Bundesamt
für Sicherheit in der
Informationstechnik

Blockchain sicher gestalten – Eckpunkte des BSI

Version 2.0

Mit Blockchain entwickelt sich momentan eine neue Technologie für die dezentrale, manipulationssichere und konsensuale Datenhaltung in verteilten Netzwerken, der großes Potenzial in nahezu allen Wirtschaftsbereichen wie auch im öffentlichen Sektor zugeschrieben wird.
Das Vertrauen im System wird nicht mehr (allein) durch die Autorität einer zentralen Stelle, sondern durch den Einsatz kryptografischer Mechanismen hergestellt.
Viele Akteure aus Forschung, Wirtschaft und Verwaltung beschäftigen sich intensiv mit dem Thema Blockchain. Es gibt eine große Zahl von möglichen Anwendungen, die sich allerdings oft noch in der Konzeptions- oder Pilotphase befinden. Aktuell schon eingesetzte Blockchain-Lösungen finden sich hauptsächlich im Finanzbereich, z.B. Kryptowährungen.
Für eine flächendeckende und langfristige Etablierung der Blockchain-Technologie in einem breiten Anwendungsspektrum sind noch eine Reihe von sicherheitstechnischen, regulatorischen, rechtlichen und soziotechnischen Fragen zu klären. Erste Ansätze dazu, z.B. bei der ISO-Standardisierung, gibt es bereits.
Für das BSI als die nationale Cybersicherheitsbehörde stehen die technisch-gestalterischen Aspekte von Blockchain mit Bezug zur IT-Sicherheit im Vordergrund:

- **Blockchain allein löst keine IT-Sicherheitsprobleme.** Die Zielcharakteristika von Blockchain wie Unveränderbarkeit, Nachvollziehbarkeit und Dezentralität sowie die starke kryptografische Fundierung können sich grundsätzlich positiv auf die Sicherheitseigenschaften von IT-Lösungen auswirken, es muss aber gleichzeitig die Sicherheit der verwendeten Hard- und Software sowie der zu Grunde liegenden Protokolle gewährleistet werden. Ebenso ist die Sicherheit von externen Schnittstellen der Blockchain, insbesondere für das authentische Einfügen oder Auslesen von Daten, zu beachten. Eine vertrauenswürdige zentrale Stelle wird auch beim Einsatz von Blockchains in vielen Anwendungen nicht vollständig überflüssig werden.
- **Die Wahl des passenden Blockchain-Modells ist wichtig.** Je nach Anwendung muss ein geeigneter Konsensmechanismus zur Herstellung einer Einigkeit über den korrekten Zustand der Blockchain gewählt werden. Außerdem kann sowohl der Zugang zum Netzwerk (unpermissioned – permissioned) als auch der Zugriff auf die Daten (public – private) sowie ein allgemeines Rollen- und Rechtemanagement individuell definiert werden. Die bei Bitcoin verwendete „unpermissioned public“ Blockchain mit „Proof-of-Work“-Konsens ist dabei für viele Anwendungen ungeeignet.
- **Bei der Konstruktion von Blockchains müssen Sicherheitsaspekte frühzeitig berücksichtigt werden.** Entsprechend den angestrebten Sicherheitszielen sind Aspekte wie Vertraulichkeit, Integrität und Authentizität der Transaktionsdaten, die sichere Ausführung von Smart Contracts und das Identitätsmanagement der Nutzer passend zu modellieren und in der Blockchain umzusetzen. Insbesondere Vertraulichkeit ist bei Blockchain-Anwendungen ein anspruchsvolles Ziel. Bei der Auswahl von Algorithmen und Protokollen sollte man sich nach den Vorgaben des BSI richten.

- **Sensible Daten mit langfristigem Schutzbedarf müssen in einer Blockchain besonders geschützt werden.** Aufgrund der langen Verfügbarkeit (bei gleichzeitig potenziell hoher Sensibilität) von Daten in der Blockchain stellt die Erreichung von Langzeitsicherheit eine besondere Herausforderung dar. Es ist sicher zu stellen, dass die Sicherheitsmechanismen der Blockchain bei Bedarf ausgetauscht werden können. Dabei sind insbesondere Anforderungen, die sich aus der Gefährdung durch potenzielle Quantencomputer und technische Fortschritte in der Kryptoanalyse ergeben, zu beachten.
- **Einheitliche Sicherheitsniveaus für Blockchains müssen definiert und durchgesetzt werden.** Die Standardisierung von Blockchains muss weiter vorangetrieben werden und dabei die Aspekte der IT-Sicherheit angemessen berücksichtigen. Auch eine Sicherheitszertifizierung ausgewählter Komponenten nach allgemein anerkannten Kriterien kann für bestimmte Anwendungen sinnvoll sein. Bei Blockchains, die transnational betrieben werden, ist eine internationale Abstimmung erforderlich. Das BSI wird die Entwicklung der Blockchain-Technologie weiter beobachten und fachgerecht bewerten und im Rahmen seiner Zuständigkeiten an Empfehlungen und Anforderungen für Sicherheitsmechanismen von Blockchains mitwirken.

Bundesamt für Sicherheit in der Informationstechnik – BSI
Godesberger Allee 185 - 189
53175 Bonn
Tel.: +49 (0) 228 99 9582-0
E-Mail: blockchain@bsi.bund.de
Internet: www.bsi.bund.de