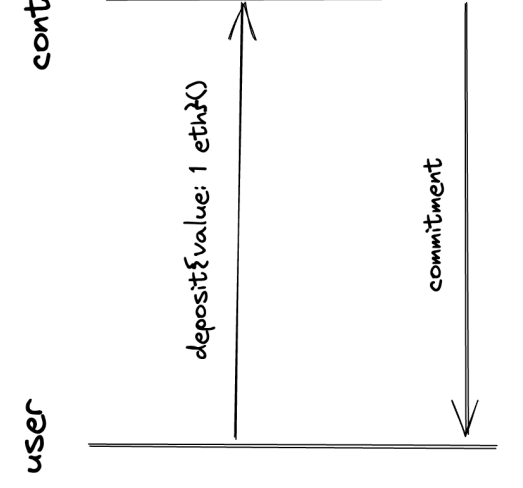
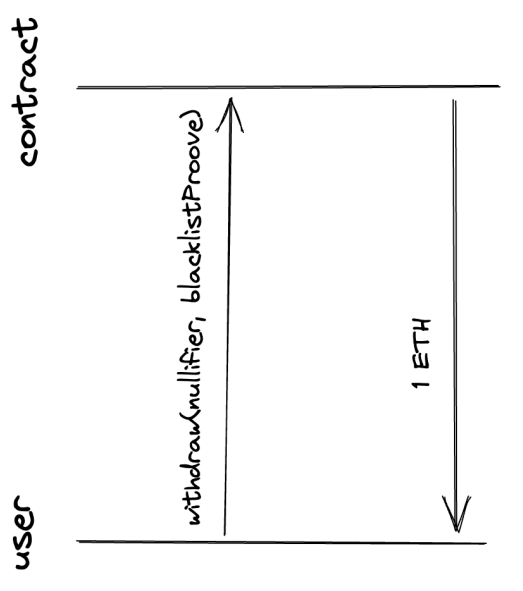


- Cada vez que un usuario deposita 1 ether recibe un "commitment"
- Luego para retirar hay que proveer un "nullifier" y una zkproof para demostrar que se depositó 1 ETH, pero nadie sabe cuál es el nullifier que está asociado al commitment. También hay que enviar un zkproof para demostrar que el origen del fondo no está blacklisted.

DEPOSIT



WITHDRAW



contract state variables
VALUE: uint256, deposito valido
ROOT: bytes32, root
nullifierHashes: mapping(bytes32 => bool), para evitar doble retiros de fondos
commitments: mapping(bytes32 => bool), sanity check en caso de que mas de un deposito tenga el mismo hash
blacklist: mapping(address => bool), indica si una wallet tiene fondo de una fuente dudosa