LRFP : Extending local routing protocols in layer 2 networks with a secure fee model

TUDelft

Oliver Neut, Dr. Stefanie Roos, Oguzhan Ersoy
o.l.c.neut@student.tudelft.nl

1 Background:

- Blockchain protocols lack in scalability
- Off-chain payment channel networks (PCNs) solve this problem
- Payment splitting across nodes is possible using local routing protocols[1]
- Fees are used to incentivize intermediaries to forward payments across the network

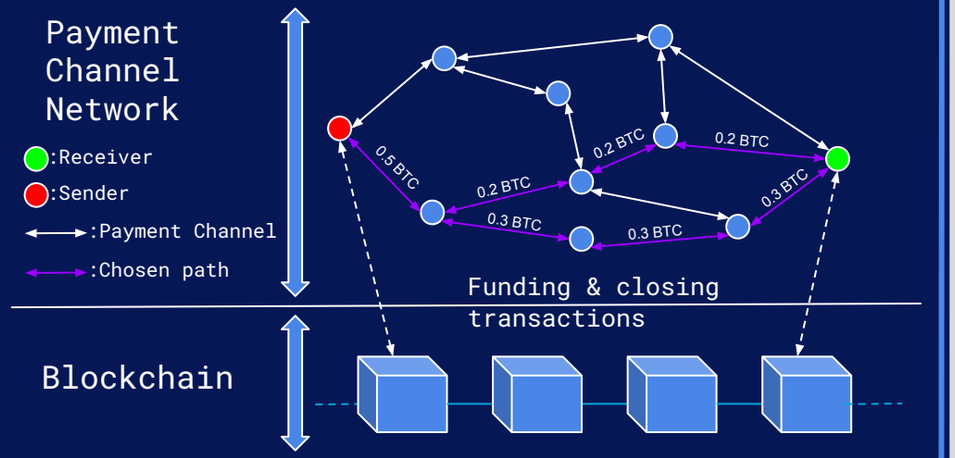

Figure 1: Illustration of a PCN

2 Main question:

- A solution to integrate fees in a PCN that uses payment splitting, while maintaining the security guarantees of such a PCN, is needed.

3 Research Method:

1. Read how payment splitting protocols work.
2. Different fee models were researched.
3. Different security properties that are needed for this protocol were concluded.
4. Verification that fee model adheres to security guarantees with help of cryptographic proofs.

Security properties[1]:

1. **Termination :** protocol terminates in finitely many rounds
2. **Balance neutrality :** bounded loss for the sender and intermediaries cannot lose coins
3. **Atomicity :** Either the transaction succeeds or it doesn't occur at all.
4. **Correctness :** if all parties are honest and the capacities are sufficient, then the transaction occurs.

These properties change slightly due to fee integration

*
v : total payment amount
$\mathbf{f}_{max}$: maximal fee amount sender is willing to pay
$\mathbf{r}_I$: base fee of intermediary **I**
R : receiver ; **S** : sender

Proposed fee model: Maximal fee[2]

Local routing : each intermediary chooses how to route payment

1. **S** sends $\mathbf{v} + \mathbf{f}_{max}$ to **R** *
2. Intermediaries **I** claim base fee $\mathbf{r}_I$ and send $\mathbf{v} + \mathbf{f'} - \mathbf{r}_I$
3. Once at least **v** coins arrived at **R**, **R** unlocks conditional payments

----------EXAMPLE----------
S sends 10 coins to **R:**

$\mathbf{v}$= 10 ; $\mathbf{f}_{max}$= 1 ; $\mathbf{r}_A$= 0.5 ; $\mathbf{r}_B$= 0.5

$\mathbf{Route}_G$ algorithm splits payment in k payments of value v_j and f_j $(\sum_{j\in[k]} v_j = v \ , \sum_{j\in[k]} f_j = f_{max})$

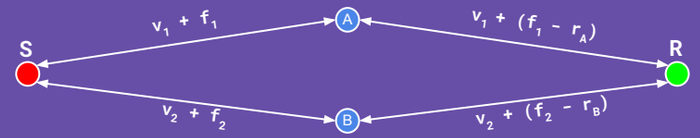

Figure 2: Example of the fee method

4 Conclusion:

- security properties are maintained
- intermediaries in network receive fees for forwarding
- room for improvement

References:

[1]: L Eckey, S Faust, K Hostáková, S Roos: Splitting Payments Locally While Routing Interdimensionally
[2]: Y. van Engelshoven, S. Roos. The Merchant: Avoiding Payment Channel Depletion through Incentives