22. Mai 2019 Studie · Web & Cloud · Blockchain

# Sicherheitsanalyse aktueller Peer-to-Peer-Netze

Der Volltext liegt derzeit nur in der Fassung „English“ vor. Die Übersetzung folgt.

**Archiviert.** Dieser Inhalt wird nicht mehr aktualisiert. Er bleibt zur Information verfügbar.

**Quelle** https://technology2.a-sit.at/veroeffentlichungen/sicherheitsanalyse-aktueller-peer-to-peer-netze/

Dieses Projekt analysiert die Sicherheitskonzepte aktuell im Einsatz befindlicher Peer-to-Peer-Netze. Unter anderem durch den Kryptowährungshype der letzten Jahre erfahren Dezentralisierungsgedanken vermehrt Zuspruch, wobei Sicherheitskonzepte im Rahmen moderner Peer-to-Peer-Systeme im Vergleich zu frühen Entwicklungen einen integralen Bestand-teil der Systemarchitektur bilden. Auf Grund von aktuellen Erkennt¬nissen zum Thema Peer-to-Peer-Sicherheit, welche aus einem vorangegangen A-SIT-Projekt hervorgingen, ergaben sich jedoch Zweifel an der Effektivität insbeson-dere von Proof-of-Work-basierter Identifikator¬generierung im Rahmen dezen-traler Peer-to-Peer-Netze. Im Speziellen wurde IPFS, das als vielseitig einsetzbarer Peer-to-Peer-Netzwerklayer und Motor für Dezentralisierungs-bestrebungen positioniert wird, auf potentielle Schwachstellen analysiert. Dabei konnten Teilerfolge in Richtung praktisch relevanter Angriffe erzielt werden und teilweise auch Netzwerkknoten vom Rest des Netzwerks abgeschnitten werden.

Darüber hinaus gibt der Projektbericht einen Überblick über die Sicherheitskonzepte von BitTorrent und Bitcoin. Zusätzlich wird ein neues Sicherheitskonzept für dezentrale Peer-to-Peer-Netze auf Basis von Android-Remote-Attestation-Verfahren vorgestellt, dessen technische Details im Rahmen einer aus diesem Projekt hervorgegangenen wissenschaftlichen Publikation ausgearbeitet wurden, die im Rahmen der 16th International Conference on Security and Cryptography 2019 präsentiert wird.