

Problem

State prev size

then State prev

grows as even non-transaction users

are submitted. This is because

 $\text{validate}(\text{State prev}, \text{Transfer}[x] \text{ tx}) == \text{Hash nextRoot}$

where to get "Hash nextRoot" all "Transfer[x] tx"

need to be applied to "State prev" and

remerketed to see if its "Hash root" is

cumulative

users

equal to "Hash nextRoot"

struct Account {

address id;

int256 value;

} and

struct State {

Account[] balances;

Hash root;

}

Merkle tree of spends

Replace with UTXO model

struct Output {

address id;

int256 value

}

and struct (Un)spent {

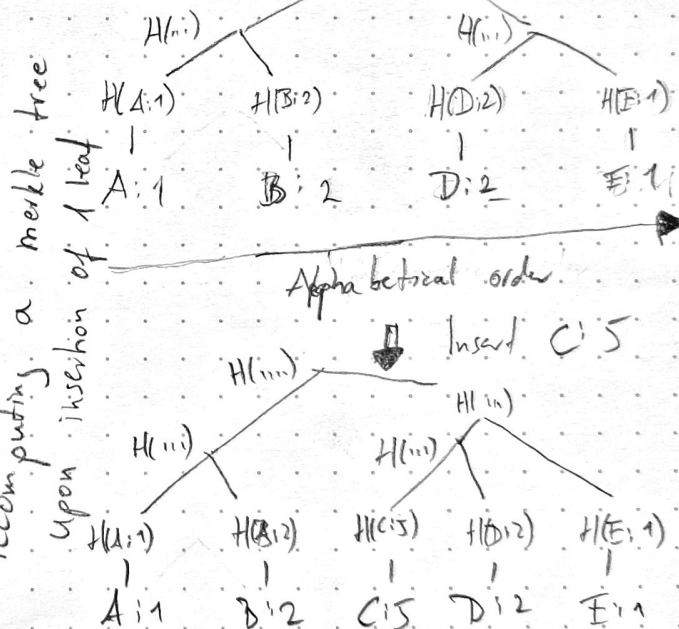
Output[] (un)spends;

}

Problem: How expensive is cost of computing merkle root for 1

leaf removal/insertion.

How expensive is recomputing a merkle tree upon insertion of 1 leaf



Hashes: 1111 what happens for larger trees?