User-Perceived Privacy in Blockchain

Simin Ghesmati

Vienna University of Technology, Vienna, Austria, SBA research, Vienna, Austria

Walid Fdhila

University of Vienna, Vienna, Austria, SBA research, Vienna, Austria

Edgar Weippl

University of Vienna, Vienna, Austria, SBA research, Vienna, Austria

Abstract

This paper studies users' privacy perceptions of UTXO-based blockchains such as Bitcoin. In particular, it elaborates – based on interviews and questionnaires – on a mental model of employing privacy-preserving techniques for blockchain transactions. Furthermore, it evaluates users' awareness of blockchain privacy issues and examines their preferences towards existing privacy-enhancing solutions, i.e., add-on techniques to Bitcoin versus built-in techniques in privacy coins. Using Bitcoin as an example, we shed light on existing discrepancies between users' privacy perceptions and preferences as well as current implementations.

Paper bibliographic citation

The paper was accepted and presented in CoDecFin22 workshop in Finacial cryptography and data security 22 (FC22).

The paper will be published in LNCS publication after the workshop.

Workshop program: https://fc22.ifca.ai/codecfin/program.html
Full paper: https://eprint.iacr.org/2022/287.pdf