16. Mai 2019 Studie · Blockchain

Sicherheit von blockchain-basierten Kryptowährungen

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/sicherheit-von-blockchain-basierten-kryptowaehrungen/

In diesem Projekt werden zuerst verschiedene Angriffe auf blockchain-basierte Kryptowährungen vorgestellt. Beispielsweise werden der 51% Angriff, verschiedene Block zurückhalte Angriffe, der „Goldfinger“-Angriff, der „Feather forking“-Angriff, der „Big Fee“-Angriff oder der sogenannte „Dust“-Angriff behandelt. Nach der Vorstellung der Angriffe werden prominente Programmierfehler und andere Probleme behandelt. Beispiele dafür sind der Integer-Überlauf-Fehler, ein Fehler der zu einer unbeabsichtigten Regeländerung führte und das Problem der Veränderbarkeit von Transaktionen (Transaction malleability). Nach diesen Problemen werden verschiedenen Techniken vorgestellt, welche für Sicherheitsanalysen verwendet werden können. Beispiele hierfür sind die Berechnungen aus dem Original Bitcoin Whitepaper, Spieletheorie sowie die Eigenschaften Blockchain-Wachstum, gemeinsames Präfix sowie Blockchain-Qualität, welche essential für eine robuste Blockchain sind.