Shaoyu Li, Guangrui Wang, Geping Chen

Background:

Blockchain, as the underlying technology of bitcoin, uses distributed systems to finish its work. Because those systems have lots of distributed nodes and these nodes need to communicate for the finance purposes in the peer to peer network, the systems need to be secure and they need to prevent information disclosure. Therefore, we need to encrypt the messages and then we can put them in the network. Other nodes can receive the ciphertexts. They can use the correct keys to decrypt the ciphertexts and get the information. If we want to keep the security of information transmission, it is better for us not to upload our keys, because we hold the idea that the network is not secure. Therefore, the better method is using asymmetric encryption, which means that we have different keys for encryption and decryption. For example, we can use public keys to encrypt and use private keys to decrypt. In blockchain systems, private keys are regarded as the identity and security credential, and they are generated and maintained by users themselves instead of third-party agencies. Therefore, if one user's private key is lost or stolen, he cannot manage his blockchain account, and then he cannot do the transaction anymore. Therefore, it is important to protect the private keys and have a mechanism to retrieve the private keys if they are lost.

Work:

We want to introduce a new mechanism of identification recovery to the case when users lose their private keys, the mechanism can help to verify their identifications and sign in. Currently, there are several solutions we can consult, one is like the mechanism adopted by weChat, the users can send a request to their friends related to these accounts, and ask them for verifying the identification. Another way is biometrics. Everytime we create a new blockchain account, a private key will be created along with the account, some of the biometric information like finger-print or finger-vein will be calculated into a specific hash value and be stored in the meantime. When users lose their private key, they can use the biometric verification mechanism to login and retrieve their private key.

Contribution:

Based on the current blockchain mechanism, we propose a new identification mechanism together with the current blockchain identification method to verify the user's identity. Our mechanism guarantees that once users lose their private key, we can support them to login to the account and recreate a new private key.