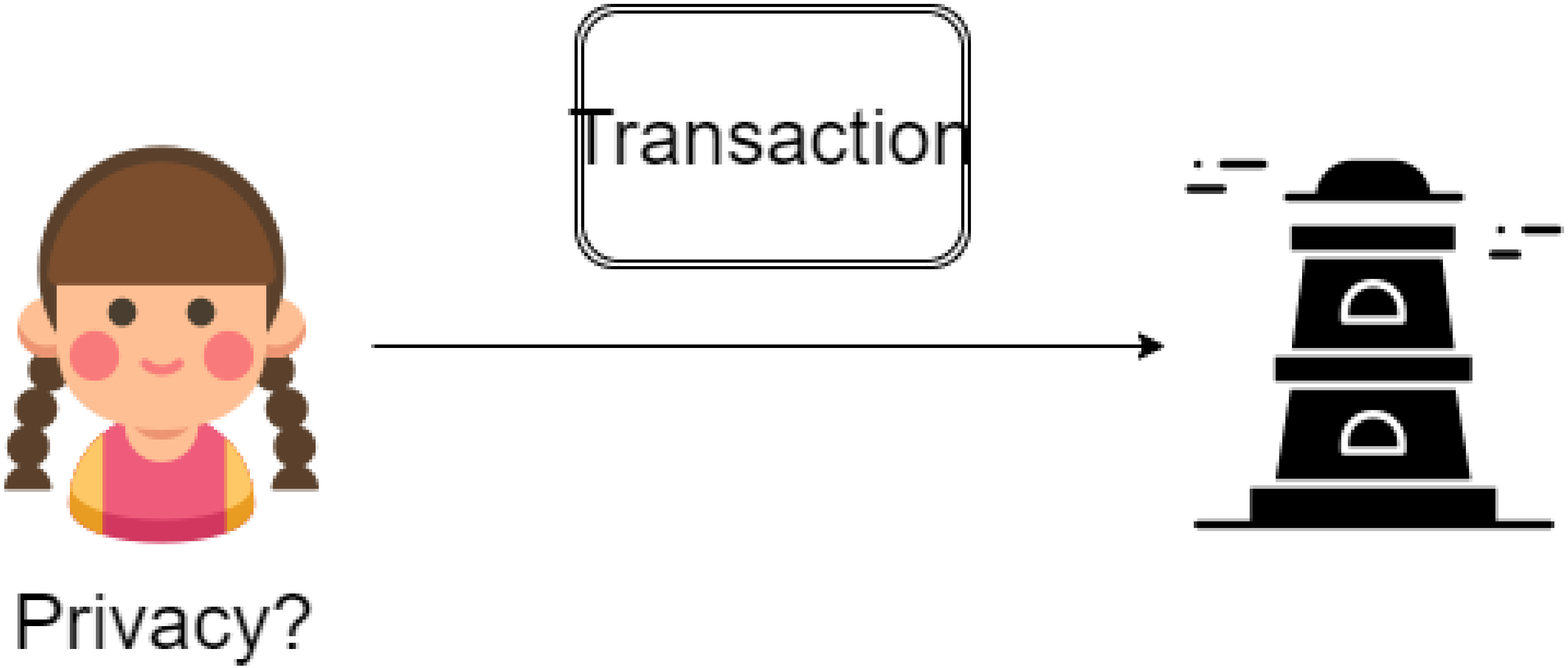
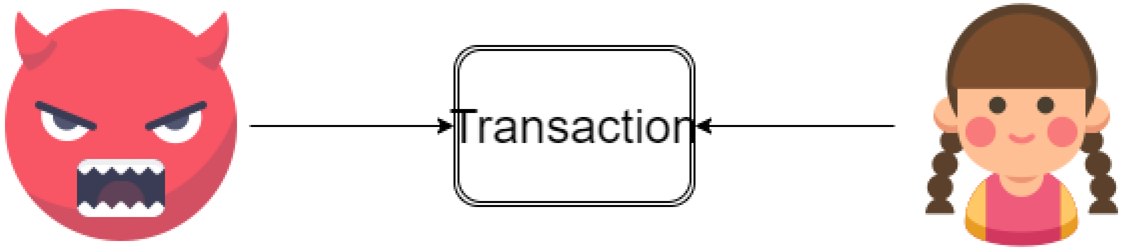
# Watchtower

- Watchtower in LND
- PISA
- TODO

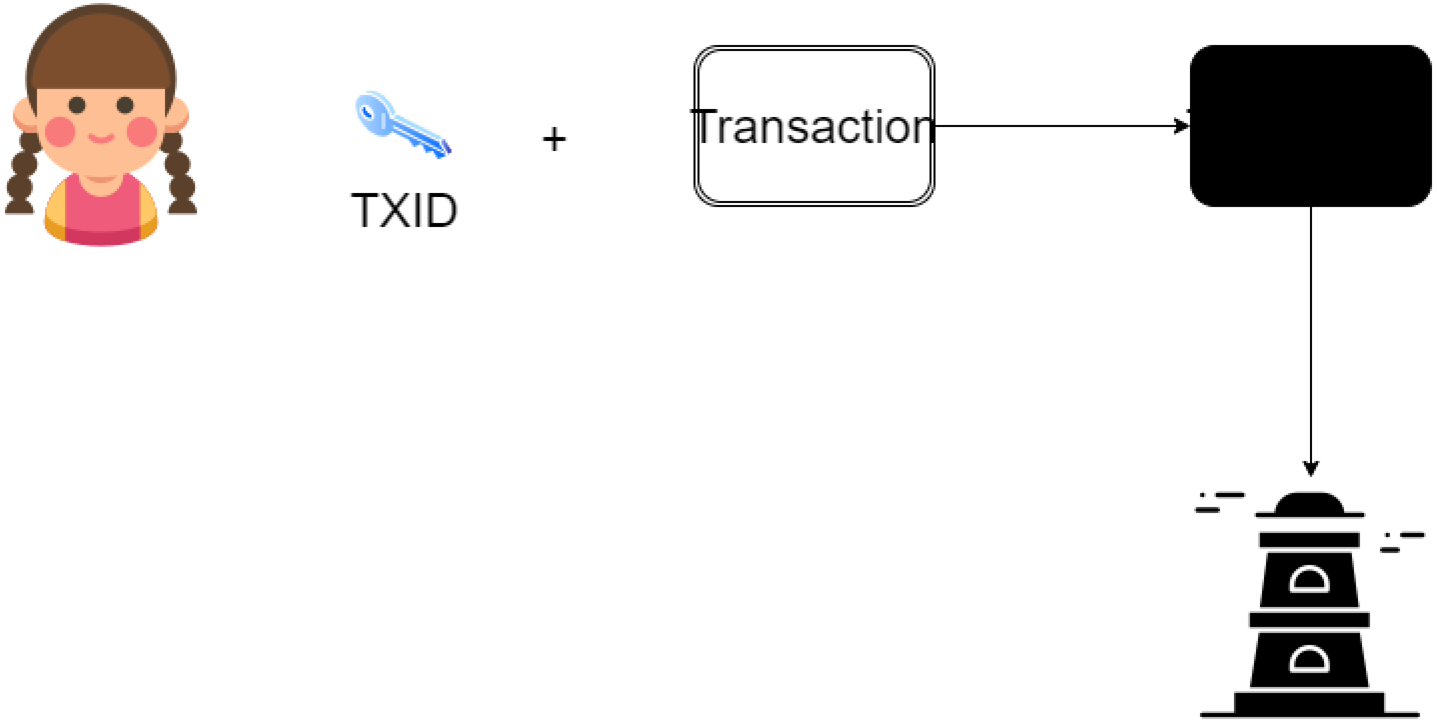


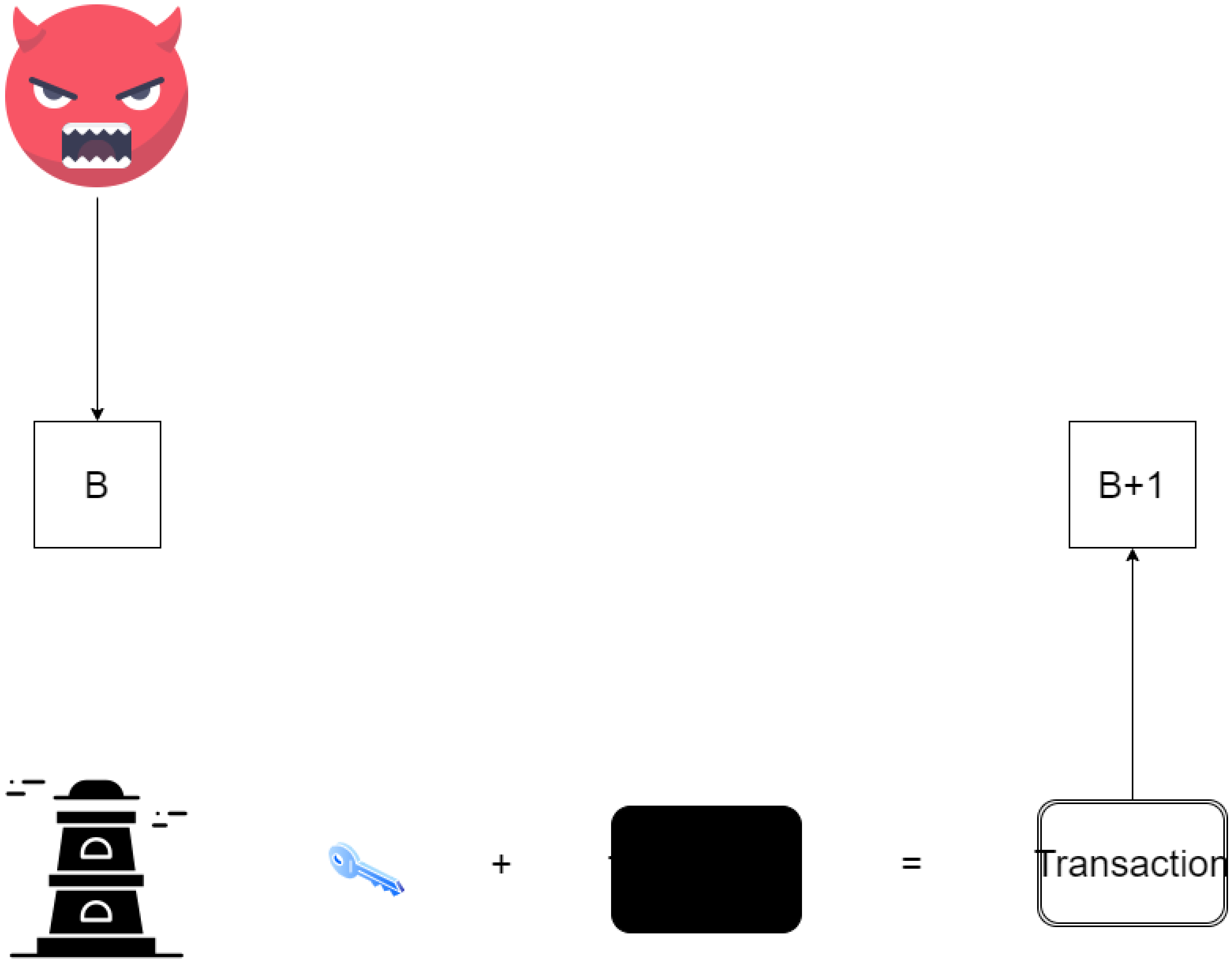
Transaction

Privacy?

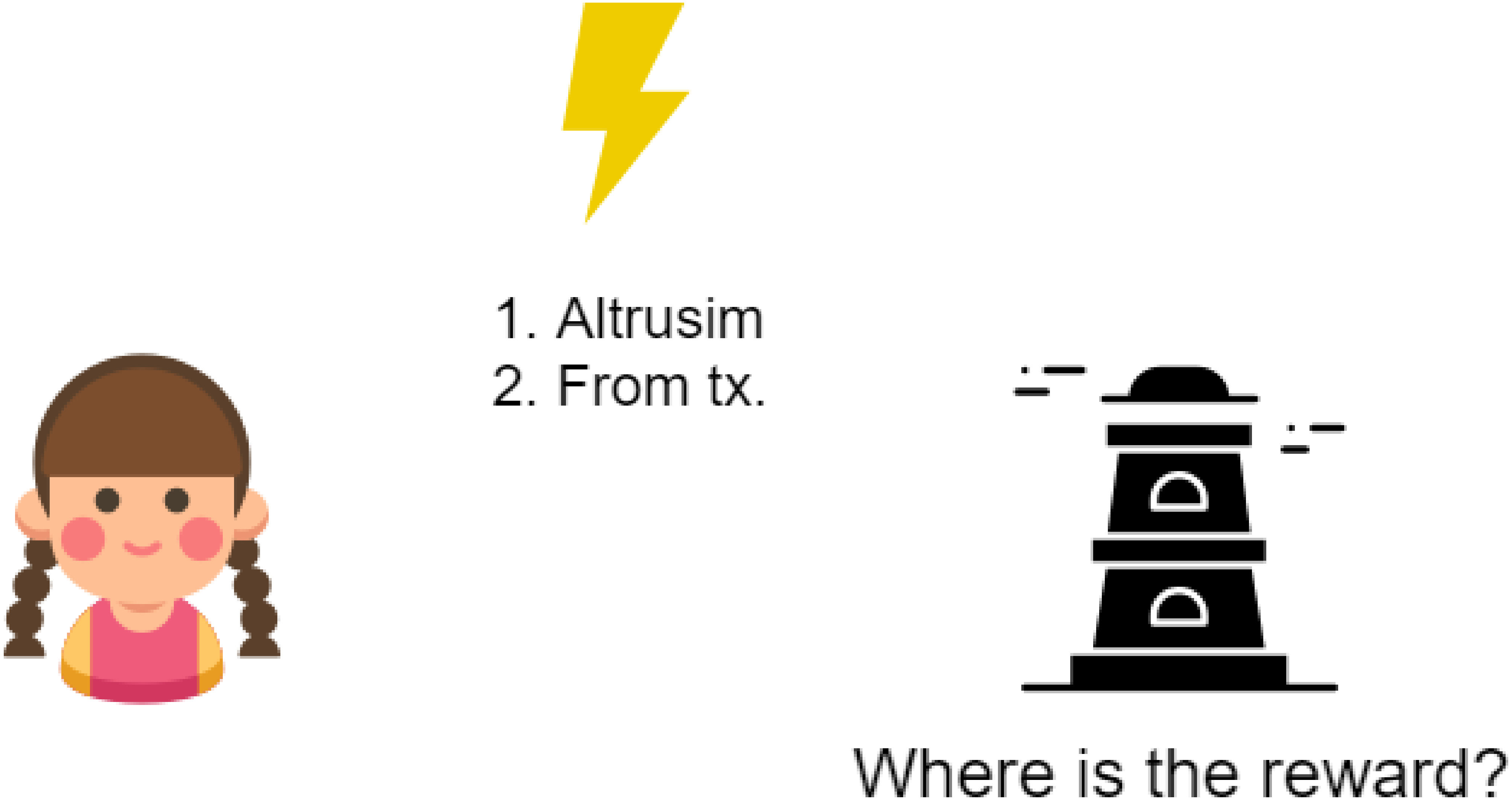


Well, the id of this tx is fixed,
I can use it as the hint, and use it to
encrypt the tx.



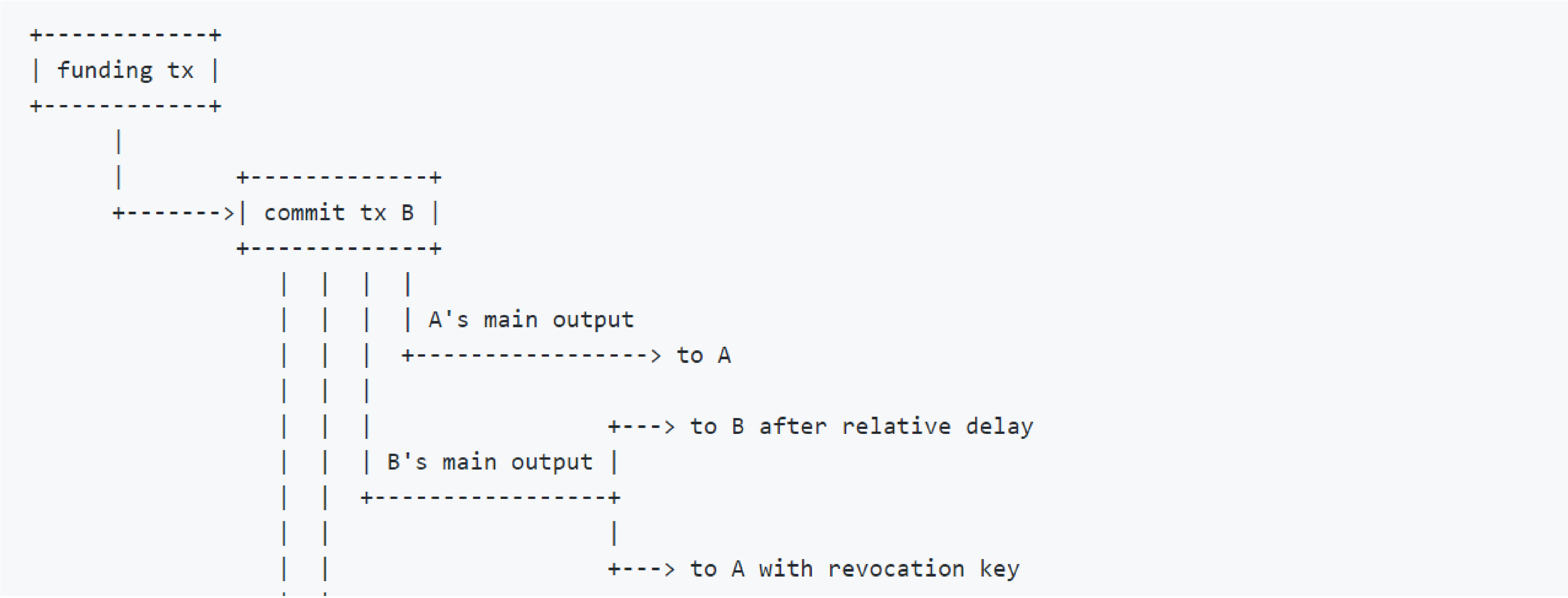


I see the txid, it is consistent
with the hint.

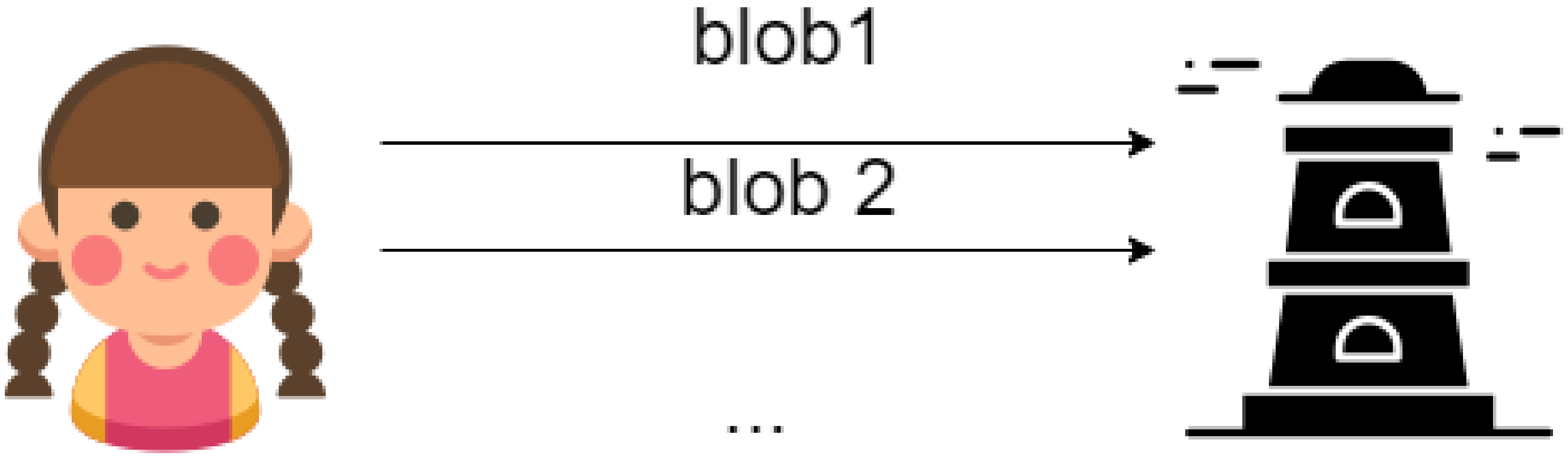


1. Altrusim
2. From tx.

Where is the reward?



```
+------------+
| funding tx |
+------------+
      |
      |        +-------------+
      +------->| commit tx B |
               +-------------+
                  |  |  |  |
                  |  |  |  | A's main output
                  |  |  |  +-----------------> to A
                  |  |  |
                  |  |  |                 +---> to B after relative delay
                  |  |  | B's main output |
                  |  |  +-----------------+
                  |  |                    |
                  |  |                    +---> to A with revocation key
```

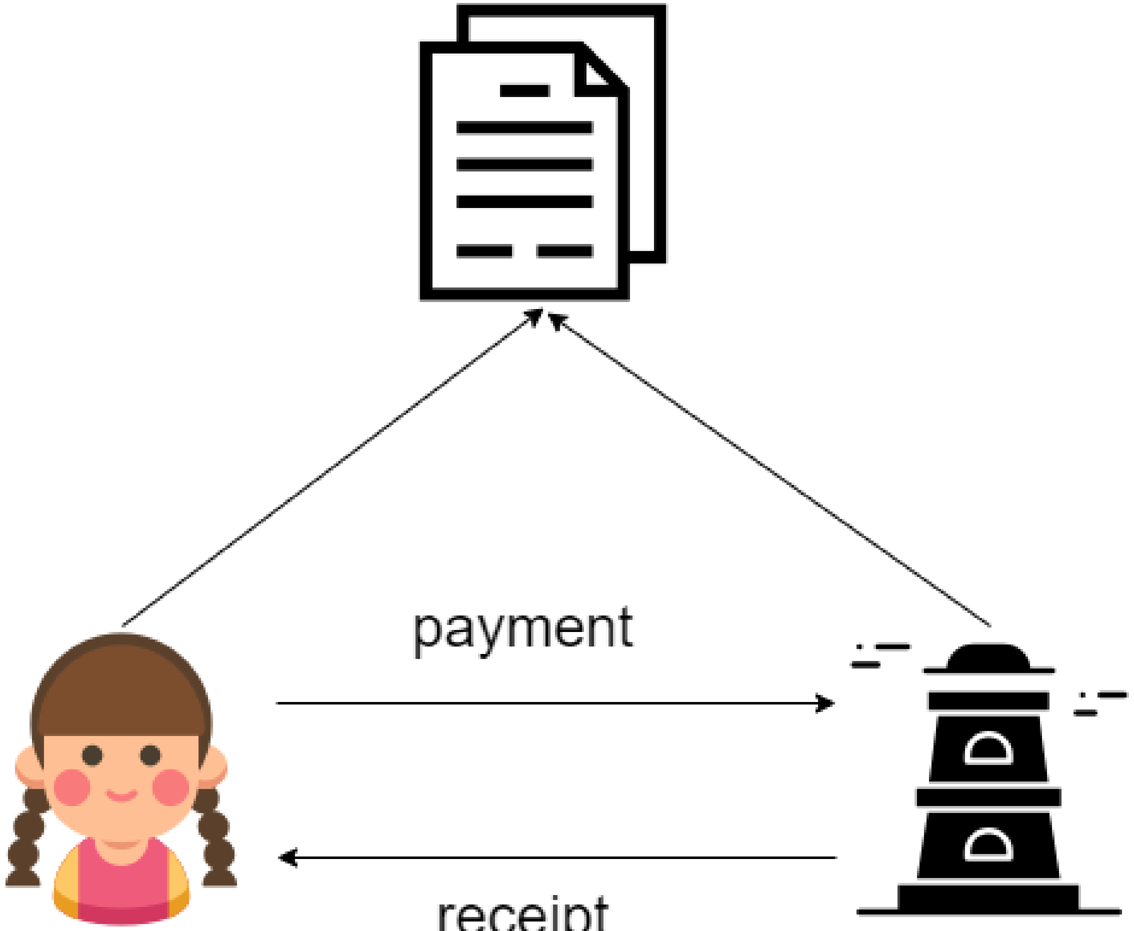


blob1

blob 2

...

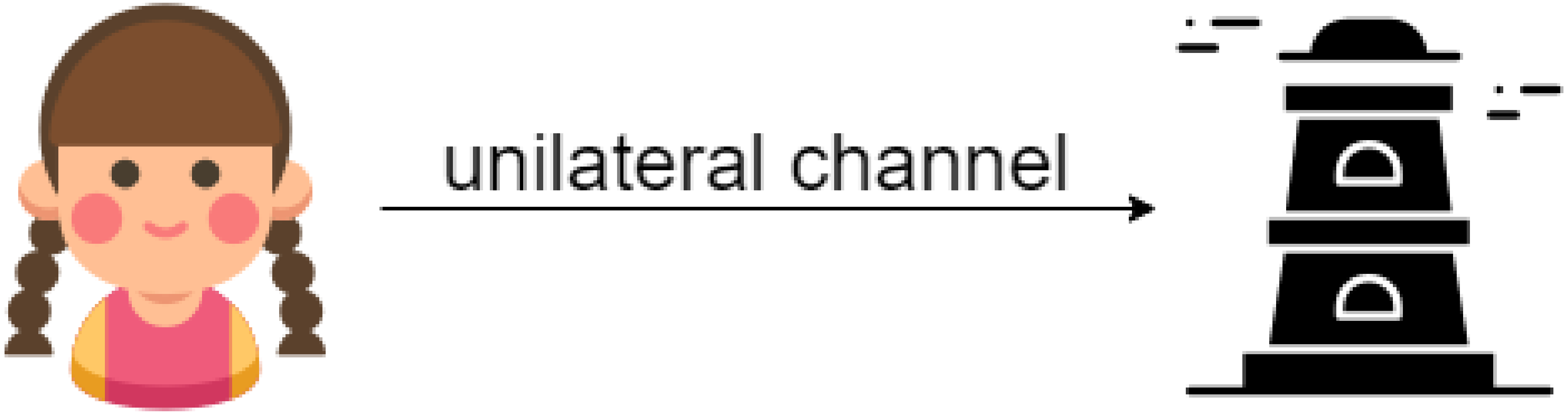
I need to keep all these blobs.
The storage is $O(\log(n))$.



payment

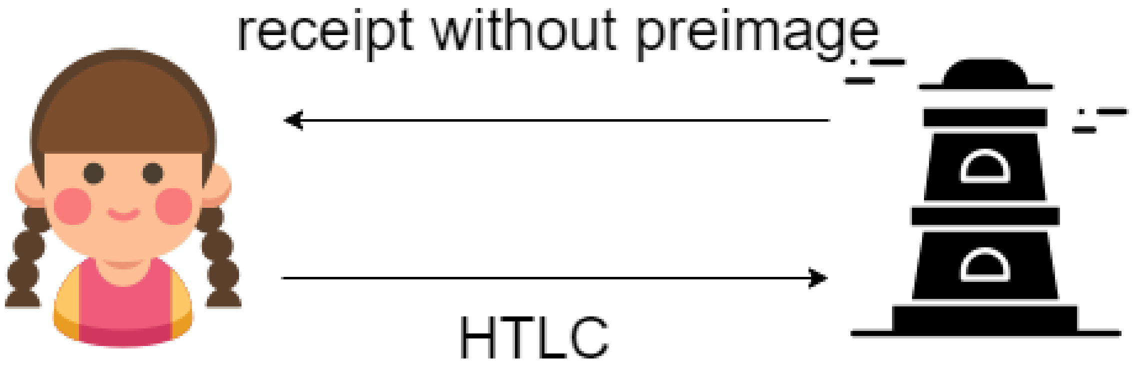
receipt

You can use
this receipt to issue a dispute.



unilateral channel

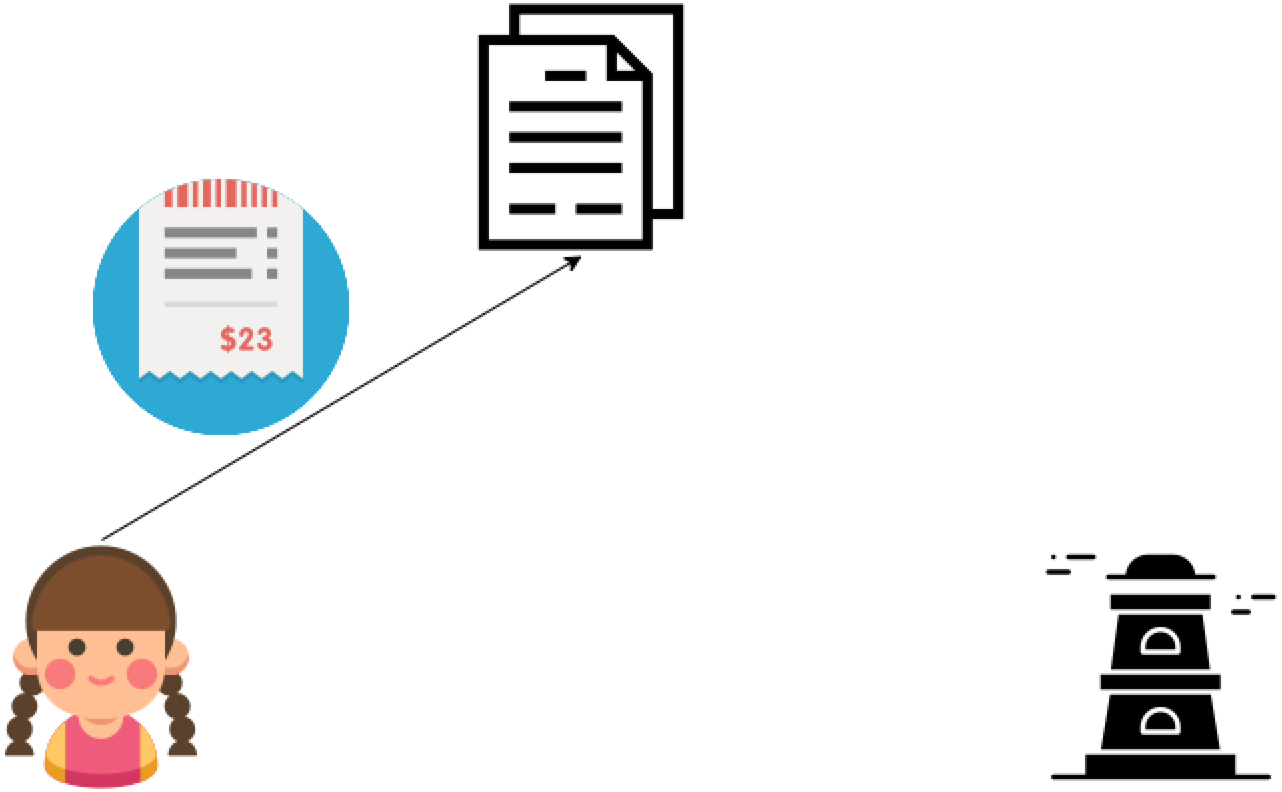
There is a hash, it is valid only
Alice knows the preimage of it.



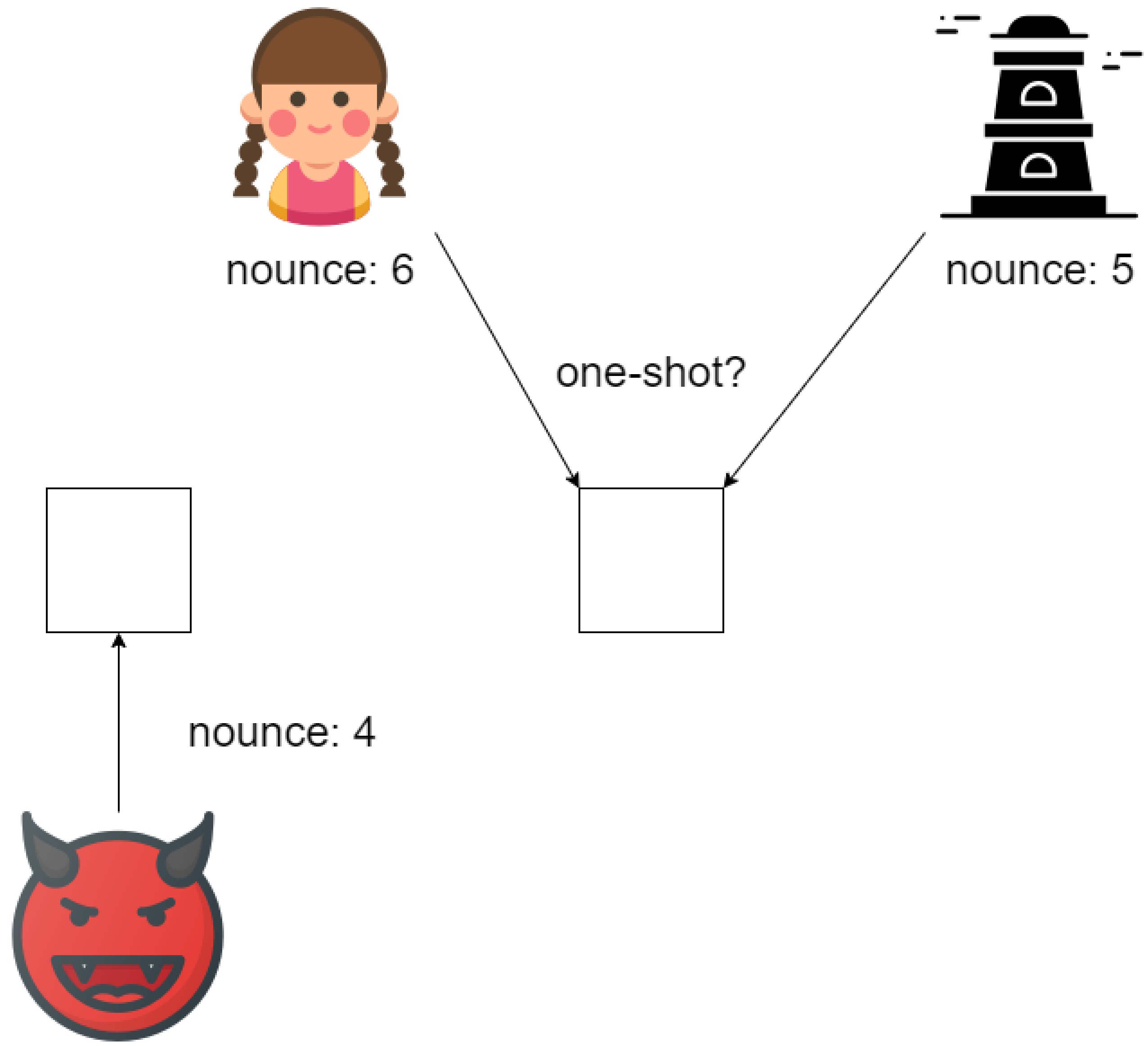
receipt without preimage

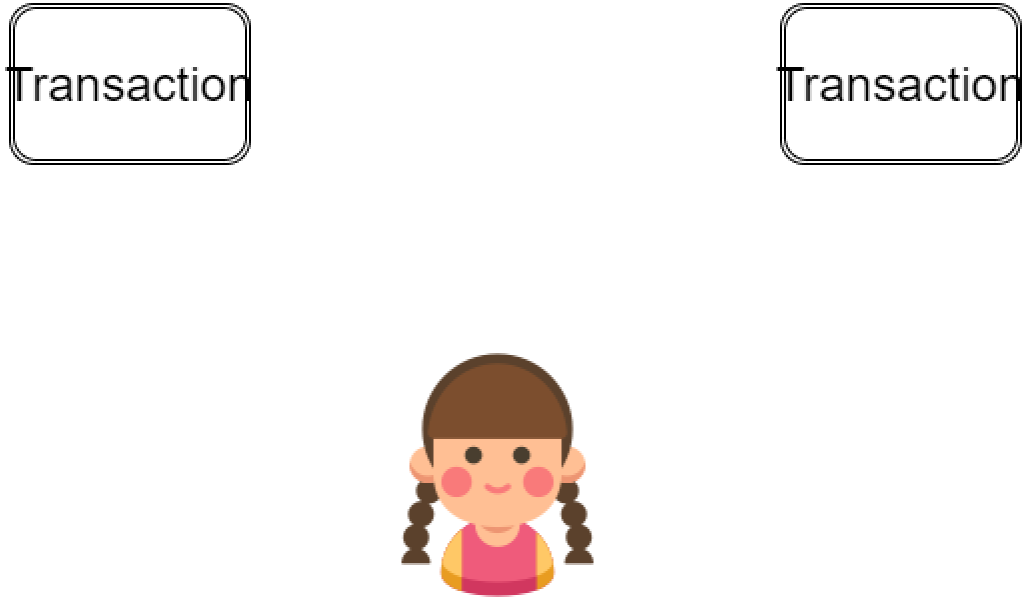
HTLC

I do nothing.



PISA does not help me!


nounce: 6
nounce: 5
one-shot?
nounce: 4



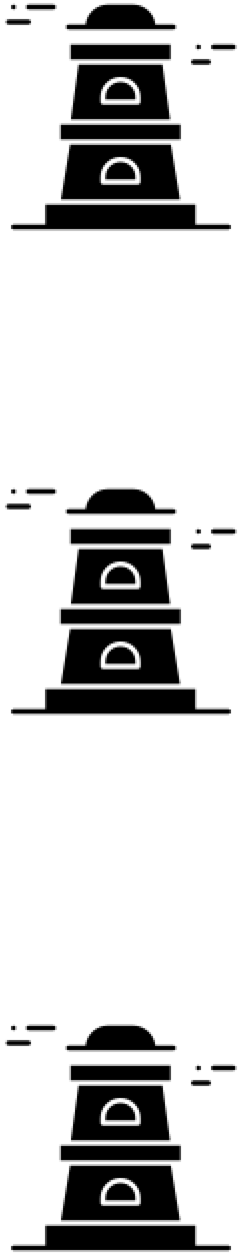
Transaction

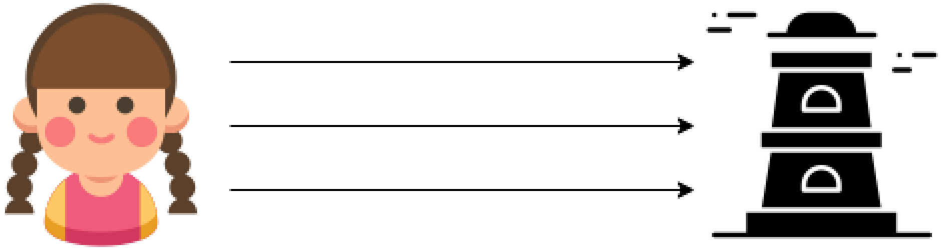
Transaction

one for watchtower, one for me.

TODO

I need multiple watchtower...





I need to pay frequently, can I just subscribe this server?