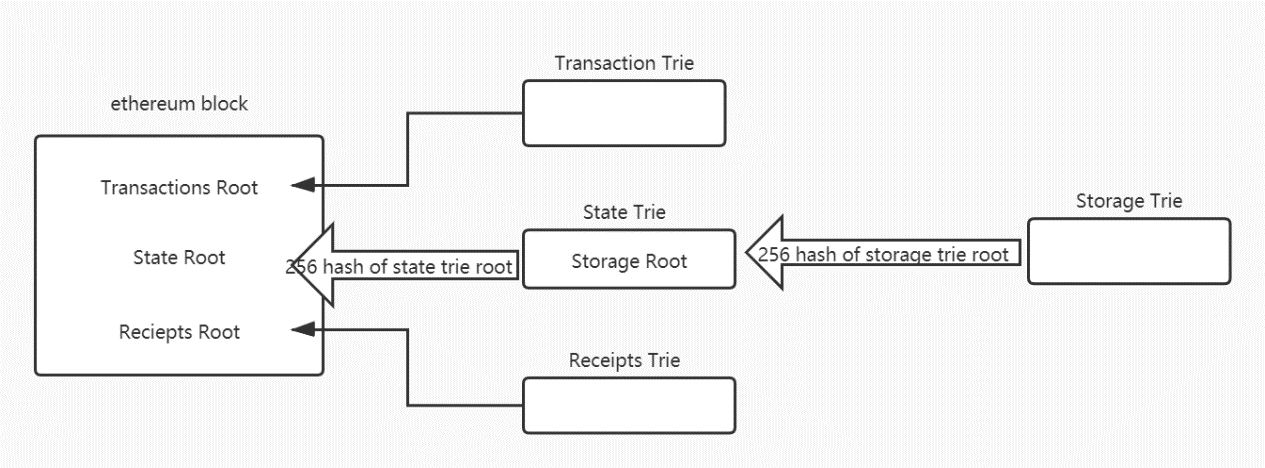
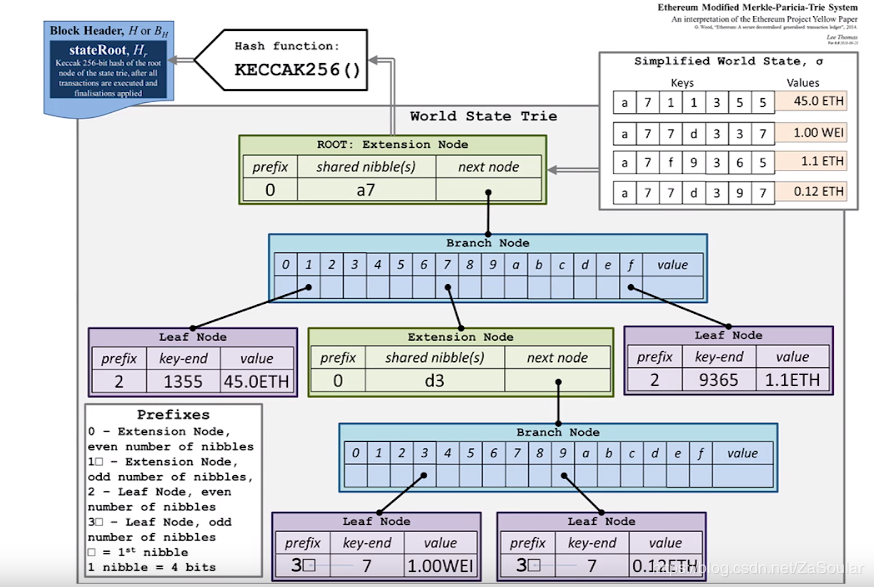
以太存储以及其Proof模型

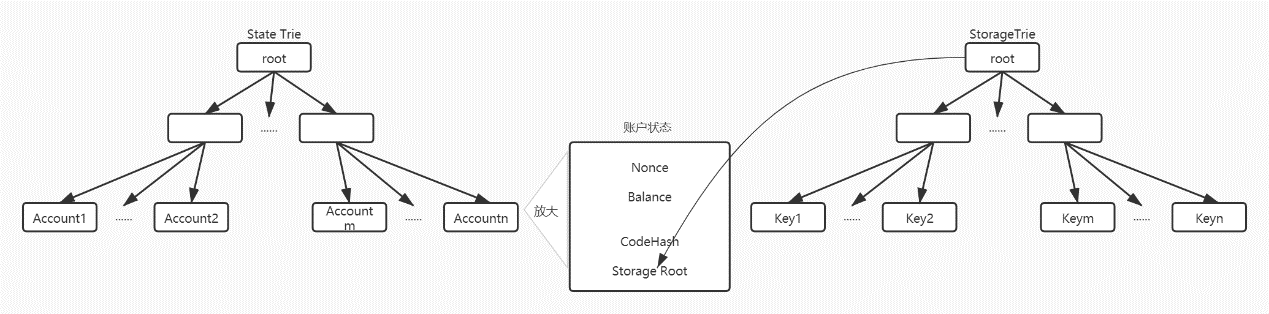
以太存储了交易，状态，收据。



以太的MPT



以太State整体结构



以太合约地址和合约的CodeHash

以太合约地址从合约部署账户和其Nonce计算得出，CodeHash是该账户下部署的合约code Hash，一旦初始化就不再可以更改。如果是非合约账户，CodeHash是0，一旦初始化账户，也是不能修改的。

测试以太合约地址计算方法的程序：



验证合约的CodeHash



以上是一份简单的合约，会生成Proof。我们部署这份合约两次，得到两个合约：

合约地址： 0x08970FEd061E7747CD9a38d680A601510CB659FB

合约code：



0x5E72914535f202659083Db3a02C984188Fa26e9f

合约code：



这两个合约的code是一样的，我们计算其hash

codeHash := crypto.Keccak256(code)

得到CodeHash：

5d2460186f7233c927e7db2dcc703c0e500b653ca82273b7bfad8045d85a470

分别获取他们的proof来验证CodeHash：

{

"jsonrpc": "2.0",

"id": 100,

"result": {

"accountProof": [

"",

"",

"",

"",

"",

"",

"0xf891808080808080a0d55dae53045c89fd34547b83782440764c8a5d691fb7239c0a4c44158eafd90a80a044ad6fdc85b0d2a9db42ad354f827f881e562d907eaa2ba1e1f4e07d4d4cb4b1808080a0bfa7fcf7722645d99b7cbb2e9e6ba2bf2a0bef7bab0e6b9b24962efcafc8c37fa00704ecf2a0660cfe67d027e119c940af22b149afdc2eb5b233ba6f3cdff13604808080",

"0xf86f9d3b1d01b11dcd8522c964ba355bc8c4f3286d30982ddca4ffe3cbb8fef5b84ff84d8089021aadbe4cb2a32001a056e81f171bcc55a6ff8345e692c0f86e5b48e01b996cadc001622fb5e363b421a0c5d2460186f7233c927e7db2dcc703c0e500b653ca82273b7bfad8045d85a470"

],

"address": "0x08970fed061e7747cd9a38d680a601510cb659fb",

"balance": "0x21aadbe4cb2a32001",

"codeHash": "0xc5d2460186f7233c927e7db2dcc703c0e500b653ca82273b7bfad8045d85a470",

"nonce": "0x0",

"storageHash": "0x56e81f171bcc55a6ff8345e692c0f86e5b48e01b996cadc001622fb5e363b421",

"storageProof": [

{

"key": "0xada5013122d395ba3c54772283fb069b10426056ef8ca54750cb9bb552a59e7d",

"proof": [],

"value": "0x0"

}

]

}

}

{

"jsonrpc": "2.0",

"id": 100,

"result": {

"accountProof": [

"",

"",

"",

"",

"",

"",

"0xf89180a0fc10d456bb2ed06d03ca292a2aacda7f9f64672d95a987810fb457733e1d8c758080a0ff53e197e118ac341ecbb3e92183f0c62f36cc54c7d4e11670f74d4ece11ecc4808080808080a0e6c0412148da236c58884d29932cbf396f42722c8ee593ec606896187dbea242a0c857d18ca88fb0541be07216ac0eba1dbf1f434e97b59c91a79bffd8b675efcc80808080",

"0xf86f9d3ee7e06fe2158d80793f1335e41c9cb74105a5428a40034256bd79a5a7b84ff84d8089023f831260a1e5b388a056e81f171bcc55a6ff8345e692c0f86e5b48e01b996cadc001622fb5e363b421a0c5d2460186f7233c927e7db2dcc703c0e500b653ca82273b7bfad8045d85a470"

],

"address": "0x5e72914535f202659083db3a02c984188fa26e9f",

"balance": "0x23f831260a1e5b388",

"codeHash": "0xc5d2460186f7233c927e7db2dcc703c0e500b653ca82273b7bfad8045d85a470",

"nonce": "0x0",

"storageHash": "0x56e81f171bcc55a6ff8345e692c0f86e5b48e01b996cadc001622fb5e363b421",

"storageProof": [

{

"key": "0xada5013122d395ba3c54772283fb069b10426056ef8ca54750cb9bb552a59e7d",

"proof": [],

"value": "0x0"

}

]

}

}

我们可以看到，这两个合约地址不一样，但其CodeHash一样，因为他们的Code是一样的。

结论: 即使合约地址不同，但只要部署的相同的合约，合约的CodeHash一样。