Frontend (JS)

Backend (Solidity)

$k, s \in \mathbb{B}^{256}$

$C = H_1(k \| s)$

deposit

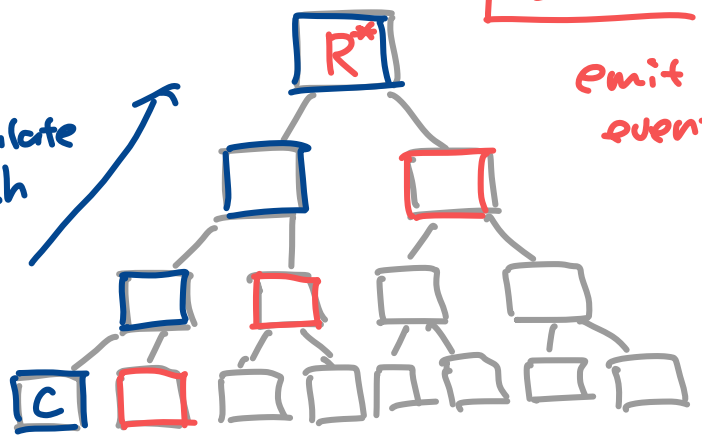
c, 1 ETH

Depositer

sister nodes

R_i^* R

emit as an event



calculate the hash path

k, s, R_i^*, R, A

$P = (\pi_p, k \cdots)$

$h = H_1(k)$

withdrawer

withdraw

P, R_i^*, h, A

1 ETH

? P → Verifier ?

Valid → add h to the spent nullifier hashes

Trusted setup using Groth 16 SnarkJS