RUNI: Blockchains and Cryptocurrencies

Homework 2

Fall Semester 2022-23 TASHPAG

Submitted by: **Yarden Fogel (yarden.fogel@post.runi.ac.il)**
Partner: Liron Cohen (liron.cohen@post.runi.ac.il)

Date: December 31, 2022

Question 1: Byzantine Agreement in the Synchronous Model

Claim. *We will assume in contradiction that BA IS possible even if* $\geq \frac{n}{2}$ *nodes are corrupt, i.e.* $f \geq \frac{n}{2}$

Assumptions:

- Every party gets an input in BA before the protocol π starts, and generates an output at some point.
- The protocol is run for some number of rounds.
- Since it's a synchronous protocol, every node receives messages in every round - from some or from all other nodes (they don't know). They then run some function (which can change by round and is a black box to us), and pass on the result as the next message.

Proof. We will prove that BA is impossible if $f \geq \frac{n}{2}$ by contradiction, using an illustrative $n = 5$ nodes, but the proof would work just as easily for any $n \geq 3$. Since we make no assumptions about protocol π, and we assume that $\geq \frac{n}{2}$ nodes, or in this case 3 nodes are corrupt, it leaves us with 2 honest nodes. We simply present different possible scenarios for this unspecific protocol π whereby we hold one honest node constant, our friend Willy Wonka aka "WW", and hold inputs constant, and rotate our 2^{nd} honest node around the other 4 possibilities. We then "weaponize" our assumption by contradiction and the powers bestowed upon us by its presumed consistency and validity, to reach contradictions and dismiss the possibility of BA if $f \geq \frac{n}{2}$

Recall that in BA, consistency implies that if two honest nodes output b_1 and b_2, then $b_1 = b_2$. Validity is slightly different than in BB in that it states that if all honest nodes receive the same input b, then all honest nodes output b.

Compiled with LaTeX on December 31, 2022.

Our proof is as follows:

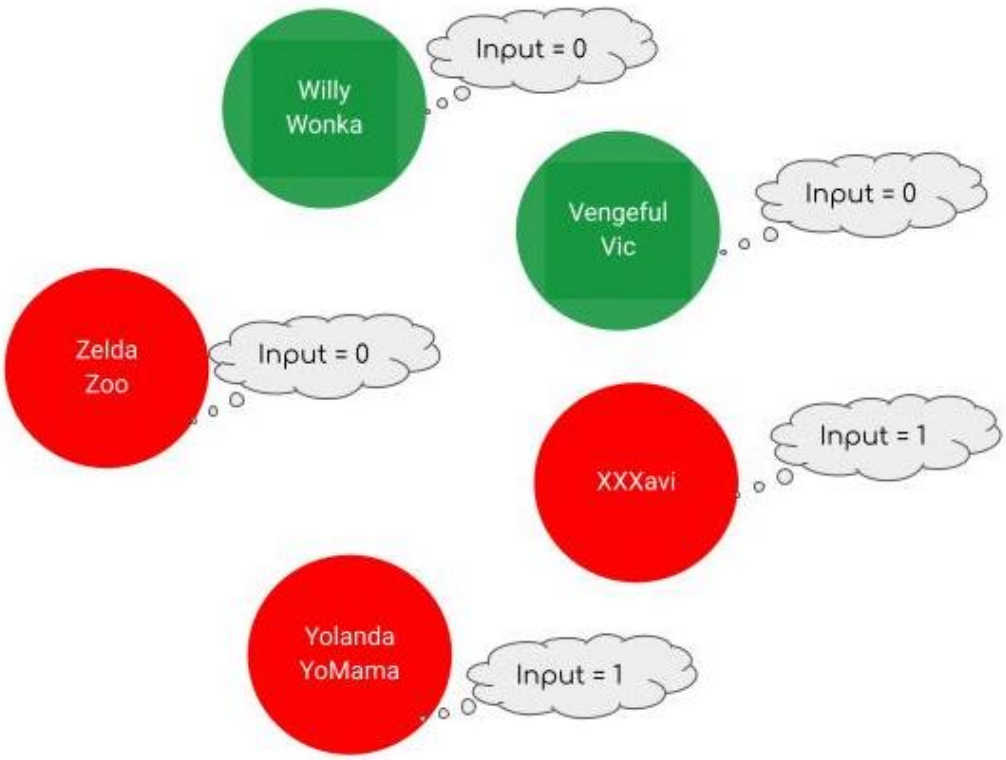

Figure 1: Scenario 1: WW, VV Honest

In **scenario 1**, with WW and VV as our 2 honest nodes, by our validity assumption, since all honest nodes received the same input (0), they both output (0). So far, so good.

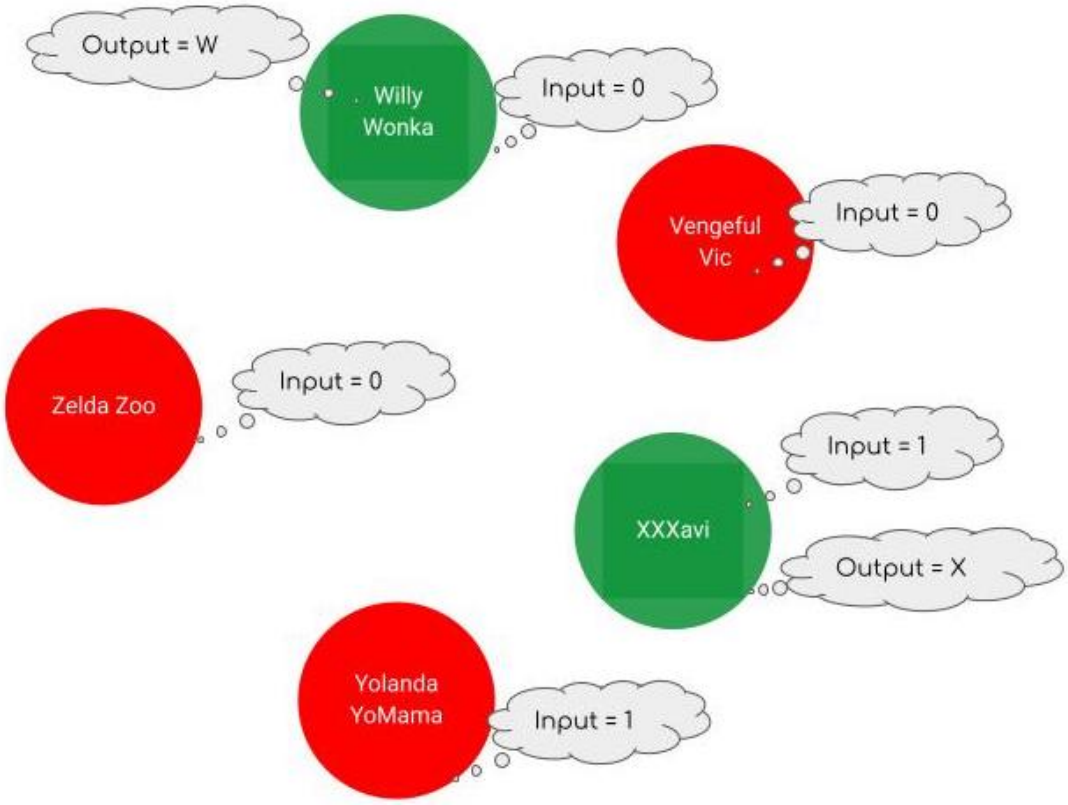

Figure 2: Scenario 2: WW, XX Honest

In **scenario 2**, Willy is still honest, can't help himself, but now VV is corrupt and our 2^{nd} honest node is XX. Again, assuming BA in contradiction, since all honest nodes don't receive the same input in this case, then WW outputs some W and XX outputs some X. By our consistency assumption, it holds that if two honest nodes, WW and XX, output W and X, then $W = X$ (which is already a contradiction since $W = 0$ and $X = 1$, but we will march on anyhow for sport!)

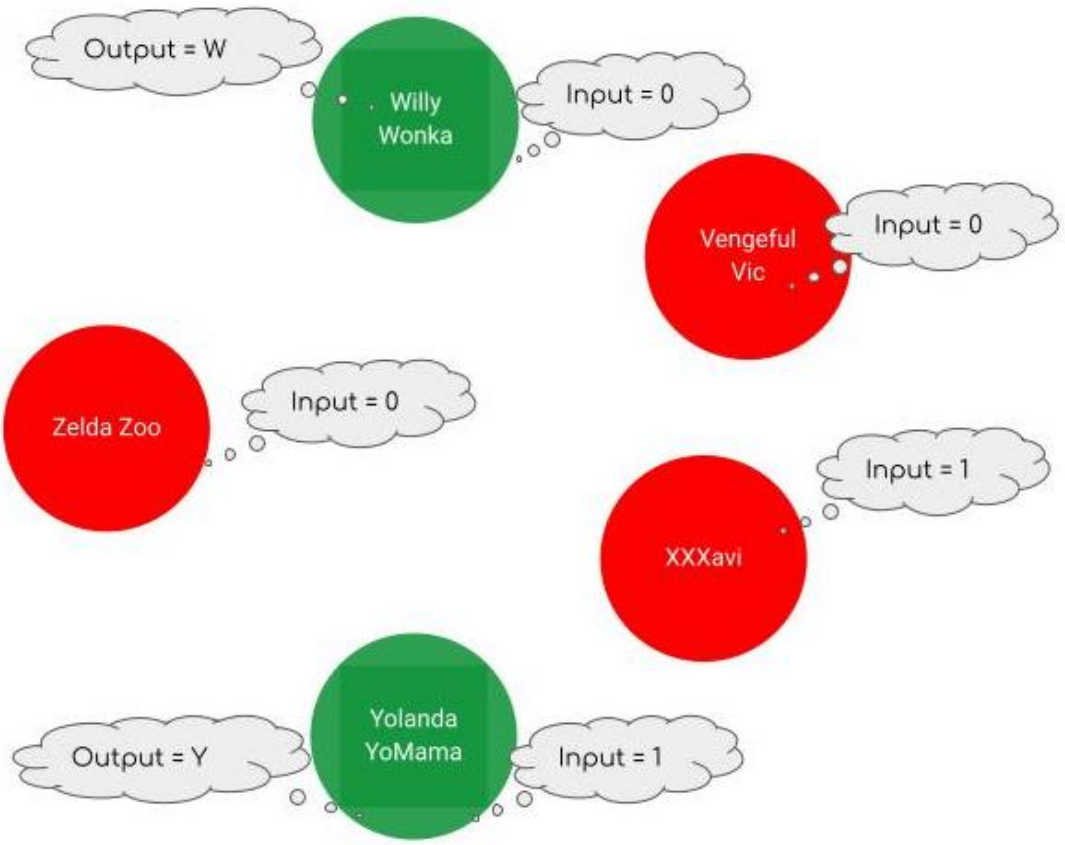

Figure 3: Scenario 3: WW, YY Honest

Here in **scenario 3**, Willy is still honest and now our old friend Yolanda YoMama is feeling ethical too, while the X-man betrayed us. Here again, since all honest nodes don't receive the same input, then WW outputs W and YY outputs Y, and by our consistency assumption, it holds that if two honest nodes output W and Y, then $W = Y$ (which we can see is also a contradiction)

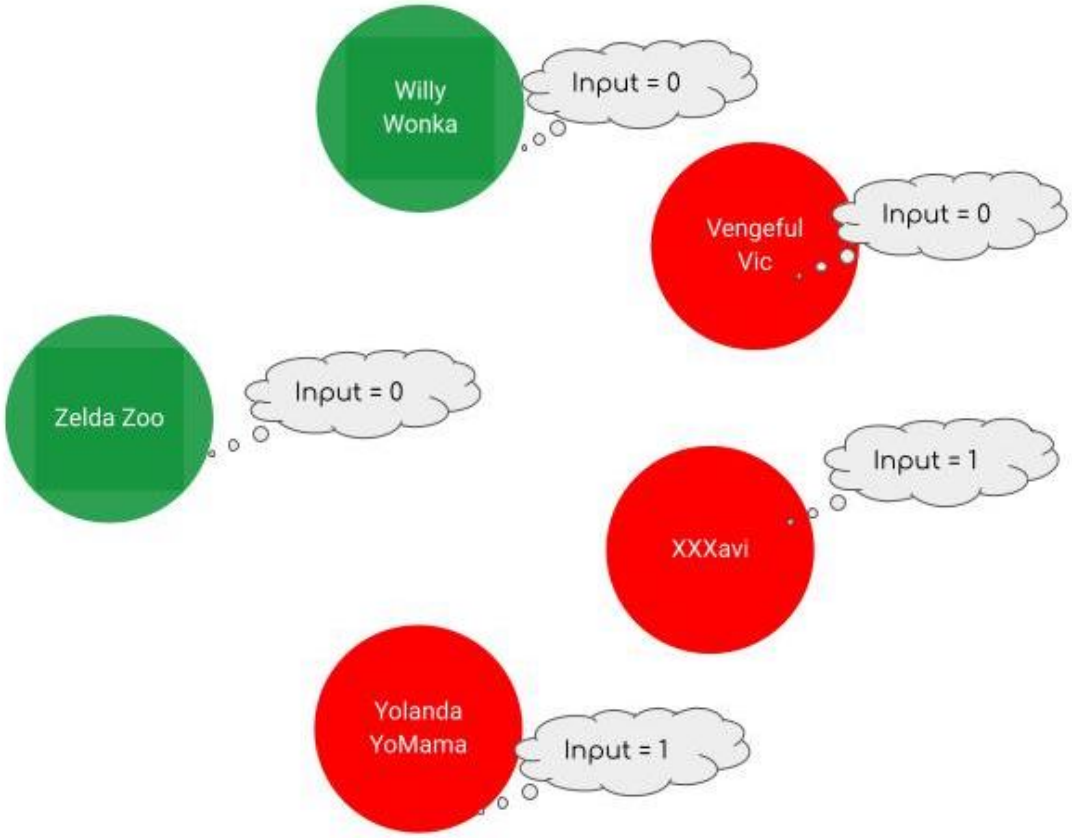

Figure 4: Scenario 4: WW, ZZ Honest

Finally, for completeness, in **scenario 4**, Zelda is honest and since all honest nodes have the same input (0), then by validity, they all (both) output 0.

As we managed to contradict our contra-assumption of BA TWICE in our first 3 scenarios, we conclude without a shadow of a doubt that BA is indeed impossible if $f \geq \frac{n}{2}$ QED Extra observation: Note the proof was rather straightforward, not to figure out, but to demonstrate, and we therefore didn't even need to get bogged down in the "details" of all sorts of messages being sent by all sorts of honest or corrupt nodes in all numbers of rounds. Validity and consistency to the rescue!

□