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 is willing to take a little risk, in everybody's benefit. He offers to lend the items he owns to his left neighbor, in the hope his neighbor would do the same, until his own right neighbor has lent the item he wants to him. He promises his left neighbor to cancel the debt once all items have moved one position to the left, in the hope each merchant will do the same, and his own right neighbor will also cancel his own debt. If this goes wrong at any point, the merchants can all just give the items back where they came from. This system seems to work at first, and all merchants are happy, until one merchant sees an opportunity to trick the system. Even though he did receive the item he wanted from his right neighbor, he quickly hides it, and tell his left neighbor sorry, I don't know what happened, but it seems the wave of transactions never made it around the tree, so please give me back the item I lent out to you. His left neighbor tell him, OK, I will give you back the item I borrowed from you as soon as I get back the item from my own left neighbor. All merchants ask their item back from their left neighbor, until somewhere someone in the chain decides they have no incentive to reverse the trade they just made, and doesn't cooperate.

The merchants now realize that this system is very brittle, since it relies on transitivity of trust: even if your own left neighbor would never steal from you, and their left neighbor would never steal from them, this doesn't mean that this third person can also be trusted not to steal from you.

1.4 Tuesday: Commodity Money

Having learned from their first experiment, on Tuesday, the merchants try out a different system. They realize that each of them eats fruits from the tree they're sitting under, and fruits on the tree are getting scarce. They decide to use fruit as a commodity currency. Each merchant offers the item they have for sale to their left neighbor in exchange for one piece of fruit. The items all move one merchant to the left, as pieces of fruit are moved to the right.

Some merchants would hold ever bigger bags of fruit, until the fruit they buy from each other is much more than they will be able to eat, and carrying the bags of fruit becomes impractical.

1.5 Wednesday: Fiat Money

On Wednesday, a banker appears in the village, and gains the trust of all merchants around the tree. He offers fruit vouchers in exchange for fruits, promising to exchange these vouchers back for one piece of fruit per voucher at any point in the future. The merchants start exchanging these vouchers instead of exchanging the cumbersome fruits themselves. The banker keeps a big pile of fruit while the merchants now only exchange pieces of paper whose value depends on the trustworthiness of this one banker. This system works quite well as long as the banker can be trusted not to eat all the fruit.

This day, all items also successfully move one merchant to the left, and fruit vouchers which all merchants bought from the banker move to the right.

1.6 Thursday: Bank Loans

On Thursday, the banker starts to offer a new service: from now on, merchants don't have to give him one piece of fruit as the only way to obtain a fruit voucher; merchants can now also borrow fruit vouchers from the banker, as long as they promise to give back either one voucher or one piece of fruit in the future, and as long as they pay an interest fee. This allows the merchants to trade more, even when they haven't plucked any fruits first. The banker soon realizes he can put more fruit vouchers into circulation than the number of fruits he actually has stocked, as long as merchants don't come and exchange their vouchers for fruits all at the same time.

This day, all items also successfully move one merchant to the left, and fruit vouchers which all merchants borrowed from the banker move to the right.

Some merchants go bankrupt and can't pay the banker back, which means the banker's fruit stock is now even smaller than he thought, the merchants all realize this and get nervous, so they ask the banker to exchange their vouchers for fruit, before the banker's stock runs out completely. And so, of course, the banker is out of fruit stock within minutes.

The merchants learn from this, and realize that if bank loans can so easily lead to an unstable system, then fiat money was maybe also not such an ideal system, since it also relies on trusting a banker instead of just trusting the two merchants sitting directly beside you.

The mayor of the village restores the banker's fruit stock, in the hope to keep trade around the tree flourishing, and to allow the banker to keep up the beautiful tradition of paying himself a bonus at the end of the year, but the merchants don't really trust the banker anymore, and they are already looking for a better financial technology.

1.7 Friday: Blockchains

On Friday, one of the merchants creates an Altcoin, mines the first few blocks in order to build up some personal stock, and then starts allowing other merchants to also mine blocks for his Altcoin. He publishes some software which allows all merchants to mine and trade his Altcoin.

Although the Altcoin has no intrinsic value, one merchant starts to offer the item he wants to sell to his left neighbor in exchange for one coin, while at the same time offering one coin for the item his right neighbor is trying to sell.

As all merchants do this, all transactions are successfully completed, and the coin effectively obtains value.

Some merchants start to speculate by selling and buying coins at strategic moments, others specialize in mining coins, and as the scarcity of the coin fluctuates, so does its value. When the value is really high, the merchant who invented the Altcoin sells his personal stock from the first few block he mined, and all merchants who owned coins at this time, suffer. The merchants decide to try something else the following day.

1.8 Saturday: Ledger Federation

On Saturday, more bankers arrive in the village, and start offering different fruit vouchers. The merchants welcome the arrival of more bankers, as they feel it spreads their risk a little more than having just one banker in the village. However, as it's very impractical to have so many different fruit vouchers, they convince their bankers to accept fruit vouchers from other bankers as well. The bankers get together and set up a Unique Node List, which lists one computer from each banker. Together, the computers in this Unique Node List are quite reliable for bankers to exchange each other's fruit vouchers among themselves.

The merchants are sad though - they don't really trust the bankers, and they are bitter to see how the bankers profit from the bail-out guarantees from the mayor. And although Altcoins briefly seemed like a promising solution, now that they have seen how it works in practice, they also don't trust the publishers of Altcoin software anymore.

1.9 Sunday: Ledger Loops

On the seventh day, one of the merchants invents LedgerLoops. What he does is actually quite simple: he creates a cryptographic challenge which he knows only he can solve, but for which anyone could verify if a given solution is correct. He tells his left neighbor: I will give you this item if you can show me the solution of this cryptographic challenge. Each merchant tells his left neighbor the same, until initiator's own right neighbor does so. After this, the correct solution is sent back in the other direction, and all trades are completed.