SEED-SICHERHEIT · BIP-39 · 2026

Entropie vs. Brute Force

Wie lange ein Angriff auf eine Bitcoin-Seed dauert – und was der Coldcard-Entropiefehler bedeutet



ERGEBNIS · BITCOIN-SEED (BIP-39) IM JAHR 2026

Entropie-Bits vs. Zeit für einen Brute-Force-Angriff

Angriffsmodell: Offline-Suche – der Angreifer kennt das Erzeugungsverfahren und prüft Kandidaten ohne das Gerät (keine PIN-Sperre).

Entropie in Bit	Einzelne RTX 5090 ≈ 1 Mio. Versuche/s	Cluster aus 16 × RTX 5090 ≈ 16 Mio. Versuche/s	Große GPU-Farm (~1.000 GPUs) ≈ 1 Mrd. Versuche/s
8	Sofort	Sofort	Sofort
16	Sofort	Sofort	Sofort
24	17 Sek.	1 Sek.	Sofort
32	1,2 Std.	4,5 Min.	4,3 Sek.
40 COLDCARD MK3	13 Tage	19 Std.	18 Min.
48	8,9 Jahre	204 Tage	3,3 Tage
56	2.280 Jahre	143 Jahre	2,3 Jahre
64	585.000 Jahre	36.500 Jahre	585 Jahre
72 COLDCARD MK4 / MK5 / Q	150 Mio. Jahre	9,4 Mio. Jahre	150.000 Jahre
80	38,3 Mrd. Jahre	2,4 Mrd. Jahre	38,3 Mio. Jahre
96	2,5 Brd. Jahre	157 Bio. Jahre	2,5 Bio. Jahre
112	165 Trio. Jahre	10,3 Trio. Jahre	165 Brd. Jahre
128 BIP-39-STANDARD	10,8 Quadrill. Jahre	674 Trd. Jahre	10,8 Trd. Jahre

≤ 1 Sekunde · Sekunden bis Wochen · Monate bis Jahrtausende · bis ~1 Mrd. Jahre · praktisch unknackbar

Zeiten für das Durchsuchen aller Möglichkeiten; im Mittel ist die Seed nach der Hälfte gefunden. Mio. = 10^6 · Mrd. = 10^9 · Bio. = 10^{12} · Brd. = 10^{15} · Trio. = 10^{18} · Trd. = 10^{21} · Quadrill. = 10^{24}

Was die Bit-Zahl bedeutet

× 2

pro zusätzlichem Bit

Jedes Bit verdoppelt die Zahl der Möglichkeiten, die ein Angreifer durchprobieren muss. 10 Bit mehr bedeuten rund 1.000-mal mehr Aufwand.

128 Bit

= Seed mit 12 Wörtern

BIP-39-Standard: $2^{128} \approx 3{,}4 \cdot 10^{38}$ mögliche Seeds – weit mehr, als es Sandkörner auf der Erde gibt.

256 Bit

= Seed mit 24 Wörtern

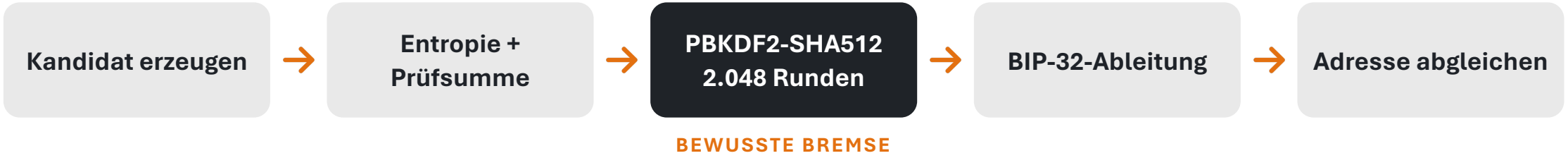
Quadriert die Zahl der Möglichkeiten nochmals. Gegen Brute Force bieten aber bereits 128 Bit mehr als genug Reserve.

40 Bit statt 128 Bit heißt nicht „ein Drittel so sicher“.

Es fehlen 88 Bit – also $2^{88} \approx 3 \cdot 10^{26}$-mal weniger Möglichkeiten. Aus einer Suche, die um ein Vielfaches länger dauert als das Universum alt ist (13,8 Mrd. Jahre), wird eine Aufgabe von Tagen für eine einzelne Grafikkarte.

Was jeder einzelne Rateversuch kostet

Ein Angreifer kann eine Seed nicht „direkt“ testen. Jeder Kandidat muss die komplette Ableitung durchlaufen, bis eine Bitcoin-Adresse entsteht, die er mit der Blockchain abgleicht:



≈ 1 Mio./s

Seed-Kandidaten pro Sekunde auf einer RTX 5090 – der aktuell schnellsten Consumer-Grafikkarte.

So entsteht der Wert

1. Eine RTX 5090 schafft gemessen rund 9 Mrd. SHA-512-Berechnungen pro Sekunde (hashcat).
2. PBKDF2 mit 2.048 Runden kostet rund 4.096 davon je Kandidat → gut 2 Mio. Kandidaten/s.
3. BIP-32-Ableitung und Adressberechnung kommen hinzu → realistisch ≈ 1 Mio./s.

GRUNDLAGEN · LESEHILFE

So ist die Tabelle zu lesen

3 Angreifer

Von der einzelnen Grafikkarte (ca. 3.000 €) über einen Cluster aus 16 Karten bis zur Farm mit rund 1.000 Karten. Jede Stufe teilt die Zeit durch die Zahl der Karten.

½

Die Tabelle zeigt die Zeit für den gesamten Suchraum. Im Durchschnitt findet ein Angreifer die richtige Seed nach der Hälfte der angegebenen Zeit.

10 Bit ≈ × 1.000

Faustregel: Zehn Bit mehr Entropie verlängern die Suchzeit um rund das Tausendfache – zehn Bit weniger verkürzen sie entsprechend.

Farbskala



Lila und Rot: in Sekunden bis Wochen knackbar. Orange: mit großem Aufwand erreichbar. Gelb und Grün: mit heutiger Technik außer Reichweite.

Hintergrund: der Coldcard-Entropiefehler

März 2021

Umstellung auf eine neue Krypto-Bibliothek. Die Seed-Erzeugung nutzt danach unbemerkt einen deterministischen Software-Zufallsgenerator statt echter Hardware-Zufälligkeit.

März 2022

Mk4, Mk5 und Q mischen zusätzlich Bytes aus den beiden Secure Elements bei – das hebt sie über das Niveau der Mk3.

31.07.2026

Hotfix-Firmware 4.2.0 (Mk3), 5.6.0 (Mk4/Mk5) und 1.5.0Q. Coinkite rät: betroffene Seeds neu erzeugen, Guthaben umziehen.

≈ 40 Bit

Mk3 (Firmware 4.0.1 – 4.1.9)

≈ 72 Bit

Mk4 / Mk5 / Q – „möglicherweise nur“

128 Bit

Ziel laut Hersteller

COLDCARD · AUSWIRKUNG

Was das für Coldcard-Seeds bedeutet

Coldcard Mk3 · ≈ 40 Bit

13 Tage	eine RTX 5090
19 Std.	16 Grafikkarten
18 Min.	GPU-Farm

Mit einer einzigen Grafikkarte in rund zwei Wochen vollständig durchsuchbar – mit einer Farm in einer Viertelstunde. Diese Seeds sind als kompromittiert zu betrachten.

Mk4 / Mk5 / Q · ≈ 72 Bit

150 Mio. Jahre	eine RTX 5090
9,4 Mio. Jahre	16 Grafikkarten
150.000 Jahre	GPU-Farm

Heute nicht per Brute Force erreichbar – aber 56 Bit unter dem Ziel, nur geschätzt und bei besserem Angreiferwissen niedriger. Die Reserve für die Zukunft fehlt.

FAZIT

Was daraus folgt



Mk3-Seeds

Sofort ersetzen

Betroffene Seeds (Firmware 4.0.1 – 4.1.9) neu erzeugen – auf einem anderen Gerät – und das Guthaben auf die neue Seed umziehen.



Mk4 / Mk5 / Q

Geplant ersetzen

Seeds, die mit Firmware unter 5.6.0 bzw. 1.5.0Q erzeugt wurden, nach Herstellerempfehlung neu erzeugen und das Guthaben umziehen.



Eigenverwahrung

Entropie nie blind vertrauen

Eigene Zufälligkeit erzeugen oder beimischen (Würfel) und eine starke Passphrase nutzen. Korrekt erzeugte 128 Bit sind auf absehbare Zeit sicher.

Quellen und Annahmen

1. **Coinkite: Firmware-Seite mit Hotfix vom 31.07.2026**
   coldcard.com/firmware

2. **OneKey: Analyse des Coldcard-Entropiefehlers**
   onekey.so/blog

3. **Burner: Zeitlinie und Ursachen (2021 / 2022)**
   burner.pro/blog

4. **hashcat-Forum: RTX-5090-Benchmarks**
   hashcat.net/forum

Annahmen:

Prüfrate ≈ 1 Mio. Seed-Kandidaten/s je RTX 5090 (Größenordnung) · Farm ≈ 1.000 Grafikkarten · Zeiten für vollständige Suche · Jahr = 365,25 Tage · Coldcard-Werte = vorläufige Herstellerschätzungen, Stand Oktober 2026.