UABDIVULGA
BARCELONA RECERCA I INNOVACIÓ

29/09/2022

Denial of service attacks on payment channels over Bitcoin

The Lightning Network (LN) is a payment network that can operate on top of Bitcoin and could potentially process countless payments simultaneously. But it is vulnerable. UAB researchers have detected that it is possible to carry out an attack that blocks payment channels.

istock/your_photo

The Lightning Network (LN) is a payment network that can operate on top of Bitcoin, and was conceived in order to overcome Bitcoin's scalability limitation. While Bitcoin can only process about 7 transactions (payments) per second, LN could potentially process an infinite number of payments simultaneously.

The LN network is composed of nodes that often also operate as Bitcoin nodes. Two nodes can establish a payment channel between them with an initial balance on which the nodes can exchange payments. The relevant part is that most of the transactions involved in the operation of the channel can be carried out between the two nodes without the Bitcoin network having to process them. This allows these transactions to be carried out very quickly.

One of the great advantages of LN is that it allows multihop payments to be executed. If there is a payment channel between A and B, and another between B and C, A can make a payment to C without the need for a direct channel between the two. A makes a payment to B and B passes this payment on to C. In other words, a chain payment is made where the intermediate nodes receive a small fee to incentivize their collaboration.

To allow multihop payments, the initial node must be able to determine a path (or chain) of payment channels to the recipient. This means that the existence of a payment channel between two nodes must be public. On the other hand, and in order to keep payments anonymous, the balance of the channels is private. Anyone can know that a channel exists between A and B, but we cannot know its balance or how it evolves over time. In other words, we cannot know what payments are made between A and B.

In this paper we present an attack that allows blocking payment channels between nodes in LN. This attack, which we call lockdown, performs a denial of service to payment channels and disables the ability of a node to act as an intermediary in multihop payments. It exploits the fact that when a multihop payment attempt is made, the balance of the participating nodes is temporarily blocked. The attack makes it possible to isolate a victim from the LN network so that no node can use its payment channels for a reasonable period of time and at a low economic cost.

Although some possible countermeasures are also proposed, these are difficult to implement without significantly affecting LN operation. The main countermeasure is to make such an attack unprofitable in economic terms. This could be achieved by introducing limitations on the type of payment channel paths that can be used in the LN. Prior to publishing the article, we notified the developers of the LN about the problem, and while we cannot currently say that the attack is completely fixed, the community is working on possible solutions or ways to mitigate the problem.

Guillermo Navarro-Arribas i Jordi Herrera-Joancomartí
CYBERCAT
Department of Information and Communications Engineering
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

References

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