

Samstag, 24. Oktober 2026

>> Bitcoin in Gefahr? Kann KI die Krypto-Währung zerstören?

>> Gewinner der Woche: Monero steigt auf den höchsten Stand seit Januar!

>> Verlierer der Woche: Starknet verliert einen Großteil seiner Kursgewinne!

>> Meine neuesten Videos...

Bitcoin in Gefahr? Kann KI die Krypto-Währung zerstören?

Liebe Leserin, lieber Leser,

künstliche Intelligenz (KI) spürt Sicherheitslücken inzwischen schneller auf als jedes professionelle Entwicklerteam. Wie groß die Folgen sein können, zeigt ein Fall aus dieser Woche: Mithilfe von KI-Modellen von OpenAI und Google fanden Sicherheitsforscher eine kritische Schwachstelle in der Programmiersprache PHP. Nach Angaben der Sicherheitsfirma Wiz laufen rund 70% aller Websites mit PHP. Der fehlerhafte Code steckte seit 2012 in der Software. Kaum war die Lücke am Mittwoch öffentlich, zählte der Netzwerkdienstleister Cloudflare bereits Millionen Angriffsversuche.



Das wirft natürlich die Frage auf, wie sicher Bitcoin tatsächlich ist. Bitcoin gilt zwar als das sicherste Blockchain-Netzwerk, doch hält es der KI auch Stand? Einer der bekanntesten Investoren des Silicon Valley Chamath Palihapitiya, hält es für möglich, dass KI den Schutz eines Tages aushebelt und die Wallet von Bitcoin-Erfinder Satoshi Nakamoto leert. Danach könnte Bitcoin »auf null« fallen, glaubt

der Gründer von Social Capital.

Ist die KI in der Lage, Bitcoin zu hacken?

Aktuell ist der Sicherheitsvorfall in der serverseitigen Programmiersprache PHP in aller Munde. Über die PHP-Lücke können Hacker ohne Passwort auf fremde Server zugreifen und dort eigene Befehle ausführen. Betroffen sind nach Angaben der US-Cybersicherheitsbehörde CISA alle PHP-Installationen, die Anfragen aus dem Internet bearbeiten. Deutschland, Frankreich und die Niederlande nahmen deshalb vorsorglich Behördenseiten vom Netz. Der US-Geheimdienst NSA riet sogar, Systeme abzuschalten, wenn sie sich nicht sofort aktualisieren lassen.

Die PHP Foundation zieht daraus eine nüchterne Bilanz: KI-Modelle fänden Fehler heute schneller als je zuvor: Davon profitieren Unternehmen, die ihre Systeme früher absichern können. Angreifer nutzen dieselben Werkzeuge allerdings ebenso.

Und die großen KI-Firmen behandeln ihre stärksten Modelle inzwischen selbst wie ein Sicherheitsrisiko. Anthropic gibt sein Modell „Claude Mythos“ seit April nur ausgewählten Organisationen frei, die kritische Software entwickeln oder betreiben. Das Modell habe Tausende schwerwiegende Lücken gefunden, darunter in allen großen Betriebssystemen und Browsern. Aus einem ähnlichen Programm von OpenAI namens „Patch the Planet“ stammt auch der PHP-Fund.

Chamath Palihapitiya hat diese Entwicklung auf Bitcoin übertragen. Wenn die KI Fehler aufspürt, die Entwickler über ein Jahrzehnt übersehen haben, bleibt aus seiner Sicht auch die größte Krypto-Währung nicht verschont.

Palihapitiya war früher Manager bei Facebook, später gründete die Beteiligungsgesellschaft Social Capital und war früh in Bitcoin investiert. Bereits 2012/2013 investierte er erhebliche Summen in Bitcoin und empfahl anderen Investoren frühzeitig, einen Teil ihres Vermögens in BTC anzulegen. Im Jahr 2013 soll Palihapitiya rund 5% aller damals existierenden Bitcoin gehalten zu haben. Darum sind seine Aussagen durchaus beachtenswert.

Im Podcast „Moonshots“ erklärte er, KI-Modelle, die sich selbst immer weiter verbessern, könnten das Sicherheitsverfahren SHA-256 angreifen und die Bestände von Satoshi Nakamoto erbeuten. Ein Angreifer würde dabei gleich zweimal verdienen: Zuerst an den gestohlenen Coins, dann mit Wetten auf fallende Kurse (Shorts), sobald er den Angriff öffentlich macht.

Einen Umstieg auf quantensichere Verfahren hält Palihapitiya für »praktisch unmöglich«, weil sich die Bitcoin-Community schon bei einfachen Fragen kaum einigen könne. Zudem sei der Wert von Bitcoin nach oben begrenzt, weil

Notenbanken die Krypto-Währung kaum halten könnten. Er selbst besitzt keine BTC mehr direkt. Sein Investment in Bitcoin habe er vor Jahren in eine Beteiligung an der Digital Currency Group umgewandelt, um sich nicht selbst um die Verwahrung kümmern zu müssen.

In einem Punkt liegt Palihapitiya allerdings technisch daneben. SHA-256 sichert vor allem das Mining ab. Die Coins selbst schützt ein anderes Verfahren: die digitale Signatur auf Basis elliptischer Kurven, kurz ECDSA. Wer sie bricht, kann aus einem öffentlichen Schlüssel (Public Key) den geheimen Schlüssel (Private Key) berechnen und damit über die Coins verfügen.

Als größte Bedrohung für dieses Verfahren galten bislang **Quanten-Computer**. Sie könnten den privaten Schlüssel mit einem speziellen Rechenverfahren weit schneller ermitteln als heutige Computer. Nach einer Studie von Google aus dem März wären dafür weniger als 500.000 physikalische Qubits nötig. Googles aktueller Quantenchip Willow kommt auf 105. Bis zu einem solchen Angriff dürften noch Jahre vergehen.

Hier gibt es aber die Sorge, dass rekursive KI schneller ans Ziel kommen könnte. Gelingt ihr ein mathematischer Durchbruch, ließe sich ECDSA womöglich schon mit herkömmlichen Rechnern brechen. Dann bliebe deutlich weniger Zeit für den Umbau des Bitcoin-Netzwerks bzw. den Umstieg, den Palihapitiya ohnehin für kaum machbar hält.

Hacker können bei Bitcoin also theoretisch an zwei Stellen ansetzen: An der Software rund um das Netzwerk oder an der Mathematik der Signaturen. Bei der Software hat KI ihre Fähigkeiten bereits bewiesen. Ob sie die Signaturen schneller bricht als ein Quanten-Computer, ist unter Fachleuten umstritten.

Hier die Grafik vergrößern...



Die größte Schwachstelle liegt bislang in der Software rund um Bitcoin (eigene Darstellung)

Wo die Gefahr für Bitcoin tatsächlich liegt

Justin Drake von der Ethereum Foundation riet er der Branche Anfang Oktober, in Ruhe einen »Bunker-Modus« vorzubereiten. Anlass waren 722 mathematische Ergebnisse, die OpenAI mit einem unveröffentlichten KI-Modell erzielt hatte. Drake hält es für denkbar, dass KI die Signaturen von Bitcoin und Ethereum noch vor dem Quanten-Computer bricht, im ungünstigsten Fall »in Monaten, nicht Jahren«.

Belege für einen solchen Durchbruch gibt es bislang nicht. OpenAI wies selbst darauf hin, dass ein Teil der Ergebnisse noch geprüft werde und Fehler enthalten könne. Auch Ethereum-Mitgründer Vitalik Buterin rät davon ab, Assets schon jetzt umzuschichten. Das Risiko müsse man aber ernst nehmen.

Echtes Geld gekostet hat KI bislang an anderer Stelle: in der Software rund um Bitcoin. Dort zeigt sich dasselbe Muster wie bei der PHP-Lücke.

Im Sommer erbeuteten Hacker bei Nutzern der Hardware-Wallet Coldcard BTC im Wert von rund 130 Mio. US-Dollar. Eine fehlerhafte Firmware hatte seit 2021 **Wiederherstellungswörter mit zu wenig Zufall erzeugt**. Wie bei PHP blieb der Fehler jahrelang unentdeckt. Der Hersteller Coinkite geht davon aus, dass die Täter ältere Versionen seiner Open-Source-Software mit KI durchsucht haben.

Und im August meldeten freiwillige Entwickler des Bitcoin Red Team fast 5.000 mögliche Schwachstellen in 390 Projekten, aufgespürt mit KI-Modellen. Nach mehreren KI-gestützten Fehlermeldungen forderten die Entwickler der Lightning-Software Core Lightning Betreiber auf, ihre Knoten zu aktualisieren oder vom Netz zu nehmen.

Am Donnerstag zog auch Bitcoin Core Konsequenzen, die wichtigste Software des Netzwerks. Entwickler Antoine Poinsot kündigte an, Lücken, die sich mit minimalem Aufwand etwa über eine einfache KI-Anfrage finden lassen, künftig sofort zu schließen und offenzulegen. Lange Sperrfristen brächten wenig, wenn KI dieselben Fehler ohnehin schnell wiederentdecke.

» Unser Fazit:

Dass KI Bitcoin in absehbarer Zeit hackt, halten wir für unwahrscheinlich. Die Mathematik hinter den Signaturen wird seit rund vier Jahrzehnten erforscht und ist bislang ungebrochen. Auch Drakes Warnung beruht auf allgemeinen Fortschritten der KI in der Mathematik und einen konkreten Angriffsweg hat bisher niemand vorgelegt. Zudem träfe ein solcher Durchbruch weit mehr als Bitcoin, denn elliptische Kurven sichern bspw. auch Online-Banking und viele verschlüsselte

Verbindungen im Internet.

Real ist dagegen, dass die KI Fehler in Wallets und Zusatzsoftware schneller findet, als manche Hersteller sie beheben können. Das zeigt der Fall Coldcard. Hinzu kommt die Stimmung am Markt. Der Rücksetzer am Donnerstag ging zwar vor allem auf den Ausverkauf bei Tech-Aktien zurück, Analysten nannten aber auch Sorgen um die Sicherheit von Software als Belastung. Ansonsten zeigt sich Bitcoin in einem schwierigen Marktumfeld dagegen bislang sehr robust.

Gewinner der Woche:
Monero steigt auf den höchsten Stand seit Januar!

Monero (XMR) gewinnt auf Wochensicht rund 10% und notiert bei etwa 610 US-Dollar. Am Donnerstag erreichte der Kurs zeitweise 650 US-Dollar und damit den höchsten Stand seit Januar. XMR lässt Bitcoin damit deutlich hinter sich. Mit einem Börsenwert von rund 11,5 Mrd. US-Dollar liegt der Privacy Coin auf Rang 13 der größten Krypto-Währungen.

Privatsphäre ist wieder gefragt

Privacy-Coins zählen 2026 zu den stärksten Segmenten des Krypto-Markts. Bislang stand vor allem **Zcash (ZEC)** im Mittelpunkt, nun auch vermehrt **Monero (XMR)** – den wirklichen Privacy-Coin. Anders als bei Zcash, wo die Nutzer selbst entscheiden, ob sie eine Transaktion verschleiern, ist bei Monero die Verschleierung Pflicht. Absender, Empfänger und Betrag bleiben bei jeder Zahlung verborgen.

Dass dies Behörden ein Dorn im Auge ist, kann sich jeder denken. Binance hat XMR deshalb bereits im Februar 2024 aus dem Handel genommen. Umso bemerkenswerter ist der Rückenwind, der Anfang Oktober aus Washington kam. Die US-Behörde FinCEN zog am 5. Oktober zwei Regelungsvorschläge zurück. Sie hätten Banken und Zahlungsdienstleistern zusätzliche Aufzeichnungs- und Meldepflichten für Zahlungen an selbstverwahrte Wallets und über sog. Mixer auferlegt. Mixer erschweren es ebenfalls, Zahlungsströme zurückzuverfolgen.

Zugleich bereitet Monero ein weitreichendes technisches Upgrade vor. FCMP++ soll die Anonymität von Transaktionen noch einmal verbessern und wird derzeit in einer Testumgebung erprobt. Ein Termin für die Einführung im Hauptnetz steht noch nicht fest.

Brandt sieht Parallelen zur Silber-Rallye

Der erfahrene Chartanalyst Peter Brandt hat sich ebenfalls bullisch zu Monero geäußert und bezeichnete XMR als seine bevorzugte Krypto-Währung. Zuletzt verglich er Moneros Chartstruktur mit der von Silber vor dessen Anstieg in Richtung 125 US-Dollar. Ein konkretes Kursziel für XMR nannte er nicht.

Mit dem Interesse nimmt allerdings auch die Spekulation zu. Nach Angaben von Santiment stieg das in XMR gemessene Volumen offener Futures zwischen dem 15. und 20. Oktober um rund 22%. Werden verstärkt gehebelte Positionen aufgebaut, können fallende Kurse Zwangsliquidationen auslösen und einen möglichen Kursrückgang beschleunigen.



Kürzel	Kurs	Marktkapitalisierung	tägl. Handelsvolumen
XMR	610 US-Dollar	11,5 Mrd. US-Dollar	186 Mio. US-Dollar

Quelle: coinmarketcap.com

Unser Fazit:

Monero profitiert von der KI-Thematik, die auch das Thema Privatsphäre wieder stärker in den Fokus rückt. Der regulatorische Gegenwind bleibt jedoch weiterhin hoch: Ab dem 10. Juli 2027 dürfen Krypto-Dienstleister in der EU nach der neuen Geldwäsche-Verordnung z.B. keine Privacy-Coins wie Monero mehr anbieten.

Verlierer der Woche:
Starknet verliert einen Großteil seiner Kursgewinne!

Bei Starknet folgt auf eine steile Rallye eine ebenso deutliche Korrektur. STRK stieg letzte Woche noch zeitweise über 12 Cent und fiel anschließend bis auf etwa 5,3 Cent zurück. Vom Hoch ist damit mehr als die Hälfte des Kurswerts verloren gegangen. Dass der Monats-Chart dennoch überwiegend grün bleibt, erklärt sich durch den niedrigen Ausgangspunkt bei rund 4 Cent.

Von Ethereum zur eigenen Blockchain

Bislang arbeitet Starknet als Ethereum-Layer-2-Netzwerk: Es bündelt Transaktionen, verarbeitet sie kostengünstig und nutzt Ethereum zu deren Absicherung. Am 8. Oktober stellte Eli Ben-Sasson, Chef des Entwickler-Unternehmens StarkWare, einen möglichen Umbau zur eigenständigen Blockchain in Aussicht. Innerhalb von drei Tagen verdoppelte sich der STRK-Kurs daraufhin.

Hinter dem Vorstoß zu einer eigenen L1-Blockchain und der Abkehr von Ethereum stehen Sicherheitsbedenken, die tatsächlich auch zu unserem Titelthema passen: Ben-Sasson will Starknet bereits 2027 gegen Angriffe durch Quanten-Computer absichern. Den für Ethereum angepeilten Zeithorizont 2029 hält er für zu spät. KI-Agenten könnten die Entwicklung neuer Angriffsmöglichkeiten zusätzlich beschleunigen. Solange Starknet bei der Verbindung zu Ethereum und der Bereitstellung seiner Transaktionsdaten auf das übergeordnete Netzwerk angewiesen sei, könne es vollständigen Quantenschutz nicht eigenständig erreichen.

Breite Zustimmung, offene Fragen

Am Donnerstag endete eine 7-tägige Abstimmung der Token-Inhaber. Rund 93,% der abgegebenen Stimmrechte entfielen auf den Vorschlag, den Umbau näher zu untersuchen, im November soll zunächst ein Whitepaper-Entwurf folgen. Über einen konkreten Umbau müssten die Token-Inhaber erneut abstimmen. STRK soll auch bei einem Wechsel der Token des Netzwerks bleiben.

Eine weitere Belastung waren offenbar auch Token Unlocks. Am 15. Oktober wurden rund 127 Millionen STRK frei (etwa 1,7% des umlaufenden Angebots). Hinzu kommt eine seit dem Kurshoch vom 11. Oktober deutlich rückläufige Netzwerkaktivität. Auf die Begeisterung über den möglichen Umbau folgt die Skepsis, ob Starknet die hohen Erwartungen auch mit tatsächlicher Nutzung unterlegen kann.



Kürzel	Kurs	Marktkapitalisierung	tägl. Handelsvolumen
STRK	0,053 US-Dollar	401 Mio. US-Dollar	68 Mio. US-Dollar

Quelle: coinmarketcap.com

Unser Fazit:

Starknets Plan mit einer eigenen Quantum-sicheren Chain in die Zukunft zu gehen ist richtig, doch bei der Umsetzung bleiben viele Fragen offen. Die Aussicht auf eine eigene Blockchain hat den Kurs zunächst beflügelt – die Rallye hatte allerdings nur kurze Beine. Wie es weitergeht, hängt nun davon ab, ob Starknet seine Pläne konkretisieren und glaubwürdig umsetzen kann.

Die heutige Ausgabe entstand wieder durch die Zusammenarbeit im Team mit Alexander Mittermeier (Chefredakteur), Philipp Henk (stellvertr. Chefredakteur) und andere Team-Mitglieder, die allesamt langjährige Erfahrungen in der Krypto-Branche mitbringen.

Offenlegung wegen möglicher Interessenkonflikte:

Die Autoren sind in den folgenden besprochenen Krypto-Währungen bzw. -Projekten zum Zeitpunkt der Veröffentlichung dieses Kommentars investiert in: **Bitcoin & Ethereum**

Weitere Informationen dazu findest Du hier...

Meine neuesten Videos





Viel Erfolg bei deinen Finanzentscheidungen &
ein schönes Wochenende wünscht Dir

Dein
Alexander Mittermeier
Chefredakteur *Krypto-Report*
www.krypto-report.de

>> Die nächste Ausgabe erscheint am 31. Oktober

investUp Media GmbH • Dollgasse 13 • 97084 Würzburg • Registereintrag: Registergericht – Amtsgericht Würzburg | Registernummer – HRB 17058 • USt-IdNr. gemäß § 27a UStG: DE365054878 • Vertreten durch: Stefan Böhm & Markus Müller • Inhaltlich Verantwortlicher i.S.d. § 18 Abs. 2 MStV: Alexander Mittermeier (V.i.S.d.P.)

Copyright © 2026 investUp Media GmbH – Alle Rechte vorbehalten.