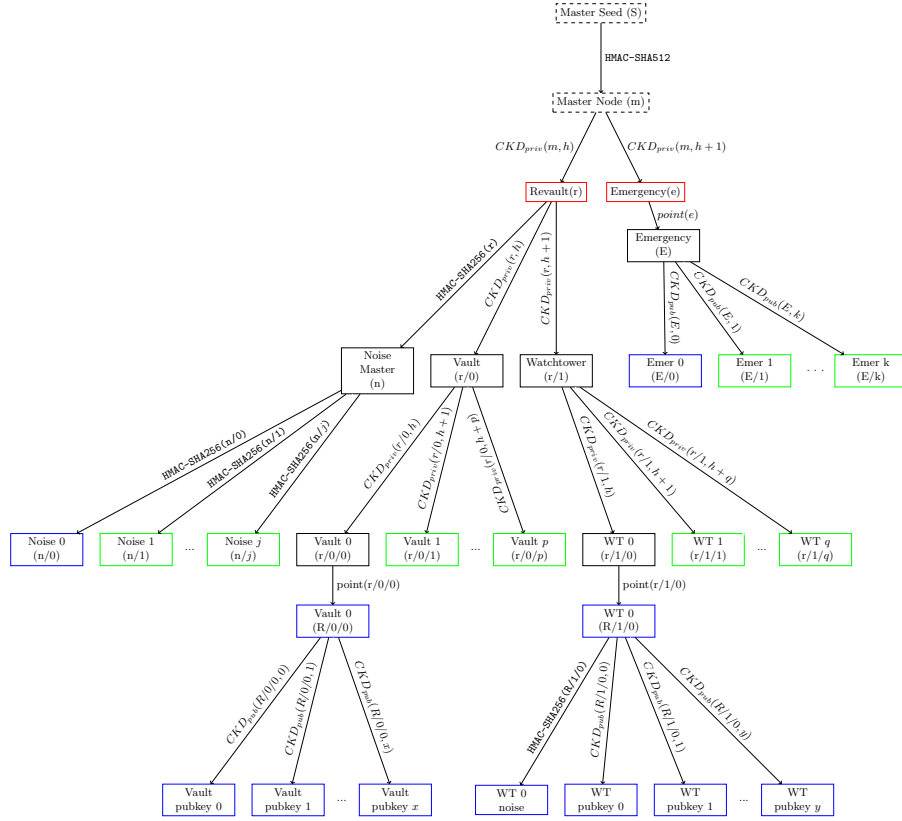# Stakeholder Key Tree Model

- - - - - Ephemeral data
———— Backup
———— Hardware wallet
———— In use
———— Not in use
$h = 2^{31}$ Hardened derivation index

Master Seed (S)

HMAC-SHA512

Master Node (m)

$CKD_{priv}(m, h)$ $CKD_{priv}(m, h+1)$

Revault(r)   Emergency(e)

$point(e)$

Emergency (E)

HMAC-SHA256 (r) $CKD_{priv}(r, h)$ $CKD_{priv}(r, h+1)$

$CKD_{pub}(E, 0)$ $CKD_{pub}(E, 1)$ $CKD_{pub}(E, k)$

Noise Master (n)

Vault (r/0)

Watchtower (r/1)

Emer 0 (E/0)   Emer 1 (E/1)   ...   Emer k (E/k)

HMAC-SHA256(n/0)   HMAC-SHA256(n/1)   HMAC-SHA256(n/j)

$CKD_{priv}(r/0, h)$ $CKD_{priv}(r/0, h+1)$ $CKD_{priv}(r/0, h+p)$

$CKD_{priv}(r/1, h)$ $CKD_{priv}(r/1, h+1)$ $CKD_{priv}(r/1, h+q)$

Noise 0 (n/0)   Noise 1 (n/1)   ...   Noise j (n/j)   Vault 0 (r/0/0)   Vault 1 (r/0/1)   ...   Vault p (r/0/p)   WT 0 (r/1/0)   WT 1 (r/1/1)   ...   WT q (r/1/q)

$point(r/0/0)$ $point(r/1/0)$

Vault 0 (R/0/0)

WT 0 (R/1/0)

$CKD_{pub}(R/0/0, 0)$ $CKD_{pub}(R/0/0, 1)$ $CKD_{pub}(R/0/0, x)$

HMAC-SHA256(R/1/0) $CKD_{pub}(R/1/0, 0)$ $CKD_{pub}(R/1/0, 1)$ $CKD_{pub}(R/1/0, y)$

Vault pubkey 0   Vault pubkey 1   ...   Vault pubkey x WT 0 noise   WT pubkey 0   WT pubkey 1   ...   WT pubkey y

Manager Key Tree Model

- - - - - Ephemeral data
——— Backup
——— Hardware wallet
——— In use
——— Not in use
$h = 2^{31}$ Hardened derivation index