UABDIVULGA
BARCELONA RECERCA I INNOVACIÓ

29/09/2022

Atacs de denegació de servei a canals de pagament sobre Bitcoin

La Lightning Network (LN) és una xarxa de pagament que pot operar sobre Bitcoin i que podria potencialment processar infinitat de pagaments de manera simultània. Però és vulnerable. Investigadors de la UAB han detectat que és possible fer un atac que bloqueja els canals de pagament.

istock/your_photo

La Lightning Network (LN) és una xarxa de pagament que pot operar sobre Bitcoin i es va concebre per poder superar la limitació d'escalabilitat de Bitcoin. Mentre Bitcoin només pot processar unes 7 transaccions (pagaments) per segon, LN podria potencialment processar infinitat de pagaments de forma simultània.

La xarxa LN està composta per nodes que solen operar també com a nodes Bitcoin. Dos nodes poden establir un canal de pagament entre ells amb un balanç inicial sobre el qual els nodes es poden intercanviar pagaments. La part rellevant és que la majoria de transaccions que comporten el funcionament del canal es poden efectuar entre els dos nodes sense que la xarxa Bitcoin hagi de processar-les. Això permet efectuar aquestes transaccions de manera molt ràpida.

Un dels grans avantatges de LN és que permet executar pagaments *multihop*. Si hi ha un canal de pagament entre A i B, i un altre entre B i C, A pot fer un pagament a C sense necessitat que hi hagi un canal directe entre tots dos. A realitza un pagament a B i B repercuteix aquest pagament a C. És a dir, es fa un pagament en cadena on els nodes intermedis reben una petita comissió per incentivar-ne la col·laboració.

Per permetre pagaments *multihop*, el node inicial ha de poder determinar un camí (o cadena) de canals de pagament fins al destinatari. Això comporta que l'existència d'un canal de pagament entre dos nodes hagi de ser pública. D'altra banda, i per mantenir els pagaments anònims, el balanç dels canals és privat. Qualsevol pot conèixer que hi ha un canal entre A i B, però no en podem saber el balanç ni com aquest evoluciona en el temps. És a dir, no podem saber quins pagaments s'efectuen entre A i B.

En aquest article presentem un atac que permet bloquejar canals de pagament entre nodes a la LN. Aquest atac, que anomenem *lockdown*, fa una denegació de servei a canals de pagament i inhabilita la possibilitat d'un node d'actuar com a intermediari en pagaments *multihop*. Per fer-ho s'explota el fet que en fer un intent de pagament *multihop*, el balanç dels nodes participants queda bloquejat de manera temporal. L'atac permet aïllar una víctima de la xarxa LN de manera que cap node no pugui utilitzar els seus canals de pagament durant un període de temps raonable i amb un baix cost econòmic.

Encara que es proposen també algunes possibles contramesures, aquestes són difícils d'aplicar sense que això afecti el funcionament de LN de manera important. La principal contramesura és fer que aquest atac no resulti rendible en termes econòmics. Això es podria aconseguir introduint limitacions al tipus de camins de canals de pagament que es poden utilitzar a la LN. Abans de publicar l'article es va notificar l'atac als desenvolupadors de la LN, i encara que actualment no podem assegurar que el problema estigui totalment solucionat, sí que s'està treballant en possibles solucions o maneres de mitigar-lo.

Guillermo Navarro-Arribas i Jordi Herrera-Joancomartí
CYBERCAT
Departament d'Enginyeria de la Informació i de les Comunicacions
Universitat Autònoma de Barcelona

Cristina Pérez-Solà
CYBERCAT
Universitat Oberta de Catalunya

Alejandro Ranchal-Pedrosa
University of Sydney

Joaquin Garcia-Alfaro
Institut Polytechnique de Paris, Telecom SudParis

Referències

Pérez-Solà, C., Ranchal-Pedrosa, A., Herrera-Joancomartí, J., Navarro-Arribas, G., Garcia-Alfaro, J. (2020). **LockDown: Balance Availability Attack Against Lightning Network Channels**. In: Bonneau, J., Heninger, N. (eds) *Financial Cryptography and Data Security. FC 2020. Lecture Notes in Computer Science*, vol 12059. Springer, Cham. https://doi.org/10.1007/978-3-030-51280-4_14

View low-bandwidth version