Technology offer

Method and device for controlling the re-identification of pseudonymized linking data in a permanent immutable distributed decentralized storage

Field of use

Blockchain

Current state of technology
Stage of Development:
Available for demonstration
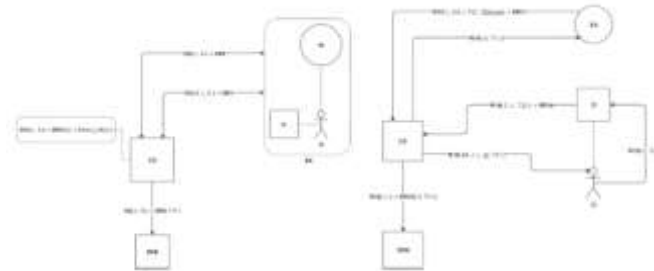
Patent status
Patent pending

Developed by

doc. dr. Muhamed Turkanović,
dr. Boštjan Kežmah,
Blaž Podgorelec,
doc. dr. Aida Kamišalić Latifić,
Marjana Heričko, prof. dr.
Marjan Heričko, mag.

Contact details
University of Maribor
Knowledge and technology
transfer office
Telefon: +386 2 23 55 298
E-mail: tto@um.si

Background

There are many options for storing data in a digital form. In most cases, the storing is performed within a private digital storage, a database, that allows for subsequent editing or deleting of data. Access to the storage and data management is enabled only to the entity that owns the database, or any other entity which is authorized by the storage owner or database manager to manage the data. In some cases, there is a requirement for a publicly available/accessible digital storage. When personal data is kept in a storage for which public access is not permitted, then such storage must be protected in such a way that an unauthorized access is not permitted, which, by default, public digital storages do not restrict. In such cases, the data can be protected using cryptographic methods that ensure data unreadability even though data is publicly available.

Description of the invention

The proposed invention presents the solution of the described problem in the form of a method and a device for storing data in a permanently immutable, distributed and decentralized storage, and the control of each separate inspection attempt of the data and the retrieval of data from a permanently immutable distributed and decentralized storage. In the storing process, the proposed method deals with the actual and linking data separately. The content of the linking data is the direct or indirect identifier of an owner of the actual data (e.g., personal data), and is de-identified several times, using various pseudonymization techniques supported by cryptography, before stored in such storage. The process of re-identification of pseudonymized data by means of the proposed method and device allows the owner control over each respective inspection request into his data stored in the permanently immutable, distributed, and decentralized storage. The proposed method and device allow storing data in compliance with regulations relating to the processing of personal data.

Main advantages

The method and device provide the storage of linking data in a public, permanently immutable, distributed and decentralized storage, which may include personal information, in a manner that is accessible to all entities that have access to the network, but are, by default, de-identified i.e. pseudonymized; storing the actual data in a readable form in a permanently immutable, distributed and decentralized storage; support for the controlled re-identification of pseudonymized linking data, and for the inspection of the readable format of actual data from permanently immutable, distributed and decentralized storage; the control of the data owner over the process of re-identification of pseudonymized linking data, and the inspection of the readable format of actual data in permanently immutable, distributed and decentralized storage, based on the authorization of the owner and a data validation mechanism; sending a request from the entity to the data owner for one-time inspection access of his actual data stored in permanently immutable, distributed and decentralized storage; control of the process of re-identification of pseudonymized linking data for each inspection request by any user device; compliance of the method and the device with the requirements of the GDPR.