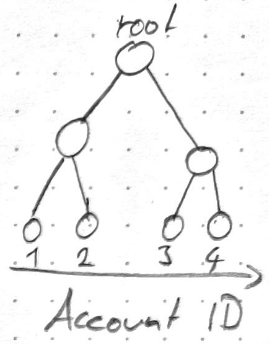
May 10, 2021

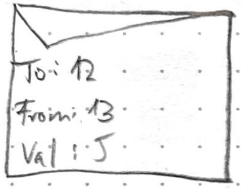
addr	ID
0xabc	1
0xdef	2
0xghi	3

In the Hubble project rollup, an address receives their index through being a leaf in the account tree.



130k · 10

500€


To: 12
From: 13
Val: 5

This MSG doesn't contain an address. ⇒ How do we know that tx "From 13" is legit?

⇓

if(ecrecover(sig) = pubkey)

3.000 gas vs. uint256 storage

16 · 32 = 512

"To get an index for a pubkey in the first place, a registry of mapping(addr => Index) needs to be maintained" ⇐ : The Problem

Contract needs access to this

179 call data

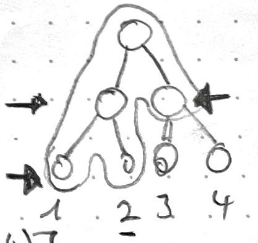
160

```
             8    11
           4  4     5        32      32       3·32  10.4
transfer(a , b , v ,addrA , root , Leaves , sig ){
  aInRoot = tree.includes(addrA , root, leaves)
  if(aInRoot && ecover(sig) = addrA){
      //do transfer stuff : a, b, v.
  }
}
```

Rollup scalability comes from BLS signatures

a = 2

⇒ "Leaves"



[1, H(1,2), H(3,4)]