Saopštenje za medije
Kancelarija Grada Beča u Beogradu

28. jun 2023.

Most između različitih kriptovaluta

Kako se može jedna kriptovaluta promeniti u neku drugu? Do sada se moralo verovati velikim kripto ponuđačima ili se zadovoljiti jednostavnim transferima. Tehnički univerzitet u Beču kreirao je decentralizovan protokol koji dozvoljava nove finansijske instrumente.
Bitkoin je danas najpoznatija kriptovaluta na svetu, ali postoje još mnoge druge koje nude razne mogućnosti. Ukoliko neko želi jednu kriptovalutu da zameni u neku drugu najčešće se koriste tzv. „mostovi“ – obično se iza toga kriju firme koje drže velike sume različitih kriptovaluta i omogućavaju transfere. Tom prilikom često su se dešavali sigurnosni problemi i spektakularni kriminalni slučajevi – ukradene su kriptovalute u vrednosti od nekoliko milijardi evra.
Na Tehničkom univerzitetu u Beču razvijen je novi protokol koji zamenu jedne kriptovalute u drugu omogućava na efikasan i bezbedan način – i to potpuno decentralizovano bez korišćenja velikog kripto-depoa od komercijalnih ponuđača. Novi Tool se zove „Glimpse“ i nudi potpuno nove opcije u svetu kriptovaluta. Rad je prihvaćen od strane „USENIX Security Symposium“, jedne od najprestižnijih informatičkih konferencija na svetu, koja se održava u avgustu u Los Anđelesu. Dokument o novoj kripto-tehnici je već na raspolaganju onlajn.

Jednostavni prenosi i Smart Contracts

Kod kriptovaluta se svaka transakcija memoriše tako da je razumljivo za svakog, na javno vidljivom blockchainu, koji sadrži kompletan tok svih dotadašnjih transakcija. Tako je uvek jasno sa kog računa se prenosi koja suma, na koji drugi račun, i ko poseduje koliko kriptovaluta. Ove transakcije mogu biti i komplikovanije nego prost bankarski transfer: „Kod različitih kriptovaluta može se u sistem ubaciti transfer koji je samo onda validan ukoliko su ispunjeni određeni uslovi“, objašnjava Giulia Scaffino, autorka protokola.
U matematički precizno definisanom jeziku se ovi uslovi ustanove, kao ugovor koji kompjuter može da pročita, tzv. „smart contract“. Kasnije se automatski verifikuje da li su uslovi ispunjeni ili nisu, i u zavisnosti od toga se transfer obavlja ili prekida.
Takve transakcije su i do sada unutar blockchaina bile moguće, ali sveobuhvatne transakcije jedne kriptovalute u drugu su komplikovanije i standardno se ne podržavaju. I upravo to će sa novim protokolom biti moguće.

Bitkoin za Ethereum

Pretpostavimo da jedna vlasnica bitkoina želi da zameni bitkoin za Ethereum. Ona pronađe vlasnika Ethereuma koji želi da menja valutu. Kako ova transakcija može pouzdano i efikasno da se sprovede ako bitkoin i Ethereum tehnički nisu povezani?
Osnovni koncept je jednostavan: najpre Ethereum-vlasnik generiše jedan slučajni broj i pošalje ga vlasnici bitkoina. Onda se u sferi Ethereuma sklapa tzv. Smart Contract koji garantuje da će određena količina Ethereuma biti preneta bitkoin-vlasnici – ali ne odmah, već najpre kada budu ispunjeni određeni uslovi. Vlasnica bitkoina prenosi bitkoine vlasniku Ethereuma i unosi u formular dobijeni slučajni broj, da bi se sprečili bezbednosni upadi drugih. Sada vlasnica bitkoina može da koristi aktuelni block bitkoina, u kojem je memorisan slučajni broj, zajedno sa prethodno dogovorenim brojem drugih blokova, da bi dokazala da su bitkoini zaista zamenjeni. Ovi podaci se koriste na Ethereum-strani, da bi se ispunio smart contract – i tako se dogovoreni iznos Ethereuma prenosi.

Efikasno, kompatibilno i fleksibilno

„Tačan protokol koji smo za to napravili trebalo bi da ispuni više važnih kriterijuma“, kaže Zeta Avarikioti. „Mora da bude efikasno, dokaz je da je suma zaista preneta, i treba da bude moguće sa

relativno malom količinom podataka. Ukoliko bi za to bili potrebni veliki delovi blockchaina, sa stotinama gigabajta podataka, to bi bilo potpuno nepraktično. Osim toga protokol bi trebalo da pokaže veliku kompatibilnost – trebalo bi da podržava što više kriptovaluta.“ Novorazvijeni protokol može se direktno integrisati u postojeći kripto-sofver – razgovori sa austrijskim finansijskim preduzećem „Bitpanda“ već su u toku.

Istraživanje je sprovedeno u okviru laboratorije Christian-Doppler „Blockchain Technologies“ na Tehničkom univerzitetu u Beču, pod vođstvom profesora Matteo Maffei. Pored Giulia Scaffino na istraživanju su učestvovali i Lukas Aumayr i Zeta Avarikioti.

Originalna publikacija

Više informacija

mr Cvijeta Radović
Balkanska 2
11000 Beograd
radovic@viennaoffices.rs
T +381 11 205 51 13
M +381 69 72 82 42
www.viennaoffices.rs
https://www.facebook.com/viennaofficeBEG
https://www.instagram.com/viennaoffices_belgrade/