KPC Verband
Krypto Protectas Capitalis

www.kpc-verband.org


# Krypto-Scams entschlüsselt:

## Ihre Strategie gegen Betrug

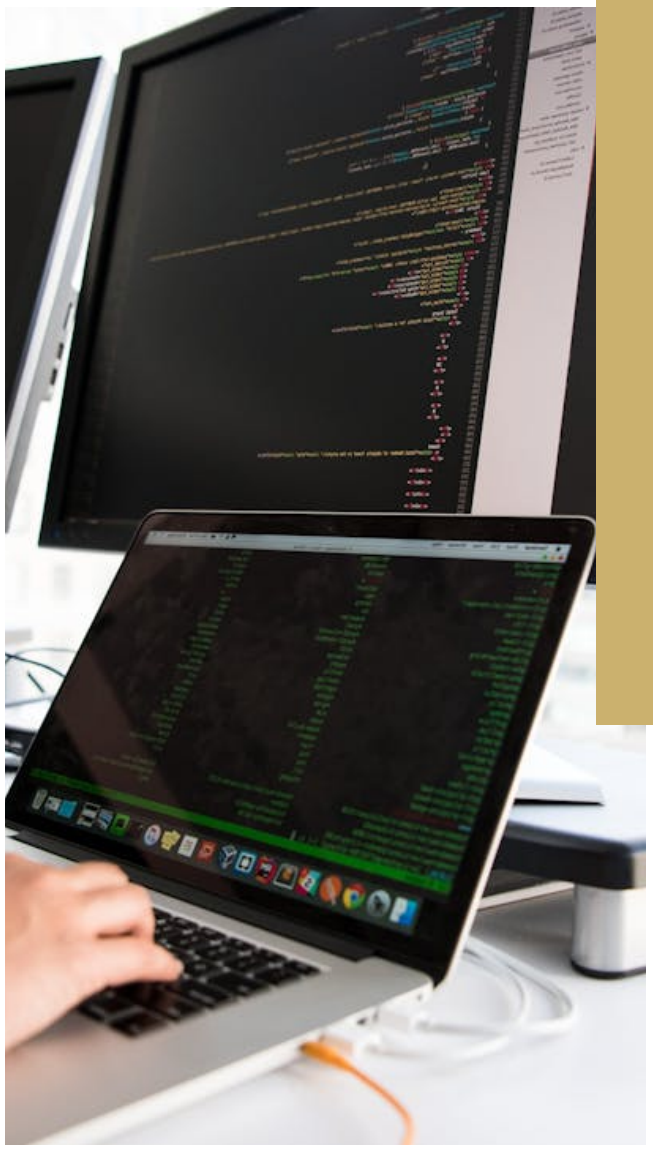
# Inhaltsverzeichnis



**Bitte beachten Sie,
dass ich Sie niemals bitten werde,
Geld irgendwohin zu senden,
aus welchem Grund auch immer.**

**Elon Musk**
CEO von Tesla und SpaceX

# Einleitung



> **Betrug blüht in der Anonymität, aber Transparenz und Wissen können Ihnen helfen, sicher zu navigieren.**
>
> **Jens Heidemann**
> Präsident, KPC Verband

Kryptowährungen haben in den letzten Jahren eine wahre Revolution in der Finanzwelt ausgelöst. Sie bieten nicht nur neue Möglichkeiten für Investitionen und wirtschaftliche Freiheit, sondern stellen auch eine faszinierende technologische Entwicklung dar, die die traditionellen Finanzsysteme herausfordert. Von Bitcoin über Ethereum bis hin zu unzähligen Altcoins – diese digitalen Währungen ziehen immer mehr Menschen in ihren Bann und eröffnen zahlreiche Chancen, doch sie bringen auch Risiken mit sich.
Doch wie in jeder aufregenden Geschichte gibt es auch hier dunkle Seiten:

Krypto-Betrügereien. Diese Betrügereien können Ihr hart erarbeitetes Vermögen und Ihr Vertrauen schnell zunichtemachen – oft ohne dass Sie es im ersten Moment bemerken. Lassen Sie uns einen Blick auf die erschreckenden Dimensionen von Krypto-Betrug werfen, indem wir einen realen Fall untersuchen, der weltweit Schlagzeilen machte

**Der Fall PlusToken: Ein milliardenschwerer Betrug**

Ein eindrucksvolles Beispiel für die Gefahren von Krypto-Betrug ist der Fall von PlusToken, einer der größten Krypto-Betrügereien der letzten Jahre. PlusToken war eine digitale Geldbörse, die 2018 in China gegründet wurde und versprochen hatte, Anlegern hohe Renditen durch eine Kombination von Krypto-Handel und Investmentstrategien zu bieten. Über ein Netzwerk von Promotern und durch aggressives Marketing zog PlusToken Millionen von Investoren an, die in der Hoffnung auf schnelle Gewinne ihre Ersparnisse investierten.

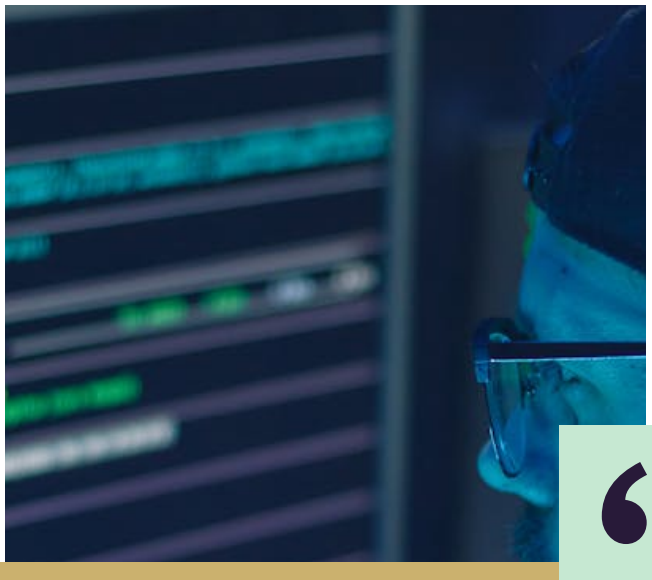
Die Versprechen waren verlockend: PlusToken warb mit Renditen von bis zu 300 % innerhalb kürzester Zeit. Die Plattform präsentierte sich als legitimes Krypto-Investment und sorgte dafür, dass viele Menschen, insbesondere in Asien, ihr Vertrauen in das Unternehmen setzten. Es gab zahlreiche Testimonials von angeblich erfolgreichen Investoren, die ihre Gewinne teilten und so das Vertrauen in die Plattform weiter steigerten.

Im Jahr 2019, nachdem PlusToken über 3 Milliarden Dollar von mehr als 2 Millionen Nutzern eingesammelt hatte, begann das Imperium zu bröckeln. Die Gründer des Projekts zogen sich plötzlich zurück und entzogen den Nutzern den Zugang zu ihren Geldern. Die Plattform wurde heruntergefahren, und viele Investoren standen vor dem Nichts. Die gesamte Angelegenheit entpuppte sich als ein gut durchdachtes Ponzi-Schema, bei dem die frühen Investoren mit den Geldern der neuen Anleger bezahlt wurden.

Nach dem Zusammenbruch von PlusToken wurden mehrere Personen festgenommen, und die chinesischen Behörden begannen mit internationalen Ermittlungen. Die Ermittler entdeckten, dass die Betrüger ein Netzwerk von Geldwäschern und -händlern aufgebaut hatten, um die Gelder ins Ausland zu transferieren. Berichten zufolge könnte der Schaden für die Anleger in die Milliarden gehen.
Dieser Fall zeigt eindrücklich, wie leichtfertig das Vertrauen in solche Plattformen geschenkt werden kann und wie schnell das eigene Vermögen in Gefahr ist. PlusToken ist nicht nur ein Beispiel für einen Betrug; es ist ein Warnsignal für jeden, der in die Welt der Kryptowährungen einsteigen möchte. Es ist entscheidend, die Mechanismen solcher Betrügereien zu verstehen und sich der Risiken bewusst zu sein.

**Fazit**

Die Krypto-Welt ist voller Chancen, aber auch von vielen Gefahren durch Betrügereien, die nur darauf warten, ahnungslose Anleger zu täuschen. Der Fall von PlusToken erinnert uns daran, dass es entscheidend ist, skeptisch zu bleiben und die Angebote, die zu gut erscheinen, um wahr zu sein, sorgfältig zu prüfen. In einer Welt, in der das Vertrauen oft auf dem Spiel steht, ist es wichtig, sich über die Risiken zu informieren und sich nicht von der Hoffnung auf schnellen Reichtum verleiten zu lassen. Indem Sie wachsam bleiben und fundierte Entscheidungen treffen, können Sie Ihre Chancen auf eine sichere und erfolgreiche Investition in die Welt der Kryptowährungen maximieren.



**Crypto ist nicht von Natur aus unsicher, aber es gibt Menschen, die immer nach Wegen suchen, Systeme auszunutzen. Die Lösung liegt in Bildung und Sicherheitsstandards.**

**Changpeng Zhao**
CEO von Binance

**Kryptowährungen verstehen**
Kryptowährungen wie Bitcoin und Ethereum haben in den letzten Jahren die Finanzlandschaft revolutioniert. Diese digitalen Währungen basieren auf komplexen mathematischen Verfahren, die als Kryptografie bekannt sind. Diese Verfahren gewährleisten, dass Transaktionen sicher, transparent und nahezu unmöglich zu manipulieren sind. Doch was genau macht Kryptowährungen so besonders? Der Schlüssel liegt in der revolutionären Technologie, die sie antreibt: der Blockchain.

**Was ist eine Blockchain?**
Stellen Sie sich eine Blockchain als ein riesiges, öffentliches Kassenbuch vor, das über tausende Computer auf der ganzen Welt verteilt ist. Jede Transaktion, die jemals in einem bestimmten Kryptowährungsnetzwerk getätigt wurde, wird in diesem digitalen Kassenbuch aufgezeichnet. Diese Aufzeichnungen sind transparent, sicher und für jeden nachvollziehbar. Anders als bei einem traditionellen Bankkonto benötigt die Blockchain keine zentrale Autorität wie eine Bank, um Transaktionen zu verifizieren.

**Beispiel:** Bei Bitcoin können zwei Personen, die sich in verschiedenen Teilen der Welt befinden, Geld direkt aneinander senden, ohne einen Vermittler wie eine Bank einbeziehen zu müssen. Dies reduziert nicht nur die Transaktionskosten, sondern beschleunigt auch den Prozess. Die Transaktion wird innerhalb von Minuten oder sogar Sekunden in der Blockchain festgehalten.

**Die verschiedenen Gruppen von Krypto-währungen**
Kryptowährungen lassen sich in verschiedene Gruppen unterteilen, die jeweils spezifische Funktionen und Anwendungsbereiche haben:

01

### Utility Tokens
Diese Tokens dienen einem bestimmten Zweck innerhalb eines Ökosystems. Ein Beispiel ist **Ethereum (ETH)**, das für Transaktionen innerhalb der Ethereum-Plattform verwendet wird. Utility Tokens ermöglichen den Zugang zu bestimmten Funktionen oder Dienstleistungen innerhalb einer Blockchain-Plattform.

02

### Security Tokens
Diese Tokens repräsentieren Anteile an einem Vermögenswert, wie z.B. Aktien oder Immobilien. Ein Beispiel hierfür ist der **tZERO Token**, der als Sicherheitsinstrument fungiert und Anlegern eine Beteiligung an den Gewinnen eines Unternehmens bietet.

03

### Stable Coins
Stablecoins sind Kryptowährungen, die an eine stabile Währung wie den US-Dollar oder Gold gekoppelt sind, um Preisschwankungen zu minimieren. **USD Coin (USDC)**, ist ein Token der sich für Handelszwecke und als Wertaufbewahrung eignet.

04

### Meme Coins

Diese Kryptowährungen sind oft humorvoll und werden in der Regel durch soziale Medien populär gemacht. Ein bekanntes Beispiel ist **Dogecoin (DOGE)**, das ursprünglich als Scherz begann, aber eine massive Anhängerschaft gewann und sogar von Prominenten wie Elon Musk unterstützt wird.

05

### Governance Tokens

Diese Tokens geben den Inhabern Stimmrechte innerhalb eines dezentralisierten Netzwerks oder Protokolls. Ein Beispiel ist **Uniswap (UNI)**, wo Token-Inhaber über Vorschläge zur Entwicklung und Verwaltung der Plattform abstimmen können

06

### Kryptowährungen für grenzüberschreitende Zahlungen

Ein herausragendes Beispiel in dieser Kategorie ist **XRP (Ripple)**. XRP wurde entwickelt, um schnelle und kostengünstige grenzüberschreitende Transaktionen zu ermöglichen. Ripple hat Partnerschaften mit vielen Banken und Finanzinstitutionen aufgebaut, um die Effizienz internationaler Zahlungen zu verbessern.

**Zentralbank-Digitalwährungen (CBDCs): Wegbereiter für eine sichere digitale Finanzwelt**

Zentralbank-Digitalwährungen (CBDCs) bieten eine innovative Lösung, um den Zahlungsverkehr effizienter zu gestalten, Kosten zu senken und den Zugang zu Finanzdiensten zu verbessern. Sie bieten dabei eine staatlich kontrollierte, digitale Alternative zu herkömmlichem Bargeld und dezentralen Kryptowährungen. Ein zentraler Vorteil liegt in der erhöhten Sicherheit, da CBDCs durch Regulierungen und technische Maßnahmen gut gegen Cyberkriminalität geschützt werden können.
In diesem Umfeld wird der **Krypto Protectas Capitalis Verband (KPC)** eine zentrale Rolle einnehmen. Durch seine Zertifizierungen und umfassenden Sicherheitsprüfungen sorgt der KPC Verband dafür, dass Unternehmen und Investoren im Bereich digitaler Vermögenswerte geschützt sind. KPC trägt maßgeblich dazu bei, das Vertrauen in CBDCs zu stärken, indem es Unternehmen dabei unterstützt, hohe Standards im Kampf gegen Krypto-Betrug zu erfüllen.

# Warum Krypto-Betrug so weit verbreitet ist.

### Angst, etwas zu verpassen (FOMO)



Die Geschichten von Menschen, die über Nacht reich geworden sind, motivieren viele, in Kryptowährungen zu investieren. Doch diese Angst, den „nächsten großen Wurf“ zu verpassen, führt oft dazu, dass Investoren unüberlegte Entscheidungen treffen – ein perfektes Einfallstor für Betrüger.

### Anonymität und fehlende Regulierung



Kryptowährungen bieten eine hohe Anonymität und operieren oft außerhalb der traditionellen Regulierung. Das macht es für Betrüger einfacher, sich zu verstecken und unentdeckt zu bleiben. Die Transparenz der Blockchain bedeutet nicht, dass die Identitäten der Nutzer offenliegen, was für Kriminelle ein Vorteil ist.

### Technologische Komplexität



Für viele Menschen ist die Technologie hinter Kryptowährungen schwer verständlich. Diese Komplexität nutzen Betrüger aus, indem sie Investoren mit scheinbar lukrativen, aber letztlich falschen Versprechungen ködern.

### Hohe Volatilität



Die Preise für Kryptowährungen können extrem schwanken. Diese Volatilität weckt die Hoffnung auf schnellen Reichtum, und viele Menschen sind bereit, riskante Investitionen einzugehen, in der Hoffnung, den nächsten großen Gewinn zu erzielen. Das macht sie anfällig für Betrügereien, die diese Hoffnungen ausnutzen.

### Globale Zugänglichkeit



Kryptowährungen kennen keine Landesgrenzen. Das bedeutet, dass Betrüger weltweit operieren und ihre Opfer überall finden können. Diese globale Reichweite macht es schwieriger, Betrüger zu verfolgen und zur Rechenschaft zu ziehen.

# Typische Krypto-Betrügereien – und wie sie funktionieren

01

## Phishing

Phishing ist eine der ältesten und dennoch effektivsten Methoden, um an Ihre persönlichen Daten zu gelangen. Die Betrüger senden Ihnen gefälschte E-Mails, die auf den ersten Blick von einer vertrauenswürdigen Quelle wie einer bekannten Krypto-Börse stammen könnten. Diese E-Mails fordern Sie auf, auf einen Link zu klicken und Ihre Anmeldedaten einzugeben, um ein angebliches Sicherheitsproblem zu beheben. Sobald Sie das tun, haben die Betrüger Zugang zu Ihrem Konto und können Ihre Kryptowährungen stehlen.

**Beispiel:** Sie erhalten eine E-Mail von Ihrer Krypto-Börse, in der behauptet wird, dass es ein Sicherheitsproblem gibt und dass Sie sofort handeln müssen. In der Aufregung klicken Sie auf den Link und geben Ihre Zugangsdaten ein – nur um später festzustellen, dass die E-Mail eine raffinierte Fälschung war. Ihre Kryptowährungen sind verschwunden, und der Schaden ist kaum wieder gutzumachen.

02

## Romance Scams

Bei dieser besonders perfiden Betrugsmasche nutzen Kriminelle emotionale Bindungen aus, um an das Geld ihrer Opfer zu gelangen. Über Dating-Plattformen oder soziale Netzwerke bauen sie Vertrauen auf und beginnen oft eine scheinbar ernsthafte Beziehung. Nach einer Weile erzählen sie eine herzzerreißende Geschichte über finanzielle Not oder eine fantastische Investitionsmöglichkeit und bitten Sie, ihnen mit Kryptowährungen auszuhelfen. Sobald Sie das Geld überwiesen haben, verschwinden sie spurlos.

**Beispiel:** Sie lernen jemanden über eine Dating-App kennen, und es funkt sofort. Die Beziehung entwickelt sich online, Sie sprechen regelmäßig und bauen Vertrauen auf. Irgendwann erwähnt Ihr „Partner“ ein finanzielles Problem oder eine vielversprechende Krypto-Investition und bittet um Ihre Hilfe. Sie überweisen Geld – und danach herrscht Funkstille. Ihr Geld und Ihr „Partner“ sind verschwunden.

“

**Es ist enttäuschend zu sehen, wie viele der Kryptowährungen-Projekte entweder oberflächlich sind, technisch inkompetent oder offen betrügerisch.**

**Naval Ravikant**
Entrepreneur und investor

03

## Schneeball- und Pyramidensysteme

Diese Betrugsmaschen basieren auf dem Prinzip, dass frühe Investoren hohe Renditen erhalten, die jedoch nicht aus realen Gewinnen stammen, sondern aus den Einzahlungen neuer Investoren. Solange immer mehr Menschen investieren, scheint das System zu funktionieren. Doch sobald der Zufluss neuer Gelder stoppt, bricht es zusammen, und die meisten Investoren verlieren ihr Geld.

**Beispiel:** Ein Bekannter spricht Sie auf eine neue Investitionsmöglichkeit an und erzählt, wie Sie durch den Kauf von Anteilen an einem Krypto-Projekt hohe Renditen erzielen können. Er ermutigt Sie, auch Freunde und Familie anzuwerben. Nach einigen Monaten merken Sie jedoch, dass die versprochenen Rückflüsse nicht real sind. Das System bricht zusammen, weil nicht genügend neue Investoren gefunden werden, und viele verlieren ihr Geld.

04

## Pumps and Dumps

Bei einem Pump-and-Dump-Betrug kaufen Betrüger große Mengen einer wenig bekannten Kryptowährung auf und verbreiten dann falsche Informationen, um den Preis in die Höhe zu treiben. Viele Investoren kaufen in der Hoffnung auf schnelle Gewinne. Sobald der Preis steigt, verkaufen die Betrüger ihre Bestände, der Preis fällt dramatisch, und die anderen Investoren bleiben auf ihren Verlusten sitzen.

**Beispiel:** Sie erfahren von einer neuen Kryptowährung, die über Social Media stark beworben wird. Die Betrüger erzeugen Hype, um den Preis in die Höhe zu treiben. Sobald er einen Höhepunkt erreicht, verkaufen sie ihre Bestände und ziehen sich zurück. Der Preis stürzt ab, und viele Investoren verlieren ihr Geld, während die Betrüger mit Gewinn davonkommen.

05

## Malware und Ransomware

Malware ist bösartige Software, die darauf abzielt, Ihre Krypto-Wallets zu hacken und Ihre digitalen Vermögenswerte zu stehlen. Ransomware hingegen verschlüsselt Ihre Dateien oder sogar Ihr gesamtes Computersystem und verlangt ein Lösegeld, meistens in Kryptowährungen, um sie wieder freizugeben.

**Beispiel:** Sie laden eine scheinbar harmlose Software herunter, die in Wirklichkeit Malware enthält. Diese sucht nach Ihren Krypto-Wallets, stiehlt Ihre Zugangsdaten und überweist Ihre Kryptowährungen an die Hacker. Alternativ könnten Sie Opfer von Ransomware werden und den Zugriff auf Ihren Computer verlieren, bis Sie das geforderte Lösegeld zahlen.

06

## Rug Pulls

Ein Rug Pull ist eine Art von Betrug, bei dem Entwickler ein Krypto-Projekt starten, es aggressiv bewerben und Investoren dazu bringen, Geld zu investieren. Sobald genügend Geld eingesammelt ist, ziehen die Entwickler alle Mittel ab und lassen das Projekt zusammenbrechen, was die Investoren mit leeren Händen zurücklässt.

**Beispiel:** Sie investieren in ein vielversprechendes neues DeFi-Projekt, das großartig aussieht und mit verlockenden Renditen wirbt. Nach ein paar Wochen beobachten Sie, wie der Wert Ihrer Investition steigt, und Sie sind begeistert von den möglichen Gewinnen. Doch plötzlich ist die Website des Projekts nicht mehr erreichbar, und alle Informationen über das Team sind verschwunden. Ihre Gelder sind verloren – ein klassischer Rug Pull.

07

## Nachahmung und falsche Give-Aways

Betrüger geben sich oft als bekannte Persönlichkeiten aus und bieten „Giveaways“ an, bei denen Sie eine bestimmte Menge Kryptowährung an eine Adresse senden sollen, um angeblich das Doppelte zurückzubekommen. In Wirklichkeit erhalten Sie aber nichts zurück.

**Beispiel:** Sie sehen auf X (vormals Twitter) einen Beitrag, der von einem berühmten Krypto-Influencer stammt und ankündigt, dass er ein großes Giveaway veranstaltet. Um teilzunehmen, sollen Sie eine bestimmte Menge Kryptowährung an eine angegebene Adresse senden, um im Gegenzug das Doppelte zurückzubekommen. Sie folgen den Anweisungen und senden Ihre Kryptowährung, nur um dann festzustellen, dass das Profil gefälscht war und das Giveaway nie stattgefunden hat. Ihr Geld ist verloren.

08

## Ponzi Schemata

Ein Ponzi-Schema ähnelt einem Schneeballsystem, bei dem frühere Investoren mit dem Geld neuer Investoren bezahlt werden. Doch sobald nicht mehr genügend neue Investoren gefunden werden, bricht das System zusammen, und die meisten verlieren ihr Geld.

**Beispiel:** Sie erfahren von einem Krypto-Investitionsangebot, das hohe Renditen bei minimalem Risiko verspricht. Der Anbieter erklärt, dass Sie durch Investitionen und das Anwerben neuer Teilnehmer monatliche Gewinne erzielen können. Anfangs erhalten Sie tatsächlich Auszahlungen, aber diese stammen nicht aus realen Gewinnen, sondern aus den Einzahlungen neuer Investoren. Das System bricht zusammen, als nicht genug neue Teilnehmer gefunden werden, und die meisten verlieren ihr Geld.

09

## Employment Scams

Bei diesen Betrugsversuchen erhalten Opfer unerbetene Jobangebote, die sie dazu verleiten, für „Schulungen“ oder „Investitionen“ in Kryptowährungen zu zahlen. Oftmals enden diese Angebote mit dem Verlust des investierten Geldes, da die versprochenen Arbeitsmöglichkeiten nicht existieren und die Anbieter der Betrugsmasche verschwinden.

**Beispiel:** Sie erhalten eine E-Mail mit einem verlockenden Jobangebot, das Ihnen die Möglichkeit verspricht, von zu Hause aus zu arbeiten und dabei hohe Gehälter zu verdienen. Der Anbieter erklärt, dass Sie für eine Schulung in Kryptowährungen bezahlen müssen, um mit dem Job zu beginnen. Nachdem Sie die Gebühr bezahlt haben, erhalten Sie jedoch keine weiteren Informationen und der Kontakt bricht ab. Ihr Geld ist verloren, und die vermeintliche Jobgelegenheit war nie real.

10

## Investment Recovery Scams

Diese Betrugsmaschen zielen auf Personen ab, die bereits Opfer eines Krypto-Betrugs geworden sind. Die Betrüger kontaktieren die Opfer und bieten an, deren verlorenes Geld zurückzuholen – oft gegen eine Gebühr. Diese „Rettungsdienste“ sind jedoch in der Regel ebenfalls betrügerisch, und die Opfer verlieren noch mehr Geld.

**Beispiel:**Nach einem finanziellen Verlust durch einen Krypto-Betrug werden Sie von einem vermeintlichen Experten kontaktiert, der Ihnen verspricht, Ihr verlorenes Geld zurückzuholen. Der Anbieter erklärt, dass er über spezielle Methoden verfügt, um die Betrüger zu verfolgen. Um seine „Dienstleistungen“ in Anspruch zu nehmen, müssen Sie eine Gebühr zahlen oder ihm Zugang zu Ihren Kontoinformationen gewähren. Nachdem Sie die Zahlung geleistet haben, hören Sie nie wieder von ihm, und Ihr Geld ist verloren

11

## Gefälschte ICOs (Initial Coin Offerings)

Ein ICO ist eine Methode, wie neue Krypto-Projekte Geld sammeln, indem sie Investoren Tokens im Austausch für ihre Unterstützung anbieten. Betrügerische ICOs locken Investoren mit großen Versprechen über ein revolutionäres neues Produkt oder eine Dienstleistung, die es in Wirklichkeit gar nicht gibt. Sobald genügend Geld eingesammelt wurde, verschwinden die Betrüger – und die Investoren bleiben auf wertlosen Tokens sitzen

**Beispiel:** Sie stoßen auf ein neues Krypto-Projekt, das über Social Media und spezielle Foren aggressive Werbung für seine bevorstehende Initial Coin Offering (ICO) macht. Das Projekt verspricht revolutionäre Technologie und hohe Renditen für Investoren. Begeistert von den Möglichkeiten investieren Sie eine beträchtliche Summe, um Anteile an der neuen Kryptowährung zu erwerben. Nach der ICO stellen Sie jedoch fest, dass die Website des Projekts offline ist und die Entwickler nicht mehr erreichbar sind. Ihre Investition ist verloren, und das Projekt war von Anfang an eine Fälschung.

12

### Gefälschte mobile Apps und Wallets

Gefälschte Apps, die wie legitime Krypto-Wallets aussehen, sind ein weiteres beliebtes Mittel von Betrügern. Diese Apps stehlen Ihre Anmeldeinformationen oder fordern Sie dazu auf, Ihre Private Keys einzugeben – und sobald Sie das tun, sind Ihre Kryptowährungen weg.

**Beispiel:** Sie suchen nach einer Krypto-Wallet-App im App Store und finden eine gut bewertete App, die viele Funktionen verspricht. Nach der Installation geben Sie Ihre Zugangsdaten und private Schlüssel ein, um auf Ihre Kryptowährungen zuzugreifen. Kurz darauf stellen Sie fest, dass Ihr gesamtes Krypto-Vermögen verschwunden ist, da die App gefälscht war und Ihre Informationen an Betrüger weitergeleitet hat.

13

### Sybil Attacke

Bei einer Sybil-Attacke erstellt ein Betrüger viele gefälschte Identitäten in einem dezentralen Netzwerk, um die Kontrolle zu übernehmen oder das Netzwerk zu manipulieren. Dies kann dazu führen, dass ehrliche Teilnehmer das Vertrauen in das Netzwerk verlieren.

**Beispiel:** Sie sind in einem dezentralisierten Netzwerk aktiv, das Abstimmungen über neue Funktionen ermöglicht. Plötzlich bemerken Sie, dass eine große Anzahl von Benutzern für einen Vorschlag abstimmt, der Ihnen fragwürdig erscheint. Nach einer näheren Untersuchung stellen Sie fest, dass viele dieser Konten neu sind und ähnliche Namen und Profile aufweisen. Es wird offensichtlich, dass ein Betrüger mehrere gefälschte Identitäten erstellt hat, um die Abstimmung zu manipulieren und das Ergebnis zu beeinflussen.

“

**„Berühmtheiten, die Krypto-Projekte unterstützen, sind nicht immer ein Warnsignal, aber oft sind sie es. Seien Sie skeptisch.“**

**Mark Cuban**
Entrepreneur und investor

# Krypto-Scams: Gefahren, Tricks und strukturellen Merkmale – und wie sie funktionieren

Die verschiedenen Arten von Krypto-Betrug sind in der Regel so gefährlich, weil sie spezifische psychologische Schwächen ausnutzen und oft sehr überzeugend gestaltet sind. Hier sind einige der Hauptgefahren und die psychologischen Tricks, die von Betrügern verwendet werden:

## Phishing

**Gefährlichkeit:** Diese Angriffe zielen darauf ab, persönliche Informationen zu stehlen, was zu Identitätsdiebstahl und finanziellen Verlusten führen kann.
**Psychologische Tricks:** Betrüger nutzen Dringlichkeit und Angst, um Nutzer dazu zu bringen, schnell zu handeln, ohne die Echtheit der Anfrage zu überprüfen. Sie verwenden oft gefälschte E-Mails, die legitim erscheinen, um Vertrauen zu gewinnen.

- **Aufbau**: Phishing-Angriffe verwenden gefälschte E-Mails oder Webseiten, um Nutzer zur Eingabe ihrer persönlichen Informationen zu verleiten.
- **Struktur**: Oft ähnlich aufgebaut wie legitime Kommunikation von Banken oder Krypto-Börsen, wobei vertraute Logos und Designs verwendet werden.
- **Ziel**: Phishing-Angriffe zielen darauf ab, persönliche Informationen durch gefälschte Kommunikationsmittel zu stehlen. Diese Betrugsform erfordert keine aktive Teilnahme von den Opfern, da sie oft unwissentlich auf Links klicken oder Informationen bereitstellen. Der Fokus liegt auf der Täuschung.

## Romance Scams

**Gefährlichkeit:** Diese Betrugsart kann zu erheblichen finanziellen Verlusten führen, da die Opfer oft emotionale Bindungen aufbauen.
**Psychologische Tricks:** Betrüger verwenden emotionale Manipulation, um Mitgefühl zu erzeugen und Vertrauen aufzubauen. Sie bringen Opfer dazu, sich schuldig zu fühlen, wenn sie nicht helfen.

- **Aufbau**: Betrüger bauen eine Beziehung über soziale Medien oder Dating-Plattformen auf und nutzen emotionale Manipulation.
- **Struktur**: Der Prozess umfasst mehrere Phasen, von der Kontaktaufnahme bis hin zu immer dringlicheren Geldanforderungen.
- **Ziel**: Hier geht es darum, emotionale Bindungen aufzubauen, um Geld zu erlangen. Im Gegensatz zu Phishing erfordert diese Betrugsart eine aktive Interaktion, da die Betrüger persönliche Beziehungen aufbauen. Der Schwerpunkt liegt auf emotionaler Manipulation.

### Schneeball- und Pyramidensysteme

**Gefährlichkeit:** Diese Systeme führen dazu, dass viele neue Teilnehmer Geld verlieren, während die Initiatoren profitieren.
**Psychologische Tricks:** Sie schaffen ein Gefühl der Gemeinschaft und des Zugehörigkeitsgefühls, während sie gleichzeitig den Druck erhöhen, neue Mitglieder zu rekrutieren, um persönliche Gewinne zu erzielen.

- **Aufbau**: Mitglieder müssen neue Teilnehmer anwerben, um eigene Gewinne zu erzielen.
- **Struktur**: Die Struktur ist hierarchisch; frühe Mitglieder werden aus den Einzahlungen neuer Mitglieder bezahlt.
- **Ziel**: Beide Systeme basieren auf der Rekrutierung neuer Mitglieder, um die älteren zu bezahlen. Die Struktur ist hier entscheidend: Während Schneeballsysteme oft informell und weniger strukturiert sind, haben Pyramidensysteme klare Hierarchien. Der Fokus liegt auf der ständigen Anwerbung.

### Pumps and Dumps

**Gefährlichkeit:** Investoren verlieren viel Geld, wenn der Preis einer Kryptowährung nach dem Verkauf der Betrüger fällt.
**Psychologische Tricks:** Betrüger erzeugen Hype und FOMO (Fear of Missing Out), um Menschen dazu zu bringen, impulsiv zu investieren.

- **Aufbau**: Betrüger erzeugen Hype um eine Kryptowährung, oft durch gefälschte Nachrichten oder Social-Media-Posts.
- **Struktur**: Der Preis wird künstlich aufgebläht, gefolgt von einem massiven Verkaufsdruck der Betrüger.
- **Ziel**: Diese Betrugsform spielt auf das Verhalten von Investoren an und erfordert, dass Betrüger Hype um eine Kryptowährung erzeugen, um den Preis zu steigern. Die Teilnahme erfolgt durch spekulative Investitionen. Der Fokus liegt auf der Marktmanipulation.

### Malware und Ransomware

**Gefährlichkeit:** Diese Angriffe können den Zugriff auf Geräte und Daten einschränken, was zu enormen finanziellen Schäden führen kann.
**Psychologische Tricks:** Betrüger verwenden Täuschung, indem sie harmlose Software präsentieren, um Nutzer dazu zu bringen, sie herunterzuladen und damit ihre Sicherheit zu gefährden.

- **Aufbau**: Schadsoftware wird oft als harmlose Software getarnt, die heruntergeladen wird.
- **Struktur**: Nach der Installation sucht die Malware nach Krypto-Wallets oder sperrt den Zugang zu Geräten.

- **Ziel**: Diese Angriffe sind technischer Natur und erfordern, dass Opfer unwissentlich schadhafte Software installieren. Die Teilnahme erfolgt indirekt, da Nutzer oft keine bewusste Entscheidung treffen. Der Fokus liegt auf dem Diebstahl von Informationen oder der Erpressung.

### Rug Pulls

**Gefährlichkeit:** Investoren verlieren ihre Gelder, wenn Betrüger plötzlich verschwinden, nachdem sie das Geld eingesammelt haben.
**Psychologische Tricks:** Sie verwenden übertriebene Marketingstrategien und bauen eine falsche Glaubwürdigkeit auf, um Investoren zu überzeugen, dass das Projekt legitim ist.

- **Aufbau**: Betrüger schaffen ein neues Krypto-Projekt, das durch aggressive Werbung beworben wird.
- **Struktur**: Nachdem Gelder gesammelt wurden, verschwindet das Team schnell.
- **Ziel**: Rug Pulls treten auf, wenn Entwickler Gelder sammeln und das Projekt abrupt einstellen. Die Teilnahme erfolgt durch Investitionen in ein scheinbar legitimes Projekt. Der Fokus liegt auf dem schnellen Abzug von Geldern.

### Nachahmung und falsche Give-Aways

**Gefährlichkeit:** Betrüger geben sich oft als bekannte Persönlichkeiten aus, um Geld von ahnungslosen Investoren zu stehlen.
**Psychologische Tricks:** Diese Betrüger verwenden gefälschte Konten und generieren ein Gefühl der Dringlichkeit, um Menschen dazu zu bringen, schnell zu handeln und Kryptowährung zu senden.

- **Aufbau**: Betrüger geben sich als bekannte Persönlichkeiten aus.
- **Struktur**: Werbung für gefälschte Give-Aways, die meist über soziale Medien verbreitet wird.
- **Ziel**: Betrüger geben sich als bekannte Persönlichkeiten aus, um Gelder von ahnungslosen Nutzern zu stehlen. Diese Betrugsart zielt darauf ab, das Vertrauen der Opfer zu gewinnen, indem sie gefälschte Konten verwenden, die legitime Personen imitieren. Die Teilnahme erfolgt durch das Klicken auf Links oder die Eingabe von Informationen, um an vermeintlichen Give-Aways teilzunehmen. Der Fokus liegt auf dem Diebstahl von Kryptowährungen oder persönlichen Daten.

### Ponzi Schemata

**Gefährlichkeit:** Diese Betrügereien führen zu enormen Verlusten für die meisten Teilnehmer.
**Psychologische Tricks:** Sie nutzen den Wunsch nach schnellen Gewinnen aus und schaffen ein falsches Gefühl der Sicherheit.

- **Aufbau**: Hohe Renditen werden versprochen, die aus den Einzahlungen neuer Mitglieder finanziert werden.
- **Struktur**: Linearer Zahlungsfluss von neuen zu alten Investoren.
- **Ziel**: Ponzi-Schemata sind strukturell ähnlich wie Schneeball-Systeme, verwenden jedoch keine aktive Rekrutierung, sondern versprechen hohe Renditen aus den Einzahlungen neuer Mitglieder. Der Fokus liegt darauf, das Geld neuer Investoren zu nutzen, um ältere Investoren auszuzahlen.

### Employment Scams

**Gefährlichkeit:** Opfer zahlen oft Gebühren für gefälschte Jobangebote.
**Psychologische Tricks:** Betrüger nutzen die Hoffnung der Menschen auf Arbeit aus.

- **Aufbau**: Gefälschte Jobangebote, die Gebühren für Schulungen erfordern.
- **Struktur**: Professionell gestaltete Angebote, die Dringlichkeit erzeugen.
- **Ziel**: Diese Betrüger bieten gefälschte Jobmöglichkeiten an und erfordern oft die Zahlung von Gebühren. Die Teilnahme erfolgt aktiv, da Opfer in der Regel direkt angesprochen werden. Der Fokus liegt auf der Ausnutzung der Hoffnung auf Arbeit.

### Investment Recovery Scams

**Gefährlichkeit:** Diese Betrüger zielen auf Menschen ab, die bereits Verluste erlitten haben.
**Psychologische Tricks:** Sie schaffen falsche Hoffnungen auf Rückerstattung und nutzen die Frustration der Opfer aus.

- **Aufbau**: Kontakt zu Opfern von Betrug mit Versprechen, verlorenes Geld zurückzuholen.
- **Struktur**: Betrüger verlangen Gebühren für vermeintliche Dienstleistungen.
- **Ziel**: Diese Betrüger bieten an, verlorenes Geld zurückzuholen, und zielen auf bereits geschädigte Personen ab. Die Teilnahme erfolgt durch die Zahlung von Gebühren für vermeintliche Dienstleistungen. Der Fokus liegt auf der Ausnutzung der Frustration und Hoffnung der Opfer.

### Gefälschte ICOs (Initial Coin Offerings)

**Gefährlichkeit:** Investoren verlieren ihr Geld, ohne jemals ein echtes Produkt oder eine Dienstleistung zu erhalten.
**Psychologische Tricks:** Betrüger nutzen das Verlangen nach schnellen Gewinnen und den Hype um neue Technologien.

- **Aufbau**: Präsentation eines nicht existierenden Krypto-Projekts mit ansprechendem Whitepaper.
- **Struktur**: Kurze Werbeaktionen, die das Vertrauen der Investoren gewinnen.

- **Ziel**: Diese Betrugsart nutzt das Interesse an neuen Krypto-Projekten aus. Die Teilnahme erfolgt durch Investitionen in Projekte, die in Wirklichkeit nicht existieren. Der Fokus liegt auf der Akquise von Geldern durch falsche Versprechungen.

### Gefälschte mobile Apps und Wallets

**Gefährlichkeit:** Diese Apps stehlen persönliche Daten und Kryptowährungen.
**Psychologische Tricks:** Betrüger nutzen gefälschte Bewertungen und ein professionelles Design, um Vertrauen zu gewinnen.

- **Aufbau**: Apps, die echte Krypto-Wallets imitieren.
- **Struktur**: Nutzer laden die App herunter und geben ihre Daten ein.
- **Ziel**: Hierbei handelt es sich um betrügerische Anwendungen, die oft mit gefälschten Bewertungen und ansprechendem Design erstellt werden. Die Teilnahme erfolgt durch den Download der App. Der Fokus liegt auf dem Diebstahl von Zugangsdaten.

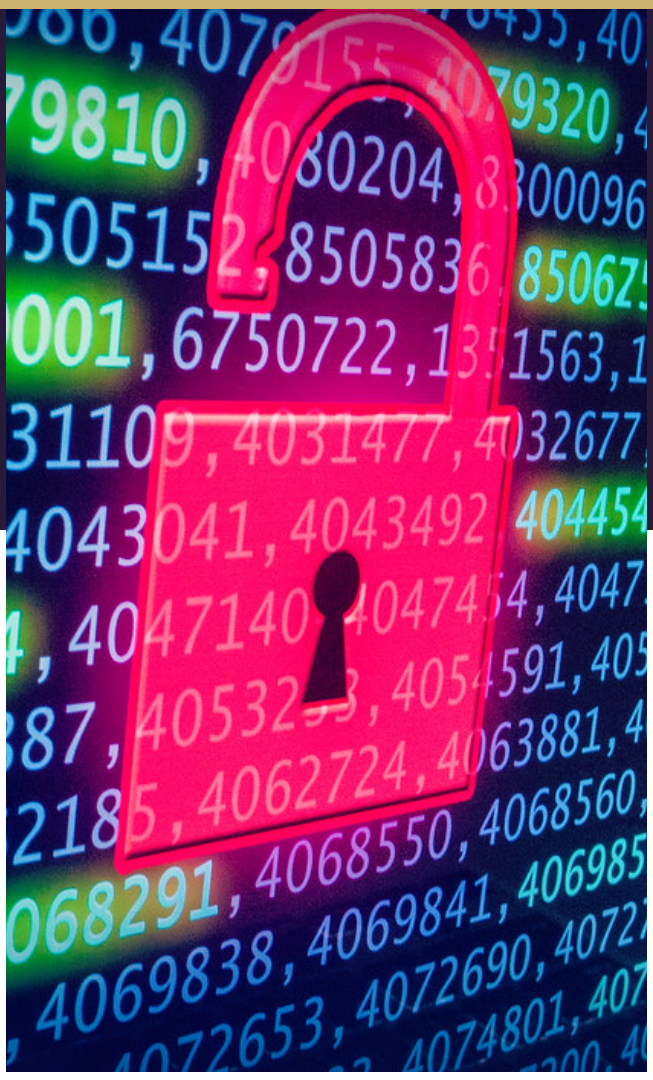
### Sybil Attacke

**Gefährlichkeit:** Diese Angriffe können die Integrität eines Netzwerks untergraben und Vertrauen in Abstimmungen und Entscheidungsprozesse zerstören.
**Psychologische Tricks:** Betrüger nutzen die Anonymität im Internet, um multiple Identitäten zu schaffen und das Gefühl der Normalität zu manipulieren, um ihr Ziel zu erreichen .

- **Aufbau**: Betrüger erstellen zahlreiche gefälschte Identitäten innerhalb eines Netzwerks.
- **Struktur**: Diese Konten werden dann genutzt, um Abstimmungen oder Entscheidungen zu beeinflussen.
- **Ziel**: Diese Angriffe erfordern die Erstellung mehrerer gefälschter Identitäten, um das Vertrauen in ein Netzwerk zu manipulieren. Die Teilnahme erfolgt aktiv durch die Erstellung von Konten. Der Fokus liegt auf der Beeinflussung von Abstimmungen oder Entscheidungsprozessen.

> **Ich möchte klarstellen, dass weder ich noch andere Ripple-Executives jemals verlangen werden, dass Nutzer XRP oder andere Gelder senden, um versprochene Rückflüsse zu erhalten.**
>
> **Brad Garlinghouse**
> CEO von Ripple

# Wie Sie sich vor Krypto-Betrug schützen können



**Kryptowährungen bieten eine hervorragende Möglichkeit, Werte zu speichern, aber die Sicherheit muss immer an erster Stelle stehen, wenn wir die Akzeptanz erhöhen wollen.**

**David Marcus**
ehemaligeger CEO von Paypal

In der dynamischen Welt der Kryptowährungen ist der Schutz vor Betrug von höchster Wichtigkeit. Angesichts der zunehmenden Zahl an Krypto-Scams, die sich in ihrer Ausführung und Raffinesse ständig weiterentwickeln, ist es entscheidend, präventive Maßnahmen zu ergreifen. Diese Betrügereien richten sich nicht nur gegen unerfahrene Investoren, sondern können auch gut informierte Nutzer in die Irre führen.

**Schutz Ihrer Kryptowerte**

Um Ihre Investitionen und digitalen Vermögenswerte zu schützen, gibt es eine Reihe von bewährten Strategien, die Sie anwenden können. In diesem Abschnitt werden wir effektive Maßnahmen erörtern, die Ihnen helfen, potenzielle Risiken zu identifizieren und zu minimieren. Ein fundiertes Sicherheitsbewusstsein sowie der Zugang zu verlässlichen Informationen sind entscheidend für ein sicheres Navigieren in der Krypto-Welt.

# Um sich vor Krypto-Betrug zu schützen, sollten Sie folgende Maßnahmen ergreifen:

**Informieren Sie sich**: Bleiben Sie über die neuesten Betrugsarten und Sicherheitspraktiken informiert. Zum Beispiel können Sie regelmäßig Webinare oder Schulungen vom **KPC-Verband** besuchen, um Ihr Wissen zu vertiefen.

**Seien Sie skeptisch**: Hinterfragen Sie unrealistische Versprechen. Wenn Ihnen jemand verspricht, dass Sie durch eine bestimmte Investition in kurzer Zeit reich werden, sollten Sie vorsichtig sein. Ein Beispiel könnte ein Angebot sein, das verspricht, dass jede Investition in ein neues Krypto-Projekt in nur einer Woche verdoppelt wird.

**Verwenden Sie sichere Wallets**: Nutzen Sie Hardware-Wallets wie Ledger oder Trezor, die bekannt für ihre Sicherheit sind. Diese bieten einen besseren Schutz als Online-Wallets.

**Prüfen Sie die Authentizität**: Achten Sie darauf, nur offizielle Webseiten und Apps herunterzuladen. Bevor Sie eine App installieren, sollten Sie die Bewertungen auf Plattformen wie Google Play oder dem App Store überprüfen, um sicherzustellen, dass sie legitim ist.

**Aktivieren Sie Sicherheitsmaßnahmen**: Nutzen Sie die Zwei-Faktor-Authentifizierung (2FA). Wenn Sie beispielsweise ein Konto bei einer Krypto-Börse haben, aktivieren Sie 2FA, um einen zusätzlichen Sicherheitsschritt einzuführen.

**Werden Sie Mitglied beim KPC-Verband**: Eine Mitgliedschaft im KPC-Verband bietet Zugang zu speziellen Schulungen, die Ihnen helfen, Risiken besser zu erkennen.

# Was tun, wenn Sie Opfer eines Krypto-Betrugs werden

Wenn Sie feststellen, dass Sie Opfer eines Krypto-Betrugs geworden sind, ist schnelles Handeln entscheidend. Hier sind einige praxisnahe Schritte, die Sie unternehmen sollten:

1

### Sofortige Meldung

Informieren Sie die Plattform, auf der der Betrug stattgefunden hat, und die zuständigen Behörden. Je schneller Sie handeln, desto größer ist die Chance, weitere Schäden zu verhindern. Nutzen Sie offizielle Kanäle oder Hotlines, um sicherzustellen, dass Ihre Meldung an die richtige Stelle gelangt.

2

### Schutz Ihrer Konten

Ändern Sie umgehend Ihre Passwörter und aktivieren Sie die Zwei-Faktor-Authentifizierung (2FA) für Ihre Konten. Übertragen Sie Ihre verbleibenden Kryptowährungen in eine sicherere Wallet, z. B. eine Hardware-Wallet, um weiteren Verlust zu vermeiden.

3

### Dokumentation

Halten Sie alle Beweise fest, einschließlich E-Mails, Transaktionsdaten und Screenshots. Diese Informationen sind wichtig, wenn Sie den Betrug melden oder rechtliche Schritte einleiten.

4

### Professionelle Hilfe

Zögern Sie nicht, sich an Experten zu wenden. Der **KPC-Verband** und ähnliche Organisationen bieten Ressourcen und Unterstützung an, um Ihnen bei der Wiederherstellung Ihrer Sicherheit zu helfen.

# Vorteile einer Mitgliedschaft im KPC Verband

In der sich ständig weiterentwickelnden Welt der Kryptowährungen ist es unerlässlich, informiert und vorsichtig zu sein. Krypto-Betrügereien sind vielfältig und nutzen verschiedene Taktiken, um ahnungslose Opfer zu täuschen.

Ein tiefes Verständnis der verschiedenen Betrugsarten sowie der implementierten Schutzmaßnahmen kann Ihnen helfen, in dieser unsicheren Umgebung sicher zu navigieren.

## Die Mitgliedschaft im KPC-Verband bietet zahlreiche Vorteile, darunter:

**Zugang zu Schulungen**: Mitglieder erhalten regelmäßige Schulungen zu den neuesten Sicherheitspraktiken und Betrugsarten, die ihnen helfen, potenzielle Risiken besser zu erkennen.

**Zertifizierung für Unternehmen**: Der KPC-Verband vergibt ein Zertifikat an Firmen, die nachweislich aktiv gegen Krypto-Betrug geschützt sind. Dieses Zertifikat signalisiert Vertrauen und Engagement für hohe Sicherheitsstandards, was es Unternehmen ermöglicht, sich als vertrauenswürdig zu positionieren.

**Netzwerkmöglichkeiten**: Der Verband fördert den Austausch von Informationen und Erfahrungen zwischen Mitgliedern, was zu einem besseren Schutz vor Betrug beiträgt. Sie können an Veranstaltungen teilnehmen, bei denen Sie mit anderen Mitgliedern über Erfahrungen sprechen können.

> **Kryptowährungen werden in der Finanzindustrie dieselben Auswirkungen haben, wie E-mail auf die Postindustrie.**
>
> **Joachim Wuermeling**
> Ökonom, Vorstand Deutscher Bundesbank

KPC Verband

Krypto Protectas Capitalis

## Contact Us

www.kpc-verband.org

info@kpc-verband.org