

Samstag, 17. Oktober 2026

>> Ledger & Co.: Wie sicher sind deine Bitcoin? Was Nutzer jetzt tun sollten!

>> Gewinner der Woche: Injective knackt die 9-Dollar-Marke!

>> Verlierer der Woche: Sinkende Gebühren belasten Raydium!

>> Meine neuesten Videos...

Ledger & Co.: Wie sicher sind deine Bitcoin? Was Nutzer jetzt tun sollten!

Liebe Leserin, lieber Leser,

eine Hardware-Wallet soll Bitcoin und andere Krypto-Währungen vor Dieben schützen. Doch genau diesen Schutz haben Kriminelle bei manipulierten Ledger-Geräten ausgehebelt: Über ein heimlich eingebautes Bauteil gelangten sie an die Seed-Phrase der Besitzer – und damit an deren Vermögen. Der Analyse-Dienst „Bitquery“ beziffert den Schaden auf rund 102 Mio. US-Dollar.



Inzwischen beschäftigt der Fall auch den deutschen Handel. Nach Berichten über verdächtige Geräte nahm **MediaMarkt** Ledger-Wallets vorsorglich aus dem Sortiment. Wie weit die Manipulationen reichen, ist noch nicht abschließend geklärt. Für Anleger stellt sich deshalb vor allem eine Frage: Ist die eigene Wallet sicher?

Wie die Täter den Schutz der Geräte umgingen

Bekannt wurde der Angriff am 9. Oktober durch Nutzer, die ihre Geräte beim südostasiatischen Ledger-Vertriebspartner **CryptoBilis** gekauft hatten und anschließend Verluste meldeten. Einen Tag später bestätigte Ledger den Fund eines zusätzlich eingebauten Bauteils. Nach Auswertungen von Bitquery lassen sich dem Vorfall bislang 324 Wallets auf sechs Blockchains zuordnen.

Die Täter setzten an einer empfindlichen Stelle an: dem Bildschirm. Nach Angaben von Ledgers Sicherheitsteam Donjon las das eingeschleuste Bauteil die Bildschirmausgabe mit. Sobald bei der Einrichtung die 24 Wiederherstellungswörter erschienen, übertrug es diese über eine eigene Mobilfunkverbindung an die Angreifer.

Hier die Grafik vergrößern...



Das Implantat greift die angezeigten Wiederherstellungswörter ab, schematische Illustration | Quelle: Ledger Donjon (13.10.2026)

Diese Wörter sind quasi der Generalschlüssel zur Wallet. Wer sie kennt, kann auf einem anderen Gerät auf die Bestände zugreifen und sie übertragen. Den ursprünglichen Ledger braucht er dafür nicht.

Besonders problematisch: Sicherheits-Chip und Betriebssystem blieben bei diesem Angriff unverändert. Deshalb konnte auch Ledgers Echtheitsprüfung die Manipulation nicht ausschließen. Ein bestandener Test und eine unbeschädigte Verpackung boten den Käufern somit keine verlässliche Sicherheit.

Was über die Fälle in Deutschland bekannt ist

Laut einem Bericht von heise meldete ein Nutzer zwei manipulierte Geräte aus unterschiedlichen MediaMarkt-Filialen. Die fusionierte Handelskette

MediaMarktSaturn stoppte daraufhin am 13. Oktober vorsorglich den Verkauf von Ledger-Wallets.

Ledger erklärte am folgenden Tag, bei der Untersuchung deutscher Händler- und Vertriebsbestände keine Auffälligkeiten gefunden zu haben. Die im Internet gezeigten Geräte habe das Unternehmen allerdings noch nicht selbst prüfen können. Verluste durch solche Implantate seien in Europa bislang nicht gemeldet worden. Die Berichte über die beiden Geräte bleiben damit ungeklärt.

In Südostasien und Hongkong forderte **Ledger** Handelspartner ebenfalls zu einem vorläufigen Verkaufsstopp auf. Nach einem Untersuchungsbericht des Herstellers vom 16. Oktober soll eine organisierte kriminelle Gruppe über Monate Original-Geräte gekauft, manipuliert und wieder in den Handel gebracht haben. Ledger-Chips, Betriebssystem und Server seien nicht kompromittiert worden.

Der Fall zeigt dennoch eine Schwachstelle: Selbst ein technisch unverändertes Sicherheitssystem schützt nicht ausreichend, wenn Kriminelle zusätzliche Elektronik im Gerät unterbringen können.

Was Du als Ledger-Nutzer jetzt tun solltest

Ein Kauf bei einem der genannten Händler bedeutet nicht automatisch, dass Deine Wallet manipuliert wurde. **Prüfe dennoch, wo und wann Du das Gerät erworben hast.** Besondere Aufmerksamkeit verdienen Käufe der vergangenen Monate über die betroffenen Vertriebswege.

Besteht ein konkreter Manipulationsverdacht, solltest Du das Gerät nicht weiter einrichten und keine zusätzlichen Krypto-Währungen darauf übertragen. Auf einen erfolgreichen Echtheits-Test allein kannst Du Dich in diesem Fall nicht verlassen.

Hast Du ein verdächtiges Gerät bereits eingerichtet, musst Du davon ausgehen, dass die Wiederherstellungswörter in fremde Hände gelangt sein könnten. Übertrage Deine Bestände dann möglichst schnell auf eine vertrauenswürdige, unabhängig eingerichtete Hardware-Wallet mit vollständig neuen Wiederherstellungswörtern. **Die bisherige Wortfolge darfst Du nicht übernehmen, sonst bleibt der Zugriff für die Täter möglich.**

Melde den Verdacht über Ledgers offizielle Website und bewahre die Kaufbelege auf. Falls bereits Krypto-Währungen gestohlen wurden, solltest Du vor dem Öffnen des Geräts die Polizei einschalten, damit mögliche Beweise erhalten bleiben.

Sei außerdem vorsichtig bei vermeintlichen Hilfs-Angeboten. Weder Ledger noch

ein seriöser Support-Mitarbeiter benötigt Deine 24 Wörter. **Gib sie niemals auf einer Website ein und teile sie niemals.**

Für Besitzer älterer Geräte besteht nach bisherigem Kenntnisstand kein Anlass zu einem Austausch. Wer seinen Ledger seit Jahren nutzt und keinen konkreten Hinweis auf eine Manipulation hat, muss aufgrund dieses Vorfalls nicht automatisch von einem unsicheren Gerät ausgehen.

Ledger verspricht besseren Schutz mit Atom

Mitten in die Aufarbeitung fällt eine Produktankündigung: Am 15. Oktober stellte Ledger sein neues Android-Gerät **Atom** vor. Es verfügt über einen gesonderten Sicherheitsmodus. Ein überwachter Bereich im Inneren soll physische Eingriffe erkennen und laut Hersteller auch einen Angriff wie den jetzt bekannt gewordenen verhindern. Unabhängige Prüfungen müssen dieses Versprechen erst bestätigen.

Hier die Grafik vergrößern...



Ledger Atom soll Krypto-Währungen durch einen abgeschotteten Sicherheitsmodus und die Erkennung physischer Manipulationen besser schützen. Die Auslieferung ist für 2027 geplant | Quelle: Ledger (Herstellerabbildung)

Die limitierte Founder's Edition soll **849 US-Dollar** kosten, die Auslieferung ist für 2027 vorgesehen. Für betroffene Anleger bietet das Gerät deshalb keine unmittelbare Lösung. Sind die Wiederherstellungswörter bereits gestohlen, kann auch neue Schutztechnik den Zugriff der Täter nicht rückgängig machen.

» Unser Fazit:

Der Angriff ist ein schwerer Vertrauensverlust für Ledger. Käufer müssen sich darauf verlassen können, dass sie ein unmanipuliertes Gerät erhalten. Wenn selbst

die Echtheitsprüfung einen solchen Eingriff nicht ausschließt, muss der Hersteller erklären, wie er seine Vertriebswege künftig besser absichert.

Die Sicherheit des Bitcoin-Netzwerks stellt der Vorfall nicht infrage. Er zeigt aber, dass zur sicheren Selbstverwahrung mehr gehört als der Kauf einer Hardware-Wallet. Auch die Herkunft des Geräts und der Schutz der Wiederherstellungswörter sind entscheidend.

Für Nutzer gilt deshalb: Prüfe, ob Dein Gerät betroffen sein könnte. Bei einem konkreten Verdacht hat der Umzug auf eine neue, sicher eingerichtete Wallet Vorrang. Doch keine Panik! Ein pauschaler Austausch sämtlicher Ledger-Geräte lässt sich aus den bisherigen Erkenntnissen nicht ableiten.

Gewinner der Woche:
Injective knackt die 9-Dollar-Marke!

Injective (INJ) legt auf Wochensicht rund 32% auf 9,26 US-Dollar zu. Der Großteil des Anstiegs entfiel auf die vergangenen 24 Stunden. Damit steigt die Marktkapitalisierung auf etwa 926 Mio. US-Dollar. Neue Partnerschaften und ein Besuch von Mitgründer Eric Chen bei US-Regulierern haben das Interesse am Netzwerk belebt.

Seit dem 8. Oktober betreibt **Gulf Labs** einen Validator auf **Injective (INJ)** und beteiligt sich damit an der Prüfung von Transaktionen. Das Unternehmen gehört zum Umfeld der thailändischen GULF-Gruppe. Gemeinsam wollen die Partner **Möglichkeiten für tokenisierte Assets und Stablecoins prüfen**. Konkrete Produkte sind bislang nicht angekündigt. Die häufig genannten 27 Mrd. US-Dollar entsprechen dem Börsenwert der GULF-Gruppe – einer Investition in Injective entspricht diese Summe natürlich nicht.

Zusätzliche Chancen eröffnet eine Umstellung beim Stablecoin USDC. Seit dem 13. Oktober gibt Circle über seinen Dienst **»Circle Mint«** keine neuen USDC mehr auf der Blockchain Noble aus. Nach Angaben von Injective soll die eigene USDC-Variante künftig als gemeinsamer Standard im Cosmos-Ökosystem dienen. **Gelingt das, könnte mehr Zahlungs- und Handelsgeschäft über Injective laufen.**

Der US-Markt weckt Erwartungen

Am Mittwoch traf Chen nach Unternehmensangaben Vertreter des Weißen Hauses

sowie der Aufsichtsbehörden SEC und CFTC. Im Mittelpunkt standen tokenisierte Vermögenswerte und die Frage, wie sich Finanzgeschäfte auf der Blockchain innerhalb des US-Rechtsrahmens abwickeln lassen. Konkrete Ergebnisse wurden nicht bekannt; die Behörden äußerten sich bislang nicht.

Zudem liegen Anträge für drei INJ-ETFs von 21Shares, Canary und REX-Osprey vor. Canary sieht in seinem überarbeiteten Antrag vor, unter Umständen mindestens 90% der gehaltenen Token zu staken. Chen rechnet mit einem ETF-Start noch vor 2027. Eine Zulassung ist damit allerdings nicht gesichert.



Kürzel	Kurs	Marktkapitalisierung	tägl. Handelsvolumen
INJ	9,26 US-Dollar	926 Mio. US-Dollar	312,6 Mrd. US-Dollar

Quelle: coinmarketcap.com

Unser Fazit:

Injective (INJ) gewinnt neue Partner. Ob dadurch auch die Nutzung und die Nachfrage nach INJ steigen, muss sich erst noch zeigen. Nach dem Sprung über den charttechnischen Widerstand bei 8,60 US-Dollar ist der Weg frei für weiter steigende Kurse Richtung 10-Dollar-Marke. Für noch weitere Kursgewinne sind allerdings messbare Fortschritte bei der Adoption und Netzwerknutzung entscheidend. Wir im „Blockchain-Investor“ sind am 8. Oktober bei 6,90 US-Dollar eingestiegen und rechnen mit weiter steigenden Kursen.

Verlierer der Woche:
Sinkende Gebühren belasten Raydium!

Raydium (RAY), unser Gewinner der vergangenen Ausgabe, verliert auf Wochensicht rund 27% auf 1,85 US-Dollar. Seit dem Hoch bei 2,57 US-Dollar am 7. Oktober beträgt das Minus etwa 28%. Die Marktkapitalisierung fällt auf knapp unter 500 Mio. US-Dollar. Trotz des deutlichen Rückgangs bleibt auf Monatssicht noch ein Gewinn von rund 46%.

In der Vorwoche hatten wir auf Raydiums Abhängigkeit vom Geschäft mit neuen Token hingewiesen. Inzwischen zeigen die Gebühreneinnahmen, wie schnell diese Dynamik nachlassen kann: Vom 9.-15. Oktober erzielten die von DefiLlama erfassten Raydium-Protokolle einschließlich LaunchLab rund 2,85 Mio. US-Dollar an Gebühren. In den 7 Tagen zuvor waren es noch 4,93 Mio. US-Dollar. Das entspricht einem Rückgang um etwa 42%.

Damit verliert ein wichtiger Grund für den vorherigen Kursanstieg an Gewicht. Im 3. Quartal hatten sich die Gebühren laut Pine Analytics auf 57,1 Mio. US-Dollar mehr als ver-3-facht. Dazu trug vor allem StonkFun bei, dessen neue Token seit September über LaunchLab an den Markt kamen. Die jüngsten Zahlen zeigen jedoch, wie unsicher es ist, einen außergewöhnlich starken Monat als Maßstab für künftige Einnahmen zu nehmen.

Warum die Gebühren für RAY wichtig sind

Ein Teil der Handelsgebühren fließt in den Rückkauf von RAY. Bei den klassischen Raydium-Pools sind dafür 12% der Swap-Gebühren vorgesehen. Weniger Handel bedeutet deshalb auch weniger Mittel für diese Rückkäufe.

Für LaunchLab gelten allerdings eigene Regeln zur Gebührenverteilung. Aus der gesamten von DefiLlama ausgewiesenen Gebührensumme lässt sich daher nicht unmittelbar auf das Rückkaufvolumen schließen. **Die Richtung bleibt dennoch klar: Lässt die Aktivität nach, fällt auch eine wichtige Stütze für die Token-Nachfrage schwächer aus.**



Kürzel	Kurs	Marktkapitalisierung	tägl. Handelsvolumen
RAY	1,85 US-Dollar	500 Mio. US-Dollar	52 Mio. US-Dollar

Quelle: coinmarketcap.com

Unser Fazit:

Raydium erzielt weiterhin nennenswerte Gebühren. Der jüngste Rückgang zeigt aber, wie stark die Einnahmen vom spekulativen Handel mit neuen Token abhängen. Für einen neuen Einstieg würden wir abwarten, bis sich sowohl die Gebühreneinnahmen als auch der Kurs stabilisiert. Werden die jüngsten Tiefs unterschritten, steigt das Risiko weiterer Verluste.

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 & Injective**

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 24. 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.