KRYPTOMONITOR

Verfahren zur forensischen Analyse von Smart Contracts und Off-Chain-Transaktionen

Programm / Ausschreibung	KIRAS, Kooperative F&E-Projekte, KIRAS Kooperative F&E-Projekte 2019	**Status**	abgeschlossen
Projektstart	01.10.2020	**Projektende**	30.09.2022
Zeitraum	2020 - 2022	**Projektlaufzeit**	24 Monate
Keywords	cryptoassets, forensics, blockchain		

Projektbeschreibung

Geldflüsse in der nach wie vor relevantesten Kryptowährung Bitcoin können derzeit noch relativ gut nachvollzogen werden. Der Bedarf nach neuen forensischen Methoden ist jedoch aufgrund der fortschreitenden technischen Entwicklung bereits vorhersehbar: virtuelle Vermögenswerte, sogenannte Kryptoassets, und Finanzprodukte werden zunehmend als Tokens bzw. Smart Contracts umgesetzt und auch durch die zunehmende Verbreitung von Off-Chain Zahlungskanälen werden etablierte Blockchain-Forensik-Werkzeuge bald an ihre technischen Grenzen stoßen.
Das Ziel des KRYPTOMONITOR Projekts liegt deshalb in der Entwicklung generischer Kryptoasset-Analysemethoden, die neben nativen Kryptowährungs-Transaktionen auch die Analyse von Smart Contracts und Off-Chain Transaktionen unterstützen. Die resultierenden Werkzeuge sollen eine effektivere Strafverfolgung durch neue forensische Analyseverfahren ermöglichen und eine faktenbasierte Entscheidungsgrundlage zur Bewertung möglicher Risiken und zur Durchsetzung regulatorischer Maßnahmen bieten. Orthogonal dazu sollen rechtliche und regulatorische Fragestellungen in Bezug auf Tokens beantwortet, Standards für einen effektiven Datenaustausch spezifiziert und Qualifizierungsstandards durch Schulungsmaßnahmen gesetzt werden.
Die zu erwartenden Projektergebnisse sind: (i) eine rechtliche Bewertung der entwickelten Methoden und Regulierungsempfehlungen hinsichtlich Tokens und Zahlungskanälen, (ii) neue forensische Methoden zur Analyse generischer Kryptoassets die als Programmbibliotheken umgesetzt und in existierende Werkzeuge (z.B.: BlockSci, GraphSense) integriert wurden, (iii) eine systematische Analyse und Risikobewertung von Tokens, (iv) Formate für einen harmonisierten Datenaustausch zwischen involvierten Stakeholdern, sowie (v) ein abgestimmtes Kryptowährungs-Forensik-Curriculum als Qualifizierungsmaßnahme für Ermittler.
Innovation ergibt sich durch die rechtliche Betrachtung neuer Vermögensformen, durch neue algorithmische Verfahren zur Analyse von Smart Contracts und Off-Chain Zahlungskanälen, durch quantitative Analysen von Cybercrime mit Kryptoasset Bezug, durch neuartige Risikobewertungsmethoden, durch neue Datenaustauschstandards und durch ein, bis dato noch nicht vorhandenes Kryptoasset-Forensik-Curriculum, das in bestehende Schulungsprogramme für Strafverfolgungs- und Regulierungsbehörden integriert werden kann.
Experten und Entscheidungsträger in Behörden sowie Compliance Mitarbeiter in FinTechs mit Kryptoasset-Bezug (z.B.: Exchanges) stellen die Benutzer-Zielgruppe des Projekts dar. Während der Projektlaufzeit werden sie von Wissenszuwachs

profitieren und die entwickelten Methoden und Tools sowohl in Form freizugänglicher Software-Komponenten nutzen können. Nach Projektende können die Resultate auch kommerziell verwertet und in Form von Produkten, Wartungsverträgen oder Dienstleistungen angeboten werden.

Abstract

Cash flows in the still most relevant cryptocurrency Bitcoin can currently still be traced relatively well. However, the need for new forensic methods can already be anticipated due to the advancing technical development: virtual assets, so-called cryptoassets, and financial products are increasingly being implemented as tokens or smart contracts, and established blockchain forensics are also becoming more common due to the increasing spread of off-chain payment channels. Therefore, existing blockchain-forensics will soon reach their technical limits.
The goal of the KRYPTOMONITOR project is therefore to develop generic cryptoasset analysis methods that support the analysis of smart contracts and off-chain transactions in addition to native cryptocurrency transactions. The resulting tools should enable more effective law enforcement through new forensic analysis procedures and provide a fact-based decision-making basis for assessing possible risks and enforcing regulatory measures. Orthogonally, legal and regulatory questions relating to tokens are to be answered, standards for effective data exchange are specified, and qualification standards are to be set through training measures.
The expected project results are: (i) a (data protection) legal assessment of the developed methods and regulatory recommendations with regard to tokens and payment channels, (ii) new forensic methods for the analysis of generic cryptoassets which are not used as program libraries and in existing tools (e.g.: BlockSci, GraphSense) were integrated, (iii) a systematic analysis and risk assessment of tokens, (iv) formats for a harmonized data exchange between involved stakeholders, and (v) a coordinated cryptocurrency forensic curriculum as a qualification measure for investigators.
Innovation arises from the legal consideration of new forms of wealth; through new algorithmic procedures for the analysis of smart contracts and off-chain payment channels; through quantitative analyzes of cybercrime with cryptoasset reference; through new risk assessment methods; through new data exchange standards; and through a hitherto not yet available Cryptoasset forensic curriculum that can be integrated with existing law enforcement and regulatory training programs.
Experts and decision-makers in public authorities as well as compliance employees in FinTechs with a cryptoasset connection (e.g.: Exchanges) represent the target user group of the KRYPTOMONITOR project. During the project period, they will benefit from increased knowledge and the developed methods and tools both in the form of freely accessible software components to be able to use. At the end of the project, the results can also be used commercially and offered in the form of products, maintenance contracts or services.

Projektkoordinator

- AIT Austrian Institute of Technology GmbH

Projektpartner

- Bundesministerium für Inneres
- Research Institute AG & Co KG
- T3K-Forensics GmbH
- Bundesministerium für Finanzen
- Universität Innsbruck