Ripple Inter Server Protocol built on a penalty system

Johan Nygren, @bipedaljoe

In 2004 Ryan Fugger invented the money system Ripple. Ripple takes banking down to the smallest possible scale by making each person-to-person relationship a “bank”. Payments rely on a process similar to traditional “inter-bank payments”. Traditionally in inter-bank payments, a payment can be transferred via multiple intermediary banks. Likewise in Ripple, the path can involve multiple “person-to-person banks” as intermediaries. Traditionally in inter-bank payments there is a central authority that coordinates the payment. The idea with Ripple is to instead coordinate the payment in a fully decentralized way. To achieve this, a penalty system is needed that enforces that each decision in the payment is passed on to the next “hop”.

The penalty system

In 2006 Ryan Fugger had started to design a penalty system. The idea was that the payment will finish from the seller and backwards towards the buyer, and that a gradual penalty would be imposed on any intermediary who did not forward the decision. This ensured that the decision to finish the payment would not get stuck (or, that if it did get stuck, the person who caused the decision to get stuck would pay for doing so). This design caused yet another problem: how could the gradual penalty be started without introducing the possibility for yet another decision to get stuck? The solution to the new “stuck payment attack vector” is yet another penalty. There, the payment should start from the buyer and forwards towards the seller, and the penalty will be imposed on the buyer. The buyer is therefore motivated to cancel the payment unless the decision managed to reach the seller (who then contacts the buyer directly). The buyer then has to tell all intermediaries that they revoke their right to cancel, so that the payment can finish from the seller and backwards towards the buyer. The problem there, is that it is yet another decision that can get stuck. Thus, so far, for every solution we have created a new problem. The solution in this case, is to combine the first solution and the second solution. In the first solution, the amount of the payment that can be finalized is gradually reduced, and in the second solution, the amount of the payment that can be cancelled is gradually reduced. The consequence is that if the decision to revoke the buyer's right to cancel gets stuck, there is two opposite penalties acting on the person at which the decision is stuck. This ensures that the person who causes the decision to get stuck also ends up having to pay for it. Thus, with these three steps, the penalty system is complete, besides for one last thing. If the buyer and seller work together to attack the system, these penalties do not work. To cover that scenario, separate fees have to be added on top of the payment. These fees are paid out by the buyer and to each intermediary (and to the seller) in proportion to how long time the payment got stuck. The fees also have the benefit of rewarding people who end up in a “stuck payment” (and the buyer is simultaneously rewarded as the person who caused the payment to get stuck ends up having to pay for it - unless of course this person was the buyer themselves).