

An anonymous key exchange technology with good security and simplicity

User ID (public-key) management method for highly anonymous decentralized services

Introduction

In cryptocurrencies such as Bitcoin, the user's offline privacy, which is linked to user ID (public-key), may be leaked by the frequent trading, because all transactions are fully disclosed on the blockchain.

This invention provides a new technology for secretly exchanging depleted user IDs whose anonymity has declined with fresh ones through collaboration among other users (support users). Compared with current technologies, it has a resistance to the support users betray without any special changing of the blockchain mechanism. Amazingly, not only user's anonymity can be ensured, but also the transparency and versatility of services including the blockchain will be retained.

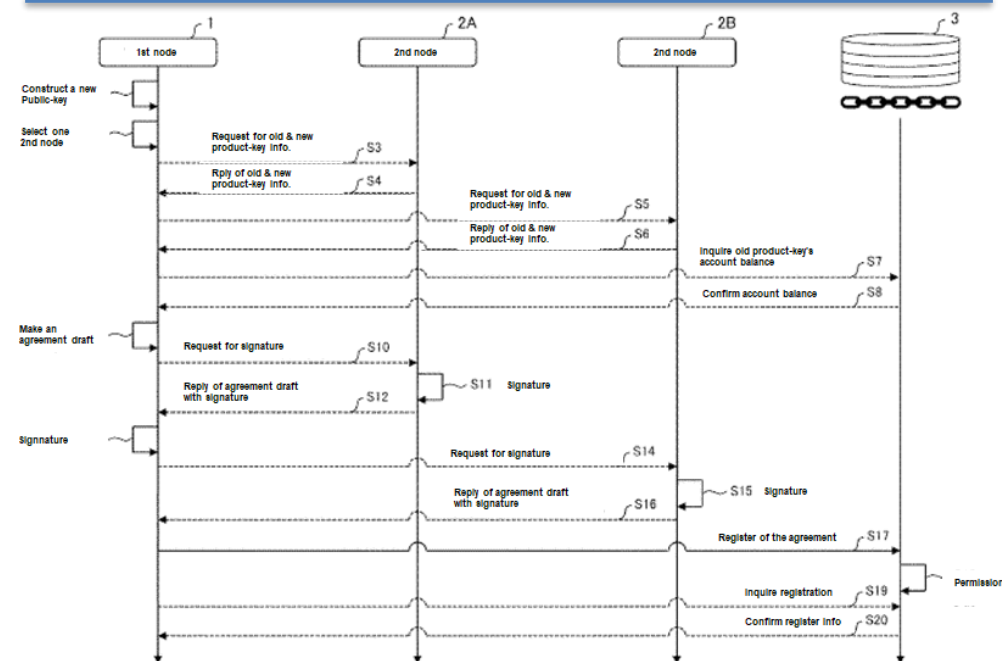
Application

- All the decentralized services (i.e. Blockchain 2.0 services) demanding user's anonymity.
- Information management server, electronic voting, etc.

Patent Data Sheet

Patent No.(Serial No.): JP6545888 (T18-057)
Inventors: SAKAI Masao, et al.

Representative sequence illustration



The input-output relation in transaction is anonymized by using two or more support users (2nd nodes).

Contact

Tohoku Techno Arch Co., LTD
TEL:+81-22-222-3049, FAX:+81-22-222-3419
[Click](#) to contact