As mentioned to @paulcadman this morning, I am trying to figure out how the nonce

, rseed

, and npk

value of a resource can/should be populated in transaction function.

In particular, I would need transaction functions to be able to create a new resource r and then use its commitment cm

in the tx.extra

data mapping.

For this to work, the r

plaintext must be complete already to produce the correct cm = h_{cm}(r)

.

My question is:

How are the above mentioned fields populated during transaction function execution time?

My guess is:

The npk

value can probably be provided as an input argument to the transaction function.

The nonce

probably shouldn't be an input because a user can pick one being already taken.

The rseed

probably shouldn't be an input because it could allow attackers to game/exploit applications.

Has anyone already thought about this and the communication between the Anoma node and an application transaction function potentially being required here?

@mariari @cwgoes @vveiln @degregat