MANTLE
Identity and Privacy Toolkit

WO2017090041A1
WO Application

Inventor
Adi BEN-ARI

Priority date
2015-11-24

Family
EP (1)WO (1)

A key element of public distributed ledger technologies is that anyone hosting a node on the network can view all confirmed transactions on that network. This level of transparency naturally creates a barrier to entry for enterprises and startups who wish to deploy blockchain applications but require an element of privacy in order to maintain their competitive advantage.

What Mantle delivers

Mantle solves the problem of privacy and anonymity by adding an additional layer of security on top of any blockchain application that supports smart contracts.

This enables confidential data to be encrypted within smart contracts and kept anonymous, whilst other data can be shared on the ledger for users to see.

Mantle enables data caching to greatly improve system performance and data retrieval to run application operations.

1 **Mantle and its layers**
3 **Encrypted data**
2 **Blockchain application**
4 **Blockchain platform**

The layers of Mantle include

Wallet
Generate and store private/public key pairs belonging to a user or to another entity, call Smart Contracts and sign transactions.

Privacy
Compatible on most blockchain platforms, and allows private data to be encrypted and accessed by selected parties

Key recovery
Provides two different key recovery mechanisms

Enterprise key management
Integration with AWS Key Management Service and Azure Key Vault

Anonymity
Cryptographic key issuance and storage to securely manage the identities of network members

Platform independent
Can be used on any blockchain application that supports smart contracts

GDPR compliance
Enables the "right to be forgotten"

AD / LDAP
Directory services integration