My Question

- I see how tampering with previous blocks in the chain is very difficult, but what makes it difficult to create an illegitimate new block?

My Question

- The conditions to add a block are:

  - Valid proof of work

  - Transactions (data) in block is "valid"

- So what makes the data "valid"?

- Say I legitimately provide valid proof of work, but I create a fraudulent transaction: "Yuwa paid me 10 million". I try to broadcast this block to all other nodes. How will the other nodes know to reject this fraudulent block?