THE LIGHTNING CONFERENCE

shitcoins.club

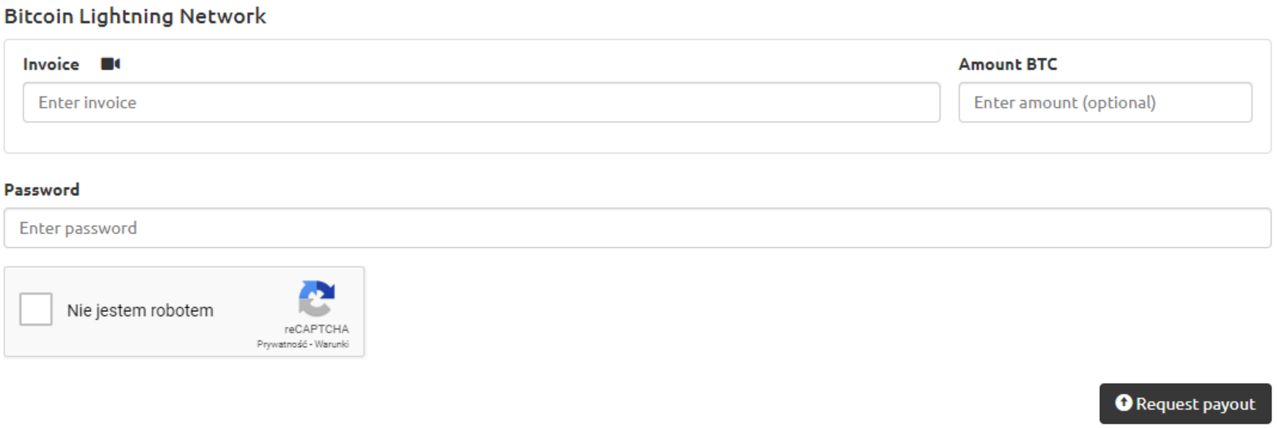
OCTOBER 19-20 BERLIN, GERMANY

The following document outlines reasons why we did not implement LN payments, our point of view in regard to the future of LN and also functionalities, which in our opinion, should be introduced to the LN infrastructure

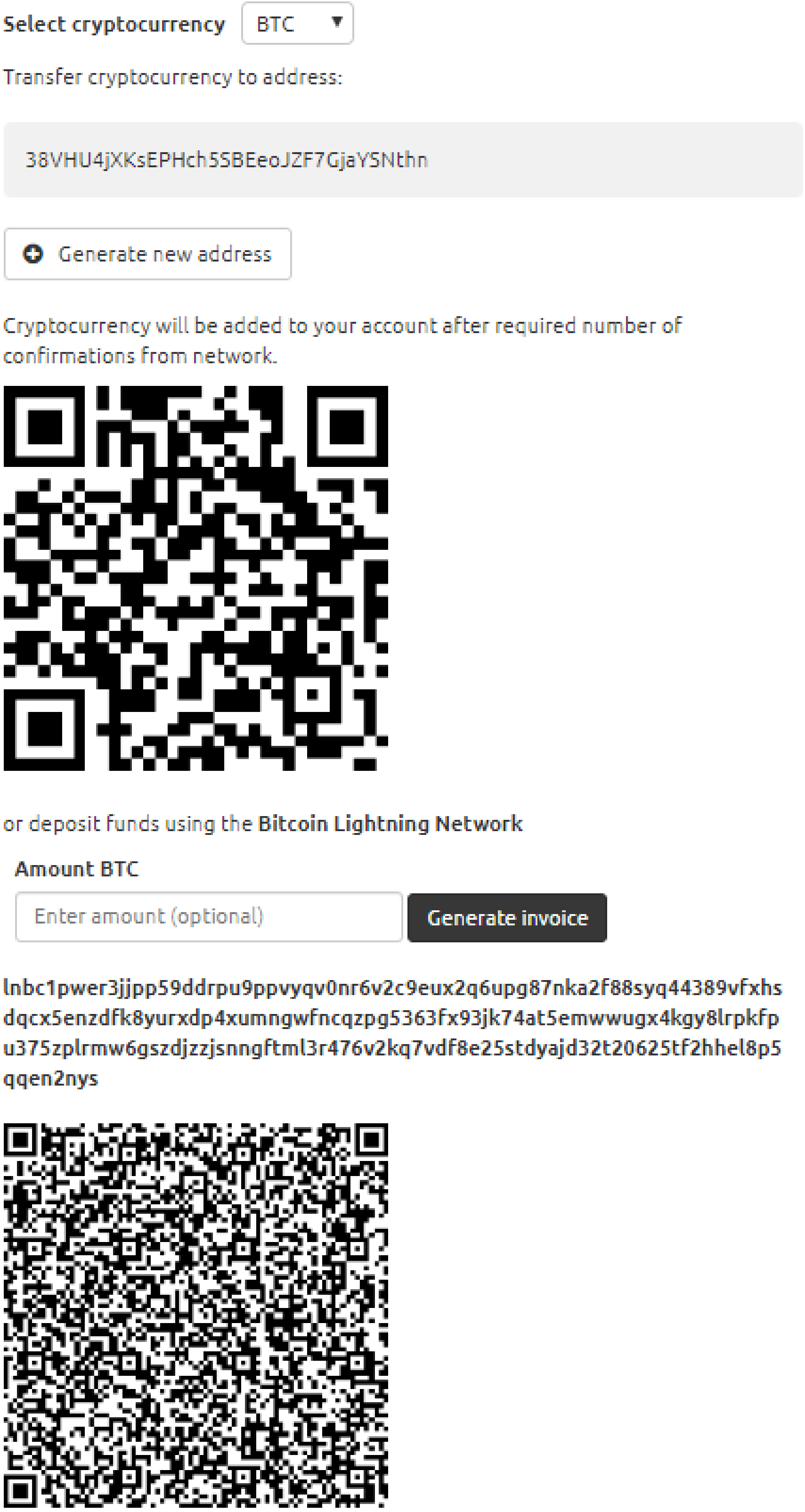
First of all I would like to outline our experiences with implementation of LN to other services offered by BTC Duke.

Apart from cryptocurrency ATMs, we also operate a lesser known cryptocurrency exchange called Btc Duke. Btc Duke is probably the first exchange to feature LN transactions.

It looks like this:
BTC Payouts



BTC pay-ins



Select cryptocurrency BTC

Transfer cryptocurrency to address:

38VHU4jXKsEPHch5SBEeoJZF7GjaYSNthn

Cryptocurrency will be added to your account after required number of confirmations from network.

or deposit funds using the **Bitcoin Lightning Network**

Amount BTC

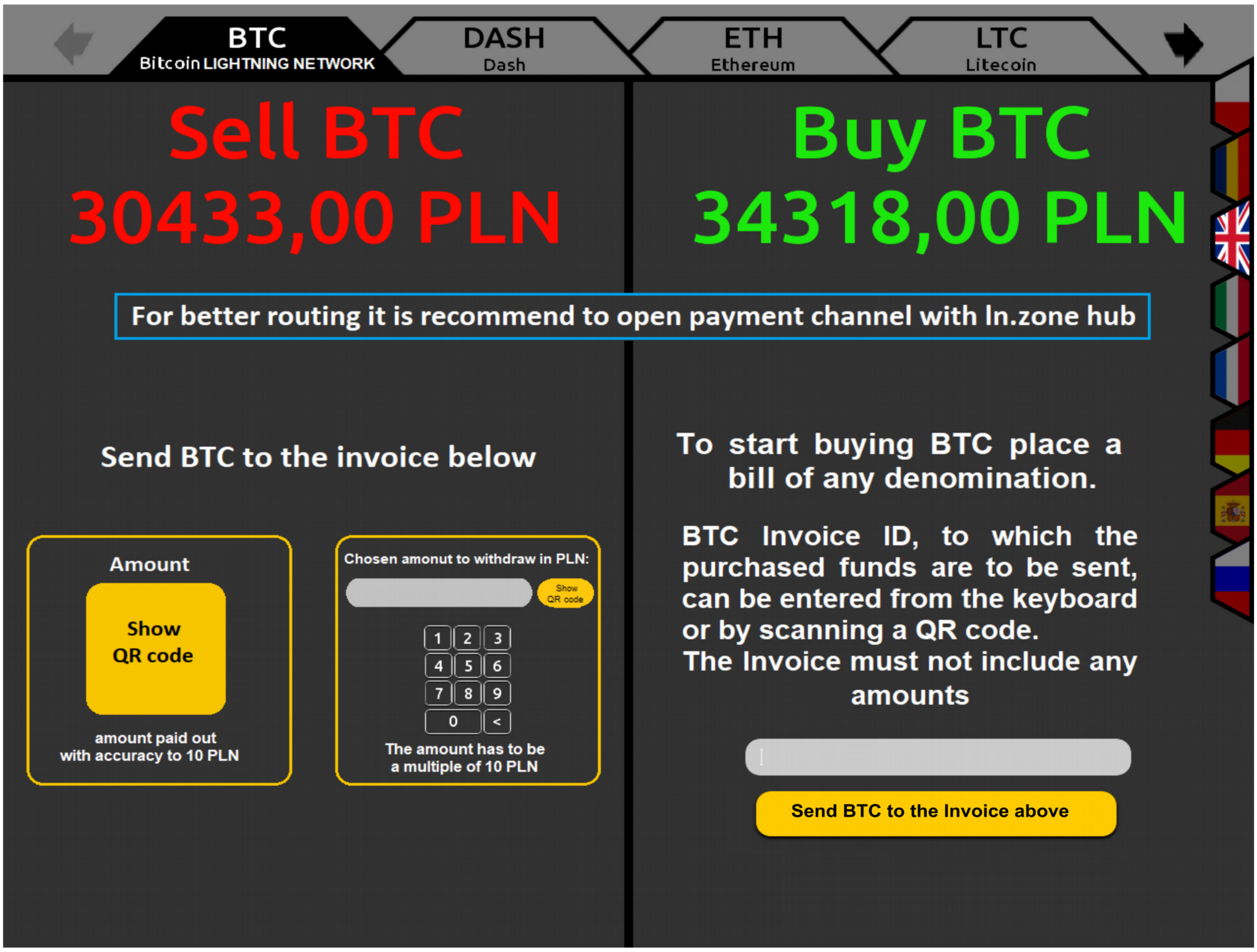
lnbc1pwer3jjpp59ddrpu9ppvyqv0nr6v2c9eux2q6upg87nka2f88syq44389vfxhsdqcx5enzdfk8yurxdp4xumngwfncqzpg5363fx93jk74at5emwwugx4kgy8lrpkfpu375zplrmw6gszdjzzjsnngftml3r476v2kq7vdf8e25stdyajd32t20625tf2hhel8p5qqen2nys

Our experience, in connection to LN functionality shows, that if it was not for the fact that we point our customers to the appropriate HUB, where they are supposed to open the channel, no payment could be routed neither from us to them nor from them to us.

Please take a look at our LN payments webpage, where we had to place a substantial clue as to which Node customers should connect to in order to route any transaction with our help. To offer such services to our customers, we had to create a separate web page for this node, which allows our customers to open a channel not only from the customer to the node but also from the node to the customer. As far as I am aware, there are many web pages of this type. Our service is available under the domain: ln.zone.

As for Lightning networks fans, it was our next idea to implement LN on our ATMs.

It was supposed to look like this:



Sell BTC
30433,00 PLN

Buy BTC
34318,00 PLN

For better routing it is recommend to open payment channel with ln.zone hub

Send BTC to the invoice below

amount paid out with accuracy to 10 PLN

Chosen amonut to withdraw in PLN:

The amount has to be a multiple of 10 PLN

To start buying BTC place a bill of any denomination.

BTC Invoice ID, to which the purchased funds are to be sent, can be entered from the keyboard or by scanning a QR code.
The Invoice must not include any amounts

Interface for transacting through lightning network was the tool for generating QR codes on the left with the appropriate amount if someone wished to sell BTC to us (also by generating empty Lightning Network invoice) and to the right tool for summing up funds inserted by the customer and once the invoice is scanned, we are attempting to send the funds.

In cases where the customer was intending to purchase BTC through LN, and there was no routing to the customer we had the intention to issue him special transaction ID and allow him to try route BTC at a later date, once he is connected to multiple payment channels. We have abandoned this solution, as BTC ATMs earn only on substantial transactions. LN is used only by hobbyists, exclusively as testing bed, and these transactions are not economically justifiable, not to mention programming costs, therefore we do not intend to introduce LN to our ATMs anytime soon.

In such case why did we request the LN conference crew to deliver this talk?

Because based on our experience we believe we know how to popularise LN services and realise its potential.

We are of the opinion, that the concept to reward routing nodes for standard transaction is insufficient and does not take into account the true cost of this entire venture, that is – frozen funds in nodes between customers.

We believe that this (i.e. frozen funds) is the essential cost of this maintaining a node in Lightning network, and not routine payments which cost only as much as electricity for the server with operating node. The first main limitation in creating nodes is the fact that users cannot open unlimited number of Lightning channels, and interact with unlimited number of nodes, as no one is in possession of unlimited funds. More importantly, every attempt by LN enthusiasts to enter the LN ecosystem and run a node independently is endangered by hacker attacks. This is not be treated lightly, because even the esteemed BTC exchanges were subjected to attacks. Taking control over a server running LN node gives equal possibilities as taking control over traditional BTC network node.

To illustrate this point, let’s use the famous example of coffee house, which would like to accept payments for coffee in BTC. In order to accept payments in BTC coffee house owner would have to establish cooperation with a HUB, who would decide on opening payment channel and holding sufficient amount of tokens to service the payments. It is naive to believe that a commercial hub would open such payments channel charitably. Let’s say that the coffee house owner genuinely believed that he would sell 1 BTC worth of coffee in short period of time. Would any commercially minded hub owner oblige a coffee house owner by freezing 1 BTC? If the coffee house owner required less that that, for example 0,01 BTC, what would a commercial hub do if in short period of time 1000 self-described coffee houses requested to open payment channels. Many of such potential coffee house could turn out to be pranksters.

It will be the first problem for every Lightning network hub, that it may have only limited amount of BTC under its control and secondly every hour of operation of such hub comes at great expense associated with protection against cyberattack.

Therefore we argue that LN nodes should be allowed to implement interface, allowing other nodes to request the following information:

1. standard cost of routing transactions (1 Satoshi)

2. additional cost of routing transactions depending on transaction size expressed in BTC / BTC (currently 0,000000001).

3. Expense of keeping BTC by HUB in payment channel expressed in BTC/BTC in a given amount of time. In my opinion it would be best to use one block as a time unit, as this would preclude any adjustments and synchronization necessary in cases of using other time units. If the HUB had to be reworded for funds tied down in payment channels, ex.10% per year, that figure would amount to 0,0000018. We also believe that capitalization of Hub’s reward should take place with every new block being excavated.

Income coming from cooperation with customer coming from 1) and 2) should be deduced from customers costs incurred by maintaining an open channel, as described in point 3). If

Hub's income came from cooperation with customers in connection with 1) and 2) exceed those described in 3), then these should not be deduced from point 3). Such policy would allow the cooperation on the same basis as described not only between hubs and ex. internet shops, but also between hub-hub. Therefore Hubs do not have to be interested in who the customer is, while establishing a channel: whether or not it is coffee house accepting LN payments or some other HUB. It will all transpire during the business relationship and clients in both cases will be most welcome by the Hub.

4. Costs in BTC HUBs, which takes remuneration for initiating channel on-chain transactions and for closing the channel.

Proposed solution, that the costs named in point 3) are reduced by the amount, which hub has earned thanks to routing clients' operations causes, that this model fits right in the cooperation between commercial hubs.

If the costs of freezing funds in the payment channel by the hub are not taken into account, then no hub would ever undertake cooperation with another Hub. No one would make the decision to open a channel with unknown business, which declares routing of a number of transactions however cannot warrant that these transaction will in fact be routed. A number of unknown Hubs could declare that they are fit and proper to conduct such routings and so the limit of requests issued to the large Hub would quickly run out. Because Hub requesting freezing of funds by another hub, would pay for that service because the income earned from routing of transactions is deduced from the reward, which will guarantee that it will be economically unjustified not to enter into business relationship with new comers to the LN ecosystem.

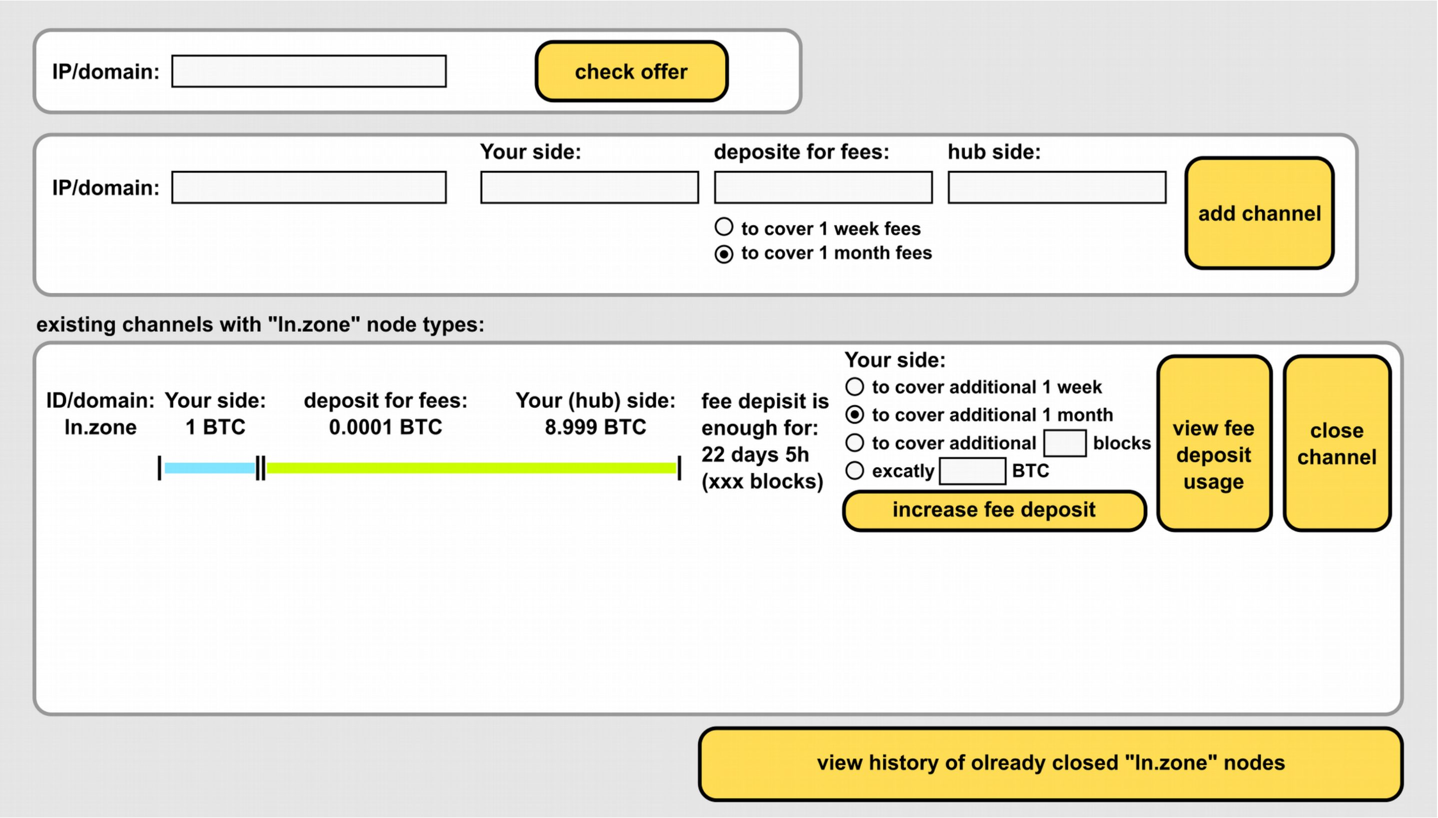
Some LN idealists respond to our way of thinking by saying that the mythical coffee house will also have to pay ex. for the goods and the LN operating costs will be balanced out by payments realised by the coffee house. However in today's world the coffee house will not be able to pay for any of its costs with use of the LN. **It is not a good idea to propagate a new payment system by the assuming that from its conception it will become the only payment system in the world.** Even if the LN will become as popular as we would like it to be, it would still be naive to demand every LN participant to spend exactly as much funds using LN as he would earn.

We believe that it is not necessary for every node to declare its costs of freezing accounts, however we do believe, that such an option should be included by the ability to ask node about the aforementioned four points. Node willing to open payment channel with a hub should send to the hub request for cooperation including:

1) capacity of payment channel to be opened with the Hub

2) how much Hub's funds should be frozen

3) how much of the remaining funds in the channel usually assigned to the client should be used as deposit for hub's costs.



IP/domain:

IP/domain:	Your side:	deposite for fees:	hub side:
		○ to cover 1 week fees ● to cover 1 month fees	

existing channels with "ln.zone" node types:

ID/domain:	Your side:	deposit for fees:	Your (hub) side:	fee depisit is enough for:
ln.zone	1 BTC	0.0001 BTC	8.999 BTC	22 days 5h (xxx blocks)

Your side:
○ to cover additional 1 week
● to cover additional 1 month
○ to cover additional □ blocks
○ excatly □ BTC

We believe, that for node-client (coffee house) interaction with the hub, such simple interface should be sufficient and include the following screen:

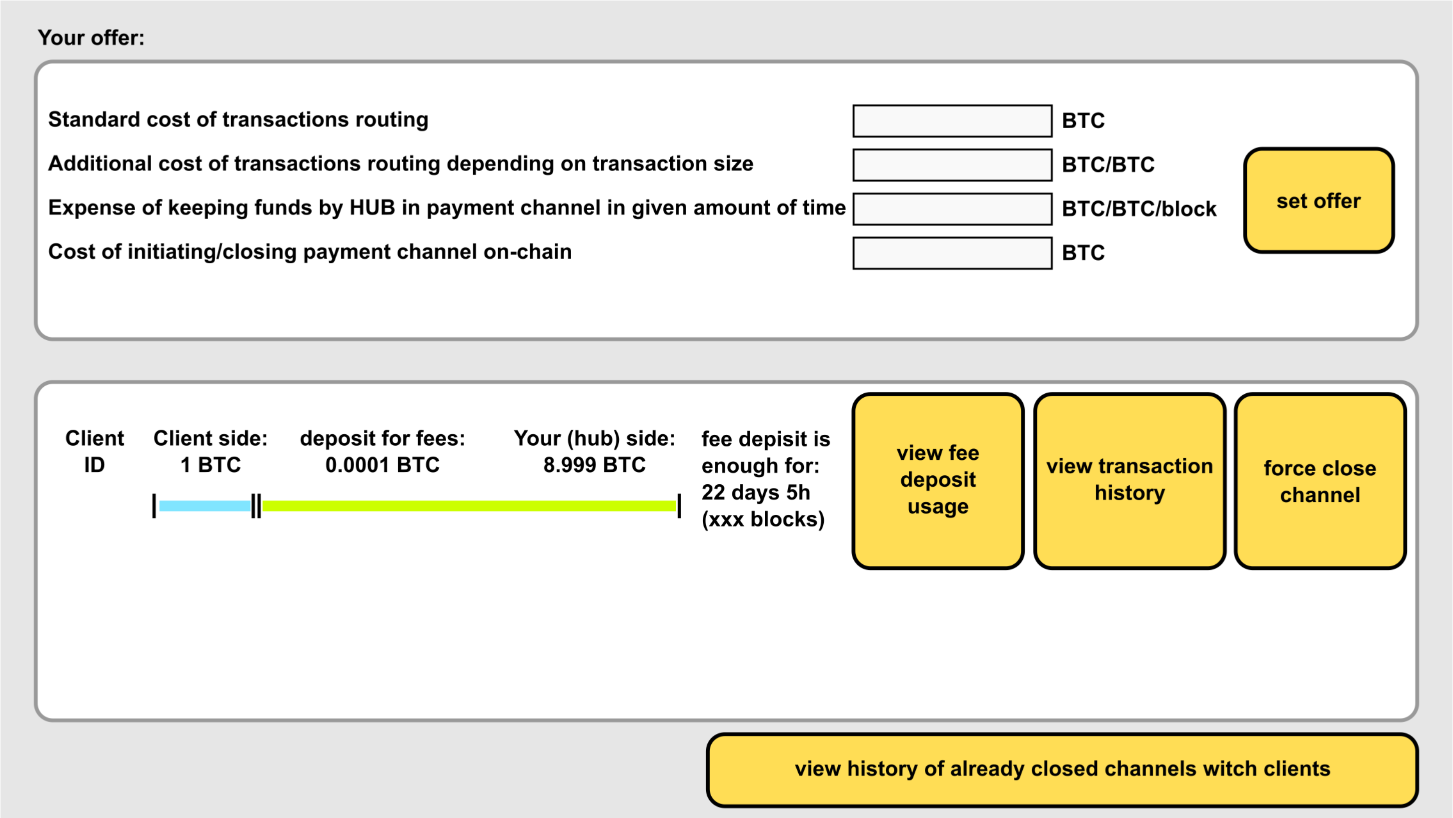
We use the first top button to check Hub's offer (when pressed, window including Hub's offer should pop up). If the offer seems interesting, we declare in request for cooperation three data required to commence the cooperation and the payment channel is opened, where funds are allocated as described on the list below.

Part of these funds belong to the client and part to the Hub. Part of these funds belonging to the hub include a small portion of what client left to the Hub as deposit covering the costs of maintaining the channel. This deposit can be at any moment increased (button "increase fee deposit"), thanks to built-in wallet option to increase that deposit by LN transaction between client and hub, one can also browse through of history of this deposit and close the channel.

Clicking "add channel" should result in sending to HUB three variables presented on the last slide, and later opening a two-way channel. We are not going to describe how to open a two-way channel. It would be best, if in fact these were two channels: first – opened by the client to the hub. Right after opening this channel client sends funds to the hub to cover fee deposit and once the transfer is cleared, HUB is able to open client's channel in the value declared by the client in three different variables. Such solution is trust-less and the only risk incurred by the customer are the deposited funds for fee. From the point of view of the client interface, we propose to hide the fact that that the two-way channel consists in fact of two separate channels.

Such reward model guarantees to the HUB, that in case the deposit runs out (in the example shown above it will run out after 22 days) it shuts down the channel automatically leaving the customer with whatever the channel's value was on customer's side.

When it comes to managing such a node from the Hub's perspective, it is our opinion that the hub may have the following interface available:



Your offer:

Standard cost of transactions routing	□	BTC
Additional cost of transactions routing depending on transaction size	□	BTC/BTC
Expense of keeping funds by HUB in payment channel in given amount of time	□	BTC/BTC/block
Cost of initiating/closing payment channel on-chain	□	BTC

Client ID	Client side:	deposit for fees:	Your (hub) side:	fee depisit is enough for:
	1 BTC	0.0001 BTC	8.999 BTC	22 days 5h (xxx blocks)

Where Hub may declare all information which may be of interest to the clients.

The Idea described above does not include such nuances like the fact the HUB should perhaps change its offer in the future. It would be possible by way of some special request, about the hub's future offer. In response to such request Hub may respond with a new offer and block from which point this offer will be enforced. This has only informative function, because hub takes from the client's deposit as much as it likes, however transfer of such information should be taken into account.

This is all I have to say about this.

We would like to implement the above by creating next layer above the LN urging both the clients of such commercial hub and hubs themselves to run applications above the LN layer. We believe this to be of such importance that this idea should be introduced within the entire LN infrastructure and we encourage LN developers to turn this idea into reality.

Adam Gramowski

shitcoins.club