Priopćenje za medije poduzeća Eurocomm-PR Zagreb
Inozemni uredi Grada Beča

14. svibnja 2021.

# Tehničko sveučilište u Beču razvilo protokol za sigurnije transakcije kriptovalutama

## Tim međunarodnih znanstvenika analizirao je probleme s kojima se susreću korisnici prilikom obavljanja transakcija kriptovalutama te je predstavio rješenje koje omogućuje sigurnije i brže transakcije.

Kriptovalute kao što je Bitcoin stječu sve veću popularnost. Kao neke od njihovih prednosti navode se anonimne, brze i povoljne transakcije, no mogući su i određeni problemi. Tako, primjerice, ponekad dolazi do prijevara, u pojedinim situacijama mogu se otkriti podaci o korisnicima koji bi trebali ostati tajni, a znaju se dogoditi i kašnjenja transakcija.

U suradnji s madridskim Institutom za softver IMDEA i američkim sveučilištem Purdue, Odjel za sigurnost i privatnost na Tehničkom sveučilištu u Beču analizirao je probleme s kojima se susreću korisnici prilikom obavljanja transakcija kriptovalutama te je razvio novi protokol koji omogućuje brže i sigurnije transakcije. Protokol je opisan u nedavno objavljenom radu pod nazivom „Blitz: Secure Multi-Hop Payments Without Two-Phase Commits" i bit će predstavljen ove godine na Simpoziju o sigurnosti USENIX – prestižnoj međunarodnoj konferenciji o IT sigurnosti.

S kriptovalutom Bitcoin i drugim *blockchain* tehnologijama dolazi do poteškoća kad se provode transakcije s većim brojem korisnika na mreži, kazao je član tima s bečkog Tehničkog sveučilišta Lukas Aumayr. U *blockchain* sustavu moguća je obrada od najviše deset transakcija po sekundi, dok neke tvrtke koje proizvode kreditne kartice mogu obraditi i na desetke tisuća transakcija diljem svijeta u jednoj sekundi. Kao rješenje za ovaj problem trenutačno se koristi takozvani *Lightning Network* – mreža transakcijskih kanala između korisnika *blockchain* sustava. Putem ove mreže korisnici mogu provesti veći broj transakcija u kratkom vremenskom razdoblju. No, prilikom stvaranja lanca s više korisnika mogu nastati određeni problemi. U pojedinim slučajevima korisnici tada mogu pristupiti podacima o drugim osobama u lancu. Osim toga, svi moraju unijeti određen iznos novca koji se blokira kao osiguranje, a u slučaju neuspjele transakcije može se dogoditi da se novac blokira na duže vrijeme.

Novim protokolom koji je razvio ovaj međunarodni tim znanstvenika mogu se, primjerice, spriječiti sigurnosne prijetnje koje su prije bile moguće kao i blokiranje novca na duže vrijeme. Da bi provjerili kako novi protokol funkcionira u praksi, znanstvenici s bečkog sveučilišta proveli su simulaciju koja je pokazala da se novom tehnologijom, na primjer, uvelike smanjuje broj neuspjelih transakcija u odnosu na *Lightning Network*.

Tehničko sveučilište u Beču već je stupilo u kontakt s organizacijama za razvoj mreže *Lightning Network*. S Tehničkog sveučilišta dodaju da se nadaju kako će njihova tehnologija ubrzo biti

implementirana ili barem ponuđena kao alternativa te ističu da bi se s tehničke strane mogla početi upotrebljavati već sada.

Više informacija možete pronaći na sljedećoj poveznici: https://www.tuwien.at/en/tu-wien/news/news-articles/news/neues-protokoll-macht-bitcoin-transaktionen-sicherer.

Slika: Kriptovalute poput Bitcoina postaju sve popularnije © Unsplash

# Kontakt

Matea Čuljak, mag. philol. germ./russ.
Suradnica za odnose s javnošću i medijima

Inozemni ured Grada Beča
Miramarska cesta 24 / 9. kat, 10000 Zagreb
T +385 1 646 26 20
M +385 99 573 51 85
E culjak@eurocommpr.hr
https://www.eurocommpr.at/hr/Inozemni-uredi-grada-Beca/Hrvatska

https://www.facebook.com/eurocommprzagreb/
https://twitter.com/EurocommPR_ZG