CSC2125: Homework #10

Due on December 3

Fan Long

Thomas Hollis

Problem 1

How does IOTA protect against a double spending attack? Hence are transaction confirmations guaranteed (like in Algorand) or probabilistic (like in Bitcoin)?

Solution

IOTA protects against double spending attacks using its main transaction processing architecture known as the Tangle. In order to explain how the Tangle protects against double spending we should first explain what the Tangle is and how it works.

The Tangle is a transaction DAG. According to the IEEE, the taxonomy of decentralised ledger technology (DLT) is laid out as follows:

1. Blockchains
A. Traditional - store transaction in a blockchain, simplest (e.g. Bitcoin)
B. Offchain - group transactions in local ledgers, better scaling (e.g. Lightning)
C. Sidechain - dynamically connect new sidechains to mainchain (e.g. LISK)
D. Altchain - alt blockchain with tokens/smart-contracts (e.g. ETH Namecoin)

2. Blockchainless DAGs
A. BlockDAG - blocks inside a DAG, usually has Tx fees (e.g. Algorand)
B. TDAG - transaction DAG, no total ordering (e.g. IOTA)

From the above taxonomy we see that IOTA's Tangle is a blockchainless TDAG allowing for free transactions without fees. The IOTA Tangle approves transactions by requiring each new transaction sender to approve two previous existing transactions, as explained in section 1 of the whitepaper. Indeed, figure 1 shows that this results in the directed edges of the Tangle whereby new transactions reference older ones and attach to them. These attachment sites are called tips. A transaction should only approve two existing tips if it verifies than none of the transactions down chain from those tips are conflicting (i.e. are double spending). Indeed, a malicious attacker could self-reference his own malicious tips, but new nodes would tend to not reference these tips because of the tip selection algorithm. Indeed, the MCMC tip selection algorithm (recommended for all nodes to use) favours honest nodes based on node weight. As a consequence, the deeper a transaction is in the Tangle, the higher its likelihood of being verified by honest nodes rather than malicious nodes. Transactions on the edge of the Tangle have a high uncertainty of being honest so are never considered verified until they reach deeper into the Tangle.

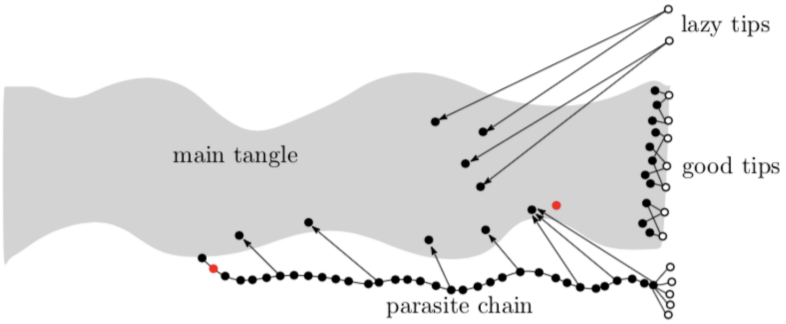
Indeed, we can therefore conclude that transaction confirmations are therefore only probabilistic, like in Bitcoin.

Problem 2

What is a parasitic tangle and how can it be created? Is this a problem in IOTA?

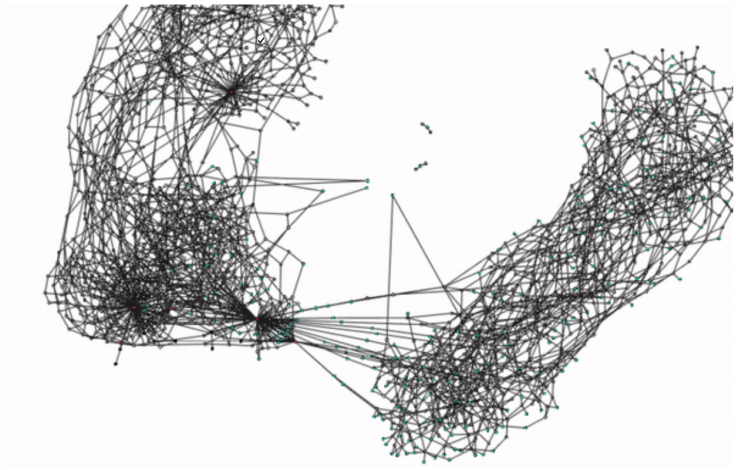
Solution

The parasitic tangle is a form of Sybil attack that can be launched against the IOTA tangle. As explained in section 4.1 of the whitepaper, an attacker can generate a subtangle, or parasitic tangle by creating transactions that mostly reference each other but occasionally reference the main tangle to gain a higher score. The official IOTA whitepaper theoretically predicted how parasitic tangles would look like and this is shown as follows:



Theoretical IOTA parasitic Tangle visualisation

While such a parasitic Tangle does currently exist in IOTA, this is not currently a problem mostly because of the Coordinator. The Coordinator prunes tips and selects transactions to validate thus artificially creating a resistance against the existing parasitic tangle that still remains in the IOTA main Tangle. As a consequence, it is very rare that a user accidentally selects a tip from the parasitic Tangle and when this happens the transaction is often dropped and must be resubmitted. As a comparison with the predicted IOTA parasitic tangle from the whitepaper shown above, here is a visualisation from one of the IOTA tangle explorers on the current state of the parasitic tangle:



Actual IOTA parasitic Tangle visualisation (right hand side)

Problem 3

Is IOTA a truly decentralized protocol? Discuss issues facing The Coordinator and IOTA's Incentive mechanism. (open ended question)

Solution

As we have seen in the previous questions, IOTA offers all users with the huge advantage of free transactions. However, because of this simple fact, we know that there is no true incentive mechanism. Indeed, there are no miners and there is no financial incentive to approve transactions on the IOTA Tangle. The only pseudo-incentive scheme that IOTA offers is that users will confirm a few transactions after sending their own simply to make sure their transaction gets approved. Indeed, this leads to a very common behaviour in IOTA known as "lazy nodes". Lazy nodes are nodes who do the bare minimum amount of work to approve their transaction so that it gets accepted. This leads to a very low overall network hashrate (typically much lower than a single Antminer S9 ASIC). Indeed, since IOTA relies on the fact the network must have less than 34% dishonest hashpower, this is a giant problem. This issue is however addressed by using a centralised Coordinator (as mentioned previously in question 2). This Coordinator, while purely centralised and under the control of the IOTA foundation, is supposed to be a temporary node for protection against double spending. The IOTA foundation claims that this Coordinator will be turned off once IOTA reaches a critical mass but this is highly disputed. As we have shown in question 4 (shown on the subsequent page), IOTA is currently nowhere near ready to turn off its centralised Coordinator.

IOTA has however shut down the Coordinator in the past without negative effects because people did not know about this so nobody tried a 34% attack at those precise times. While the IOTA foundation claim they will turn it off permanently, they have never committed to a timeframe or maximum transaction per second (TPS) speed.

I would therefore personally say that IOTA is currently not truly decentralised, although it does have a potential for future decentralisation.

Problem 4

Consider the fact that people contribute to the network hash rate only when they send transactions and for each transaction they only compute 150M SHA256 hashes. Consider the speed of the current SHA256 ASIC miner speed as 13.5TH/s, how many TPS IOTA would require for it to turn off coordinator so that a single SHA256 ASIC miner cannot do double spending?

Solution

Bitmain's most recent SHA-256 ASIC (Antminer S9) is capable of 13.5 TH/s so the IOTA network hashpower must be at least 13.5 TH/s. In order to achieve 51% resistance against a single Antminer S9 ASIC, the IOTA network TPS must be around 90 000 TPS. In order to reach this number, we must first assume that a generous upper bound for a user to confirm a single IOTA transaction is 60s on a regular modern computer (currently takes about 1s in IOTA). This assumption is a fair one because if a full IOTA node cannot confirm a transaction in 60s on a regular desktop computer, it will never be able to be used on small IoT devices or by the general public as a whole. This would defeat the entire purpose of IOTA. Under this assumption, the proof that the TPS needs to be at least 90 000 is as follows:

$H_{att} = H_{honest}$ (condition for 51% attack)

$H_{honest} = TPS \times H_{transaction}$ ($H_{transaction}$ estimated to be 60×2.5 MH/s i.e. 60s of an average computer)

$\therefore TPS = \frac{H_{att}}{H_{transaction}} = \frac{(13.5 \times 1'000'000)}{60 \times 2.5} \approx 90'000$ TPS

For reference, at time of writing, IOTA's transaction rate is around 5 TPS (but can go much higher to more than 200 TPS when they have the spammer 'ON'). Indeed, unless you live in a world filled with IOTA-running IoT devices, this requirement to protect IOTA from a single Antminer S9 is unrealistic (in fact we don't think IOTA can even support such high TPS due to network latency). It is worth noting here that the estimate of 90 000 TPS is a generous one as the IOTA protocol actually breaks down beyond 33% malicious hash power.

However, some of the IOTA Staff (David Sonstebo) constantly claim that there is "no fixed number of TPS required to turn off the Coordinator" because it depends on what tip selection algorithm users choose (since you cannot force people to use MCMC and since IOTA are working on better tip selection algorithms). Nonetheless, I believe that this is just a marketing cover-up. Indeed, it seems to me that IOTA is, as of now, fundamentally nowhere near ready to turn off the Coordinator.