

Contents

1	block	1
2	Transaction in $st = Vec < Transaction >$	1
2.1	ideal transaction	1
2.2	real transaction	1
2.3	local storage of transaction	1

1 block

layout of the block structure

$$B = (tx_{lead}, st)$$

$$st = Vec < Transaction >$$

st: is the encoded directed transactions , general purpose transactions,or public transactions (for everyone).

$$tx_{lead} = (LEAD, st \vec{x}_{ref}, stx_{proof})$$

$st \vec{x}_{ref}$: is the vector of previous tx_{lead} done with the same coin (in case the same coin is used for competition).

$$stx_{proof} = (cm_{c'}, sn_c, ep, sl, \rho, h, ptr, \pi)$$

$cm_{c'}$: coin commitment sn_c : coin serial number ep : epoch number sl : slot index ρ : coin nonce defined as $\mu^{sk_{sl}^{COIN}}$ h : hash of the block ptr : hash of previous block π : proof of leadership

2 Transaction in $st = Vec < Transaction >$

2.1 ideal transaction

$$tx_{xfer}^{ideal} = ((PUBLIC, TRANSFER), (pk_r, (pk_4^{COIN}, v_4)), (pk_s, (id_1, v_1), (id_2, v_2), (id_3, v_3)))$$

2.2 real transaction

$$tx_{xfer}^{real} = (TRANSFER, stx_{proof}, c_r)$$

c_r is the slot encrypted of stx_{rcpt} by pk_r

$$stx_{rcpt} = (\rho_{c3}, r_{c3}, v_{c3})$$

$$stx_{proof} = (cm_{c3}, cm_{c4}, sn_{c1}, sn_{c2}, \tau, root, \pi)$$

2.3 local storage of transaction

from decrypted real transaction calculate only store the ideal transaction, beside $(pk_c^{COIN}, \rho_c, r_c, v_c)$ for spending.