

Contents

1	Crypsinous blockchain	1
1.1	LEAD statement	1
2	Crypsinous leaderelection	1

this is an effort to break down the building blocks of crypsinous blockchain

1 Crypsinous blockchain

Each part U_p stores it's own local view of the Blockchain $C_{loc}^{U_p}$. C_{loc} is a sequence of blocks B_i ($i>0$), where each $B \in C_{loc}$

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

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

$st \vec{x}_{ref}$ it's a vector of tx_{lead} that aren't yet in C_{loc} . $stx_{proof} = (cm_{lc}, sn_c, ep, sl, \rho, h, ptr, \pi)$ the Blocks' st is the block data, and h is the hash of that data. the commitment of the newly created coin is: $(cm_{lc}, r_{lc}) = COMM(pk^{COIN} || \tau || v_c || \rho_{lc})$, sn_c is the coin's serial number revealed to spend the coin.

$$sn_c = PRF_{root_{sk}^{COIN}}^{sn}(\rho_c)$$

$$\rho = \eta^{sk_{sl}^{COIN}}$$

η is from random oracle evaluated at $(Nonce || \eta_{ep} || sl)$, ρ is the following epoch's seed. ptr is the hash of the previous block, π is the NIZK proof of the LEAD statement.

1.1 LEAD statement

2 Crypsinous leaderelection

TODO