RingSig Protocol

A Decentralized, Regulated Solution for Supervised Privacy Transaction

RINGSIG

Team Background

RINGSIG

Kevin Lin

Project Manager
Develpment & Product
GitHub: token_lin
@0xkevinlin
1st prize, On-Chain InnovationTrack, 2023 ETH HongKong Hackathon

Arthur

Development
GitHub: supredu
@Donny1296389
1st prize, On-Chain InnovationTrack,
2023 ETH HongKong Hackathon

0xjuliechen

Branding & IR
@0xjuliechen
UPenn Graduate,
prev. A&T Capital, SevenX Ventures
Ambassador of Solana Foundation

Intro

RINGSIG x ARTELA

RingSig: a decentralized, regulated privacy solution based on Artela.
Core Feature: Utilizes ring signature proof to enhance privacy.

Functionality:

- Enables smart contracts to accept deposits in maincoin (ART).
- Allows withdrawals from any address on the Artela network.

Privacy Assurance:

- Breaks the link between deposit and withdrawal addresses.
- Ensures asset privacy with each transaction.

Regulatory Compliance :

- **Users are verified as legitimate by ASPECT before protocol use .**

Our Advantages

RINGSIG

1. Market Gap:

First decentralized privacy solutions on Artela.
Unique use of ring signature technology.

2. Advantages Over Competitors (e.g., Tornado.cash):

- ✓ Fast Off-Chain Proof Generation: Works efficiently on typical household computers.
- ✓ Simplified Usage: No trust settings required.
- ✓ Enhanced Security: Proof binds to recipient address, preventing leaks.

3. Regulatory Compliance:

- ✓ Incorporates regulatory contracts.
- ✓ Offers dual regulatory functions leveraging ring signature features.

4. Target Users:

Focused on compliant users with privacy needs.
Ideal for anti-witch-hunt in airdrops, and privacy-conscious 'whales'.

ASPECT Used in Ringsig Protocol

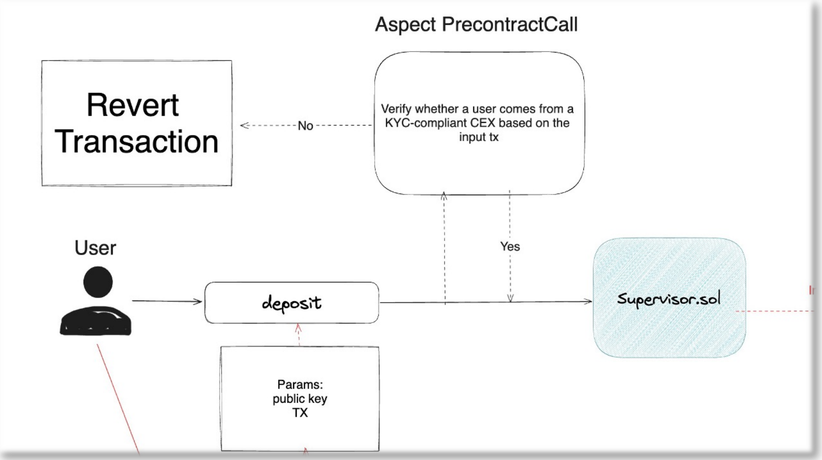
- **Functionality:**

✓ Verify whether the users come from a KYC CEX using the input TX through Aspect's preContractCall (tx.from address should be in whitelist which are CEX address).

- **Benefits:**

✓ Legitimacy verification and the deposit operation are completed within a single transaction.

✓ Automating the legitimacy verification process enhances protocol security and decentralization.



Aspect PrecontractCall

Revert Transaction

No

Verify whether a user comes from a KYC-compliant CEX based on the input tx

Yes

User

deposit

Supervisor.sol

Params:
public key
TX

Protocol Characteristics

RINGSIG

1. Decentralization:

- All transactions executed on-chain for transparency and security.

2. Off-Chain Auxiliary Program:

- Generates public keys for on-chain deposits.
- Produces ring signature proof using private keys for on-chain verification during withdrawals.

3. Efficient Ring Signature Proof Generation:

- Quickly generated by average household computers in seconds.

4. Flexible Withdrawals:

- Available at any time.

Protocol Characteristics

RINGSIG

5. Secure Withdrawal Proof:

- Contains recipient address.
- Allows proxy withdrawals without risk of proof leakage.

6. Withdrawal Fee:

- Set by the depositor and charged to the withdrawer.

7. Dynamic Proof Generation:

- Allows creation of multiple withdrawal proofs with varying public keys and recipient addresses.
- Invalidates other proofs once a successful withdrawal occurs.

Protocol Characteristics

RINGSIG

8. Fixed Withdrawal Amount:

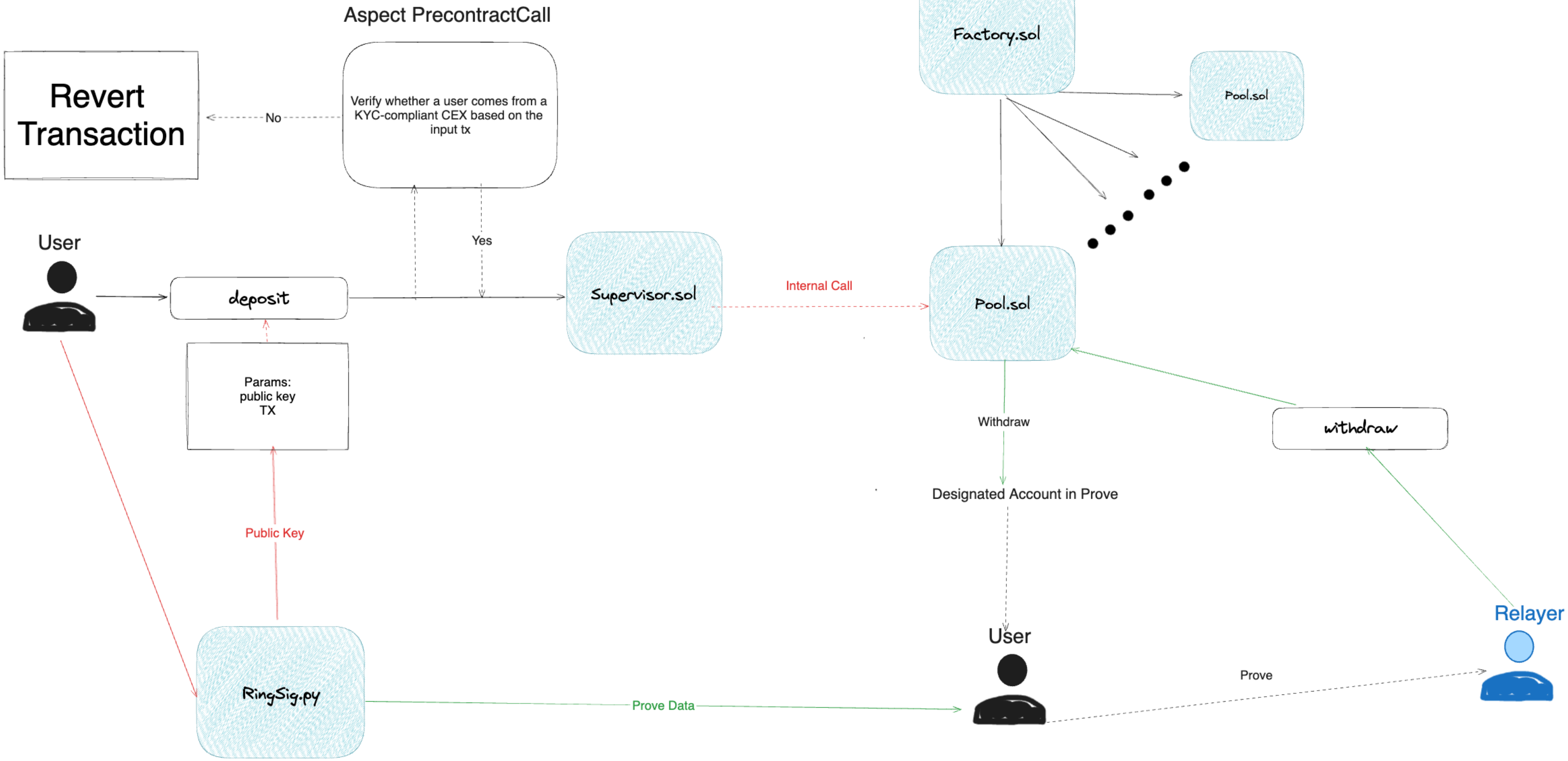
- Ensures consistency and predictability.

9. No Trust Settings Required:

- Simplifies user experience.

10. Enhanced Privacy:

- Averages 100 public keys per signature verification，achieves a privacy-preserving set of approximately 10,000.



Aspect PrecontractCall

Revert Transaction

No

Verify whether a user comes from a KYC-compliant CEX based on the input tx

Yes

User

deposit

Params:
public key
TX

Public Key

RingSig.py

Supervisor.sol

Internal Call

Factory.sol

Pool.sol

Pool.sol

Withdraw

Designated Account in Prove

withdraw

Prove Data

User

Prove

Relayer

Thanks again !

ARTELA

Alibaba Cloud

DoraHacks