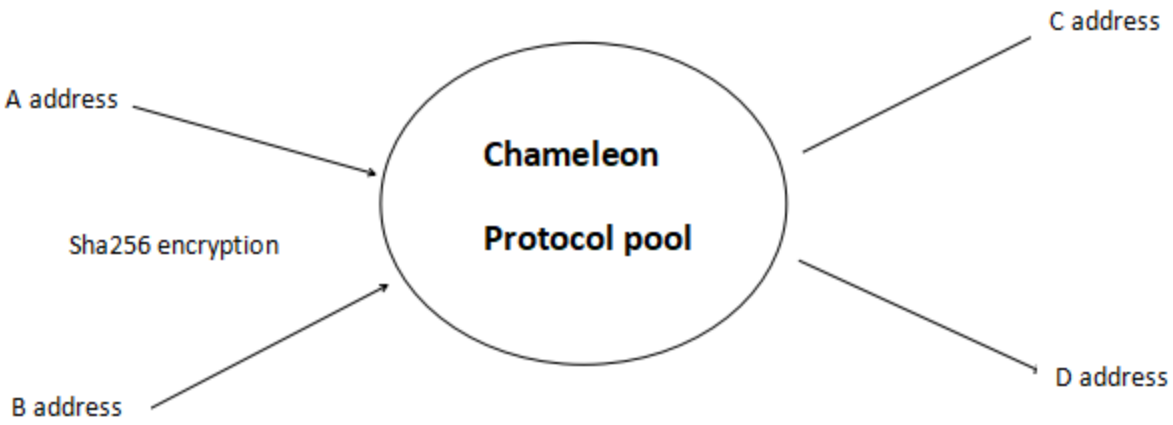
ChameleonProtocol

A New Generation of Multi-chain USDT Coin Mixing Protocol Based on Anonymous Privacy Cryptography



I. Product Introduction

Chameleon Protocol, a very powerful anonymous coin mixing protocol that

supports multi-chain USDT coin mixing transfer technology to insure the transfer of assets on the chain have privacy and untraceability.

--Shadow anonymity protocol for privacy

--Cryptographic algorithms for asset security

--Liquidity incentivizes multi-asset scale

--Converging multi-chain USDT eco

--Fast exchange in very short time

II. Analysis of Anonymous Smart Contract Implementation

Chameleon Protocol's smart contract is designed to be combinable and can technically achieve complete anonymity. The implementation is far away as described below.

The user deposit process is as follows:

Withdrawal Address: 2 in total, sent to the smart contract in encrypted form.

Address rules: Only these 2 addresses agreed upon at the time of deposit are allowed for the withdrawal operation. The first withdrawal must be the principal of the deposit (the principal after deducting the handling fee), and the 2nd withdrawal can withdraw the interest generated. Interest calculation will be stopped after withdrawing the principal amount. Withdrawal of principal address is only for principal and interest withdrawal address is only for interest.

Pledged Deposits to Smart Contracts: Immediately after the user pledges a deposit to interact with the smart contract, the pooling fee is deducted (now the default setting is 1%), the deposit is taken as a cycle of 24 hours. Within 24 hours, no interest is generated; after 24 hours, deposit a full cycle (i.e. 24 hours) can generate cycle interest (interest is also known as earnings). The interest rate is randomly generated and the interest rate algorithm is: (take a random number %9+2)/100, where 100 can change and will be adjusted according to the pool's expected swap conditions. For example, if a user deposits in the pool for 50 hours, then the interest is calculated as: (50-24)/24=1. So the interest will be calculated for one cycle.

III. Analysis of Encryption Algorithm

Chameleon Protocol consists of several encryption algorithms to encrypt the protocol of platform assets and ensure the security of users' asset side. We will explain them separately according to user deposits and user withdrawals.

User Deposit: When a user makes a deposit, three encrypted withdrawal hashes (GetcapitalHash), (GetinterestHash) and (Callhash) are transferred in

and stored in the blockchain. The withdrawal hash is encrypted by the algorithm: sha256(sha256(address,privatekey),publickey,address); the final encryption form is two-layer encryption, sha256 encryption is asymmetric encryption, irreversible. The privatekey is a random 64-bit string generated by the front-end of the user, and each generated string is random and unique. Only the user holds the privatekey for withdrawal.

User Withdrawal: When the user withdraws the assets, he or she transfers the encrypted result of the first layer encryption to the contract after the encryption of sha256(address,privatekey), and after the contract gets this encrypted value, it encrypts again according to sha256(hash one layer encryption parameter value,publickey,address). If the encrypted result matches with the second layer encrypted hash saved at the time of deposit, the verification is passed. After the withdrawal hash is used once, it will be invalidated, and the query hash (i.e. callhash) can be reused.

IV. Fourth, the platform pledge rewards

After the user pledges on the platform, he or she will be rewarded with a random interest of 0.2%-1.1% as a daily income (the reward may continue to change as the project is upgraded, and the pledge needs to exceed a pledge cycle before the interest will be calculated), and if the project is launched initially, there will be rewards for airdrop tokens.

After pledging, the user cannot check the interest rate by default, because the interest rate is a random blind box. If the user needs to check the interest rate,

he or she needs to buy a "Rate Peek Card" and pay the corresponding tokens to check the current interest rate. When the user feels that the current rate is too low, the user can purchase a "Rate Reset Card" to reset the rate, however, the reset rate is still a random blind box, and each order can be reset up to three times, and the more times it is repeated, the more tokens need to be paid.

V. Chameleon Anonymity Protocol

Chameleon Protocol can realize the anonymous transfer of tokens through the shadow anonymity protocol. The principle of implementation is as follows.

After a user pledges in from address A, he or she can be allowed to withdraw coins from address B. The pledge address is not related to the withdrawal address. The amount pledged by the user is a fixed amount (e.g., 100 USDT, 1000 USDT, etc.), and the amount of principal withdrawal is also the amount after deducting a fixed rate of fees.

Interest (i.e. revenue) Generation: We ingeniously designed a random blind box interest rate, and set the interest generation period to 24 hours, which means that there may be many orders within 24 hours to play a confusing role, and because of the randomness of the interest rate, it is impossible to guess which address generated the interest by looking at the interest withdrawal records on the chain. Moreover, the interest withdrawal address is separate from the original coin deposit address.

We have introduced a unique two-layer asymmetric algorithm in the encryption algorithm, and the information submitted to the block is asymmetrically encrypted when making coin withdrawals. At the same time, the encrypted private key is in the hands of the user himself, and the encrypted private key is unique, which effectively blocks the possibility of guessing the solution by analyzing the data of the block and protects the privacy and security of the user's data.

VI. Token Economy

Chameleon Protocol governance tokens are CLP with a total of 100 million issued, and CLP have multiple benefits.

--Governance rights: Token holders can participate in the governance of the platform

--Revenue rights: Users can participate in the platform's deposits/pledges, etc. to obtain the rewards of the platform token

80% CLP for Mining Incentives; 10% for technical incentives; 5% for marketing/operations, etc.; 5% for ecological cooperation.

Mining Incentive 80% : 80 million

Chameleon Protocol's mining method is divided into liquidity mining, transaction mining, and single-coin mining. The ratio of the three types of mining output will be stated when the platform is officially launched.

Technology Incentive 10% 10 million

We are a distributed technology team with technical teams from multiple countries and regions around the world. The technical team incentive is unlocked on a daily linear basis for 12 months of smart contracts after the platform is launched.

Marketing/Operations 5% : 5 million

This portion is used for initial liquidity pool creation as well as marketing, operations, airdrops, etc.

Ecological Cooperation 5%: 5 million

This portion is used for ecological cooperation, including but not limited to technical protocol layer cooperation, institutional cooperation etc. It is locked in the early stage and will be unlocked proportionally when eco-cooperation is conducted.