Deutscher Bundestag **Drucksache 21/765**

21. Wahlperiode 07.07.2025

Kleine Anfrage

der Abgeordneten Edgar Naujok, Ruben Rupp, Robin Jünger, Alexander Arpaschi, Sebastian Maack, Lars Haise, Tobias Ebenberger, Thomas Ladzinski, Kay Gottschalk, Jörn König, Christian Douglas, Hauke Finger, Rainer Groß, Reinhard Mixl, Iris Nieland, Diana Zimmer, Thomas Korell und der Fraktion der AfD

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

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).

Aus Sicht der Fragesteller zeigen die genannten Vorfälle eine zunehmende Bedrohung durch Hackergruppen sowie fortschreitende Dechiffrierungsmöglich-

keit im Zusammenhang mit der Quantentechnologie für die Sicherheit digitaler Vermögenswerte.

Wir fragen die Bundesregierung:

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?
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?
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?
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?
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?
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?
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)?
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?
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?
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?
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)?

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?
13. Plant die Bundesregierung, die in TR-02102-1 genannten quantensicheren Verfahren in nationale Standards für Finanzdienstleister zu integrieren, und wenn ja, inwieweit?
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?
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?
16. Welche Erkenntnisse hat die Bundesregierung ggf. über die aktuelle Implementierung quantensicherer Kryptografie in bestehenden Kryptowährungsnetzwerken, und wie wird ggf. deren Wirksamkeit bewertet?
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?

Berlin, den 3. Juli 2025

Dr. Alice Weidel, Tino Chrupalla und Fraktion

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