Deutscher Bundestag **Drucksache 21/928**

21. Wahlperiode 17.07.2025

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Edgar Naujok, Ruben Rupp, Robin Jünger, weiterer Abgeordneter und der Fraktion der AfD
– Drucksache 21/765 –

Aktuelle und zukünftige Sicherheitsrisiken für Bestände an Kryptowährungen durch Quantencomputer und Hackergruppen

Vorbemerkung der Fragesteller

Laut Berichterstattung vom 18. Mai 2025 wurde durch den Vermögensverwalter BlackRock vor möglichen Gefahren für Kryptowährungen durch Quantencomputer gewarnt. So könne es die fortschreitende Entwicklung dieser Technologie Hackern ermöglichen, die derzeitige Verschlüsselung von Kryptowährungen auf der Blockchain zu überwinden und somit potenziell erhebliche finanzielle Schäden verursachen (vgl. www.telepolis.de/features/Kryptowaehrungen-Werden-Hacker-bald-reich-10387395.html). Ebenso ist Anfang Juni 2025 aus einer Studie des Unternehmens Google hervorgegangen, dass Quantencomputer erheblich früher als gemeinhin angenommen RSA- und Bitcoin-Verschlüsselungen zu bedrohen imstande seien (vgl. www.finanzen.net/nachricht/devisen/quantenressourcen-im-blick-google-studie-quantencomputer-bedrohen-rsa-und-bitcoin-verschluesselung-frueher-als-gedacht-14532698). Zudem wurde bekannt, dass die nordkoreanische Hackergruppe „Lazarus“ im Februar 2025 Kryptowährungen im Wert von 1,46 Mrd. US-Dollar von der Börse „Bybit“ entwendet habe (de.investing.com/news/cryptocurrency-news/bybit-erleidet-massiven-hack-uber-146-milliarden-usdollar-in-ethereum-entwendet-93CH-2886434).

Im Zusammenhang mit der Dechiffrierung durch Quantencomputer hat sich u. a. in Hackergruppen eine „Store Now, Decrypte Later“-Strategie etabliert, wobei immense Datenmengen systematisch vorrätig gesammelt und erst später dechiffriert werden (www.keyfactor.com/de/blog/harvest-now-decrypt-later-a-new-form-of-attack/).

Im März 2025 hatte das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Technische Richtlinie TR-02102-1 mit Empfehlungen und Schlüssellängen zu kryptografischen Verfahren veröffentlicht (www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile&v=13). Ausgewiesenes Ziel der Bundesregierung ist es, bis 2026 eine Strategie zur Migration zu Post-Quanten-Kryptografie in Deutschland vorzulegen (vgl. Antwort der Bundesregierung auf die Kleine Anfrage auf Bundestagsdrucksache 20/8104).

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 17. Juli 2025 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

Aus Sicht der Fragesteller zeigen die genannten Vorfälle eine zunehmende Bedrohung durch Hackergruppen sowie fortschreitende Dechiffrierungsmöglichkeit im Zusammenhang mit der Quantentechnologie für die Sicherheit digitaler Vermögenswerte.

1. Sind der Bundesregierung die aktuellen Warnungen vor Sicherheitsrisiken für Kryptowährungen durch die Entwicklung von Quantencomputern bekannt, und wenn ja, hat sie sich dazu im Hinblick auf Vermögenswerte deutscher Privatpersonen sowie privatrechtlicher und öffentlicher Unternehmen und Institutionen (siehe Vorbemerkung der Fragesteller) eine eigene Auffassung gebildet, und wenn ja, wie lautet diese Auffassung?

Das Bundesamt für die Sicherheit in der Informationstechnik (BSI) hat bereits in seinem 2019 erschienenen Leitfaden „Blockchain sicher gestalten“ auf die Sicherheitsrisiken für Blockchains durch die Entwicklung von kryptografisch relevanten Quantencomputern hingewiesen und die aus BSI-Sicht zentralen „Eckpunkte für den sicheren Betrieb einer DLT-basierten Kryptowährung“ in einem Papier zusammengefasst. Die Sicherheitsrisiken für Kryptowährungen, stimmen mit den Risiken aller Systeme, die asymmetrische Kryptografie verwenden, überein. Die Auffassung zum Risiko durch Quantencomputer des BSI im Allgemeinen ist, dass es sich um ein sehr ernst zu nehmendes Risiko handelt. Diesem Risiko begegnet das BSI, indem über die Bedrohung und die Notwendigkeit zur Migration auf quantensichere Kryptografie informiert und die Migration vorangetrieben wird. Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) beobachtet im Rahmen ihres Aufsichtsmandates die Entwicklungen im Bereich Kryptowerte und Quantencomputing und nimmt mögliche Gefährdungen der Cybersicherheit sehr ernst.

Zusätzlich wird auf die Vorbemerkung der Bundesregierung zur Kleinen Anfrage des Abgeordneten Edgar Naujok der Fraktion der AfD auf Bundestagsdrucksache 20/8104 verwiesen.

2. Beabsichtigt die Bundesregierung, gezielte Maßnahmen zu ergreifen, um die Sicherheit von Kryptowährungen gegenüber Angriffen durch Quantencomputer zu gewährleisten, und wenn ja, welche sind dies, und innerhalb welchen Zeitraums sollen diese zur Umsetzung kommen?

Die Bundesregierung prüft fortlaufend Maßnahmen zur Gewährung der Sicherheit von Kryptowerten gegenüber Angriffen mit Quantencomputern.

Im Übrigen wird auf den Leitfaden des BSI (vgl. Antwort zu Frage 1) im Hinblick auf die dort erwähnten Maßnahmen verwiesen.

3. Hat die Bundesregierung Erkenntnisse zu spezifischen gegenwärtigen und sich abzeichnenden Bedrohungslagen durch Hackergruppen und bzw. oder Quantentechnologie für deutsche Vermögenswerte, und wenn ja, welche sind dies?

9. Hat die Bundesregierung Erkenntnisse zu aus- und inländischen Hackergruppen, welche eine potenzielle Bedrohung für deutsche Investoren in Kryptowährungen darstellen, und wenn ja, welche sind dies?

Die Fragen 3 und 9 werden gemeinsam beantwortet.

Insbesondere nordkoreanische Cyberakteure setzen ihre Angriffsoperationen gezielt zur Devisenbeschaffung ein, um das stark sanktionierte Regime und sein Nuklearprogramm zu finanzieren. In der Vergangenheit wurden umgerech-

net Hunderte Mio. Euro an Kryptowährungen durch nordkoreanische Hackergruppen erbeutet. Die diesbezügliche Bedrohungslage ist insofern anhaltend hoch. Deutsche Kryptowährungsbörsen oder Unternehmen sind grundsätzlich einer abstrakten Gefahr ausgesetzt. Beispielhaft für erfolgreiche, nordkoreanische Cyberoperationen sind der 2022 erfolgte Angriff auf das Krypto-Spiel „Axie Infinity“, bei dem 625 Mio. US-Dollar (zum Zeitpunkt des Diebstahls) in der Kryptowährung Ethereum entwendet wurden. Ein weiteres Beispiel ist der 2024 erfolgte Angriff auf die Kryptobörse Bybit mit Sitz in Dubai. Dabei wurden umgerechnet 1,5 Mrd. US-Dollar in der Kryptowährung Ethereum erbeutet.

Eine grundsätzliche Gefährdung ergibt sich zudem im perspektivischen Einsatz von Quantencomputing zur Entschlüsselung von chiffrierten Daten, bspw. im Kommunikationsverkehr. Sollte perspektivisch die Quantentechnologie soweit gebräuchlich entwickelt sein, könnten die heutigen Standardverschlüsselungsverfahren dadurch teilweise aufgebrochen und damit in dem Umfang obsolet werden. Die langfristige Sicherstellung der Vertraulichkeit von Daten wäre so nicht mehr vollumfänglich zu gewährleisten.

Bzgl. gegenwärtiger Bedrohungslagen durch Hackergruppierungen wird zusätzlich auf das jährlich durch das Bundeskriminalamt veröffentlichte Bundeslagebild Cybercrime und monatlichen Ausführungen zur IT-Sicherheitslage des BSI verwiesen.

4. Sieht die Bundesregierung Handlungsbedarf bei der Regulierung und Überwachung von Kryptowährungsbörsen, um mögliche Sicherheitslücken zu schließen und den Schutz der Anleger zu gewährleisten, und wenn ja, inwieweit?

Die Cybersicherheit von Kryptobörsen wird durch verschiedene europäische Verordnungen geregelt, u. a. die MiCA-VO (Markets in Crypto Assets) und die DORA-VO (Digital Operational Resilience Act). Die Vorschriften erfassen auch Risiken durch Angriffe mit Quantencomputern. Die BaFin wendet diese Regelungen und die nationalen Umsetzungsvorschriften im Rahmen ihrer Aufsicht an. Insofern besteht kein unmittelbar zusätzlicher Handlungsbedarf.

5. Wie weit ist die Erstellung einer Strategie der Bundesregierung zur Migration zur Post-Quanten-Kryptografie, welche bis 2026 erstellt werden soll (siehe Vorbemerkung der Fragesteller), gegenwärtig fortgeschritten?

Ende Juni dieses Jahres wurde von der EU-Kommission eine „Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography“ veröffentlicht, die von den EU-Mitgliedstaaten im Rahmen der NIS-Kooperationsgruppe erarbeitet wurde. Die Bundesregierung war gemeinsam mit den Regierungen Frankreichs und Niederlande federführend an der Erstellung dieser Strategie beteiligt. Aus dieser Roadmap ist die Ableitung zu einer nationalen Roadmap zur Umstellung auf Post-Quanten-Kryptografie avisiert. Zum jetzigen Zeitpunkt kann zu diesem Prozess noch keine weitere Aussage getroffen werden.

6. Wird die Strategie der Bundesregierung zur Migration zur Post-Quanten-Kryptografie gezielt der potenziellen Gefahr für Kryptowährungen Rechnung tragen, und wenn ja, inwiefern, und welche Handlungsmöglichkeiten sollen ggf. dafür herangezogen werden?

Die in der Antwort zu Frage 5 genannte EU-Roadmap macht allgemeine Empfehlungen zur Umstellung auf Post-Quanten-Kryptografie, keine speziellen Empfehlungen für einzelne Anwendungen. Dies wird ggfs. in weiteren Versionen der Roadmap weiter ausgearbeitet. Eine deutsche Strategie wird sich hierbei an der EU-Roadmap orientieren.

Mit der Richtlinie „Post-Quanten-Kryptografie in die Anwendungen bringen“, veröffentlicht im Bundesanzeiger vom 30. Dezember 2022, unterstützt die Bundesregierung außerdem im Rahmen des Forschungsrahmenprogrammes zur IT-Sicherheit „Digital.Sicher.Souverän.“ und der „Agenda Cybersicherheitsforschung“ die Migration zur Post-Quanten-Kryptografie.

7. Befassen sich derzeit Behörden des Bundes mit der Analyse von Gefahren für deutsche Investoren in Kryptowährungen und Hackergruppen, und wenn ja, welche, und welche Kapazitäten werden dafür aufgewendet (bitte ggf. aufschlüsseln)?

Cyberangriffe richten sich nicht nur gegen staatliche Stellen, sondern auch gezielt gegen Unternehmen aus den unterschiedlichsten Bereichen wie dem Kryptowährungssektor. Die Aufklärung von Cyberangriffen und der Schutz deutscher Stellen vor Ausspähung und Sabotage ist zentrale Aufgabe der sicherheitsbehördlichen Cyberabwehr. Dies schließt auch solche Cyberangriffe ein, die einem staatlichen Akteur zugeordnet werden können und sich gegen Unternehmen aus dem Kryptowährungssektor richten. Die Cyberabwehrbehörden analysieren hierfür die Angriffe und ordnen sie einem Profil zu, das sowohl die technischen Fähigkeiten als auch die sozio-politischen Interessen der staatlichen Angreifer (mit)einbezieht. Die dafür eingesetzten personellen und technischen Kapazitäten variieren im Einzelfall je nach fallspezifischem Informationsaufkommen und ggfs. vorhandenen Ansatzpunkten für den Einsatz informationserhärtender Maßnahmen bzw. nachrichtendienstlicher Mittel. Da viele zentrale Technologien und Sicherheitslösungen in der Privatwirtschaft entwickelt werden, kommt ihr ebenfalls eine entscheidende Rolle in der Cyberabwehr zu. Im Rahmen ihres Aufsichtsmandates analysiert die BaFin ebenfalls laufend Risiken für den deutschen Finanzmarkt.

8. Sind Behörden des Bundes bei der Analyse von Gefahren für deutsche Investoren in Kryptowährungen und Hackergruppen auf europäische und internationale Zusammenarbeit angewiesen, und wenn ja, inwiefern?

Staatliche Cyberakteure profitieren von der globalen Vernetzung, verfügen über enorme Ressourcen, eine hohe technische Expertise und verfolgen langfristige Angriffsstrategien. Die Zukunft einer erfolgreichen Cyberabwehr hängt daher maßgeblich von einer erfolgreichen internationalen Zusammenarbeit ab. Sei es bei der Entwicklung neuer Schutzmechanismen, der Identifikation und Schließung von Schwachstellen oder der Abwehr akuter Bedrohungen.

Die Bundesregierung arbeitet daher mit einer Vielzahl europäischer und internationaler Partner zusammen, um Gefährdungen der Cybersicherheit von Kryptowerten und durch Hackergruppen zu begegnen. Die Bundesregierung kooperiert u. a. mit anderen EU-Mitgliedstaaten, mit den G7-Partnern und bilateral mit weiteren Staaten. Die Zusammenarbeit umfasst u. a. den Austausch von Informationen und best practices.

Auch auf Ebene der Sicherheitsbehörden erfolgt eine konstruktive und enge Zusammenarbeit mit zahlreichen Behörden auf europäischer und internationaler Ebene. In der Vergangenheit wurden u. a. regelmäßig Sicherheitshinweise zu Cyberaktivitäten (Joint Cybersecurity Advisories [JCSA]) gemeinsam mit internationalen Partnern veröffentlicht, um vor aktuellen Cyberbedrohungen zu warnen. Die darin aufgeführten Erkenntnisse zu Schwachstellen, Angriffsarten oder Aktivitäten von Cyberakteuren ermöglichen es den Betroffenen, präventive Maßnahmen zu ergreifen, etwaige Angriffe abzuwehren und mögliche Schäden zu begrenzen.

10. Wie bewertet die Bundesregierung die vom BSI empfohlene hybride Nutzung klassischer und quantensicherer Verfahren zum Schutz vor dem sogenannten „Store Now, Decrypte Later“-Szenario (vgl. Vorbemerkung der Fragesteller) im Kontext von Kryptowährungen?

Hybride Ansätze, die sowohl klassische als auch quantenresistente Algorithmen kombinieren, sind eine sinnvolle Übergangslösung, bis quantenresistente Verfahren vollständig etabliert sind. Die Bundesregierung bewertet daher generell die Nutzung von hybriden kryptografischen Verfahren als wichtigen Schritt hin zu sicheren und agilen kryptografischen Infrastrukturen, somit auch bei Kryptowährungen. Um sich vor diesem Szenario zu schützen, wird intensiv an Post-Quanten-Kryptografie geforscht, die auch gegen Angriffe von Quantencomputern resistent sind. Das BSI hat zudem bereits im Dezember 2021 den Leitfaden Kryptografie quantensicher gestalten veröffentlicht. Dieser aktualisiert die im April 2020 veröffentlichten Handlungsempfehlungen für die „Migration zu Post-Quanten-Kryptografie“, ergänzt sie und ordnet sie durch eine ausführliche Darstellung der Hintergründe ein.

11. Prüft die Bundesregierung derzeit die Einführung gesetzlicher Mindestanforderungen an kryptografische Verfahren für Betreiber von Kryptowährungsbörsen, Wallet-Anbietern oder Smart-Contract-Plattformen im Hinblick auf die Post-Quanten-Sicherheit, und wenn ja, inwiefern, und in welchem regulatorischen Rahmen sollen diese ggf. umgesetzt werden (z. B. Bundesanstalt für Finanzdienstleistungsaufsich (BaFin), EU-MiCA (Markets in Crypto-Assets Regulation), IT-Sicherheitsgesetz)?

Es wird auf die Antworten zu den Fragen 1 und 2 verwiesen.

12. Beabsichtigt die Bundesregierung, Maßnahmen zu ergreifen, um Betreiber von Kryptowährungsbörsen und Wallet-Dienstleistern bei der Migration zu quantensicheren Kryptoverfahren zu unterstützen – insbesondere hinsichtlich der in TR-02102-1 empfohlenen Verfahren, und wenn ja, welche sind dies, und innerhalb welchen Zeitraums sollen diese durchgeführt werden?

Die Bundesregierung sensibilisiert die Finanzmarktteilnehmer regelmäßig für die Herausforderungen des Quantencomputings, insbesondere im Hinblick auf die Cybersicherheit. So hat der Präsident der BaFin mehrfach auf die notwendige Beschäftigung der Finanzindustrie mit der Gefährdung von Verschlüsselungstechniken durch Quantencomputing hingewiesen. Das BSI hat die Weiterentwicklung der Kryptobibliothek Botan unterstützt und damit allgemein die Verfügbarkeit sicher implementierter Post-Quanten-Algorithmen verbessert. Die Bibliothek ist Open Source und steht damit jedem – Betreibern von Kryptowährungsbörsen und Wallet-Dienstleistern eingeschlossen – zur freien Verfügung.

Im Übrigen wird auf die Antwort zu Frage 2 verwiesen.

13. Plant die Bundesregierung, die in TR-02102-1 genannten quantensicheren Verfahren in nationale Standards für Finanzdienstleister zu integrieren, und wenn ja, inwieweit?

Die relevanten Vorgaben sind weitgehend auf EU-Ebene geregelt (insbesondere DORA-VO). Sollte sich Anpassungsbedarf nationaler Vorschriften zeigen, wird die Bundesregierung geeignete Maßnahmen prüfen.

14. Welche gezielten Strategien verfolgt die Bundesregierung, um sicherzustellen, dass deutsche Kryptowährungsinfrastrukturen bis spätestens 2030 auf quantensichere Kryptografie umgestellt sind, wie es in der TR-02102-1 empfohlen wird?

Es wird auf die Antworten zu den Fragen 2 und 5 verwiesen.

15. Wie unterstützt die Bundesregierung ggf. die Forschung und Entwicklung von quantensicheren Kryptoverfahren, insbesondere im Hinblick auf deren Anwendung in der Blockchain-Technologie und bei Kryptowährungen?

Die Bundesregierung fördert die Erforschung und Entwicklung der Post-Quanten-Kryptografie und der Quantenkommunikation im Rahmen des Forschungsrahmenprogramms der Bundesregierung zur IT-Sicherheit „Digital.Sicher.Souverän.“ und der „Agenda Cybersicherheitsforschung“.

Die Richtlinien „Post-Quanten-Kryptografie in die Anwendungen bringen“, Bundesanzeiger vom 30. Dezember 2022, „Sicherer Einsatz von Quanten-kommunikation in der Anwendung“, Bundesanzeiger vom 30. Dezember 2022, „Transfer und Netzintegration der Quantenkommunikation“, Bundesanzeiger vom 16. Januar 2025, befinden sich dazu in Umsetzung. Zwei der laufenden Vorhaben adressieren Anwendungen im Finanzsektor. Das BSI hat zudem in der Vergangenheit die Implementierungssicherheit von Blockchain-Anwendungen in einer Studie untersucht.

16. Welche Erkenntnisse hat die Bundesregierung ggf. über die aktuelle Implementierung quantensicherer Kryptografie in bestehenden Kryptowährungsnetzwerken, und wie wird ggf. deren Wirksamkeit bewertet?

Der Bundesregierung liegen keine Erkenntnisse zur Implementierung quantensicherer Kryptographie in bestehenden „Kryptowährungsnetzwerken“ vor.

17. Beabsichtigt die Bundesregierung, die Empfehlungen der TR-02102-1 in internationale Kooperationen und Standards einzubringen, um eine globale Sicherheit von deutschen Investoren in Kryptowährungen gegenüber Quantencomputern zu gewährleisten, und wenn ja, in welcher Weise, und innerhalb welchen Zeitraums?

Das BSI orientiert sich auf Basis eigener Sicherheitsuntersuchungen bei den Empfehlungen in der TR-02102-1 an internationalen Standards und wirkt auch als Editor von Standards, um Interoperabilität zu ermöglichen. Insofern ist eine gewisse Harmonisierung mit internationalen Standards bereits gewährleistet.

Im Übrigen wird auf die Antworten zu den Fragen 1 und 2 verwiesen.

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.bundesanzeiger-verlag.de
ISSN 0722-8333