DeFiTrace

Daten-getriebene Methoden zur Analyse illegaler Zahlungsströme in Ledger-übergreifenden DeFi-Ökosystemen

Programm / Ausschreibung	KIRAS, Kooperative F&E-Projekte, KIras Kooperative CS F&E Projekte (KFE CS_2022)	**Status**	laufend
Projektstart	01.10.2023	**Projektende**	30.09.2025
Zeitraum	2023 - 2025	**Projektlaufzeit**	24 Monate
Keywords	Decentralized Finance, Kryptoassets, Geldwäsche		

Projektbeschreibung

In jüngster Zeit werden illegale Zahlungsströme zunehmend durch Decentralized Finance (DeFi)-Dienste verschleiert. Diese Dienste bilden ein neues Finanzparadigma auf Basis von Kryptoassets und bieten neuartige Finanzdienstleistungen wie Kreditvergabe, Investitionen oder Tausch von Kryptoassets an, ohne dass regulierte Institutionen, wie z. B. Kryptobörsen, beteiligt sind. Dazu gehören dezentrale Kryptoasset-Exchanges (DEXs), Stablecoins (z. B. Tether) und nicht fungible Vermögenswerte (NFTs). Die Verwendung dieser komplexen Dienste erschwert die ohnehin schwierige Nachvollziehbarkeit von Zahlungsströmen zusätzlich, bringt die bislang verfügbaren Analysewerkzeuge an ihre Grenzen und stellt Behörden vor noch ungelöste Herausforderungen.

Das Ziel des DeFiTrace-Projekts besteht daher in der Entwicklung neuer algorithmischer Lösungsansätze zur automatisierten Analyse illegaler Zahlungsströme in Ledger-übergreifenden DeFi-Ökosystemen. Die resultierenden algorithmischen Methoden und Werkzeuge sollen mittelfristig eine effizientere und effektivere Verfolgung inkriminierter Gelder durch komplexe, Ledger-übergreifende dezentrale Finanz-Konstrukte ermöglichen und auch eine empiriebasierte Durchsetzung regulatorischer Maßnahmen unterstützen. Das Projekt wird durch die Beantwortung rechtlicher und regulatorischer Fragestellungen im Kontext aktueller regulatorischer Entwicklungen (MiCA und DAC8) flankiert, sowie durch die behördenübergreifende Etablierung von Schulungen und Weiterbildungsstandards im Themenbereich Kryptoassets.

Die erwarteten Projektergebnisse umfassen: (i) eine systematische Analyse des regulierungsrechtlichen Rahmens sowie einen klaren rechtlichen und regulatorischen Rahmen für den Einsatz der angestrebten Ermittlungswerkzeuge; (ii) neue, weitgehend automatisierbare forensische Methoden zur Analyse von Zahlungsströmen, die Ledger-übergreifende DeFi-Dienste verwenden; (iii) die Integration und systematische Validierung dieser Methoden in Open-Source Forensik-Werkzeuge (z. B. GraphSense); sowie (iv) neue Schulungsinhalte zum Thema Decentralized Finance, die während der Projektlaufzeit in Form zweier Trainings vermittelt werden und anschließend in die jeweiligen Weiterbildungsprogramme der Bedarfsträger integriert werden.

Der Innovationsgehalt des Projekts liegt im empiriebasierten Ansatz bei der Beantwortung rechtlicher und regulatorischer

Fragestellungen, in der datenbasierten Herangehensweise bei forensischen Untersuchungen komplexer, Ledger-übergreifender DeFi-Finanzkonstrukte, sowie im Aufbau bis dato nicht vorhandener, behördenübergreifender Schulungsinhalte und Weiterbildungsstandards.

Die unmittelbare Zielgruppe des DeFiTrace Projekts sind Expertinnen und Experten in den jeweiligen Fachabteilungen der direkt involvierten Bedarfsträger (BMI, BMF, BMJ) und assoziierten Partner (FMA, OeNB, ZCB). Sie werden vom Wissenszuwachs profitieren und die im Projekt entwickelten Methoden und Werkzeuge nutzen können.

Abstract

Recently, illegal payment flows are increasingly being obscured by Decentralized Finance (DeFi) services. These services represent a new financial paradigm based on crypto assets and offer novel financial services such as lending, investing, or exchanging crypto assets without the involvement of regulated institutions such as crypto exchanges. These include decentralized crypto asset exchanges (DEXs), stablecoins (such as Tether), and non-fungible assets (NFTs). The use of these complex services further complicates the already difficult traceability of payment flows, challenges existing analysis tools, and presents unresolved challenges to authorities.

The aim of the DeFiTrace project is to develop new algorithmic solutions for the automated analysis of illegal payment flows in ledger-crossing DeFi ecosystems. The resulting algorithmic methods and tools should enable a more efficient and effective tracking of incriminated funds through complex, ledger-crossing decentralized financial constructs, as well as support empirical enforcement of regulatory measures. The project is accompanied by addressing legal and regulatory questions in the context of current regulatory developments (MiCA and DAC8) and the establishment of inter-agency training and continuing education standards in the field of crypto assets.

The expected project results include: (i) a systematic analysis of the regulatory framework and a clear legal and regulatory framework for the use of the desired investigation tools; (ii) new, largely automatable forensic methods for analyzing payment flows using ledger-crossing DeFi services; (iii) the integration and systematic validation of these methods into open-source forensic tools (such as GraphSense); and (iv) new training content on Decentralized Finance, which will be taught in the form of two training courses during the project and subsequently integrated into the respective continuing education programs of the stakeholders.

The innovation of the project lies in the empirical approach to answering legal and regulatory questions, the data-based approach to forensic investigations of complex, ledger-crossing DeFi financial constructs, and the creation of previously non-existent, inter-agency training content and continuing education standards.

The immediate target group of the DeFiTrace project are experts in the respective departments of the directly involved stakeholders (BMI, BMF, BMJ) and associated partners (FMA, OeNB, ZCB). They will benefit from the knowledge gained and can use the methods and tools developed.

Endberichtkurzfassung

Das DeFiTrace-Projekt entwickelte innovative Methoden zur Verfolgung von Finanzkriminalität in dezentralen Finanzsystemen (DeFi). Eine Ausgangsstudie, die als Teil des Projekts erarbeitet wurde, dokumentierte über 1.100

Cybercrime-Fälle mit mehr als 30 Milliarden US-Dollar Schaden zwischen 2017 und 2022.

Das Projekt lieferte drei zentrale Ergebnisse: Erstens wurden rechtliche Rahmenbedingungen für DeFi im Kontext europäischer Regulierungen (MiCA, DAC8, Transfer of Funds Regulation) in enger Zusammenarbeit mit österreichischen Ministerien analysiert. Zweitens entwickelte das Team mehrere innovative technische Lösungen, darunter eine Methode zur Cross-Chain-Analyse, welche über 1,5 Millionen Krypto-Adressen mit Verbindungen zu mehreren Blockchain-Systemen identifizierte. Ein weiteres Ergebnis war die quantitative Analyse der Governance-Struktur von DeFi-Projekten. Die Ergebnisse zeigten, dass in über 20% der Projekte zumindest eine wichtige Entscheidung ausschließlich von zentralen Akteuren getroffen wurde.
Drittens wurden Schulungen für Ermittler durchgeführt und dauerhaft in die Ausbildung der Bundesfinanzakademie integriert. Die Ergebnisse wurden einer breiten Öffentlichkeit in 16 Vorträgen bei Organisationen wie EUROPOL und INTERPOL präsentiert. Über das Projekt wurde in Medien wie ORF Ö1 und dem Kurier berichtet.

Die entwickelten Methoden stehen nachhaltig als Open-Source-Software zur Verfügung und in Zusammenarbeit mit dem Industriepartner Iknaio als prototypische Lösungen. Darüber hinaus hat das Projekt innovative neue Ansätze, wie das QuickLock-System, zur automatisierten Auswertung für die Verfolgung verdächtiger Zahlungsströme entwickelt.
Die wissenschaftliche Exzellenz manifestiert sich in sieben internationalen Publikationen, dem Houska-Preis 2024 und der Organisation der AFT'24-Konferenz in Wien.

Projektkoordinator

- Complexity Science Hub Vienna CSH - Verein zur Förderung wissenschaftlicher Forschung im Bereich komplexer Systeme

Projektpartner

- Bundesministerium für Justiz
- Universität Innsbruck
- Iknaio Cryptoasset Analytics GmbH
- Bundesministerium für Inneres
- AIT Austrian Institute of Technology GmbH
- Bundesministerium für Finanzen