

Incentive system for decentralized multi-hop payments

Multi-hop payments across one or more intermediaries has the problem that a decision can get stuck if an intermediary does not forward it to the next “hop”. The solution to this problem is an incentive system. With the correct incentives, the decision-making in a decentralized payment chain can be guaranteed to either end with a successful payment or with a cancelled payment. The incentives have to enforce that an agreement is made to either succeed with the payment or cancel the payment.

The decision to either succeed or cancel has to be centralized down to a single authority. 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 (the receiving end of a decision can be certain that previous hops agreed on it, but the sender cannot be certain that hops further down the chain will agree on it). Thus logically, the authority for the decision should be either the buyer or the seller.

The incentive needed is a penalty that forces the buyer to make the decision to either succeed with or cancel the payment, and, a penalty to enforce that this decision is agreed on by everyone else in the payment chain. To enforce that the buyer makes the decision, the penalty should gradually decrease the amount that the buyer can cancel, thus forcing the buyer to either cancel, or “seal” the payment (and when “sealed” the payment will always succeed, one way or another). To enforce that either decision is agreed on by everyone in the payment chain, the same gradual decrease in the amount that can be cancelled will enforce the cancel agreement, and a gradual decrease in the amount that can be finalized will enforce a “finalize” agreement (with the “seal” agreement in between enforced by a combination of both effects, acting on either end of an intermediary).

These two penalty mechanisms, that can act on either a person's outgoing balance (the continuous finalization) or a person's incoming balance (the continuous cancellation), enforce agreements in every scenario, except when both the buyer and seller attack the system (i.e., both the buyer and seller deliberately cause the payment decision-making to get stuck). When both the buyer and seller attack, the two penalty mechanisms have no effect (the attacker ends up sending money to himself or ends up cancelling the full payment). To deter “stuck decision” attacks in that scenario, fees are added on top of the payment, paid by the buyer to everyone else in proportion to how long the payment got 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.