

CRYPTOFRAUD: HOW TO NOT GET SCAMMED

1 EINLEITUNG

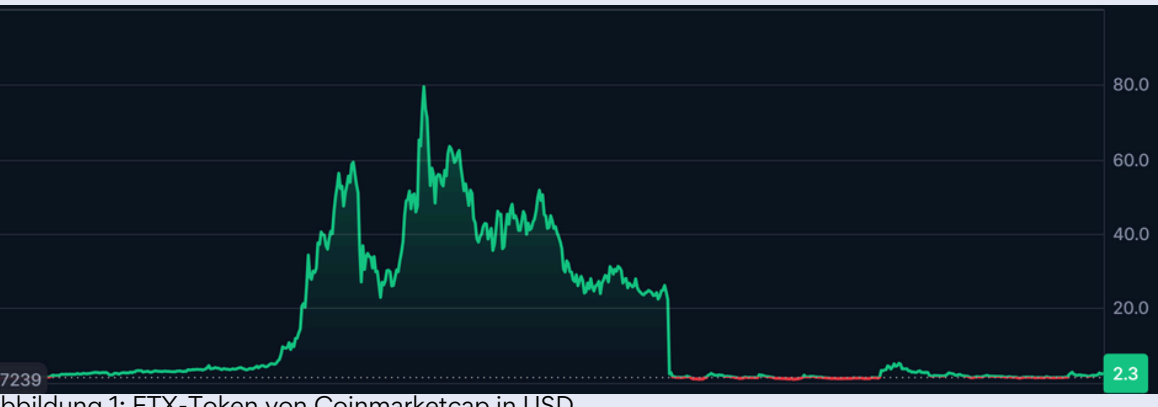
Kryptowährungen haben die Finanzwelt revolutioniert und bieten dezentrale und innovative Alternativen zu traditionellen Systemen. Doch das schnelle Wachstum hat auch eine Vielzahl an Betrugsmaschinen hervorgebracht, die von mangelnder Regulierung und fehlendem Wissen der Öffentlichkeit profitieren. Dieses Poster beleuchtet die häufigsten Arten von Kryptobetrug, ihre Mechanismen und gibt praktische Hinweise, wie man sich davor schützen kann. Ziel ist es, Menschen zu befähigen, die Risiken der Krypto-Welt zu erkennen und sicherer damit umzugehen.

2 FRAGESTELLUNG & RELEVANZ

Wie können Betrugsmaschinen und Betrugscoins im Bereich Kryptowährungen erkannt und vermieden werden? Die Relevanz dieser Fragestellung ergibt sich aus der zunehmenden Verbreitung von Kryptowährungen und der Vielzahl an Betrugsfällen, die Investoren weltweit Milliarden gekostet haben. Das Verständnis typischer Betrugsmechanismen ist entscheidend, um finanzielle Verluste von vielen Investoren zu minimieren. Vor allem kleinere private Investoren, welche neu im Kryptosektor unterwegs sind und vielleicht auch noch sehr emotional auf News, Preisbewegungen sowie andere Meinungen zu Coins reagieren, sind sehr anfällig auf Kryptoscams und können noch deutlich besser von Totalverlusten geschützt werden.

3 ANALYSE

FTX-TOKEN

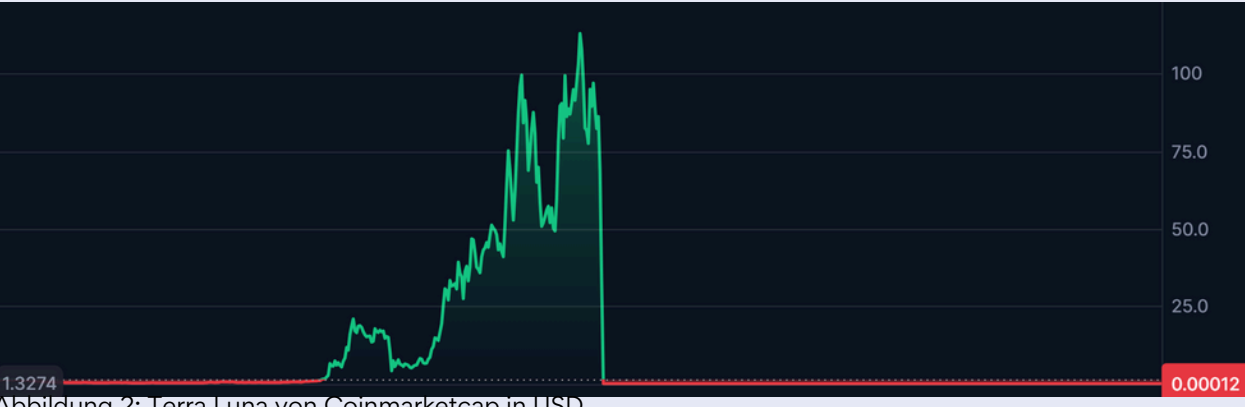


BEER COIN



Abbildung 3: Beer Coin von Coinmarketcap in USD

TERRA LUNA



TEDDY DOGE

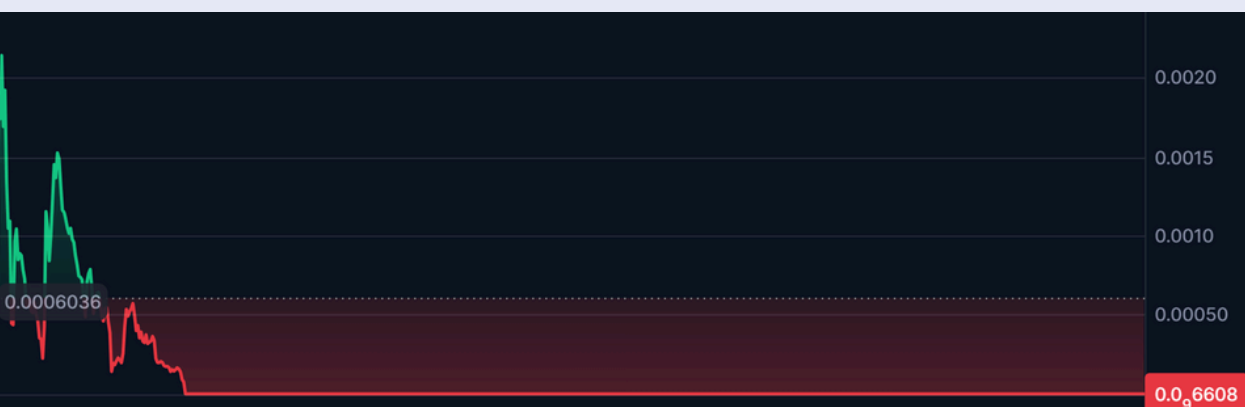


Abbildung 4: Teddy Doge von Coinmarketcap in USD

Investitionen in Scamcoins führen oft zu Totalverlusten, da diese Projekte keine echte Substanz oder langfristige Nutzbarkeit haben. Ihr Wert basiert meist auf künstlichem Hype, der zum Beispiel über Social Media Plattformen wie Twitter oder Reddit verbreitet wird, und Manipulation, anstatt auf tatsächlicher Nachfrage oder innovativer Technologie. Sobald der Betrug aufgedeckt wird oder das Vertrauen der Investoren schwindet, verkaufen viele ihre Anteile in Panik, was den Preis schnell auf oder gegen null drückt (siehe Abbildung 1 - 4). Zudem ziehen die Entwickler häufig die gesamte Liquidität aus dem Projekt ab (sogenannter Rug Pull), wodurch das System komplett kollabiert und der Token wertlos wird. In den beispiel oben sind vier Coins zu sehen, welche nach der Aufdeckung des Scams oder nach dem vollenden des Scams sehr stark eingestürzt sind und sich nicht mehr erholt haben.

RUG PULL / EXITSCAM

- **Liquiditytheft:** Entwickler klauen die Gelder aus Liquiditätspools
- **Wertverlust:** Der Coin wird nach dem Exit wertlos.
- Investoren werden per **Social Media** mit **Bots** gelockt

PONZI SCAMS

- **Täuschung durch Legitimität** (Fake-Zertifikate, Websites etc.)
- **Versprochene hohe Renditen**
- **Kollaps bei Mittelzufluss-stopp**

FAKE-ICO

- **Versprechungen:** Unrealistische Renditen und revolutionäre Projekte.
- **Plötzliches Verschwinden:** Nach dem Einsammeln von Geld.
- **Kein Produkt:** Tokens ohne echte Funktion oder Anwendung.

PUMP AND DUMP

- Gezielte **Kursmanipulation** durch Insiderkäufe und später Verkäufe
- Irreführende Werbung (**FOMO**) für Investoren Anlockung
- Kleinanlegerverluste nach **Dump**

Abbildung 5: Scamstrategien der Betrüger

5 FAZIT

Scam Coins lassen sich oft an der Art und Weise erkennen, wie sie auf Social Media beworben werden. Wenn ein Coin nahezu ausschliesslich in übertrieben positiver Sprache präsentiert wird und viele Accounts mit ähnlichen, botartigen Beiträgen aktiv sind, ist Vorsicht geboten. Solche Marketingmethoden zielen darauf ab, künstlichen Hype zu erzeugen und Vertrauen zu manipulieren. Kritisches Hinterfragen und sorgfältige Analyse der Social-Media-Präsenz eines Projekts können dabei helfen, dubiose Coins frühzeitig zu entlarven und Totalverluste zu vermeiden. In unserer Challenge X gehen wir vor allem den Social Media Beiträgen zu Scam Coins auf den Grund und versuchen mit Deep Learning Modellen vorherzusagen anhand der Posts vorherzusagen ob Coins Scam sind oder eher nicht.

4 STRATEGIE & SCHUTZMASSNAHMEN



Do your own research



Don't get manipulated by opinions of others



Only make rational investment decisions



Check who is behind Accounts or Coins

Scamcoins nutzen menschliche Schwächen wie Unwissenheit, Manipulation der Meinung und emotionale Entscheidungen. Wie kann ich mich richtig schützen?

• Wurde eigene gründliche Reasearch über den Coin gemacht?

- Viele verlassen sich auf **Hype** statt **Fakten**. Ohne tiefere Analyse bleiben Betrügereien unerkant.
- Lösung: **Do your Own Research**. Prüfen Sie Whitepaper, Team und Technologie, bevor Sie investieren.

• Wurde meine Meinung durch fremden Einfluss gesteuert?

- **Herdentrieb, Bots** und **Influencer-Marketing** verleiten Investoren zu unüberlegten Entscheidungen und locken sie in Scamcoins
- Lösung: **Don't Get Manipulated by Opinions**. Vertrauen Sie auf **eigene Recherchen** statt auf fremde Meinungen. Lassen Sie sich auch nicht durch extrem übertriebene Wortwahl, wie "This Coin will go to the Moon", beeinflussen. Fremde Meinungen sind dann von Vorteil, wenn es sich um ausgewiesene Experten handelt (Bankberater, etc.), die keine finanziellen Vorteile aus ihren Handlungsentscheidungen ziehen.

• Ist das geplante Investment Emotional bedingt?

- **FOMO** und **Gewinnversprechen** führen oft zu **impulsiven Handlungen**.
- Lösung: **Only Make Rational Investment Decisions**. Investieren Sie überlegt und setzen Sie **klare finanzielle Limits**. Wenn Sie starke **Emotionen** spüren, sollten sie das Investment zuerst einmal **stoppen** und sich nochmal **rational Gedanken** darüber machen. Auch hier bauen Bots oft mit bestimmter Wortwahl auf FOMO auf.

• Habe ich verifizierte Info's der Founder Identitäten?

- Viele Scam-Projekte verstecken sich hinter anonymen oder **gefälschten Identitäten**. Betrüger nutzen erfundene Teammitglieder, **gefälschte Profile** oder verschleiern ihre Herkunft, um Vertrauen zu gewinnen. Auch Accounts auf Social Media welche einen Coin pushen können **Bots** sein.
- Lösung: **Check Who Is Behind Accounts or Coins**. Überprüfen Sie, wer hinter einem Projekt steht. Verlangen Sie Transparenz beim Team, und achten Sie auf **verifizierte Informationen** wie berufliche Hintergründe oder öffentliche Auftritte der Verantwortlichen. **Misstrauen** Sie anonymen oder **schwer nachvollziehbaren Projekten**.

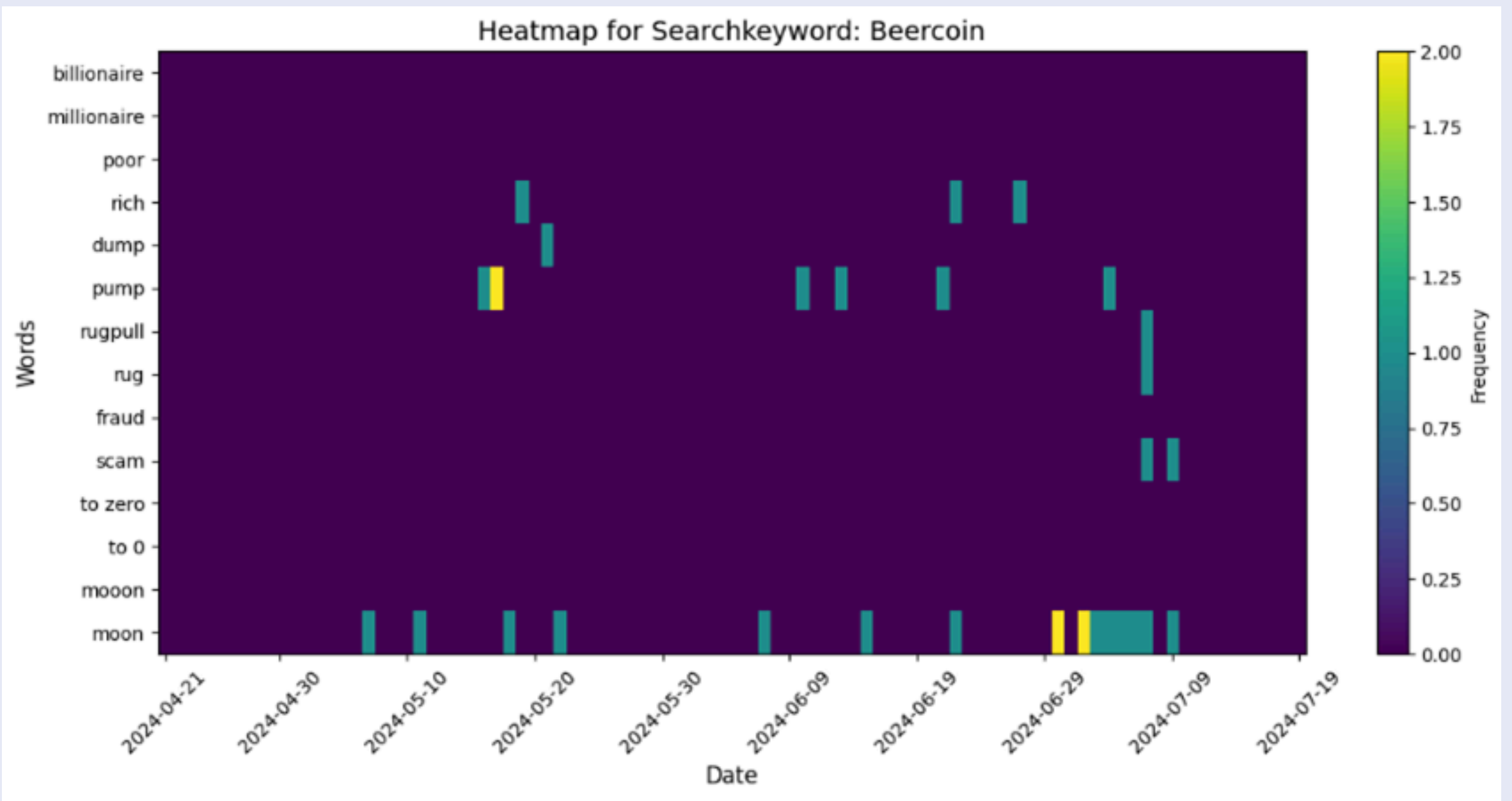


Abbildung 6: Wortanalyse auf Tweets zu Beercoin

Auf diesem Plot ist eine einfache Wort Analyse von Tweets zu einem Scamcoin (Beercoin) über die Zeit zu sehen. Es ist klar zu sehen wie sehr häufig Wörter wie "Pump" oder "Moon" genutzt werden. Diese könnten von Bots genutzt worden sein, welche damit versucht haben andere Investoren in den Coin zu locken.

Quellen:

<https://coinmarketcap.com/currencies/ftx-token/>
<https://coinmarketcap.com/currencies/terra-luna-v2/>
<https://coinmarketcap.com/currencies/beercoin/>
<https://coinmarketcap.com/currencies/teddydoge/>
<https://www.coingecko.com/learn/rug-pull>