

Contents

1	Dao propose	1
1.1	Create dao proposal	1
2	Circuit checks	1

1 Dao propose

$$X = (cm^{token}, root^{bulla}, proposal, cm_x^{value^{total}}, cm_y^{value^{total}})$$

$$W = (value^{total}, blind^{value^{total}}, blind^{token}, proposal_x^{destination}, proposal_y^{destination}, proposal^{amount}, proposal^{tokenId}, blind^{proposal})$$

$$\mathcal{L} = \{X : (X, W) \in \mathcal{R}\}$$

1.1 Create dao proposal

- Calculate, and reveal [token commitment](#)
- Calculate, and reveal [bulla](#)
- Calculate, and reveal [proposal](#)
- Calculate, and reveal total proposers funds [commitment](#)

Public input	Description
cm^{token}	proposal token commitment as field element
$root^{bulla}$	root of bulla in merkle tree
proposal	dao proposer proposal
$cm_x^{value^{total}}$	total funds commitment 's x coordinate
$cm_y^{value^{total}}$	total funds commitment 's y coordinate

Witnesses	Description
$value^{total}$	total proposal funds value
$blind^{value^{total}}$	blinding value for $value^{total}$ commitment
$blind^{token}$	token commitment blinding factor
$proposal_x^{destination}$	destination public key x coordinate
$proposal_y^{destination}$	destination public key y coordinate
$proposal^{amount}$	amount in proposal token
$proposal^{tokenId}$	proposal token id
$blind^{proposal}$	proposal commitment blinding term
proposerLimit	governance token necessary for the vote to be valid
quorum	minimum number of votes necessary to pass the proposal
$approvalRatio_{quot}$	proposal approval ratio quotient
$approvalRatio_{base}$	proposal approval ratio base
tokenId	governance token id
pub_x	proposal public key x coordinate
pub_y	proposal public key y coordinate
$blind^{bulla}$	bulla commitment blinding factor
pos	bulla leaf position in the merkle tree
path	path of the bulla leaf at position pos

2 Circuit checks

- $proposal^{amount} > 0$
- $proposerLimit \leq value^{total}$