A-SIT Technology
E-Government Innovation Center

1 October 2018 Study · Blockchain · Privacy & Crypto

Redactable Blockchain

The full text is currently only available in the Deutsch version. A translation will follow.

Archived. This content is no longer updated. It remains available for reference.

Version 2018-09-07
Source https://technology2.a-sit.at/en/publications/redactable-blockchain/

This project report starts by giving an overview of various data insertion methods available in Bitcoin. After this introduction, the report introduces two approaches that allow redacting data on the blockchain, without breaking its integrity. The first approach, published by Ateniese u. a., uses Chameleon hash functions, while the second approach, published by Puddu u. a. is based on encryption. Additionally, the study presents a third approach, which legitimates data redaction by using a second block chain.