bahwa outpoints (36-bytes) bersifat acak dan unik secara global.

Instruksi pemrograman, disebut **OP_PUSHINPUTREF** ke output. **,** digunakan untuk melampirkan referensi Instruksi menerima tepat satu parameter 36-byte yang harus cocok dengan 1) outpoint dari salah satu keluaran yang dikeluarkan, atau 2) nilai 36-byte yang sama sudah muncul di OP_PUSHINPUTREF yang ditentukan sebelumnya di salah satu keluaran yang **dikeluarkan .** Satu-satunya cara agar nilai tertentu muncul dalam keluaran transaksi adalah melalui beberapa transaksi leluhur, nilai tersebut cocok dengan titik keluar dari transaksi basis aset pencetakan awal. Transaksi yang menentukan nilai yang tidak memenuhi salah satu syarat tidak valid.

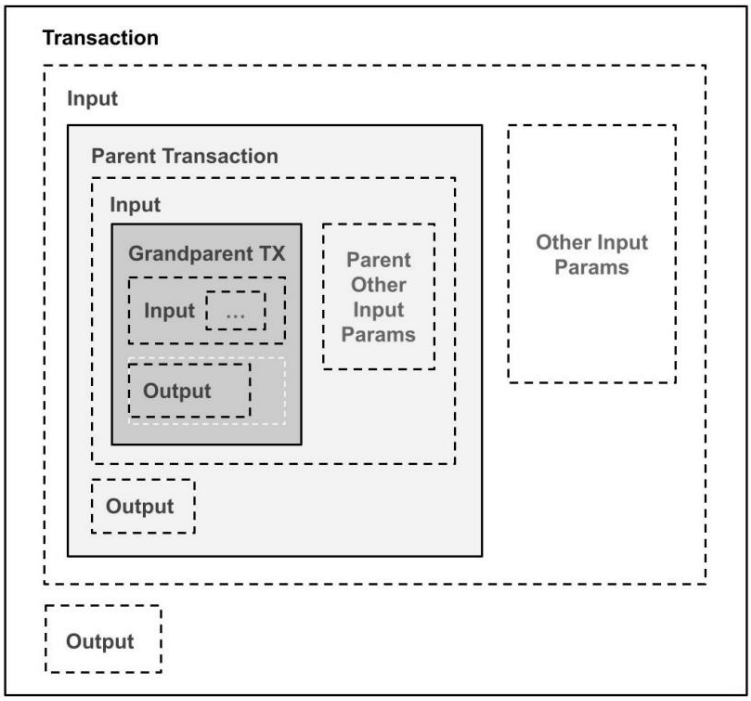


> Diagram 5. Pengidentifikasi unik diinisialisasi dengan mencocokkan titik keluar dari salah satu keluaran yang digunakan, dan kemudian dipertahankan selama setidaknya salah satu keluaran yang dikeluarkan berisi pengenal unik yang sama di badan skrip.

Instruksi pemrograman sederhana ini memberikan pengidentifikasi unik yang dapat digunakan sebagai referensi stabil untuk membuat aturan lanjutan. Misalnya, berbagai jenis koin, aset digital, kini dapat bergantung pada jenis koin lainnya. Karena semua data bersifat lokal untuk transaksi, melalui transaksi masukan induk langsung, mudah bagi klien dan layanan untuk memvalidasi keaslian aset digital dalam O(1) waktu dan ruang yang konstan, menghindari kebutuhan akan layanan tepercaya .

5. Pembuktian Dengan Induksi

Dimungkinkan untuk membuat pengidentifikasi unik dengan cara alternatif dan juga menyediakan mekanisme untuk pembuktian induksi matematika [5] menggunakan algoritma hash transaksi yang dimodifikasi. Dengan mengizinkan skrip input untuk menerima transaksi induk yang dibelanjakan, aturan dapat memverifikasi bahwa induk, dan kakeknya sesuai dengan aturan yang diperlukan. Masalah yang jelas adalah bahwa karena setiap salinan lengkap dari transaksi induk disematkan, ledakan ukuran eksponensial terjadi dan mencegah penggunaan teknik secara praktis. Apa yang dibutuhkan adalah cara untuk mengompresi transaksi, sehingga struktur data berukuran tetap dapat digunakan sebagai gantinya untuk memperoleh hash transaksi, alih-alih membutuhkan konten transaksi penuh.



> Diagram 6. Validasi full parent transaction, pembuktian induksi matematis dengan memasukkan full parent transaction ke dalam input yang menghasilkan peningkatan ukuran transaksi secara eksponensial.

Kita dapat melakukannya dengan memodifikasi algoritme hash transaksi yang digunakan dalam Bitcoin, di mana intisari sha-256 ganda dihitung dari transaksi berseri, menjadi versi baru yang terlebih dahulu meringkas konten transaksi untuk memperoleh hash. Kami memperkenalkan algoritma hash transaksi versi 3, untuk membedakannya dengan penggunaan versi 1 dan versi 2 di Bitcoin. Prosesnya adalah mencirikan setiap bidang, atau komponen transaksi, ke hash perantara, yang dapat digunakan sebagai input ukuran tetap dan dengan demikian menghindari pertumbuhan ukuran transaksi eksponensial.

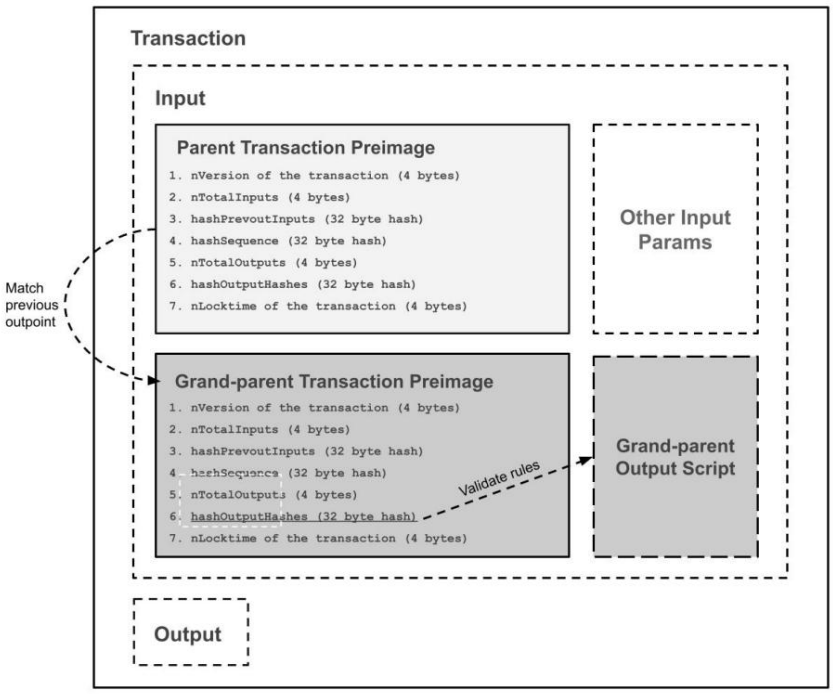
Kami menggunakan struktur data 112-byte berikut, alih-alih byte transaksi berseri lengkap, yang pada gilirannya di-hash sha-256 ganda untuk akhirnya mendapatkan hash transaksi.

Versi Transaksi 3 Kolom Hash Preimage:

> 1. nVersion(=3) transaksi (4 byte little endian)
> 2. nTotalInputs (4 byte little endian)
> 3. hashPrevoutInputs (hash 32 byte)
> 4. hashSequence (hash 32 byte)

> 5. nTotalOutputs (4 byte little endian)
> 6. hashOutputHash (hash 32 byte)
> 7. nLocktime transaksi (4 byte little endian)

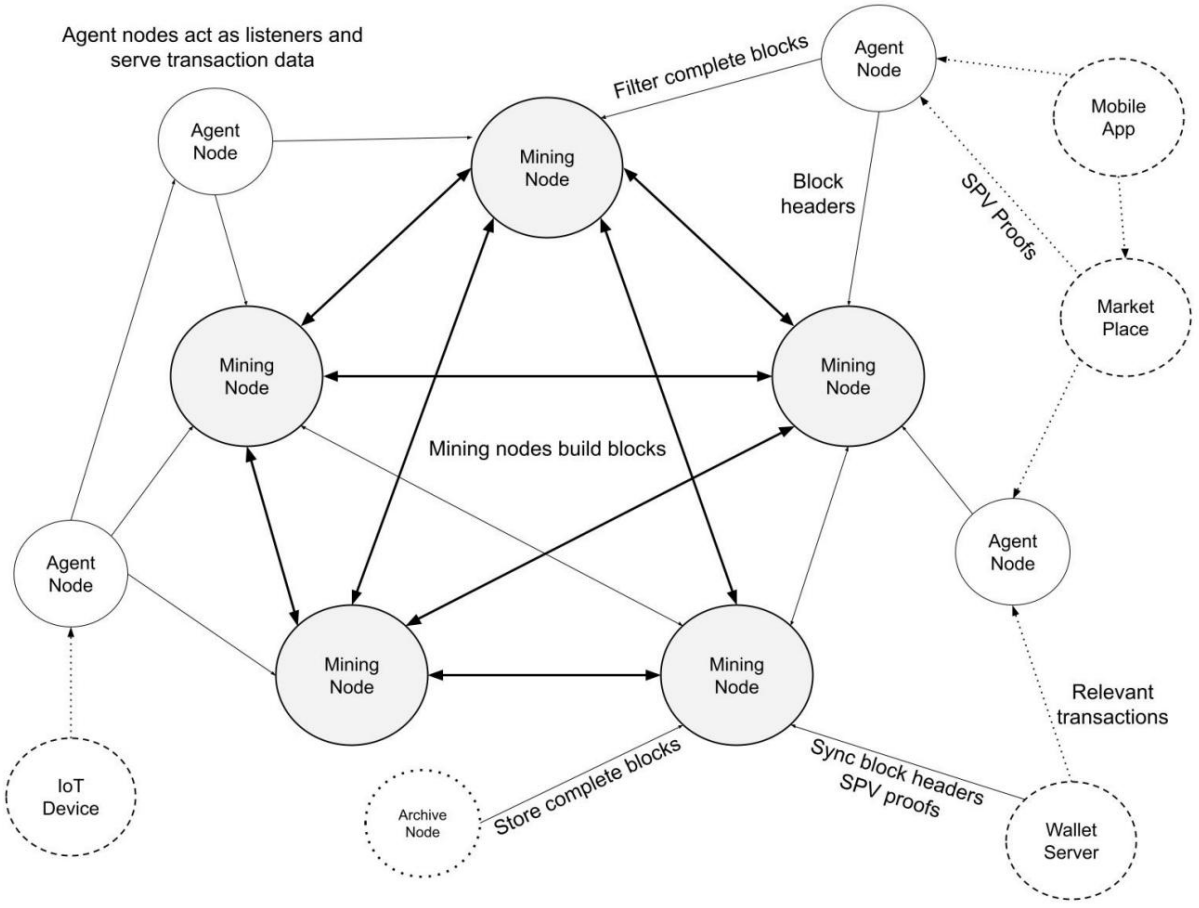
Dengan menggunakan algoritme hash transaksi untuk transaksi versi 3, kami dapat menyematkan transaksi induk dan kakek-nenek di setiap langkah bukti induksi matematis untuk mencegah peningkatan ukuran transaksi, dan dapat menerapkan aturan apa pun yang diperlukan.



> Diagram 7. Validasi transaksi induk terkompresi, bukti induksi matematis dengan menyematkan struktur data preimage hash transaksi versi 3 dari induk dan kakek-nenek untuk menegakkan aturan dan batasan yang sewenang-wenang.

6. Jaringan

Topologi jaringan adalah grafik yang hampir lengkap, di mana setiap Node Penambangan terhubung ke setiap Node Penambangan lainnya. Langkah-langkah untuk menjalankan jaringan sama dengan Bitcoin, dengan beberapa perbedaan untuk jenis node yang berbeda: Node Penambangan, Node Agen, Node Arsip. Mining Nodes adalah penerbit blok aktif dan mempertahankan konsensus dengan semua node lain, Node Arsip melayani data blok historis, dan Node Agen dirancang untuk memfilter blok dan melacak transaksi yang menarik ke aplikasi yang mereka layani. Arsip dan Node Agen dapat beroperasi pada jaringan peer-to-peer yang sama namun tidak menghasilkan blok. Non-Mining Nodes seperti Archive dan Agent Nodes terkadang disebut sebagai "node pendengar" untuk membedakan peran mereka dalam jaringan.



> Diagram 8. Mining Node terhubung dengan baik dan dibangun di atas blok masing-masing. Node arsip menyimpan blok lengkap untuk analisis historis dan tujuan bootstrap. Node agen adalah node pendengar yang memfilter dan menyimpan transaksi untuk melayani klien.

Node Penambangan terhubung dengan baik ke dalam grafik yang hampir lengkap antara Node Penambangan lainnya. Tugas mereka adalah membangun di atas blok satu sama lain dan mempertahankan konsensus untuk beberapa ratus blok terbaru, dan mempertahankan set UTXO untuk pencegahan pengeluaran ganda.

Agen Node hanya perlu menyimpan subset transaksi, misalnya jenis koin tertentu atau aset digital. Bahkan dengan blok besar, Agen Node dapat dengan cepat memfilter transaksi dengan referensi atau urutan byte tertentu, lalu menyimpan transaksi tersebut untuk ditayangkan melalui antarmuka pemrogram aplikasi. Di antara agen yang bekerja sama, root hash Merkle Tree dapat diumumkan secara publik untuk transaksi di setiap blok yang cocok dengan pola yang telah ditentukan sebelumnya untuk memberi sinyal kepada Agen dan konsumen lain tentang transaksi mana yang telah diproses oleh Agen.

Node Arsip digunakan untuk membuat salinan cadangan seluruh blok untuk berbagai aplikasi termasuk pergudangan data, analitik, dan pembelajaran mesin. Karena Archive Nodes tidak terlibat langsung dalam penambangan, mereka tidak memiliki kinerja waktu nyata dan kebutuhan bandwidth yang sama dengan Mining atau Agent Nodes.

7. Perhitungan

Kami mempertimbangkan skenario di mana jaringan Radiant terus tumbuh dan apa yang diperlukan untuk persyaratan pemrosesan Mining, Archive, dan Agent Nodes. Sebagai perbandingan, pada saat penulisan, ada sekitar 83 juta keluaran transaksi yang tidak terpakai untuk blockchain Bitcoin, dengan total sekitar 6 GB data yang diperlukan untuk mencegah pengeluaran ganda. Hanya perlu bahwa beberapa ratus blok terbaru disimpan oleh Mining Nodes, dengan blok yang lebih lama tersedia dari Archive Nodes. Untuk Agent Nodes, penting untuk menjaga partisi yang relevan dari output transaksi yang tidak terpakai yang berkaitan dengan aplikasi yang mereka layani, penskalaan adalah fungsi bandwidth dan bukan persyaratan penyimpanan.

Untuk tujuan kami, kami berasumsi bahwa akan ada blok berukuran 3 GB setiap 5 menit untuk diberi stempel waktu dan didistribusikan ke seluruh jaringan, atau sekitar 20.000 transaksi per detik dengan ukuran transaksi rata-rata 500 byte, atau sekitar 6.000.000 transaksi per blok. Kami menunjukkan bahwa untuk setiap jenis node, jaringan dapat diskalakan secara memadai untuk memenuhi permintaan global. Ini sama dengan sekitar 1 transaksi setiap 5 hari untuk masing-masing dari 8 miliar orang di planet ini.

Node Penambangan

Nodes penambangan adalah satu-satunya tipe node yang dibangun di atas blok masing-masing. Untuk mempertahankan konsensus, cukup menyinkronkan kumpulan output transaksi yang tidak terpakai (UTXO), dan hanya mempertahankan sekitar seratus blok terakhir. Pada saat penulisan, solid-state drive komoditas kinerja tinggi mampu mencapai lebih dari 120.000 IOPS, dengan biaya sekitar $500 USD untuk 280 GB, dan karenanya dapat menangani sekitar 20.000 transaksi per detik (dengan asumsi setiap transaksi memiliki 2 input dan 2 output) . Ada 2 pembacaan untuk input, 2 pembaruan input, dan 2 penulisan untuk output baru: 120.000/6 = 20.000 transaksi/detik.

Node Arsip

Node Arsip menyediakan data blok historis dan cocok untuk pembelajaran mesin, analitik, dan aplikasi pergudangan data. Node Arsip dapat melengkapi bootstrap Node Penambangan dan untuk menjalankan pemeriksaan konsistensi berkala pada set UTXO. Pada saat penulisan, hard disk komoditas 18 TB tersedia dengan harga sekitar $350 USD. Dengan asumsi 3 GB data setiap 5 menit sama dengan 732 GB kebutuhan penyimpanan data per hari, atau sekitar 22 TB per bulan. Biaya perangkat keras selama setahun adalah 15 hard disk, dengan kapasitas 18 TB, dengan biaya tambahan tahunan sebesar $5.000 USD.

Node Agen

Skala Agen Nodes paling mudah di antara jenis node karena mereka hanya memproses jenis transaksi yang relevan untuk aplikasi yang mereka layani. Hasilnya, Agent Nodes dapat berkisar dari server web hingga perangkat IoT ringan dengan kemampuan pemrosesan dan penyimpanan terbatas, namun tetap tenang dengan blok 3 GB, atau 20.000 transaksi per detik. Misalnya, perusahaan mungkin ingin melacak penggunaan poin loyalitasnya, dibuat sebagai aset digital, dan oleh karena itu hanya perlu memilih sebagian kecil pembaruan transaksi dari setiap blok yang cocok dengan pengidentifikasi unik untuk jenis koin tersebut.

Pada saat penulisan, perangkat komputasi komersial, Raspberry Pi 4, dijual seharga sekitar $275 USD yang memiliki prosesor quadcore 1,5 GHZ dan RAM 4 GB, yang dapat digunakan untuk memfilter dengan cepat, dan membuang transaksi yang tidak relevan, dengan kecepatan 5.000 transaksi per inti. Tentu saja, ini hanyalah contoh betapa masuk akal untuk memproses blok besar, dalam aplikasi web biasa mungkin ada lebih banyak inti yang tersedia.

Kecepatan bandwidth rata-rata dari 25 negara teratas melebihi 100 MBPS, atau sekitar 10 MB/detik unduhan, dengan banyak penyedia layanan internet menawarkan unduhan tanpa batas. Persyaratan bandwidth untuk blok 3 GB setiap 5 menit adalah sekitar 10 MB/detik dengan total 22 TB per bulan. Hierarki Node Agen juga dapat dibuat untuk memfilter kebutuhan total bandwidth untuk Node Agen dengan kapasitas bandwidth yang lebih rendah.

8. Kesimpulan

Kami telah mengusulkan sistem manajemen aset digital tanpa mengandalkan kepercayaan. Kami mulai dengan blok bangunan dasar koin yang terbuat dari tanda tangan digital, yang memberikan kontrol kepemilikan yang kuat. Dari aturan dan insentif yang diperlukan, kami memperkenalkan dua metode baru untuk mengautentikasi dan melacak aset digital dalam ruang dan waktu O(1) yang konstan. Kedua metode secara independen menyediakan sistem bukti induksi matematika umum yang dapat menyandikan konfigurasi aset digital yang memungkinkan. Sistem Turing Lengkap di dalam dan melintasi batas transaksi, tanpa perlu lapisan sekunder. Radiant adalah desain terobosan yang memberikan manfaat kinerja dan paralelisme dari blockchain output transaksi yang tidak terpakai (UTXO), tetapi dengan kemampuan kontrak dari blockchain berbasis akun berdasarkan Ethereum Virtual Machine (EVM).

Referensi

[1] Satoshi Nakamoto, URL "Bitcoin: Sistem Uang Elektronik Peer-to-Peer" https://bitcoin.org/bitcoin.pdf, 2009.

[2] Vitalik Buterin, "Ethereum: Kontrak Cerdas Generasi Berikutnya dan Platform Aplikasi Terdesentralisasi." URL https://ethereum.org/en/whitepaper/, 2014.

[3] Kontributor Wikipedia. "Turing kelengkapan." Wikipedia, ensiklopedia gratis. Wikipedia, Ensiklopedia Gratis, URL https://en.wikipedia.org/wiki/Turing_completeness, 21 Juli 2022

[4] RC Merkle, "Protokol untuk kriptosistem kunci publik," Dalam Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, halaman 122-133, April 1980.

[5] Britannica, T. Editor Ensiklopedia. "induksi matematika." Ensiklopedia Britannica, URL https://www.britannica.com/science/mathematical-induction, 2018