zkVoting

项目概述

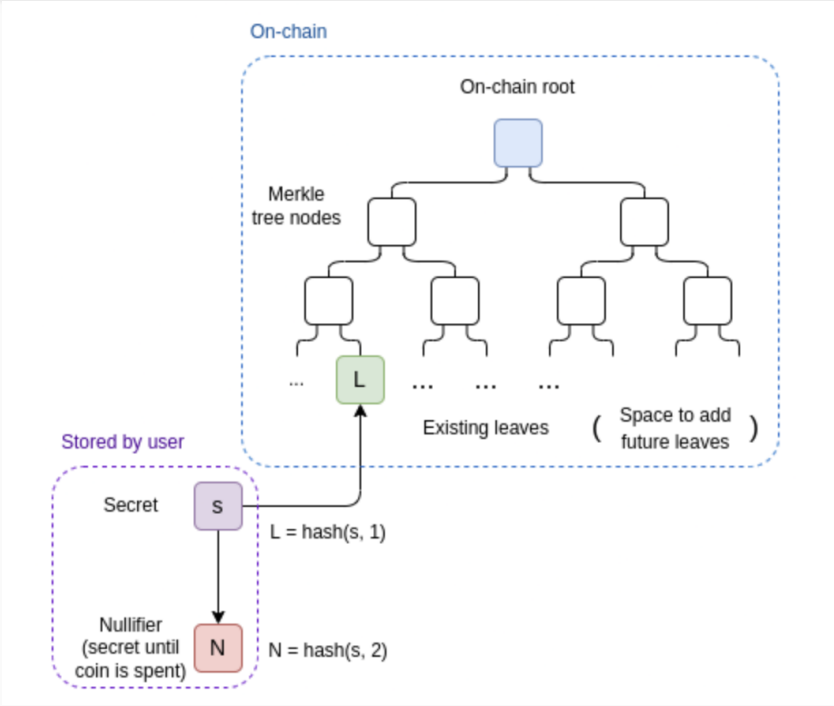
利用零知识证明实现去中心化的匿名投票系统：

- 投票人不泄漏任何个人信息。
- 投票人对每个需要投票的事项只能进行一次投票。
- 系统简洁， 高效， 部署在以太坊链， 投票消耗的gas少。

基本原理

根据Merkle Tree的某个叶子计算出根节点。
利用零知识证明生成上述过程的证明：

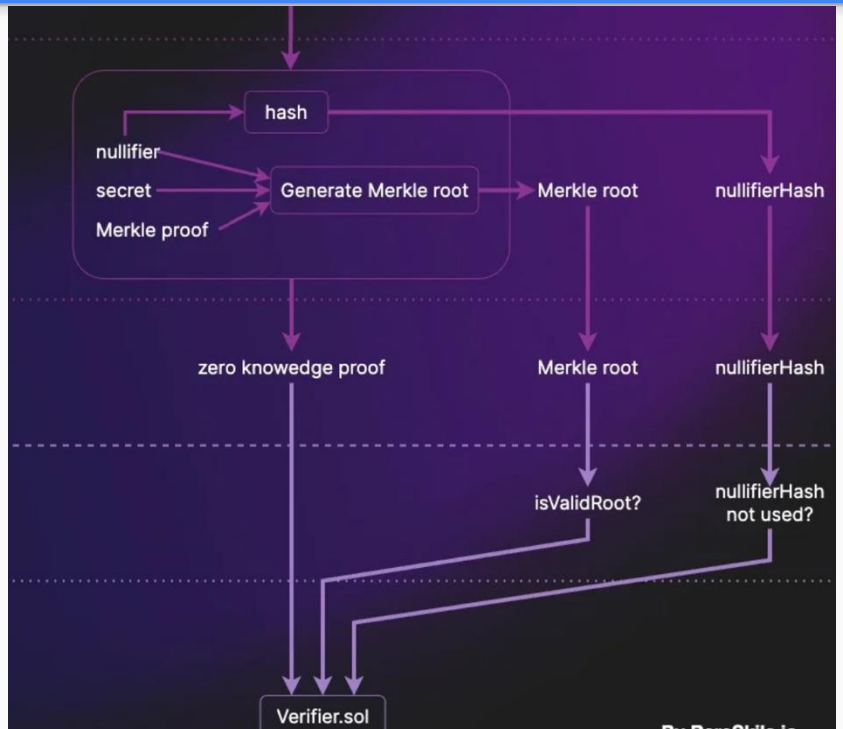
- 叶子由用户的secret和Nullifier，通过hash生成
- 根节点存储在链上
- 证明只有根节点和用户的销根号(hash(Nullifier))可见



流程简述

- 首先用户由链下随机生成secret和nullifier，这两个是用户的凭证，需要保存好，不能泄漏。
- 用户注册：根据凭证中的secret和nullifier进行hash计算，并提交链上，链上添加新叶子并更新根节点。
- 用户投票：链下通过凭证，和需要投票的序号和投票结果，进行零知识证明的生成。根据生成的证明再提交链上进行验证。

流程简图


hash
nullifier
secret
Merkle proof
Generate Merkle root
Merkle root
nullifierHash
zero knowedge proof
Merkle root
nullifierHash
isValidRoot?
nullifierHash
not used?
Verifier.sol

后续改进

可以再利用零知识证明，实现与Web2的账户例如google账号等绑定起来，实现基于web2账户进行登录的功能，让Web2和Web3无缝衔接起来。

Thank You

please contact: lkw040535@gmail.com