Summary Cryptonote

Bitcoin telah berhasil mengimplementasikan konsep uang elektronik peer to peer. Saat ini, basis pengguna uang elektronik tumbuh dengan kecepatan yang stabil; pelanggan tertarik dengan biaya rendah dan anonimitas yang disediakan oleh uang elektronik dan pedagang menilai emisi yang diprediksi dan terdesentralisasi. Bitcoin memilikinya dan secara efektif membuktikan bahwa uang tunai elektronik dapat sesederhana uang kertas dan senyaman kartu kredit.

Sayangnya, Bitcoin mengalami beberapa kekurangan. Misalnya, sistem terdistribusi sifatnya tidak fleksibel, mencegah penerapan fitur baru hingga hampir semua pengguna jaringan memperbarui klien mereka. Beberapa kelemahan kritis yang tidak dapat diperbaiki dengan cepat menghalangi Bitcoin propagasi luas. Dalam model yang tidak fleksibel seperti itu, akan lebih efisien untuk meluncurkan proyek baru daripada terus-menerus memperbaiki proyek asli.

Salah satu solusi untuk kekurangan utama Bitcoin adalah sistem yang mempertimbangkan solusi yang kami usulkan akan mengarah pada persaingan yang sehat antara sistem kas elektronik yang berbeda. Kami juga mengusulkan uang elektronik kami sendiri, dan CryptoNote adalah sebuah nama yang menekankan terobosan berikutnya dalam uang elektronik. Solusi yang memungkinkan pengguna untuk mempublikasikan satu alamat dan menerima tanpa syarat pembayaran yang tidak dapat ditautkan. Tujuan dari setiap keluaran CryptoNote (secara default) adalah kunci publik, berasal dari alamat penerima dan data acak pengirim. Keuntungan utama melawan Bitcoin adalah bahwa setiap kunci tujuan unik secara default (kecuali pengirim menggunakan data yang sama untuk masing-masing transaksinya ke penerima yang sama). Oleh karena itu, tidak ada masalah seperti "penggunaan kembali alamat" oleh desain dan tidak ada pengamat yang dapat menentukan apakah ada transaksi yang dikirim ke alamat atau tautan tertentu dua alamat bersama-sama.

CryptoNote berisi algoritme penargetan yang mengubah kesulitan setiap blok. Ini mengurangi waktu reaksi sistem ketika hashrate jaringan tumbuh atau menyusut secara intens, mempertahankan laju blok yang konstan. Metode Bitcoin asli menghitung hubungan actual dan target rentang waktu antara blok 2016 terakhir dan menggunakannya sebagai pengganda untuk saat ini kesulitan. Jelas ini tidak cocok untuk perhitungan ulang yang cepat (karena inersia besar) dan menghasilkan osilasi.

Ide umum di balik algoritme ini adalah menjumlahkan semua pekerjaan yang diselesaikan oleh node dan membaginya dengan waktu yang mereka habiskan. Ukuran pekerjaan adalah nilai kesulitan yang sesuai di setiap blok. Tetapi karena stempel waktu yang tidak akurat dan tidak tepercaya, kami tidak dapat menentukan dengan tepat interval waktu antar blok. Seorang pengguna dapat menggeser stempel waktunya ke masa depan dan waktu berikutnya interval mungkin sangat kecil atau bahkan negatif. Agaknya akan ada beberapa insiden semacam ini, jadi kita bisa mengurutkan stempel waktu dan memotong outlier (yaitu 20%). Kisaran dari nilai sisanya adalah waktu yang dihabiskan untuk 80% dari blok yang sesuai.

itur-fitur yang menguntungkan ini dan pengembangan berkelanjutan membuat sistem kas elektronik baru CryptoNote Pemenang hadiah Nobel Friedrich Hayek dalam karyanya yang terkenal membuktikan bahwa keberadaan mata uang independen saat ini memiliki efek positif yang sangat besar. Setiap penerbit mata uang mencoba menarik pengguna dengan meningkatkan produknya. Mata uang seperti komoditas: itu dapat memiliki manfaat dan kekurangan yang unik dan mata uang yang paling nyaman dan tepercaya memiliki permintaan terbesar. Misalkan kita memiliki mata uang yang mengungguli Bitcoin: itu berarti Bitcoin akan berkembang lebih cepat dan menjadi lebih baik. Dukungan terbesar sebagai proyek open source akan dating dari penggunanya sendiri, yang tertarik dengannya. Kami tidak menganggap CryptoNote sebagai pengganti penuh Bitcoin. Sebaliknya, memiliki dua (atau lebih) mata uang yang kuat dan nyaman lebih baik daripada hanya memiliki satu. Menjalankan dua dan proyek yang lebih berbeda secara paralel adalah aliran alami ekonomi kas elektronik