Ledger Loops and the Tale of the Whispering Merchants (Work in Progress)

Michiel B. de Jong

November 2016

Abstract

LedgerLoops is a solution to the Whispering Merchants problem, where merchants sit in a loop and can only communicate with the persons sitting immediately left and right of them. Each merchant offers an item for sale to the person on their left, and is interested in the item offered by the person on their right. Beyond these two direct neighbors, none of the merchants knows or trusts the other participants in the loop. This whitepaper introduces a solution to the Whispering Merchants problem, based on semi-anonymous, semi-blind, cryptographic challenges. One of the merchants semi-anonymously creates a LedgerLoops challenge, in the sense that the other merchants know that it was created by one of the other merchants in the loop, but they do not know by which one. The LedgerLoops challenge is then used semi-blindly to complete each of the local trade transaction, in the sense that the creator of the challenge can roughly know the value of the trades it was used in, but cannot know exactly how many trades occurred, nor who participated in them, nor what the asset was that was traded.

1 The Tale of the Whispering Merchants

1.1 The old bench around the Tree

Once upon a time, around an old tree on the village square, a circular wooden bench was made. Merchants would sit on this bench, with their backs to the tree, to seek shade and, of course, trade. Each merchant would chat with the person sitting directly to their left, and the person sitting directly to their right. They can't see or directly communicate with anyone beyond their immediate neighbors.

As the merchants tend to speak in whispers, none of them know exactly how many people are sitting around the tree, nor who the other merchants are, nor what trades they are discussing - except of course, for their own direct neighbors.

Wild rumours would often circulate around the tree in either direction, but would often change or be exaggerated along the way, meaning that all merchants soon learn to only trust first-hand information, from either of the two persons they can see and speak to.

1.2 Peer-to-peer Barter, and the Deadlock Situation

On some days, trade would be plentiful, as each merchant would bring various items, trade some of those against other items with their left neighbor, do the same with their right neighbor, always looking for items they think they can sell again in a next barter transaction. Sometimes items would travel halfway around the tree before they reach a merchant who cannot sell it on further.

But on this particular Monday, none of the merchants is able to reach a barter trade with either of their neighbors. The problem is that each merchant has an interesting item to offer to the person on their left, but not to the person on their right.

Conversely, each merchant is only interested in the item offered by the person on their right, but not in the item offered by the person on their left.

Each merchant would be willing to trade in either direction, but since the person on their left has nothing to offer to them, and they have nothing to offer to the person on their right, none of the conversations lead to a trade, and the merchants all go home disappointed, still holding the item they had hoped to sell.

Trade stays blocked for weeks, as each merchant brings the same item with them every day, and sits at their usual spot inbetween the two neighbors they trust, but is unable to trade with either of them.

Word goes round the tree that each merchant is in the same situation, wanting to sell an item to the left, and wanting to buy an item from the right. This makes the merchants even more frustrated, because they realize everyone could trade, if they would only have some system of cooperation. The merchants all realize they will have to invent some sort of financial technology, or stay in this deadlock situation forever.

1.3 Monday: Transitivity of Trust

The next Monday, one merchant has an idea: he explains to his left neighbor that he is interested in an item from his right neighbor, and