8th TICC International Conference 2024
Integrating Perspectives from Different Disciplines for Current and
Emerging Society Needs towards Sustainable Development Goals (SDGs)
February 1st - 2nd, 2024, Bangkok, Thailand

Seperation Key with ZK Proof Chain: A New Crypto Key Pair Holding Solution

Huifeng Jiao and ??
International College of Digital Innovation, Chiang Mai University, Chiang Mai, 50200, Thailand[1]
E-mail: huifeng_jiao@cmu.ac.th

ABSTRACT

The blockchain industry is heavily depend on encryption theory, such as asymmetric and symmetric encryption theories. The digital signature of the key pair, which protects all the data in blockchain. Many encryption algorithms have become strongger and stronger, but users still keep their key pairs in a bare way, just keeping by memonic words or private key.

This paper proposes a new method called the separation key method, which allows users to keep only a basic credential, such as a mobile phone number, to control the total life of the key pair: create, sign transactions, migrate, and more. The key pairs of users are kept in a decentralized server controlled by a multi-signature council. All transactions will be signed by the corresponding user's key pair with a ZK proof and a verification. This guarantees that any signature comes from the user's intention.

The separation key method has several advantages over traditional key management methods:

1. It is more secure: The key pairs are stored in a decentralized server, making them more resistant to theft and hacking.
2. It is more convenient: Users only need to remember a single credential, such as a mobile phone number, to manage all of their key pairs.
3. It is more flexible: The separation key method allows users to create, sign transactions, migrate, and revoke key pairs in a flexible way.

The separation key method is a new and innovative approach to key management. It has the potential to make the blockchain and crypto industry more secure, convenient, and flexible.

KEYWORDS: Blockchain, Key Pair, Seperation Key, Zero Knowledge Proof