**Anlagebetrug: Gewinne sollten durch Investitionen und Handel mit Kryptowährungen erzielt werden.**

# 0,33 Prozent Rendite täglich

**Betrügern gelang es, Zehntausende „Anleger“ mit dem Versprechen hoher Rendite auf Krypto-Anlageprodukte hereinzulegen. Experten raten zu Vorsicht bei derartigen Anlagesystemen.**

Ein Mix aus Gier, Unwissenheit und dem Versprechen hoher Renditen auf Krypto-Anlageprodukte verschaffen weltweit kriminellen Geschäftsmodellen einen millionenfachen Zulauf. Die großen Gewinner sind Hintermänner und ein Vertriebsapparat auf Multi-Level-Marketing-Basis (MLM). Diese verdienen am Verlust vieler. Doch sind virtuelle Währungen wirklich das perfekte Mittel, um Betrugsmodelle im großen Umfang aufzuziehen? Wer in das Krypto-Anlagesystem „Plus Token“ investierte, dem versprachen die Anbieter 0,33 Prozent tägliche Rendite, was einen Jahresgewinn von 120 Prozent ergeben hätte.

Im April 2018 wurde ein „Token“ (Synonym für Coin/Münze) namens „Plus Token“ (PT) mit einer Gesamtstückanzahl von 500 Millionen auf der Ethereum-Blockchain programmiert, als eines von Tausenden anderen Tokenprojekten weltweit. Geschickte Programmierer bieten diese Dienstleistung für ein paar Tausend US-Dollar (USD) im Internet legal an. Der Unterschied ist der Verwendungszweck. Der „Plus Token“ wurde geschaffen, um ein Betrugsmodell anzukurbeln und solange am Leben zu erhalten, bis sich der Ausstieg daraus für die Hintermänner auszahlt. Im August 2018 wurde Mitgliedern der „Community“ 10.000 Stück dieses Tokens einfach für das Folgen des Plus-Token-Twitteraccounts gutgeschrieben. Etwa elf Monate später war ein Token über 124 USD wert. Die Marktkapitalisierung lag bei knapp 62 Milliarden USD, und „Plus Token“ war damit die Kryptowährung Nummer zwei hinter dem Bitcoin. Das Mitglied, das den Token bis dahin gehalten hatte, konnte sich über einen fiktiven Wert von 1,24 Millionen USD freuen.

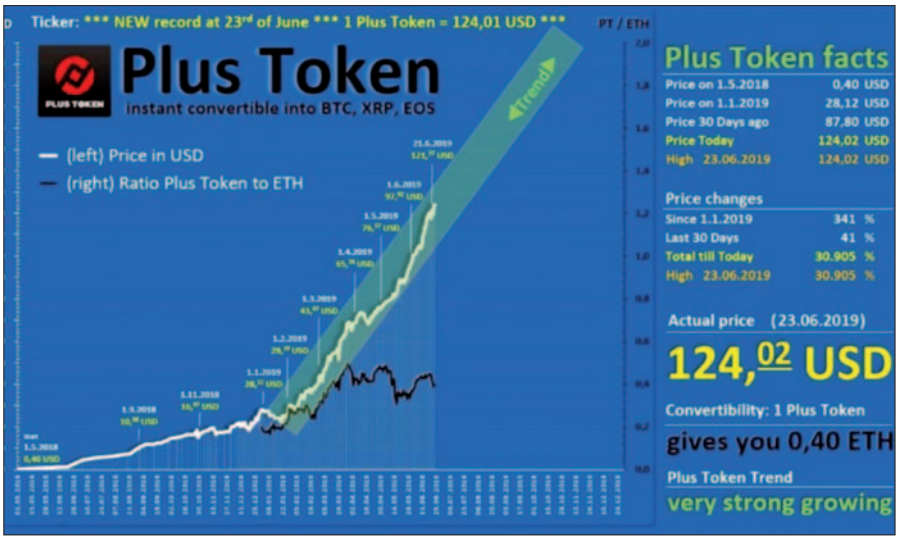
**Perfide Betrugsmasche.** Wie ist diese „Kursrallye“ eines „Shitcoins“ (Name für einen wertlosen Token/Coin) möglich? Alles begann mit einem Versprechen von 0,33 Prozent Rendite auf eingesetztes Kryptokapital. Ein Arbitragetradingprogramm – genannt AI-Dog – war programmiert worden, um diese Rendite fix zu erwirtschaften. Die Gewinne sollten durch Investitionen und Handel mit Kryptowährungen erzielt werden, die an einer Börse „billiger“ gekauft und an einer anderen Börse „teurer“ verkauft werden. Als Investor (Opfer) musste man lediglich Kryptowährungen im Mindestwert von 500 USD in eine davor auf dem Handy installierte App „senden“. Für dieses „Einlagern“ und somit der Zurverfügungstellung der Arbitragesoftware bekam der App-Inhaber die Rendite auf seine Assets in Form von „Plus Token“ gutgeschrieben. Dem Investor wurde durch Vertriebspartner/Werber/Empfehler und die App versichert, dass die Einlagerung sicher sei, denn nur der Inhaber hätte Kenntnis über die „Private Keys“ der durch die App verwalteten Kryptowallets (Konto für Kryptowährungen). Der „Shitcoin“ „Plus Token“ wurde als „Belohnung“ für Investoren (Opfer) zum jeweiligen PT-Kurs der „Shitbörse“ „PsEx Exchange“ gutgeschrieben, wo nicht nur ein Tag nach Einzahlung der Bitcoin, Ethereum usw.

FOTO: EISENHANS/STOCK.ADOBE.COM

diese „wegtransferiert“ wurden, sondern auch persönliche Daten gestohlen wurden. Die App gab es nicht im App Store, man musste ihre Installation mittels Sonderlinks selbst als Admin vornehmen, weil das Handy vor einer fremden Software warnt. Zusätzlich waren (diverse) Zugriffsrechte der App am Handy direkt zu gewähren. Für die Registration und das Laufen der App wurde ein Standard-KYC-Anmeldeprozess (Know your Customer) integriert, der den Investor (Opfer) eine gültige und aktuelle Ausweiskopie sowie seinen Adressnachweis per Bild hinterlegen ließ, danach konnte man Krypto-Assets an die App „übertragen“ und den AI-Dog aktivieren. Der Vertriebspartner/Werber/Empfehler verdiente an der Anmeldung mit und konnte sich zusätzlich auf bis zu 0,6 Prozent täglicher Rendite auf das eingesetzte Kapital der anderen Nutzer freuen.

Das Empfehlungsmodell war mit zehn Stufen ausgestattet und durch Multi-Level-Marketing der Vertriebsturbo für die „Downline“. Die Einzahlungen wurden solange umverteilt, bis das System einbrach. Der Kurs des „Plus Tokens“ wurde täglich auf der Krypto-Börse „PsEx Exchange“ dargestellt. Die Webseite wies kein Impressum auf und hatte nur die Aufgabe: mittels gefälschter Bestellungen eine riesige Kurssteigerung des „Plus Tokens“ darzustellen (von null auf 124 USD). Die Erfinder dieses „Systems“ – angeblich ein Russe und ein Südkoreaner – tauchten wie die Exchange, ohne offiziellen Namen oder in Verbindung mit einer offiziellen Firma auf.

**Angeblicher Cyber-Angriff.** Seit 24. Juni 2019 ist kein offizieller Handel mehr mit „Plus Token“ möglich. Durch einen angeblichen „Cyber-Angriff“ auf die zentralen Server der App und gleichzeitig auf die „Shitcoinbörse“ „PsEx“ waren alle Systeme offline. Kein Investor (Opfer) konnte seine App mehr starten und der Onlinezugriff zur Exchange war nicht möglich. Ohne App konnten auch die eingelagerten Kryptowährungen nicht mehr transferiert werden. Dies auch, weil ohne Wissen der Nutzer von den Hintermännern bereits die Kryptoassets weitergeleitet wurden. Dies zeigen Transaktionsanalysen der Bitcoinblockchain, wo man diese nachverfolgen konnte. Ab diesem Zeitpunkt war die Aufregung in der „Community“ groß und es wurden Telegram-Gruppen oder Whats-App-Hilfegruppen erstellt, die über die weiteren Angaben zum Angriff Auskunft geben sollten. Im Nachhinein war es eine reine Hinhaltetaktik, um wieder und wieder den Go Live der App hinauszuzögern und um Zeit zu gewinnen, sich im Hintergrund mit Krypto-Assets im angeblichen Wert von fast drei Milliarden USD abzusetzen. Alleine im DACH-Raum (Deutschland, Österreich, Schweiz) werden zehntausende Opfer vermutet. Seit September 2019 macht ein angeblicher Börsegang von „Plus Token“ die Runde. Man kann sich im Pre-IPO (Aktienausgabe) ab 2.500 Euro beteiligen. Das ist vermutlich ein neuerlicher Betrugsversuch. Experten raten, die Finger davon zu lassen. Diese „Anlagemodelle“ werden dafür konzipiert, möglichst schnell und möglichst anonym viel Geld zu machen. Die Modelle ähneln einander in punkto Gewinnversprechen, hohe tägliche Rendite, Gewinnmethode (Trading, Arbitrage, sonstiges …), gängiger technischer Infrastruktur (App oder Desktop Wallet inkl. KYC sowie individueller „Depotführung“) und vor allem der vertrieblichen Vorgehensweise. *Matthias Reder*




**„Plus-Token-Betrug“: Manipulierte Kursschaubilder wurden zur Kundenakquise eingesetzt.**

*Der Autor ist Leiter von Compliance und AML bei Coinfinity GmbH und Ansprechpartner für Großkunden sowie Banken und Behörden (www.coinfinity.co).*

## ANLAGEBETRUG

### Handlungsempfehlungen für „Plus-Token“-Opfer

- Alle Details zur Anwerbung (Chatverläufe, Aufzeichnungen, Vertriebsvideos usw.) und zur Abwicklung der App bzw. der Transaktionen dokumentieren; soweit noch vorhanden – etwa durch Fotos in einer eigenen Datei sichern.
- Bei der nächsten Polizeidienststelle Anzeige wegen Betruges erstatten, gegen „Plus Token“ und gegen jene Person, die dieses System „empfohlen“ hat. Auch wenn es sich um Freunde oder Bekannte handelt, ist es wichtig, um Rückschluss auf die Hintermänner zu erhalten.
- Ein neues Handy kaufen. Die App könnte Zugriff auf das Handysystem gehabt und möglicherweise Handlungen/Aktivitäten (Passwörter oder Ähnliches) ausspioniert haben.
- Eine andere Bankkontonummer und eine andere Kreditkarte besorgen, wenn man über das Handy online mit Kreditkarte bezahlt hat oder eine Banking-App auf dem Handy bedient hat.
- Weitere sensible Anmeldungen via App überprüfen und mit dem neuen Handy sofort das Passwort bei der nächsten Anmeldung ändern.

Trotz dieser Maßnahmen ist man nicht davor gefeit, dass die Identität der Opfer im Zusammenhang mit weiteren illegalen Aktivitäten weltweit auftaucht. Die Strafanzeige und deren Zeitpunkt ist als Nachweis sehr wichtig für Betroffene.

Screenshot: Coinfinity