Summary Privacy, Mixers and Monero

Cryptocurrency blockchain publik seperti Bitcoin secara radikal transparan di tingkat protokol: transaksi dapat dilihat dan tidak dapat diubah untuk semua orang selamanya di buku besar blockchain. Mereka tidak anonim, melainkan pseudonim, seperti alamat email. Dan seperti halnya seseorang dapat memilih untuk menggunakan teknik perlindungan privasi ekstra untuk email, pengguna cryptocurrency dapat mengadopsi teknologi kriptografi khusus untuk mengamankan lebih banyak privasi untuk diri mereka sendiri.

Penjelasan ini akan menjelaskan beberapa teknik pelestarian privasi paling populer di ruang cryptocurrency dan akan menjelaskan cara kerjanya. Seperti yang akan kita lihat, ada banyak cara untuk mencapai privasi ekstra dengan transaksi mata uang kripto, dan banyak alasan mengapa pengguna mungkin ingin mengadopsi metode ini.

Ada dua teknik umum untuk mendapatkan lebih banyak privasi dengan transaksi Bitcoin. Seorang pengguna dapat mencari layanan "mixer", yang umumnya ditawarkan oleh kustodian pihak ketiga, atau melakukan transaksi "CoinJoin", yang selalu non-penahanan.

Mixer, juga dikenal sebagai “tumbler,” adalah salah satu teknik privasi Bitcoin awal. Prosesnya mudah: pengguna cryptocurrency yang mencari privasi akan mengirim transaksi ke layanan mixer yang, dengan imbalan biaya, kemudian akan "mencampur" kumpulan cryptocurrency bersama-sama untuk memutuskan jalur transaksi.

Awalnya, layanan mixer hanya ditawarkan oleh pihak ketiga yang harus dipercaya. Sentralisasi ini berarti bahwa pengguna mixer berada di bawah kekuasaan penyedia layanan. Pencampur yang tidak jujur dapat secara diam-diam menyimpan catatan transaksi atau mencampur koin dengan buruk. Dalam kasus ekstrem, seorang pencampur bisa dengan mudah melarikan diri dengan uang itu.

Tetapi pencampuran terpusat yang sederhana memiliki kelemahan besar bahkan ketika mixer benar-benar jujur dan mampu: pengguna mixer non-kriminal dapat menerima koin yang dinodai oleh penjahat yang menggunakan layanan pencampuran yang sama. Dengan kata lain, meskipun privasi dapat lebih terjaga dengan mixer terpusat sederhana, pengguna non-kriminal masih dapat menerima koin dengan "noda" kejahatan orang lain. Karena menerima koin yang tercemar tidak diinginkan, ini menciptakan masalah ketidaksempurnaan fungibilitas karena koin yang tidak tercemar mungkin bernilai lebih dari koin yang tercemar.

Cryptocurrency pelestarian privasi populer lainnya disebut Monero, dari kata Esperanto untuk uang. Dengan Monero, semua pengirim, penerima, dan jumlah disembunyikan secara default, tetapi pengguna memiliki opsi untuk membagikan informasi tertentu dengan penerima yang dituju jika mereka menginginkannya. Inilah sebabnya mengapa proyek Monero menggambarkan dirinya sebagai "pribadi secara default dan opsional semi-transparan."

Monero menjaga privasi pengirim melalui apa yang disebut tanda tangan cincin. Ketika pengguna Monero menyiarkan transaksi, tanda tangan pribadi mereka digabungkan ke dalam sekelompok tanda tangan pengguna Monero lainnya sehingga pengamat tidak dapat membedakan tanda tangan mana yang benar-benar menghasilkan tanda tangan awal. Setiap transaksi Monero terstruktur dengan cara ini secara default, jadi tidak ada pengguna yang menarik perhatian mereka dengan memilih apakah akan menggunakan tanda tangan cincin atau tidak.

Alat privasi default terakhir di Monero disebut alamat siluman, yang menyembunyikan penerima. Setiap pengguna memiliki alamat publik yang terdiri dari 95 karakter dan dimulai dengan 4. Tapi setiap kali seseorang mengirim uang ke alamat publik, itu sebenarnya dikirim ke alamat siluman yang dibuat secara otomatis yang tidak dapat dilihat oleh pengamat yang tidak terkait. Pengguna Monero memiliki opsi untuk mengungkapkan transaksi dan saldo akun mereka jika mereka ingin jika mereka memilih untuk mengungkapkan kunci tampilan pribadi mereka. Tetapi transaksi Monero terstruktur untuk menjadi pribadi secara otomatis secara default.

Seperti halnya Bitcoin dan Zcash, Monero menghadirkan kelemahan tertentu. Misalnya, pertanyaan seputar kemampuan audit Monero. Transparansi radikal Bitcoin menghadirkan tantangan untuk privasi, tetapi itu membuat audit teknologi entitas individu dan total pasokan mata uang menjadi mudah. Privasi default Monero membuat audit semacam itu lebih sulit; misalnya, bug yang belum ditemukan dapat meningkatkan suplai uang Monero dengan cara yang sulit dideteksi. (Namun, bug inflasi juga terjadi dengan cryptocurrency blockchain publik seperti Bitcoin dan cryptocurrency hybrid seperti Zcash.) Pengembang Monero mengakui keterbatasan ini dan mendesak pengguna untuk mengevaluasi preferensi risiko mereka sendiri yang terkait dengan tradeoff privasi/auditabilitas. (Transaksi Zcash terlindung menghadirkan masalah kemampuan audit yang serupa.)

Zcash dan Monero hanyalah dua cryptocurrency yang menjaga privasi. Kami telah menyoroti keduanya untuk membedakan dua pendekatan yang berbeda dan menjelaskan beberapa alat yang mereka gunakan. Contoh lain termasuk implementasi Mimblewimble seperti Grin dan Beam (yang menggunakan teknik transaksi rahasia) dan Komodo (yang merupakan fork dari Zcash).