

Game Design to study Lightning Payment Streams to avoid DoS and Congestion

For subsequent economic investigations, we implement a game at the HAK für Wirtschaftsinformatik Imst that encourages users to collect and exchange information. Users can send micropayments starting at 1 milli Satoshi (msat) to a Lightning bolt12 address. This causes a light show to be created in a classroom. The same number of msat will always produce the same light pattern in the same classroom. The difficulty is figuring out which classroom this is taking place in. Since there are numerous light patterns per classroom, this also encourages collecting. So the payment serves as direct game control in the form of a payment stream. The payment provides an incentive and makes the game valuable. At the same time, it prevents denial of service attacks by flooding the service, because it would get too expensive.

School classes are equipped with microcontrollers that can give physical feedback in the form of light signals with four different-colored LEDs via a radio network that is separate from the WLAN. The radio signals are broadcast from a central server running a Bitcoin and a Lightning node.

When a payment is received at the Lightning Node, a salted hash is generated from the amount paid. The first byte is used to select a classroom. The next 2 bytes are divided into four by four bits to create a light show on the four LEDs of the corresponding classroom microcontroller. This ensures that every amount of msat has a completely randomly different effect. However, the same amount always has the same effect.