Anonymous year validator by free TON zkSNARK

Author

Telegram: @podlodkin

Twitter: https://twitter.com/podlodkin82

GitHub: https://github.com/podlodkin

Free TON address:

0:424c3fdf6ea1bff797767c3989e275e3f0ffdaf3a95c67cc3006b08c22923ac0

Description

Progress is the engine of development. The progress gives the vector of movement to the modern world. We use various gadgets every day, leave traces on the Internet and open our privacy everywhere. But confidentiality is very important and it would be correct to hide some information about yourself. How can we use this? zk-SNARKs - Zero Knowledge Proof.

The purpose of zero knowledge proofs is for the verifier to be able to verify that the verifier has knowledge of a secret parameter called proof that satisfies some relationship without disclosing the proof to the verifier or anyone else - for example:

- If I want to go to any event with a high MPAA rating and am not ready to disclose my personal information to others;
- If I want to participate in extreme sports games and I want to hide this information from my bank / lender;
- If I want to buy alcohol, cigarettes, but I am not ready to reveal my age;
- If I want to get medical care, but I do not want anyone to know about it.
- One of the important criteria for all these scenarios is the confirmation of my age (and it's limitation by law).

The main idea of this solution is to protect privacy (age) from anyone and begin to reduce the existing leakage of confidential information of each of us by introducing blockchain technologies into our life!

Solution

GitHub (source code)

https://github.com/podlodkin/podlodkin-freeton-year-control

zsSnark-Logic

C++ application based on blueprint library. You can:

- Generate proving.key and verification.key
- Generate and save proof to file
- Generate and save and primary_input to file
- Check/Verify the proof

Free TON Blockchain

Free TON Contract to validate zsSnark proof using Vergrth16 TVM. A verification key is stored in the Free TON Solidty contract. It can be setted/changed using the setupKey method:

```
    // Setup validation key
    function setupKey(bytes vkey) public {
        // security validation
        require(msg.pubkey() == tvm.pubkey(), 150);
        tvm.accept();
        m_vkey = vkey;
    }
```

Demo server application (node) and HTML page

This demo interactively generates and validates proofs by user inputted data:

Proof is generating by node solutions (which use znSnarkl-Logic CLI application);

Proof is validating by Free TON blockchain using Verification Free TON Solidity contract.

Unfortunately, NIL network is switched off and I can't publish my contract to it. So I've been testing my contract locally.

Compilation & usage

Please use detalizated instruction from my GitHub:

https://github.com/podlodkin/podlodkin-freeton-year-control#compilation--usage