Fachhochschule Nordwestschweiz
Hochschule für Technik

Crypto-Frauddetection

Betrug im Cryptospace

Windisch, Januar 2025

Studenten	Florian Baumgartner Aaron Brülisauer Can-Elian Barth
Fachexperte	Adrian Brändli
Modul	GEDP
Studiengang	BSc DS

Fachhochschule Nordwestschweiz, Hochschule für Technik

1 Einleitung

Die rasante Entwicklung von Kryptowährungen und digitalen Vermögenswerten hat nicht nur neue finanzielle Möglichkeiten geschaffen, sondern auch ein Umfeld, in dem Betrug gedeihen kann. Das Verständnis von Betrugsmechanismen im Kryptobereich ist entscheidend, um Investoren zu schützen und die Integrität der Finanzmärkte zu wahren. Im Rahmen der Challenge-X wird dieses Thema untersucht. Anhand von Daten aus sozialen Medien und Kursverläufen von Krypto-Coins soll als Challenge-X ein Warnsystem entwickelt werden, das aufzeigt, wie betrügerisch ein Coin sein könnte.

Um ein solches Warnsystem effektiv zu gestalten, muss Betrug in diesem Kontext zuerst klar definiert werden. Das Verständnis dessen, was Betrug im Kryptobereich bedeutet und ab wann ein Coin als betrügerisch einzustufen ist, bildet die Grundlage. Die Betrachtung konkreter Beispiele ermöglicht es, die angewendeten Strategien der Betrüger zu identifizieren und deren Methoden detailliert zu analysieren.

Die Untersuchung der Gegebenheiten und Eigenschaften der Opfer, die einen Betrug ermöglichen oder erleichtern, spielt ebenfalls eine wesentliche Rolle. Durch die Analyse, welche Gefühle — wie Gier oder die Angst, etwas zu verpassen — ausgenutzt werden und welche Schwächen der Opfer Betrüger anvisieren, lässt sich nachvollziehen, warum bestimmte Personen anfällig für solche Machenschaften sind.

In diesem Essay werden die genannten Fragestellungen anhand einer Literaturrecherche untersucht und die bereitgestellten Quellen analysiert. Dadurch wird ein grundlegendes Verständnis für Betrug im Kryptobereich erarbeitet, das als Grundlage für die Entwicklung des Warnsystems dient.

Inhaltsverzeichnis

Abbildungsverzeichnis

2 Betrug im Allgemeinen

Betrug ist ein strafrechtliches Delikt, das in verschiedenen Bereichen der Gesellschaft vorkommt und erhebliche wirtschaftliche sowie soziale Schäden verursachen kann. Im schweizerischen Recht wird Betrug in Artikel 146 des Strafgesetzbuches (StGB) definiert:

> „Wer in der Absicht, sich oder einen andern unrechtmässig zu bereichern, jemanden durch Vorspiegelung oder Unterdrückung von Tatsachen arglistig irreführt oder ihn in einem Irrtum arglistig bestärkt und so den Irrenden zu einem Verhalten bestimmt, wodurch dieser sich selbst oder einen andern am Vermögen schädigt, wird mit Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe bestraft."
>
> (Schweizerisches Strafgesetzbuch, 2024)

Nach der gesetzlichen Definition in Artikel 146 des Schweizerischen Strafgesetzbuches (StGB) setzt Betrug mehrere zentrale Elemente voraus. Erstens die arglistige Irreführung, die in einer bewussten Täuschung durch falsche Angaben oder das Verschweigen wesentlicher Tatsachen besteht. Zweitens die Bereicherungsabsicht, bei der der Täter die Absicht hat, sich selbst oder einem Dritten einen unrechtmässigen Vermögensvorteil zu verschaffen. Drittens den Vermögensschaden, der eintritt, wenn das Opfer oder ein Dritter aufgrund der Täuschung einen finanziellen Nachteil erleidet.

3 Was ist Betrug im Kryptobereich bzw. wann ist ein Coin Betrug?

Betrug im Kryptobereich manifestiert sich in vielfältigen Formen, von betrügerischen Initial Coin Offerings (ICOs) bis hin zu sogenannten „Rug Pulls“ bei DeFi-Projekten. Alexander und Cumming (2022) definieren finanziellen Betrug als jede vorsätzliche Handlung, die darauf abzielt, durch Täuschung finanzielle Vorteile zu erlangen. Im Kontext von Kryptowährungen ist der Umstand der Täuschung gegeben, wenn Initiatoren bewusst falsche Informationen verbreiten oder wesentliche Fakten verschweigen, um Investitionen anzuziehen. Dies kann die Übertreibung technologischer Fähigkeiten, das Versprechen unrealistischer Renditen oder das Vortäuschen nicht existierender Partnerschaften umfassen.

Scharfman (2024) betont, dass die spezifischen Eigenschaften des Kryptobereichs — wie Anonymität, Dezentralisierung und fehlende Regulierung — betrügerische Aktivitäten erleichtern. Die technische Komplexität der Blockchain-Technologie und die globale Reichweite von Kryptowährungen erschweren es Investoren, die Glaubwürdigkeit eines Projekts zu beurteilen und rechtliche Massnahmen zu ergreifen. Ein Coin gilt als Betrug, wenn die Herausgeber absichtlich Investoren täuschen, um sich finanziell zu bereichern, ohne die versprochenen Produkte oder Dienstleistungen zu liefern. Typische Indikatoren sind das plötzliche Verschwinden der Entwickler nach der Kapitalbeschaffung oder die Veruntreuung der eingesammelten Mittel für persönliche Zwecke.

4 Beispiele im Crypto-Bereich

Im Kryptowährungssektor haben sich in den letzten Jahren immer wieder Betrugsfälle ereignet, die Fragen zu Sicherheit und Vertrauenswürdigkeit aufwerfen. Diese Ereignisse haben das Vertrauen vieler Investoren beeinträchtigt und zeigen, wie wichtig klare Regeln und Transparenz sind. Im Folgenden werden einige Beispiele betrachtet, um die Definition des Betrugs an praktischen Beispielen zu erläutern.

4.1 FTX und der FTT Token

Die Kryptobörse FTX, einst als eine der führenden Plattformen im Kryptowährungssektor angesehen, geriet im November 2022 in einen Skandal, der die gesamte Branche erschütterte. Im Zentrum des Geschehens stand der hauseigene Token von FTX, der FTT Coin, der eine entscheidende Rolle bei den Ereignissen spielte, die zum Zusammenbruch der Börse führten. FTX wurde 2019 von Sam Bankman-Fried und Gary Wang gegründet und etablierte sich schnell durch innovative Handelsprodukte und eine benutzerfreundliche Plattform.

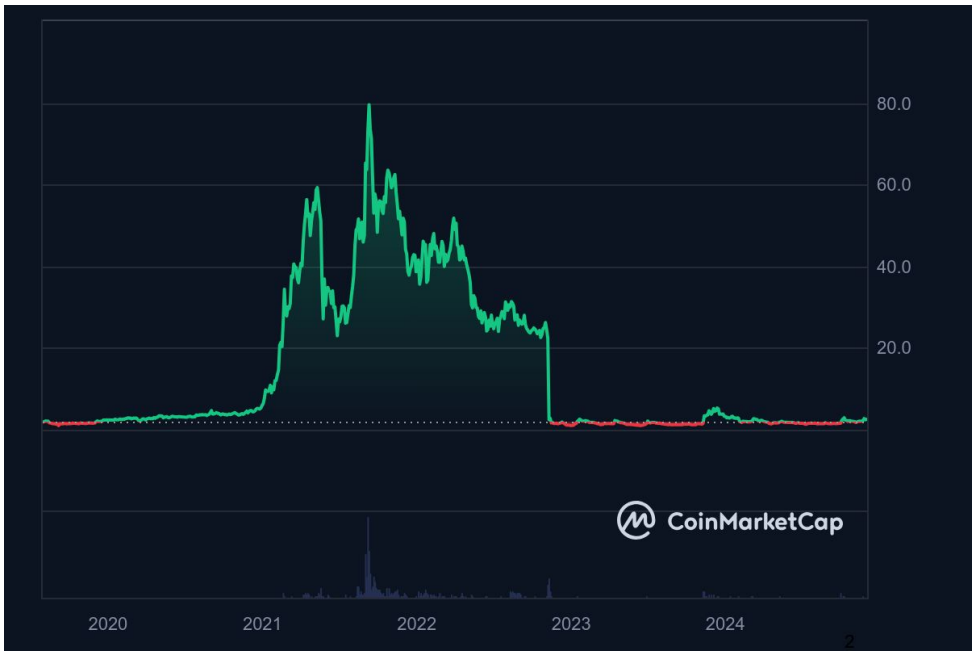

Abbildung 4.1: FTX Token (Coinmarketcap)

Der FTT Coin wurde von der Kryptobörse FTX als hauseigener Token geschaffen und sollte Nutzern verschiedene Vorteile bieten, wie zum Beispiel reduzierte Handelsgebühren. Allerdings gab es Bedenken, dass der Coin genutzt wurde, um den Anschein von Wert und Liquidität zu erzeugen, der in Wirklichkeit nicht wirklich vorhanden war. Ein zentrales Problem war die enge Verflechtung zwischen FTX und dem Handelsunternehmen Alameda Research, das ebenfalls von Sam Bankman-Fried gegründet wurde. Alameda hielt grosse Mengen an FTT Coins und nutzte diese als Sicherheiten für Kredite und Finanzgeschäfte (Allison, 2022). Da der tatsächliche Marktwert des FTT Coins weitgehend von FTX kontrolliert wurde, war es möglich, den Preis künstlich hochzuhalten.

Um dieses System aufrechtzuerhalten, mussten immer mehr Investoren in den FTT Coin investieren. Durch Marketing und Anreize wurden Nutzer ermutigt, den Token zu kaufen, was die Nachfrage erhöhte und den Preis stabil hielt oder steigen liess. Dieses Vorgehen ähnelte einem

Schneeballsystem, bei dem die Gelder neuer Investoren verwendet werden, um die Illusion von Wert und Rendite für bestehende Investoren aufrechtzuerhalten (Locke, 2022).

Durch diese Strukturen und Transaktionen konnte Sam Bankman-Fried & Co persönlich von den Geldern profitieren, die Investoren in den FTT Coin und die Plattform einbrachten, indem diese Gelder in Teilen in hochspekulative Investments und andere in die Taschen der FTX-Gründer flossen (Wile, 2023).

4.2 Safemoon

Eine ganz andere Betrugsstruktur ist im Coin Safemoon zu finden. Safemoon ist eine Kryptowährung, die im März 2021 eingeführt wurde und schnell an Popularität gewann. Sie versprach ihren Investoren hohe Renditen durch ein einzigartiges Tokenomics-Modell, das Halter belohnt und Verkäufer bestraft. Doch trotz des anfänglichen Hypes geriet Safemoon bald in die Kritik und wurde von einigen als potenzieller Betrug oder Ponzi-Schema bezeichnet.

Abbildung 4.2: SafeMoon Kurs (Coinmarketcap)

Im Dezember 2023 meldete SafeMoon Insolvenz an, nachdem leitende Angestellte des Unternehmens wegen Betrugs und Geldwäsche angeklagt worden waren. Laut der US-Börsenaufsichtsbehörde SEC haben die Führungskräfte von SafeMoon über 200 Millionen US-Dollar aus dem Projekt abgezogen und für persönliche Zwecke verwendet, darunter der Kauf von Luxusautos und -immobilien. Die Verantwortlichen versprachen, den Token ßicher zum Mondßu bringen (deshalb auch der Name SafeMoon), lieferten jedoch keine Gewinne. Stattdessen vernichteten sie Millionen an Marktkapitalisierung und nutzten Investorengelder für persönliche Zwecke (U.S. Securities and Exchange Commission, 2023).

Das Tokenomics-Modell wurde entwickelt, um langfristiges Halten der Token zu belohnen und kurzfristigen Verkauf zu entmutigen. Dieses Ziel erreichte Safemoon durch die Erhebung einer Transaktionsgebühr von 10 % beim Verkauf vom Token. Von dieser Gebühr wurden 5 % automatisch an alle aktuellen Token-Inhaber verteilt. Diese Ausschüttung erfolgte proportional zur Anzahl der gehaltenen Token, was bedeutet, dass Investoren umso mehr Belohnungen erhielten,

je mehr Token sie besassen und je länger sie diese hielten. Die verbleibenden 5 % der Gebühr wurden verwendet, um die Liquidität des Tokens zu erhöhen. Dazu wurden sie in Binance Coin (BNB) umgewandelt und zusammen mit Safemoon-Token zu Liquiditätspools auf dezentralen Börsen wie PancakeSwap hinzugefügt. Durch dieses System wurden Investoren kurzfristig davon abgehalten, zu verkaufen und gleichzeitig dazu ermutigt, neue Investoren in das System zu bringen, um Teile von ihren Transaktionsgebühren als Rendite zu erhalten.

An einem Punkt haben die Führungskräfte ihre Anteile abgestossen sowie Gelder aus den Liquiditätspools gestohlen. Investoren erlitten erhebliche Verluste, da der Wert des SFM-Tokens nach Bekanntwerden der betrügerischen Aktivitäten und der Insolvenz rapide sank (Lindrea, 2023). Viele verloren ihr gesamtes investiertes Kapital.

5 Welche Strategien werden angewendet?

Betrüger im Bereich der Kryptowährungen nutzen eine Vielzahl von Strategien, um Investoren zu täuschen und finanzielle Gewinne zu erzielen. Eine gängige Methode ist das sogenannte Pump-and-Dump-Schema, bei dem der Preis eines Coins künstlich in die Höhe getrieben wird, um Anleger anzulocken. Nachdem der Preis signifikant gestiegen ist, verkaufen die Betrüger ihre Anteile und verlassen den Markt, was zu einem abrupten Preisverfall führt (Gee, 2014).

Fake ICOs und Token Sales wie zum Beispiel OneCoin (WirtschaftsWoche, 2023) werden als Mittel eingesetzt, um Gelder von Investoren zu sammeln. Betrügerische Projekte inszenieren hierbei vorgespielte Finanzierungsrunden, ohne die Absicht, ein tatsächliches Produkt zu entwickeln oder den Investoren einen Mehrwert zu bieten (Padgett, 2014).

Eine weitere verbreitete Strategie ist der Rug Pull, insbesondere im Kontext dezentraler Finanzprojekte (DeFi). Hierbei erstellen Betrüger ein scheinbar legitimes Projekt oder einen Token und sammeln Investitionen von Anlegern. Sobald genügend Kapital angezogen wurde, entziehen sie dem Projekt abrupt die Liquidität, indem sie alle Mittel aus den Liquiditätspools abheben. Dies führt zu einem drastischen Wertverlust des Tokens, und die Investoren bleiben mit wertlosen Vermögenswerten zurück (Scharfman, 2024). Die Anonymität der Entwickler und das Fehlen von Regulierungen im DeFi-Bereich begünstigen diese Art von Betrug. Bekannte „Rug Pull“-Beispiele waren Squid Game und Thodex (CoinGecko, 2023).

Zusätzlich sind Phishing und Social Engineering häufig angewandte Vorgehen. Durch gezielte Manipulation und Täuschung werden Investoren dazu gebracht, ihre Zugangsdaten oder privaten Schlüssel preiszugeben. Dies ermöglicht den Betrügern den unautorisierten Zugriff auf die digitalen Vermögenswerte der Opfer (Dove, 2020).

Die immer wichtiger werdende Rolle von künstlicher Intelligenz bei der Verbreitung von Desinformationen wird durch Hutchens (2023) diskutiert. Sie betonen, dass fortschrittliche Technologien Betrügern neue Werkzeuge an die Hand geben, um Investoren zu täuschen und ihre betrügerischen Aktivitäten effektiver zu gestalten.

6 Welche Gegebenheiten und Eigenschaften der Opfer ermöglichen/-vereinfachen einen Betrug?

Die dezentrale Natur von Kryptowährungen und das Fehlen globaler Regulierungsstandards schaffen ein ideales Umfeld für Betrug, wie Wells (2018) hervorhebt. Ohne einheitliche gesetzliche Rahmenbedingungen können Betrüger grenzüberschreitend agieren und rechtliche Grauzonen ausnutzen. Beispielsweise ermöglicht das Fehlen von "Know Your Customer"(KYC)-Verfahren auf einigen Krypto-Börsen Kriminellen, anonym zu bleiben und illegale Aktivitäten zu verschleiern. Diese mangelnde Regulierung verhindert, dass die üblichen Kontrollen und Aufsichtsmechanismen greifen, die in traditionellen Finanzsystemen etabliert sind.

Darüber hinaus führen psychologische Faktoren wie Gier und das Phänomen des "Fear of Missing Out"(FOMO) dazu, dass Investoren vorschnelle Entscheidungen treffen (Dove, 2020). Die Aussicht auf schnelle Gewinne verleitet viele Anleger dazu, in Initial Coin Offerings (ICOs) oder neue Token zu investieren, ohne die zugrunde liegenden Projekte ausreichend zu prüfen. Betrüger nutzen diese Emotionen aus, indem sie unrealistische Renditen versprechen oder künstliche Knappheit erzeugen, um Druck auf potenzielle Investoren auszuüben. Diese emotional getriebenen Handlungen beeinträchtigen das Urteilsvermögen und erhöhen die Anfälligkeit für betrügerische Aktivitäten.

Ein weiterer kritischer Aspekt ist die technische Komplexität von Kryptowährungen. Viele Investoren verstehen die technischen Details nicht vollständig, was es Betrügern erleichtert, komplexe Schemata zu verschleiern und Investoren zu täuschen (Bartneck et al., 2021). So können etwa Ponzi-Systeme oder

Pump and Dump-Strategien hinter komplexem Jargon und technischen Begriffen verborgen werden. Dieses Wissensdefizit erschwert es Anlegern, fundierte Entscheidungen zu treffen und potenzielle Risiken richtig einzuschätzen. In diesem Kontext unterstreichen Ayres und Klass (2008), wie unaufrichtige Versprechungen und die Manipulation von Erwartungen zentrale Elemente von Betrug sind.

Die Kombination aus fehlender Regulierung, mangelndem technischem Verständnis und der Ausnutzung menschlicher Eigenschaften wie Gier schafft ein Umfeld, in dem betrügerische Aktivitäten im Zusammenhang mit Kryptowährungen florieren können.

7 Schlussfolgerung

Betrug im Kryptobereich ist ein komplexes Phänomen, das durch eine Kombination aus technischen, psychologischen und regulatorischen Faktoren begünstigt wird. Ein umfassendes Verständnis der angewandten Strategien und ausgenutzten Schwachstellen ist unerlässlich, um effektive Gegenmassnahmen zu entwickeln und das Vertrauen in Kryptowährungen als Finanzinstrumente zu stärken.

Im Kontext der Challenge-X wird Betrug spezifisch als das vorsätzliche Täuschen von Investoren durch die Initiatoren eines Coins definiert, mit dem Ziel, sich unrechtmässig zu bereichern. Dies umfasst Handlungen wie das Verbreiten falscher oder irreführender Informationen, das Verschweigen wesentlicher Fakten, unrealistische Renditeversprechen sowie das plötzliche Entziehen von Liquidität (Rug Pull).

Ein Coin gilt in diesem Kontext als betrügerisch, wenn solche Praktiken angewendet werden.

Dieses Verständnis wird genutzt, um mithilfe von Beiträgen aus sozialen Netzwerken und den Kursverläufen von Kryptowährungen Indikatoren für potenziellen Betrug zu identifizieren. Durch die Analyse von Mustern in sozialen Medien – etwa ungewöhnlich positive oder negative Kommentare, wiederholt auftretende Schlüsselwörter oder plötzliche Hypes – sollen Auffälligkeiten erkannt und bewertet werden.

Quellenverzeichnis

Alexander, C., & Cumming, D. (2022, Dezember). *Corruption and Fraud in Financial Markets: Malpractice, Misconduct and Manipulation* [Google-Books-ID: QTSiEAAAQBAJ]. John Wiley & Sons.

Allison, I. (2022, November). *Divisions in Sam Bankman-Fried's crypto empire blur on his trading titan Alameda's balance sheet* [Accessed: 2022-11-02]. https://www.coindesk.com/business/2022/11/02/divisions-in-sam-bankman-frieds-crypto-empire-blur-on-his-trading-titan-alamedas-balance-sheet/

Ayres, I., & Klass, G. (2008, Oktober). *Insincere Promises: The Law of Misrepresented Intent*. Yale University Press.

Bartneck, C., Lütge, C., Wagner, A., & Welsh, S. (2021). *An Introduction to Ethics in Robotics and AI*. Springer International Publishing. https://doi.org/10.1007/978-3-030-51110-4

CoinGecko. (2023). *Rug Pull Explanation on CoinGecko* [Accessed: 2023-11-29]. https://www.coingecko.com/learn/rug-pull

Dove, M. (2020, Dezember). *The Psychology of Fraud, Persuasion and Scam Techniques: Understanding What Makes Us Vulnerable* [Google-Books-ID: 7KoLEAAAQBAJ]. Routledge.

Gee, S. (2014, Dezember). *Fraud and Fraud Detection, + Website: A Data Analytics Approach* [Google-Books-ID: iHETBwAAQBAJ]. John Wiley & Sons.

Hutchens, J. (2023, November). *The Language of Deception: Weaponizing Next Generation AI*. John Wiley & Sons.

Lindrea, B. (2023, Dezember). *Krypto-Betrugsprojekt SafeMoon meldet Insolvenz an, SFM-Kurs bricht schlagartig ein* [Accessed: 2023-12-15]. https://de.cointelegraph.com/news/safemoon-bankruptcy-sfm-token-falls-31-percent-fraud-sec

Locke, T. (2022, November). *How FTX's own token FTT was the final nail in its coffin* [Accessed: 2022-11-18]. https://fortune.com/crypto/2022/11/18/how-ftx-own-token-ftt-was-the-final-nail-in-its-coffin/

Padgett, S. (2014, Dezember). *Profiling The Fraudster: Removing the Mask to Prevent and Detect Fraud* [Google-Books-ID: _xruBQAAQBAJ]. John Wiley & Sons.

Scharfman, J. (2024). *The Cryptocurrency and Digital Asset Fraud Casebook, Volume II: DeFi, NFTs, DAOs, Meme Coins, and Other Digital Asset Hacks*. Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-60836-0

Schweizerisches Strafgesetzbuch. (2024). Art. 146: Betrug [Stand am 1. Januar 2024]. Verfügbar 29. November 2024 unter https://www.admin.ch/opc/de/classified-compilation/19370083/index.html#a146

U.S. Securities and Exchange Commission. (2023, November). *SEC Charges Crypto Company SafeMoon and its Executive Team for Fraud and Unregistered Offering of Crypto Securities* [Press release, accessed: 2023-11-01]. https://www.sec.gov/newsroom/press-releases/2023-229

Wells, J. T. (2018, Juni). *International Fraud Handbook* [Google-Books-ID: nI9aDwAAQBAJ]. John Wiley & Sons.

Wile, R. (2023, November). *Sam Bankman-Fried convicted of fraud, theft in FTX cryptocurrency exchange collapse* [Accessed: 2023-11-02]. https://www.nbcnews.com/business/business-news/sam-bankman-fried-verdict-ftx-trial-rcna123158

WirtschaftsWoche. (2023, Dezember). *Kryptobetrug OneCoin: Prozess um vermeintlichen „Bitcoin-Killer" endet mit harten Haftstrafen* [Accessed: 2023-12-01]. https://www.wiwo.de/finanzen/geldanlage/kryptobetrug-onecoin-prozess-um-vermeintlichen-bitcoin-killer-endet-mit-harten-haftstrafen/29589026.html