SUCCESS STORY

IT-SICHERHEIT IN DER BLOCKCHAIN

SBA Research gemeinnützige GmbH (gGmbH)
Floragasse 7, 1040 Wien
Tel. +43 (1) 505 36 88
office@sba-research.org

Förderung: BRIDGE-Programm

Smart Contract Informationssicherheit ganzheitlich betrachtet

IDENTIFIKATION NEUER SPANNUNGSFELDER UND ANFORDERUNGEN IN DEZENTRALEN SYSTEMEN

Innovative Technologien wie Smart Contracts stellen Entwickler*innen vor neue Herausforderungen, da kleinste Fehler bei der Konzeption und Umsetzung großen finanziellen Schaden verursachen können.

Innovationspotential

Durch **Grundlagenforschung** können die **Risiken und Chancen von Blockchain- und Smart Contract Technologien** besser verstanden und bewertet werden noch bevor sie breiten Einzug in unsere Gesellschaft finden.

Nutzen

- **Verbessertes Verständnis** für die Anforderungen von Blockchain-Technologien
- **Identifikation möglicher Schwachstellen** und Angriffsvektoren
- **Neuartige Algorithmen** zur Umsetzung von Blockchain-Protokollen

Foto: Das Team von Herrn Judmayer beim Diskutieren von neuen Angriffen auf Blockchains im Rahmen eines von SBA Co-organisierten Dagstuhl Seminars.

Österreichische Forschungsförderungsgesellschaft mbH
Sensengasse 1, A-1090 Wien
T +43 (0) 5 77 55 - 0
office@ffg.at
www.ffg.at

SUCCESS STORY

Smart Contract Sicherheit ganzheitlich betrachtet

Gemäß der Devise „Eine Kette ist so stark wie ihr schwächstes Glied“ müssen bei komplexen Technologien verschiedenste Aspekte berücksichtigt werden, **um ihre Sicherheit und Korrektheit zu gewährleisten**. Um diese Anforderungen besser verstehen und abschätzen zu können, wurde im BRIDGE 1-Forschungsprojekt **„SESC - Secure Execution of Smart Contracts“ praxisnahe Grundlagenforschung** betrieben, die sich nicht nur mit Smart Contracts sondern auch mit deren zugrunde liegenden Blockchains ganzheitlich auseinandersetzt.

Forschung abseits des Hypes

Kryptowährungen und damit der Einsatz von Blockchain Technologien haben sich in den letzten Jahren vom belächelten Nischenthema in ein zukunftsträchtiges Entwicklungsfeld verwandelt, das mittlerweile auch von Institutionen wie der Europäischen Zentralbank durchaus ernst genommen wird. Hierbei **spricht man gerne von den Vorzügen der Blockchain hinsichtlich Transparenz, Sicherheit und Unabänderlichkeit von Transaktionsdaten**, jedoch sind diese Ansichten oftmals nicht auf sachlich belegten und erforschten Tatsachen begründet.

Im Rahmen des SESC-Projekts haben Forscher*innen von SBA Research **nicht nur viele offene Fragestellungen der Wissenschaft adressiert**, sondern auch **wichtige Aufklärungsarbeit an Universitäten und in der Privatwirtschaft durch Vorlesungen und Workshops** geleistet. Durch die gesamtheitliche Betrachtung von Blockchain-Technologien als komplexe Systeme haben sich zudem auch spannende Forschungsarbeiten, wie beispielsweise die **Sicherheit von Stromnetzen in Bezug auf Proof-of-Work Mining**, ergeben, denen mit einem isolierten Blickwinkel vielleicht **keine Beachtung geschenkt worden wäre**.

Innovation durch Verstehen

Die erzielten exzellenten Forschungsergebnisse beruhen auf einem tiefgehenden Verständnis der Blockchain-Technologien, welches bei SBA Research als Teil des Projekts aufgebaut und vertieft werden konnte. Hierdurch wurden **Probleme, wie etwa das energieaufwendige Mining** oder die **Bestechlichkeit von Miner*innen**, schon frühzeitig als zentrale Hindernisse in diesen Technologien erkannt und innerhalb des SESC-Projekts alternative Lösungsansätze entwickelt.

Wer ist SBA?

SBA Research ist eine auf Informationssicherheit spezialisierte außeruniversitäre Forschungs-einrichtung. Seit 2014 wird auch das Thema „Blockchain“ intensiv behandelt, wodurch SBA eine nationale Vorreiterrolle und tragende Säule in der Forschung in diesem Bereich eingenommen hat.

*Abbildung 1: Gruppenfoto der Mitarbeiter*innen von SBA Research*

Zukunftsträchtige Technologie?

Die Popularität von Smart Contract Plattformen wird aufgrund ihrer vielseitigen Nutzungsmöglichkeiten **wie etwa für DeFi (Decentralized Finance)** voraussichtlich weiterwachsen. Mit einher gehen jedoch **Risiken wie Sicherheitslücken und neuartige Angriffe**, die es zu vereiteln gilt.

Österreichische
Forschungsförderungsgesellschaft mbH
Sensengasse 1, A-1090 Wien
T +43 (0) 5 77 55 - 0
office@ffg.at
www.ffg.at