Notebook - Routing_Payments_on_the_Lightning_Network

Page 4 | Highlight

> Another proposal, which follows a different approach, is to deploy the Lightning Network (LN). The LN allows to significantly increase the throughput of Bitcoin in term of transactions, while keeping the bandwidth requirements low and therefore the network more decentralized.

Page 4 | Highlight

> While the LN approach seems promising, there still are, though, important issues to be addressed before it can be deployed and exploited to the full extent. The first one is a routing problem, i.e. defining how payments should be routed. The routing problem is in turn dependent on how the LN nodes apply the fees for processing payments. Currently, as defined by the BOLT specifications [1], intermediate nodes apply a fixed charge plus a proportional fee for forwarding a payment. As a first contribution of this work, we show that such an approach is not optimal in terms of guaranteeing the best network performance and propose a new, more general way of specifying fees.

Page 7 | Highlight

> version version of the block format
>
> • prev block the hash pointer to the previous block, i.e. SHA256 hash of the previous block header
>
> • merkle root The merkle root of the block, i.e. a SHA256 hash representing all the transactions included in this block
>
> • timestamp Timestamp of when the block was created
>
> • nonce The nonce value used to generate this block (used in the mining process)
>
> • txn coint Number of transactions in this block set always to zero

Page 8 | Highlight

> the coinbase transaction

Note:

What is the coinbase trasection

Page 11 | Highlight

> As current transactional capability is not enough for the Bitcoin currency to be adopted at large scale, proposals have been made to overcome such a limit. One the proposals consists in changing or eliminating altogether the limit on block size. Such a proposal, though, is not encountering a broad support from the Bitcoin stakeholders, such as the main Bitcoin developers, because of fear of losing the decentralization property of the network.

Note:

İlk teklif neden kabul edilmedi
burada ve aynı zamanda bu sorunu çözen
oradığı belli

Page 11 | Highlight

> hard fork of the protocol,

Note:

Benzer bir sorunda ethereum buna başvurmuştu.

Soft vs Hard fork bak!!!

Page 12 | Highlight

> Such a protocol makes use of payment channels. A payment channel is a logical connection between two Bitcoin peers where multiple off-chain bitcoin transactions can be made. Such transactions involves only such two entities and can happen as fast as the network between them allows.

Page 12 | Highlight

> each peer signs a Revokable Committment Transactions (RCT) which allows the other peer to unilaterally close the channel and get the amount it committed back (to avoid the perennial lock of the funds in the channel should the other peer become unresponsive).

Page 13 | Highlight

> To recap, peers can create as many RCTs they want, thus changing the balances of the channels and performing payments.

Page 14 | Highlight

> The advantage of the payment channel is that many transfers can be made between the two participants, without any cost for the network as a whole. The disadvantage is that the channel needs to be created and then closed (which requires two Bitcoin transactions), which makes the use of the payment channel feasible only when the involved entities plan to perform many transactions among themselves.

Note:

Genel bir özet olmuş bunu tezin başında kullanabilirsin

Page 19 | Highlight

> Such a strategy can be convenient in the case there is no single path that alone can transfer the entire amount or when, by splitting the payment on more paths, it is possible to reduce the total amount of fees paid.

Note:

Tek bir yol olması fee'in en az
olacağı anlamına gelmez

Page 19 | Highlight

> maximum fee of 0.13mBT C.