Slovak University of Technology
Faculty of Informatics and Information Technologies

Practical usage of Zero-knowledge in different use-cases in blockchains

Lukáš Častven
xcastven@stuba.sk

Introduction

Zero Knowledge Proofs (ZKPs) provide a unique way to prove information without actually revealing the information itself[3, 2]. This makes them ideal for enhancing anonymity and privacy in blockchain networks. This work explores the use of ZKPs to create stealth addresses on Ethereum blockchain [1].

ZKPs replace elliptic curve cryptography in stealth address schemas. This provides another method for proving ownership of a stealth address while protecting the recipient's identity.

Contributions

1. **Blockchain Privacy Advancement:** This work highlights the power of ZKPs in developing privacy-focused cryptocurrency solutions.
2. **ZKPs for Stealth Addresses:** Successful demonstration of using ZKPs in designing stealth address schema.
3. **Trustless Ownership Proof:** Proposed scheme enables trustless proof of stealth address ownership without compromising privacy.

Solution Design

The core principle behind the solution is that both receiver and sender generate a random value[1]. These two values can then be used to prove to a stealth address that whoever owns these values is the owner of the stealth address, and can control it.

Bob, as a receiver, publishes the hash of his random value to a public registry. With this hash he also publishes his public key, which corresponds to his private key. This tuple is Bob's meta stealth address, visualized in Figure 1.

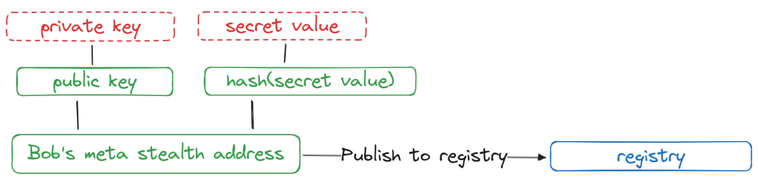

Figure 1: Bob's Meta Stealth Address

When Alice wants to send funds to Bob, she finds his meta stealth address in the public registry, generates her own random value and hashes it together with Bob's hash to create a code. Then she deploys a new stealth wallet contract with this code in it, and amount of funds that she wanted to send to Bob. After that, she encrypts her random value with Bob's public key, this encrypted value is called ephemeral key. Alice publishes it to a public registry. This whole process is depicted in Figure 2.

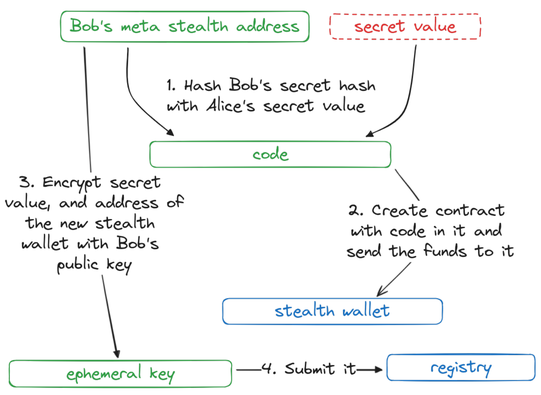

Figure 2: Alice sends funds

Bob then scans the registry, tries to decrypt ephemeral keys. When the decryption is successful, Bob can save the decrypted Alice's secret value and the address of the corresponding stealth wallet.

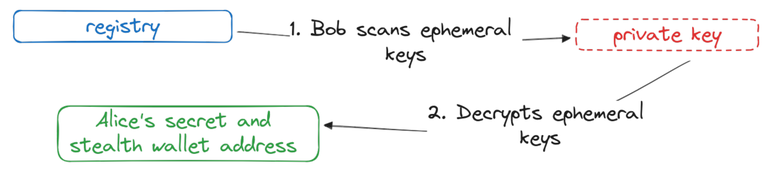

Figure 3: Bob scans ephemeral keys

To use the funds, Bob must generate a ZK proof and submit it to the stealth wallet. This proof proves that Bob knows Alice's random value and his own random value, such that

$$code = hash(hash(Bob's\ value),\ Alice's\ value)$$

where *code* is the one submitted by Alice into the stealth wallet contract.

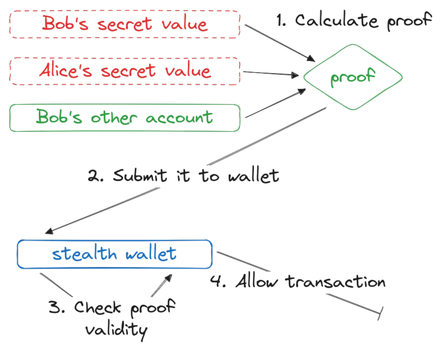

Figure 4: Bob's interaction with wallet

The proof is computed and validated according to this Circom circuit:

```
pragma circom 2.0.0;
include "./circomlib/circuits/poseidon.circom";

template Ownership() {
    signal input owner_secret;
    signal input sender_secret;
    signal input code;
    signal input withdrawee_address;
    signal input msg_sender;

    component owner_secret_poseidon = Poseidon(1);
    owner_secret_poseidon.inputs <== [owner_secret];

    component code_poseidon = Poseidon(2);
    code_poseidon.inputs <== [owner_secret_poseidon.out, sender_secret];

    code === code_poseidon.out;
    msg_sender === withdrawee_address;
}
component main {public [code, msg_sender]} = Ownership();
```

Figure 5: Circom circuit for proving ownership

Conclusions

This work demonstrates a successful use of Zero-Knowledge Proofs to enhance privacy on Ethereum blockchain. By utilizing ZKPs to prove stealth address ownership, it offers a novel approach to protect transaction participants identities. This work highlights the potential of ZKPs to significantly improve blockchain anonymity.

References

[1] An incomplete guide to stealth addresses — vitalik.eth.limo. https://vitalik.eth.limo/general/2023/01/20/stealth.html.

[2] Oded Goldreich, Silvio Micali, and Avi Wigderson. Proofs that yield nothing but their validity or all languages in np have zero-knowledge proof systems. *Journal of the ACM (JACM)*, 38(3):690–728, 1991.

[3] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof systems. *SIAM Journal on Computing*, 18(1):186–208, February 1989.