9. Risk Control And Insurance Of CEP

9.1 Smart Contract Audit

Open finance relies on smart contracts, and smart contracts, as a computer program, are difficult to get rid of bugs. Once a security breach is exploited, it is very likely to lead to catastrophic consequences, such as loss of cryptocurrency and disrupting financial order. According to sampling statistics, quite a few Ethereum smart contracts are not secure.

CEP's smart contracts will cooperate with the industry's best smart contract security audit team, and through the most stringent security audits, to ensure that CEP's contracts are free from any loopholes, so as to ensure the safety of assets during the ETF transfer process.

9.2 Client Security Detection

The security of open finance is not only at the back-end smart contract level, but also the security of the front-end client cannot be ignored. This has been proven by a series of security incidents. Therefore, in addition to strict security audits at the smart contract level, CEP will also conduct comprehensive security checks on user-facing clients to ensure that the front and back ends are sufficiently secure to form a complete closed loop of risk-free operation.

9.3 Insurance

The cryptocurrency market is volatile and risky, and user asset insurance is particularly important.

In the current hot situation of the entire cryptocurrency open finance market, both the lock-up amount of smart contracts and the market value of cryptocurrencies have explosive growth.

In addition, the cryptocurrency market itself is volatile and risky, and we should think about how to deal with the huge risks behind it.

CEP will innovatively access proven decentralized insurance agreements such as Nexus Mutual and OPYN to provide further protection for users' assets. We believe that with the gradual maturity of decentralized insurance, the infrastructure of the CEP industry will also enjoy the highest level of security.