Decision-making system for decentralized multi-hop payments

Multi-hop payments across one or more intermediaries revolve around a singular decision: cancel or or start the payment (and once started the payment will always succeed, one way or another). Each person in the payment chain has to agree on the outcome of this decision. To guarantee that the decision-making succeeds (i.e., either cancels or starts the payment), an incentive system is needed. The incentive used is a financial penalty, that either increases a person's outgoing balance or reduces their incoming balance (or does both at the same time). The penalty both enforces that the decision is made and enforces that each person agrees with it. The decision itself (cancel or start) has to be centralized to a single person. When it comes to agreements along a chain of people, the only person who can be certain about if everyone agreed is the last person in the chain. Thus logically, the authority for the decision should be either the buyer or the seller. To enforce the decision, the penalty only works on the buyer, thus the authority for the decision has to be the buyer.

Prior to making the decision to cancel or start the payment, the buyer asks the payment chain if they agree to start the payment (or to “commit” to the payment). Every intermediary that “commits” does so indefinitely (i.e., until the buyer either cancels or starts - “seals” - the payment). If the payment chain does not agree to “commit”, the buyer is forced to cancel (as their outgoing balance is continuously increasing, i.e., the amount that can be cancelled is continuously decreasing). If the payment chain does agree, the buyer is motivated to “seal” the payment and revoke their right to cancel the payment (thereby stopping the gradual increase of their outgoing balance). At each intermediary, the agreement to “seal” is enforced by a combination of the two penalty mechanisms, a gradual increase in the outgoing balance and a gradual decrease in the incoming balance (relative to the payment amount). Note that once the buyer has issued “seal” and revoked their right to cancel, the payment will always succeed, one way or another.

Once the payment chain has agreed to “seal” and the agreement reaches the seller, the seller will issue the “finalize” command, thereby claiming the payment from the intermediary prior to them and removing themselves from the payment (and at this point, the payment has succeeded as the seller has gotten paid). The next “hop” is incentivized to agree to “finalize” as their incoming balance is gradually decreasing (i.e., the amount that can be finalized is gradually decreasing) relative to the outgoing amount that they already finalized to the seller. This gradual decrease in incoming balance acts on each “hop” to enforce that each hop agrees to “finalize”, and once “finalize” reaches the buyer the payment is finished for everyone involved.

The penalty enforces compliance with the decision-making system in all scenarios except for when the attacker is a combination of people such that they end up sending the penalty to themselves. During “seal” this always has to include the buyer and the seller (as the seller is guaranteed to get paid), and during “commit” it always has to include the first person of the chain and the last person of the chain. To deter attacks in this scenario, fees have to be added on top of the payment, that are paid out to each person in the payment in proportion to how long the payment was stuck. These fees also have a secondary effect of compensating victims of a stuck decision, and the buyer also gets compensated at the same time because the attacker ends up paying the seller.