VRG18-002 - COnFIDE - Cryptographic Foundations of Privacy in Distributed Ledgers

Zusammenfassung

Dezentralisierung ist heute ein wichtiger Trend, der sich in Technologien wie der Blockchain, oder allgemeiner „Distributed Ledgers“, widerspiegelt. Diese Technologien machen Währungen ohne Banken (wie z.B. Bitcoin), Tausch-Plattformen ohne kommerzielle Anbieter u.v.m. möglich. Ein Grundprinzip ist dezentrale Kontrolle: Jeder kann überprüfen, dass erfolgte Transaktionen gültig sind, wodurch Vertrauen in zentrale Akteure obsolet wird. Bei Bitcoin sind zum Beispiel alle Zahlungen in der Blockchain einsehbar; allerdings steht diese Transparenz im Widerspruch zum Schutz der Privatsphäre, der in Zeiten der DSGVO auch politisch an Bedeutung gewinnt. Das Ziel von COnFIDE ist es, diesen Widerspruch zu überwinden und mittels Kryptographie die dezentrale Kontrolle mit dem Schutz der Privatsphäre in Einklang zu bringen. Gleichzeitig gilt es, die Effizienz und Nachhaltigkeit dezentraler Systeme zu verbessern, um enormen Stromverbrauch wie beim Schöpfen von Bitcoins zu vermeiden und Systeme zu schaffen, die den Anforderungen der Zukunft gerecht werden.

Wissenschaftliche Disziplinen:
Cryptology (90%) | IT security (10%)

Keywords:
cryptography; zero-knowledge; privacy; blockchains; distributed ledgers

---

VRG leader:	Georg Fuchsbauer
Institution:	TU Wien
Proponent:	Matteo Maffei
Institution:	TU Wien

Status: Laufend (01.01.2020 - 31.12.2027)
GrantID: 10.47379/VRG18002

Weiterführende Links zu den beteiligten Personen und zum Projekt finden Sie unter
https://www.wwtf.at/funding/programmes/vrg/VRG18-002/