Medienmitteilung vom 29. Januar 2019
ZHAW Zürcher Hochschule für Angewandte Wissenschaften

Erstmals elektronische Signatur für Blockchain entwickelt

Bisher verhinderte die fehlende Unterschriftsmöglichkeit sichere Transaktionen mit der Blockchain-Technologie. Deshalb haben die ZHAW und Swisscom erstmals eine Anwendung entwickelt, um die qualifizierte elektronische Signatur auf der Blockchain einzusetzen. Damit lassen sich rechtsgültig Verträge abschliessen und Vermögenswerte übertragen.

Die Blockchain-Technologie verändert den Güteraustausch über das Internet. Denn sie ermöglicht, dass Transaktionen ohne zentrale Instanz und vollkommen transparent abgewickelt werden können. Bislang liess sich aber eine qualifizierte elektronische Signatur nicht direkt auf einer Blockchain einsetzen. Die qualifizierte elektronische Signatur ist anstelle der eigenhändigen Unterschrift nötig. Denn Verträge und andere Rechtsgeschäfte müssen häufig schriftlich abgeschlossen, somit von allen Parteien unterschrieben werden. Diese Schriftform dient als Beweis, schützt vor übereiltem Handeln oder gewährt Informationen für die andere Vertragspartei.

Smart Contract macht Unterschrift überflüssig

Die fehlende Schriftform galt bisher in vielen Bereichen als Hindernis für den rechtssicheren Einsatz einer Blockchain. Im Rahmen eines gemeinsamen Forschungsprojekts hat nun ein interdisziplinäres Team aus Juristen und Ingenieuren der ZHAW zusammen mit Swisscom einen Prototyp eines Smart Contract entwickelt, mit dem sich das Schriftformerfordernis auf der Blockchain erfüllen lässt. Smart Contracts sind Computerprogramme, mit denen die Übertragung von Vermögenswerten gesteuert werden kann. Der auf der Ethereum-Blockchain basierende Smart Contract enthält eine Schnittstelle zum Unterschrifts-Service von Swisscom. Dadurch können Transaktionen auf der Blockchain rechtsgültig mit einer qualifizierten elektronischen Signatur versehen werden. Nach erfolgreicher Prüfung der Signatur wird direkt die gewünschte Wirkung auf der Blockchain ausgelöst, etwa die Übertragung des Vermögenswerts oder der Abschluss eines Vertrags. Laut dem ZHAW-Experten Harald Bärtschi werden dadurch die bis jetzt bestehenden rechtlichen Unsicherheiten beseitigt. «Für die Schweiz ist dies besonders wichtig, weil es bei uns ein Schriftformerfordernis gibt für die Übertragung von Forderungs- und ähnlichen Rechten. Bisher war es oft zweifelhaft, ob Übertragungen auf der Blockchain rechtlich wirksam sind.»

Einfach in Blockchain-Systeme integrierbar

Mit dem entwickelten Smart Contract lassen sich so auf der Blockchain rechtsgültig Verträge abschliessen und Vermögenswerte übertragen. «Die vorliegende Lösung kombiniert die Vorteile der dezentralen Blockchain-Infrastruktur mit der hohen Sicherheit und Vertrauenswürdigkeit der zertifizierten Signatur», so Bärtschi. Sie lässt sich vergleichsweise einfach in bestehende Blockchain-Systeme wie die Ethereum-, Hyperledger- oder

Corda-Blockchain integrieren. Unterstützt werden nicht nur Signaturen gemäss schweizerischen Anforderungen, sondern auch solche nach der eIDAS-Verordnung der Europäischen Union. «Damit eröffnet sich eine Vielzahl internationaler Anwendungsmöglichkeiten», wie Peter Amrhyn von Swisscom erklärt.

Kontakt

Prof. Dr. iur. Harald Bärtschi, Leitung Zentrum für Unternehmens- und Steuerrecht, ZHAW School of Management and Law, Tel. 058 934 76 60, E-Mail harald.baertschi@zhaw.ch
Prof. Dr. sc. Jörg Osterrieder, Institut für Datenanalyse und Prozessdesign, ZHAW School of Engineering, Tel. 058 934 45 94, E-Mail joerg.osterrieder@zhaw.ch
ZHAW Corporate Communications, Telefon 058 934 75 75, E-Mail medien@zhaw.ch