Quantencomputer und Bitcoin: Kann ein Quantenrechner die Blockchain knacken?

QUANTENCOMPUTER

Ende März 2026 veröffentlichte ein Team von Google Quantum AI, zusammen mit Forschern der Ethereum Foundation und der Stanford University, eine neue Schätzung. Ein ausreichend großer Quantencomputer könnte demnach den geheimen Schlüssel zu einer Bitcoin-Adresse in etwa neun Minuten berechnen, und dafür bräuchte er weniger als eine halbe Million Qubits [1]. Frühere Studien waren noch auf viele Millionen gekommen [2].

Heißt das, dass Bitcoin bald geknackt wird? Nein, aber die Frage ist ernster geworden. Hier steht, was ein Quantencomputer bei Bitcoin angreifen könnte, was nicht, und wie weit die Technik davon noch entfernt ist.

Dieser Artikel erklärt Technik. Er ist keine Anlageberatung und keine Empfehlung, Kryptowährungen zu kaufen oder zu verkaufen.

Wie Bitcoin geschützt ist

Bitcoin kennt keine Konten. Jeder Betrag ist mit einer Art kryptografischem Rätsel verschlossen, und nur wer den passenden privaten Schlüssel kennt, kann eine gültige digitale Unterschrift erzeugen und das Geld ausgeben [1]. Zu jedem privaten Schlüssel gehört ein öffentlicher Schlüssel. Aus dem privaten lässt sich der öffentliche leicht berechnen, umgekehrt ist das für heutige Computer praktisch unmöglich. Dahinter steckt ein mathematisches Problem auf sogenannten elliptischen Kurven, bei Bitcoin auf der Kurve secp256k1 [1].

Für einen Quantencomputer gilt das nicht. Der Algorithmus, den Peter Shor 1994 vorgestellt hat, kann genau solche Probleme effizient lösen. Ein großer, fehlerkorrigierter Quantencomputer könnte damit aus einem öffentlichen Schlüssel den privaten berechnen [1]. Wie Shors Algorithmus funktioniert, erklärt der Artikel über die Quantenalgorithmen.

Wie viele Qubits man bräuchte

Laut der neuen Google-Schätzung braucht Shors Algorithmus für die Bitcoin-Kurve höchstens 1200 logische Qubits und 90 Millionen sogenannte Toffoli-Gatter, oder 1450 logische Qubits und 70 Millionen Gatter. Logische Qubits sind fehlerkorrigierte Rechen-Qubits, die jeweils aus vielen physikalischen Qubits bestehen. Auf supraleitender Hardware mit einer Fehlerrate von 0,1 Prozent kämen die Forscher auf weniger als eine halbe Million physikalische Qubits und eine Rechenzeit von Minuten [1].

Zum Vergleich: Eine Studie von 2022 hatte unter ähnlichen Annahmen noch 13 Millionen physikalische Qubits für einen Angriff innerhalb eines Tages und 317 Millionen für einen Angriff innerhalb einer Stunde berechnet [2]. Der Chip Willow, den Google Ende 2024 vorstellte, hat 105 Qubits [3]. Bis zu einem Rechner, der Bitcoin gefährlich werden kann, fehlt also noch ein Faktor von mehreren Tausend (Abb. 1). Wie teuer heutige Quantencomputer sind, steht im Artikel Was kostet ein Quantencomputer?

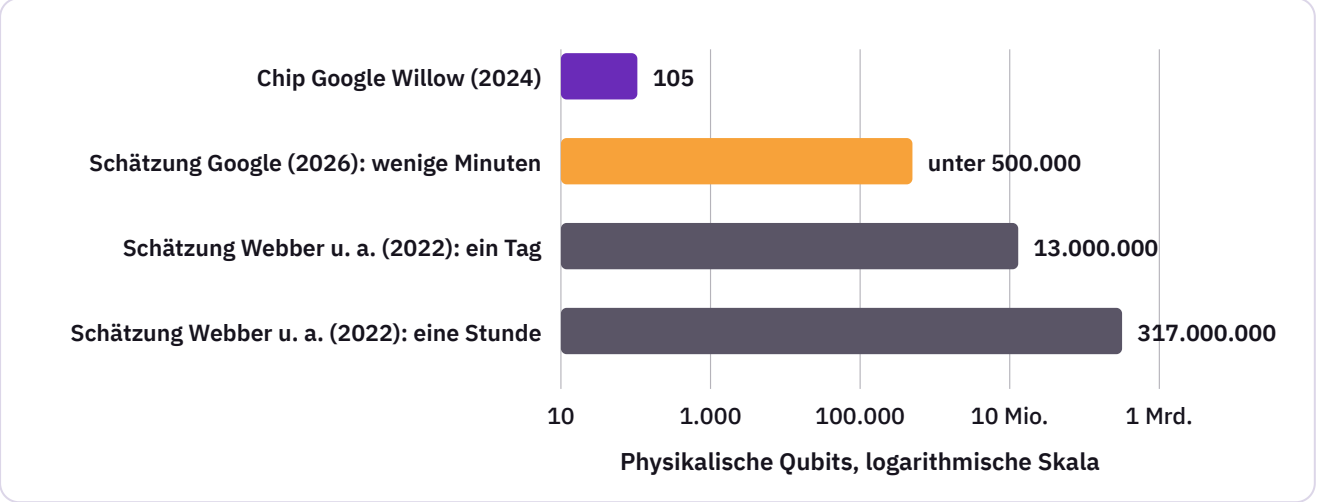

Abb. 1: Was heute existiert und was ein Angriff auf eine Bitcoin-Signatur bräuchte. Die Schätzungen gelten für supraleitende Qubits mit einer Fehlerrate von 0,1 Prozent. Werte nach [3],[1],[2].

Bemerkenswert ist, wie Google die Ergebnisse veröffentlicht hat. Um Angreifern keine Bauanleitung zu liefern, legten die Forscher die Schaltungen nicht offen, sondern belegten ihre Zahlen mit einem sogenannten Zero-Knowledge-Beweis. Damit lässt sich prüfen, dass die Angaben stimmen, ohne den Angriff selbst zu verraten [1].

Welche Bitcoin gefährdet wären

Entscheidend ist, ob der öffentliche Schlüssel schon sichtbar ist. Bei den ältesten Bitcoin-Adressen, dem Typ Pay-to-Public-Key, steht er offen in der Blockchain. Darauf liegen gut 1,7 Millionen Bitcoin,

fast 9 Prozent aller Bitcoin, darunter viele Belohnungen aus den Anfangsjahren des Netzes [1]. Ein Quantencomputer könnte diese Beträge in aller Ruhe angreifen, man spricht von At-Rest-Angriffen.

Bei den meisten neueren Adressen steht in der Blockchain nur ein Hashwert des öffentlichen Schlüssels, eine Art digitaler Fingerabdruck. Aus dem lässt sich der Schlüssel auch mit einem Quantencomputer nicht zurückrechnen. Sichtbar wird der öffentliche Schlüssel erst, wenn man Geld von der Adresse ausgibt [1]. Dann bleibt allerdings ein Zeitfenster: Bis die Transaktion in einem Block bestätigt ist, vergehen im Schnitt etwa zehn Minuten. Ein Quantenrechner, der den Schlüssel in rund neun Minuten berechnet, könnte in dieser Zeit eine eigene Transaktion dazwischenschieben. Google schätzt die Erfolgschance eines solchen On-Spend-Angriffs unter idealisierten Annahmen auf knapp 41 Prozent [1].

Ein besonderes Problem sind ruhende Bestände, deren Schlüssel verloren sind oder deren Besitzer sich nie mehr melden. Sie lassen sich nicht in sichere Adressen umziehen. Die Google-Studie beziffert die ruhenden, angreifbaren Bitcoin auf bis zu 2,3 Millionen und diskutiert, wie die Gemeinschaft und die Politik damit umgehen könnten [1].

Adresstyp	öffentlicher Schlüssel sichtbar	angreifbar
Pay-to-Public-Key (P2PK), sehr alt	immer	jederzeit und beim Ausgeben
Pay-to-Public-Key-Hash (P2PKH)	erst beim Ausgeben	nur beim Ausgeben
Pay-to-Script-Hash (P2SH)	erst beim Ausgeben	nur beim Ausgeben
Taproot (P2TR)	immer	jederzeit und beim Ausgeben

Wie verschiedene Bitcoin-Adresstypen einem künftigen Quantenangriff ausgesetzt wären, vereinfacht. Wird eine Adresse mehrfach verwendet, ist der Schlüssel nach dem ersten Ausgeben sichtbar. Quelle: [1].

Und das Mining?

Oft heißt es, Quantencomputer könnten auch das Bitcoin-Mining übernehmen. Das halten die Google-Forscher für unrealistisch. Für das Mining wäre der Algorithmus von Lov Grover zuständig, der aber nur einen kleinen Geschwindigkeitsvorteil bringt, und den fressen die Kosten der Fehlerkorrektur fast vollständig auf. Selbst unter der fantastischen Annahme, ein Quantenrechner schaffe eine Hash-Berechnung pro Mikrosekunde, käme er auf 0,25 Terahash pro Sekunde, mehr als hundertmal weniger als ein verbreitetes Mining-Gerät mit rund 110 Terahash [1].

Was gegen die Gefahr hilft

Die Lösung gibt es schon: Post-Quanten-Kryptografie. Das sind Verfahren, die auch ein Quantencomputer nach heutigem Wissen nicht knacken kann. Im August 2024 hat das

amerikanische Normungsinstitut NIST die ersten drei solchen Standards veröffentlicht [4]. Was dahintersteckt, erklärt der Artikel über die Post-Quanten-Kryptographie.

Für Bitcoin wird an einem Umstieg gearbeitet. Ein Entwurf namens BIP-360 schlägt etwa einen neuen Adresstyp vor, der den öffentlichen Schlüssel nicht mehr offenlegt. Gegen Angriffe beim Ausgeben schützt er noch nicht, dafür braucht es neue, quantensichere Signaturen [1]. Die Google-Forscher rufen alle betroffenen Kryptowährungen auf, den Wechsel ohne Verzögerung zu beginnen [1].

Fragen zu Quantencomputern und Bitcoin

Können Quantencomputer Bitcoin knacken?

Heute nicht. Ein Angriff bräuchte nach einer Schätzung von Google aus dem Jahr 2026 knapp eine halbe Million physikalische Qubits, der Google-Chip Willow hat 105. Ein ausreichend großer, fehlerkorrigierter Quantencomputer könnte aber aus einem öffentlichen Schlüssel den privaten berechnen.

Wie viele Qubits braucht man, um Bitcoin zu knacken?

Laut Google höchstens 1200 bis 1450 logische Qubits, auf supraleitender Hardware mit 0,1 Prozent Fehlerrate weniger als 500.000 physikalische Qubits. Eine Studie von 2022 kam noch auf 13 Millionen Qubits für einen Angriff innerhalb eines Tages.

Welche Bitcoin sind durch Quantencomputer gefährdet?

Vor allem Bitcoin auf Adressen, deren öffentlicher Schlüssel schon sichtbar ist. Das betrifft die ältesten Adressen mit gut 1,7 Millionen Bitcoin, Taproot-Adressen und mehrfach verwendete Adressen.

Können Quantencomputer Bitcoin minen?

Praktisch nicht. Der Vorteil des Grover-Algorithmus wird von der Fehlerkorrektur aufgezehrt, ein Quantenrechner wäre selbst unter sehr günstigen Annahmen langsamer als ein gewöhnliches Mining-Gerät.

Was ist Post-Quanten-Kryptografie?

Verschlüsselungs- und Signaturverfahren, die auch ein Quantencomputer nach heutigem Wissen nicht brechen kann. Die ersten drei Standards hat NIST im August 2024 veröffentlicht.

Quellen

1. R. Babbush, A. Zalcman, C. Gidney u. a.: *Securing Elliptic Curve Cryptocurrencies against Quantum Vulnerabilities: Resource Estimates and Mitigations.* Google Quantum AI, Whitepaper, 30. März 2026, quantumai.google (PDF).
2. M. Webber, V. Elfving, S. Weidt, W. K. Hensinger: *The impact of hardware specifications on reaching quantum advantage in the fault tolerant regime.* In: AVS Quantum Science 4 (2022), 013801, doi:10.1116/5.0073075.
3. H. Neven: *Meet Willow, our state-of-the-art quantum chip.* Google Blog, 9. Dezember 2024, blog.google.
4. NIST: *NIST Releases First 3 Finalized Post-Quantum Encryption Standards.* 13. August 2024, nist.gov.

Zitiervorschlag

```
quanten.de: Quantencomputer und Bitcoin: Kann ein Quantenrechner die Blockchain knacken? Stand: November 2026. URL: https://quanten.de/quantencomputer_bitcoin.html
```


Texte und Abbildungen © 2026 quanten.de. Nutzung mit Quellenangabe und Link gern, kommerzielle Nutzung nach Absprache: info@quanten.de

Weiterlesen: Quantencomputer · Shor und Grover · Post-Quanten-Kryptographie · Was kostet ein Quantencomputer?