Sicherheit und Vertrauenswürdigkeit kryptografisch verketteter Datenblöcke

Blockchain-Technologie unter der Lupe

Die Blockchain-Technologie ist eine spannende und faszinierende IT-Technologie, die das Potenzial hat, Politik, Verwaltung und Wirtschaftszweige zu revolutionieren. Sie ist eine Querschnittstechnologie mit hohem disruptiven Potenzial für viele Wirtschaftsbereiche und bietet kooperative Vertrauensdienste. Die Blockchain-basierten Systeme könnten in vielen Bereichen zentrale Instanzen wie Treuhänder, Banken oder Notare, ablösen. Das ist möglich, weil die verteilten Konsensfindungs- und Validierungsverfahren der Blockchain-Technologie ganz ohne solche Intermediäre die Vertrauenswürdigkeit und Sicherheit der aufgezeichneten Transaktionsdaten garantieren.

Bei einem zentralen herkömmlichen Transaktionsspeicher wird die Zusammenarbeit oder das Eigentum von digitalen Werten durch eine zentrale Instanz oder einen Treuhänder verwaltet und verifiziert. Beispiel einer zentralen Instanz ist eine Public-Key-Infrastruktur (PKI) und ein Treuhänder, ein Notar, der die Abwicklung eines Vertrages kontrolliert und verwaltet. In einem dezentralen Blockchain-Transaktionsspeicher wird die Zusammenarbeit oder das Eigentum von digitalen Werten durch die Nodes eines Peer-to-Peer Netzwerkes mit Hilfe von smarten IT-Sicherheits- und Vertrauenswürdigkeitsmechanismen verwaltet und verifiziert. Daher ist keine kostenaufwendige zentrale Instanz notwendig. In den Abbildungen 1 und 2 werden eine herkömmliche zentrale Architektur und die dezentrale Blockchain-Architektur von Transaktionsspeichern dargestellt.

Unterschiedliche Sichtweisen auf die Blockchain-Technologie

Die verschiedenen Disziplinen können die Blockchain-Technologie aus sehr unterschiedlichen Blickwinkeln betrachten und bewerten. Für einen Informatiker etwa produziert die Blockchain-Technologie eine einfache Datenstruktur, die Blockchain, die Daten als Transaktionen in einzelnen Blöcken verkettet und in einem verteilten Peer-to-Peer-Netz redundant verwaltet. Die Alternative wäre eine konventionelle Datenbank, die kontinuierlich von allen Teilnehmern repliziert wird.

Für IT-Sicherheitsexperten hat die Blockchain-Technologie den Vorteil, dass die Daten als Transaktionen in den einzelnen Blöcken manipulationssicher gespeichert werden können, das heißt, die Teilnehmer der Blockchain sind in der Lage, die Echtheit, den Ursprung und die Unversehrtheit der gespeicherten Daten zu überprüfen. Die Alternative wäre hier zum Beispiel ein PKI-System als zentraler Vertrauensdienstanbieter.

Für den Anwendungsdesigner bedeutet die Nutzung der Blockchain-Technologie eine vertrauenswürdige Zusammenarbeit zwischen verschiedenen Organisationen, ohne die Einbindung einer zentralen Instanz, eines PKI-Systems, eines Notars etc. Die Alternative könnte hier ein kostenintensiver Treuhänder sein, der die Zusammenarbeit und Eigentumsübertragung zwischen den verschiedenen Organisationen verwaltet und verifiziert. Da die Blockchain-Technologie dies automatisiert macht, werden durch die vertrauenswürdige Zusammenarbeit die Prozesse auch sehr viel schneller und effek-

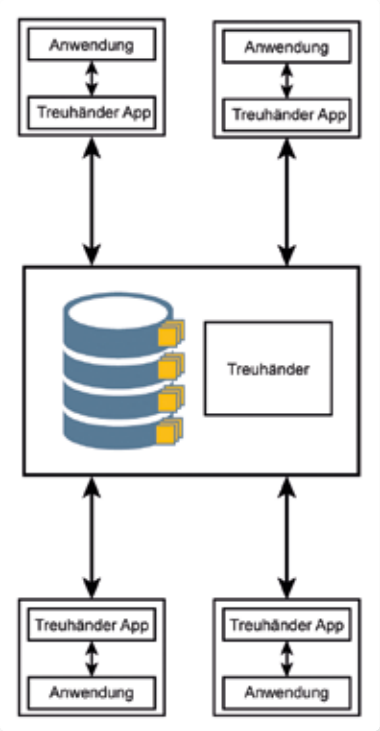

Abb. 1: Herkömmliche zentrale Architektur

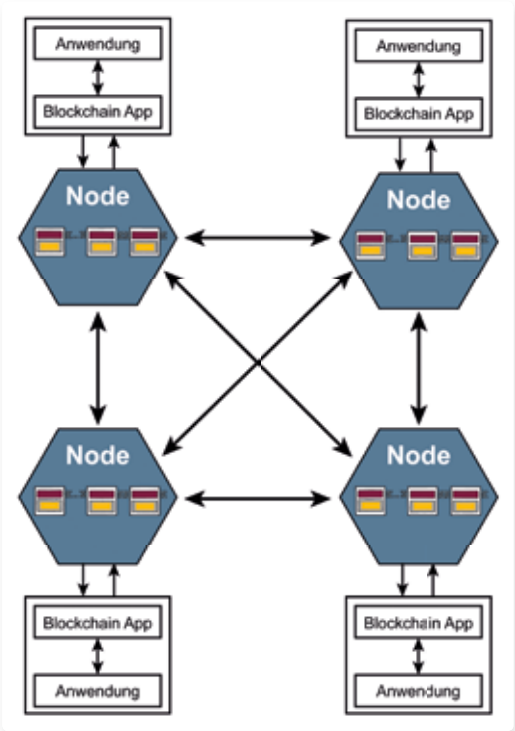

Abb. 2: Dezentrale Blockchain-Architektur

tiver. Dies ist ein wichtiger Aspekt für die Nutzung der Blockchain-Technologie in den verschiedenen Anwendungsfeldern.[1]

Die Blockchain-Technologie als Kollaborations-Tool

Grundsätzlich wird mit der Blockchain-Technologie eine verschlüsselte Kette vernetzter Datenblöcke erzeugt. In diesen fälschungssicheren, verteilten und redundanten Datenstrukturen sind alle Transaktionen in der Zeitfolge protokolliert nachvollziehbar, unveränderlich und ohne zentrale Instanz abgebildet. Die Sicherheitseigenschaften werden prinzipiell mit den folgenden Mechanismen umgesetzt:

- „fälschungssicher" mithilfe von One-Way-Hash-Funktionen und digitalen Signaturen von Public-Key-Verfahren
- „verteilte, redundante Datenstrukturen", viele Nodes des Peer-to-Peer-Netzwerkes haben die Daten in der Blockchain verteilt und redundant gespeichert
- „Transaktionen in der Zeitfolge protokolliert nachvollziehbar, unveränderlich", wird durch die Art der Verkettung mithilfe der Hash-Werte HashPrev und den Merkle Hash über die Daten in den Transaktionen sichergestellt
- „ohne zentrale Instanz", wird durch geeignete verteilte Vertrauenswürdigkeitsverfahren, wie verteilte Konsensfindungsverfahren und verteilte Validierungsprozesse erzielt.

Datenstruktur, Aufbau und Zusammenhänge einer Blockchain

Mit der Blockchain-Technologie wird eine gemeinsame Blockchain für alle Blockchain-Teilnehmer erzeugt, die eine einfache Datenstruktur darstellt.

Die Daten (gelbe Quadrate in Abbildung 3) werden in der Blockchain in einzelnen, chronologisch miteinander verketteten Blöcken als Transaktionen (graue Rechtecke in Abbildung 3) manipulationsgesichert verwaltet. Die Daten in einer Blockchain sind Transaktionsdaten mit Geldeinheiten, Zertifikaten, Produktionsdaten, Sensordaten, Source Code oder ganz allgemein „digitale Werte". Ein interessanter Aspekt ist der Quellcode. Der Quellcode heißt bei Blockchain-Technologien zum Beispiel Smart Contract und hilft, den Prozess der Blockchain-Anwendung automatisiert zu steuern.

Transaktionen mit Daten werden vom Blockchain-Teilnehmer erstellt und signiert (rotes „Sign" in Abbildung 3). Dazu hat jeder Blockchain-Teilnehmer ein Wallet, in dem der notwendige geheime Schlüssel gespeichert ist. Der passende öffentliche Schlüssel wird auch in die Transaktion gespeichert (grüner Schlüssel in der Abbildung 3).

Wenn eine Transaktion vom Blockchain-Teilnehmer erstellt wurde, wird sie direkt über eine Node über das Peer-to-Peer-Netzwerk verteilt. Als Ergebnis haben alle Nodes alle Transaktionen gespeichert. Ein Blockchain-Teilnehmer kann eine Person oder ein Prozess in einem IT-System sein, wie zum Beispiel in einem Auto, einem IoT-Gerät, einem Produktionssystem etc. Ein Blockchain-Teilnehmer besitzt eine Wallet-App, in der die privaten und öffentlichen Schlüssel gespeichert sind. Der öffentliche Schlüssel wird auch verwendet, um eine Adresse der Blockchain eines Teilnehmers zu berechnen, welchem die Transaktionen zugeordnet sind.

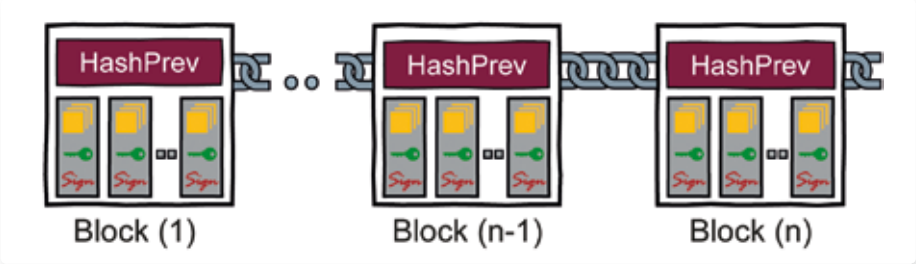

Abb. 3: Datenstruktur einer Blockchain

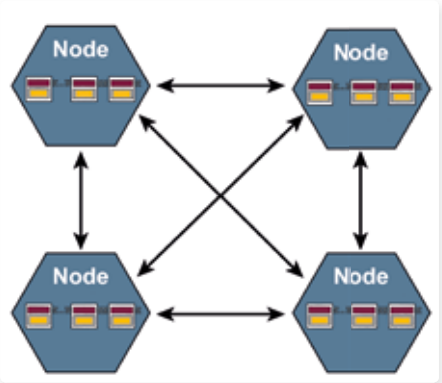

Abb. 4: Blockchain Peer-to-Peer-Netzwerk

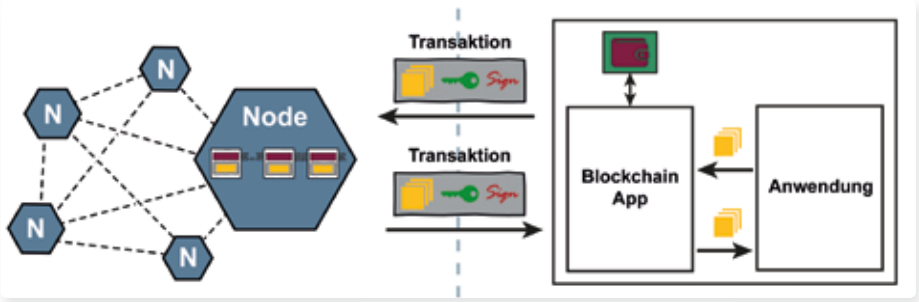

Abb. 5: Sicherheit und Vertrauenswürdigkeit der Blockchain-Technologie

Ein Block in einer Blockchain ist ein strukturierter Datensatz, der im Prinzip beliebige Transaktionen mit Daten enthalten kann und vor Manipulationen gesichert ist. Der Hash-Wert HashPrev sichert die Blockverkettung der Blöcke der Blockchain. In definierten Zeitintervallen werden die vorhandenen Transaktionen von einem mithilfe eines Konsensfindungsverfahrens ausgewählten Node als Block gruppiert und entsprechend validiert. Der ausgewählte Node verteilt den neuen Block über das Peer-to-Peer-Netzwerk. Alle anderen Nodes validieren ebenfalls den empfangenen neuen Block. Die verteilte Validierung aller Blöcke in den verschiedenen Nodes ist wichtig, um ein gemeinsames Vertrauen aufzubauen. Bei der Bitcoin-Blockchain wird zum Beispiel alle zehn Minuten ein neuer Block erstellt. Für die Auswahl einer Node wird ein Konsensfindungsverfahren verwendet.[2]

Die Blockchain beinhaltet alle Blöcke (Daten), die miteinander verkettet sind. Auf jeder Node eines bestimmten Peer-to-Peer-Netzwerkes ist eine Version der Blockchain gespeichert. Damit kann ein verteilter und redundanter Transaktionsspeicher für manipulationssichere Daten genutzt werden.

Hohe Sicherheit und Vertrauenswürdigkeit

Damit die Blockchain-Technologie langfristig sicher und vertrauenswürdig genutzt werden kann, müssen Kommunikations-, Sicherheits- und Vertrauenswürdigkeitsaspekte berücksichtigt werden. Um die Sicherheitsaspekte besser diskutieren zu können, teilen wir die Blockchain-Technologie in Blockchain-Infrastruktur und Blockchain-Anwendung.

Auf der linken Seite in Abbildung 5 sind die Blockchain-Infrastruktur mit dem Peer-to-Peer-Netzwerk, die Nodes mit allen Kommunikations- und Sicherheitsfunktionen und die Blockchain als Datenstruktur angeordnet. Auf der rechten Seite sind die Blockchain-Anwendung, eine mögliche Blockchain-App, ein Wallet mit den Schlüsseln und die eigentliche Anwendung zu sehen. Die Transaktionen werden als Schnittstelle zwischen der Blockchain-Infrastruktur und der Blockchain-Anwendung betrachtet. Im Folgenden diskutieren wir die zuvor schon genannten Sicherheitseigenschaften und die dazu notwendigen Sicherheitsmechanismen der Blockchain-Technologie hinsichtlich ihrer Wirksamkeit und Robustheit.

1.) Sicherheitseigenschaften: Verfügbarkeit der Daten („verteilt und redundant“)

Mithilfe des Peer-to-Peer-Netzwerks der Blockchain-Infrastruktur werden die Daten in der Blockchain auf die Nodes verteilt, also vielfach redundant gespeichert. Damit wird eine sehr hohe Verfügbarkeit der Daten erzielt. Das Peer-to-Peer-Netzwerk muss dafür robust sein, um zuverlässig die Verfügbarkeit der Daten und die Vertrauensdienste erbringen zu können. Auch DDoS-Angriffe auf eine Blockchain sollten keinen nachhaltigen Einfluss auf die Funktionalität der Blockchain-Technologie haben.

Aspekte, die bei der Robustheit eine Rolle spielen sind: die Anzahl der Nodes, die Bandbreite zwischen den Nodes sowie die Speicherplatz- und Rechnerkapazität auf den Nodes. Eine Bitcoin-Blockchain ist zum Beispiel größer als 160 Gigabyte. Außerdem muss die Verteilfunktion von neuen Transaktionen und Blöcken robust sein, damit alle Elemente immer vollständig auf allen Nodes verteilt werden.

2.) Sicherheitseigenschaften: Integrität und Authentizität der Daten in den Transaktionen („fälschungssicher/unveränderlich“)

Die Integrität und Authentizität der Daten in den Transaktionen ist eine wichtige Sicherheitseigenschaft, um die Sicherheitsattribute fälschungssicher und unveränderlich umsetzen zu können. Dazu spielt die Kryptografie-Agilität der Blockchain-Technologie eine besondere Rolle.

Kryptografie-Agilität der Blockchain-Technologie

Eine Blockchain-Technologie nutzt ein Public-Key-Verfahren für die Signierung und Verifikationen von Transaktionen, um die Echtheit, den Ursprung und die Unversehrtheit der Daten überprüfen zu können. Hash-Funktionen dienen der Blockchain-Adresserzeugung, der notwendigen Verkettung der Blöcke (HashPrev) und der Berechnung des Merkle-Hash-Wertes zur Integritätsüberprüfung aller Transaktionen in einem Block.

Für eine sichere und vertrauenswürdige Nutzung der Blockchain-Technologie müssen das verwendete Public-Key-Verfahren und die Hash-Funktionen dem Stand der Technik genügen. Außerdem müssen die passenden Schlüssellängen verwendet wer-

den. Der Stand der Technik kann aus der Technischen Richtlinie des BSI: „Kryptographische Verfahren: Empfehlungen und Schlüssellängen" entnommen werden. In der BSI-Richtlinie steht beschrieben, welche kryptografischen Verfahren und Schlüssellängen genutzt werden sollten, damit sie für die nächsten zehn Jahre als sicher gelten. Die BSI-Empfehlungen aus 2018 zur Nutzung von Kryptografieverfahren lauten zum Beispiel:

- Public-Key-Verfahren: RSA mit einer Schlüssellänge von 3.000 Bit
- Hash-Funktionen: SHA-3 mit einer Hash-Wertlänge von 256 Bit

Außerdem müssen langfristig Post-Quantum-Kryptoverfahren berücksichtigt und genutzt werden. Daher ist bei der Wahl der Krypto-Eigenschaften von Anfang an die Lebensdauer einer Blockchain ins Kalkül zu ziehen, damit die Werte in einer Blockchain auch langfristig geschützt werden können (zum Beispiel wenn die Lebensdauer länger als zehn Jahre ist).

Bei den Kryptografieverfahren spielt aber auch die Schüssel- und Zufallszahlengenerierung eine sicherheitsrelevante Bedeutung. Bei der Erzeugung der Schlüssel besteht das Risiko, dass der Anwender einen zu einfachen Schlüssel wählt. Wird zum Beispiel der eigene Vorname als Schlüssel verwendet, können selbst ungeübte Angreifer dies leicht erraten. Aus diesem Grund sollten die Schlüssel immer mithilfe von echten Zufallszahlengeneratoren berechnet und der vollständige Schlüsselraum ausgenutzt werden. Darüber hinaus sind Aspekte wie Streuung, Periodizität und Gleichverteilung zu beachten.

3.) Sicherheitseigenschaften: Integrität der Blockchain („in der Zeitfolge protokolliert nachvollziehbar")

Die Sicherheitseigenschaft Integrität der Blockchain ist wichtig, um die Abläufe der Transaktionen in der Zeitfolge nachvollziehen zu können. Für diese Sicherheitseigenschaft wird zusätzlich noch eine geschickte Verwendung der Hash-Funktionen (Transaktionen, Blockverkettung) genutzt.

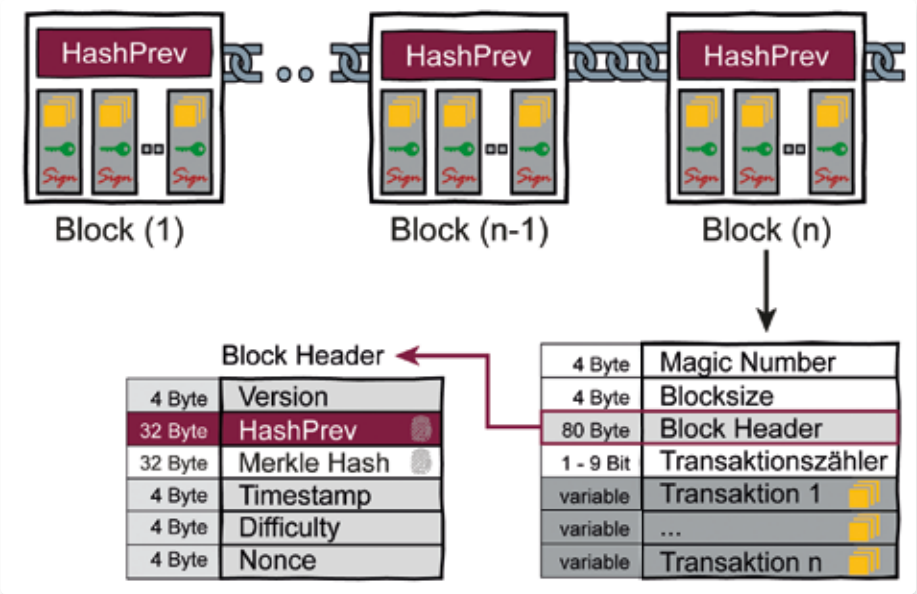

Abb. 6: Clevere Nutzung von Hash-Funktionen

In Abbildung 6 sind die Elemente eines Blocks exemplarisch für die Bitcoin-Blockchain zu sehen. Der Block Header beinhaltet den Merkle-Hash, einen Hash-Wert der aller Transaktionen in einem Block einschließt und damit den Inhalt eines Blocks überprüfbar macht (siehe Abbildung 7). Timestamp, Difficult und Nonce sind Werte für das Mining-Verfahren.

Mithilfe des Hash-Wertes „HashPrev" im Block Header wird die Blockverkettung der Blockchain sichergestellt. „HashPrev" ist das Ergebnis der Hash-Funktion (H) der als Input den letzten Block Header nutzt.

$$HashPrev_n = H\,(Block\text{-}Header_{n-1})$$

Die Blockverkettung ist ein wichtiger Aspekt für die Überprüfbarkeit der Reihenfolge der Blöcke, aber sie macht es unmöglich, die Daten in der Blockchain zu löschen. Dies kann wiederum zu Datenschutzproblemen oder zu Problemen mit unerwünschten Inhalten führen.

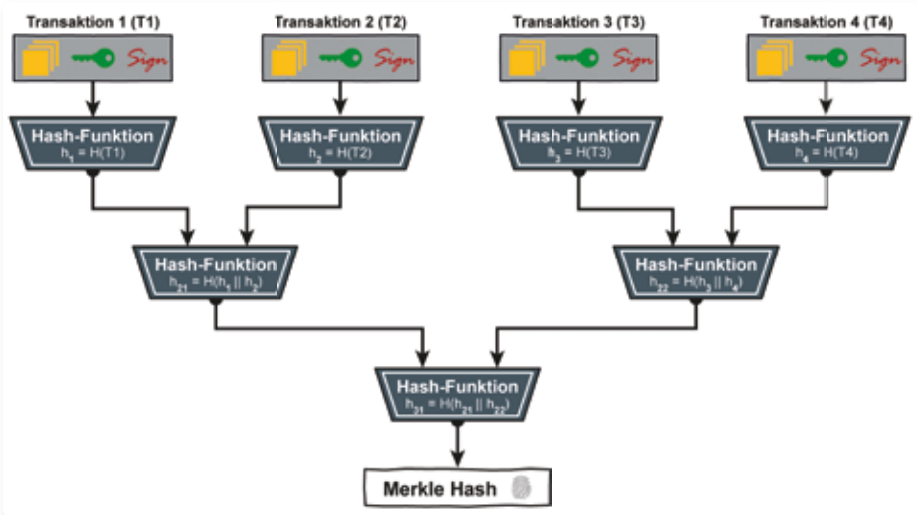

Abb. 7: Merkle-Hash-Verfahren

4.) Sicherheitseigenschaften: „ohne zentrale Instanz“

Die Blockchain-Technologie bietet „programmiertes Vertrauen“ mithilfe verschiedener IT-Sicherheits- und Vertrauensmechanismen. Alle IT-Sicherheits- und Vertrauensfunktionen sind inhärent als „Security-by-Design“ in die Blockchain-Technologie integriert.

Für die Blockchain-Anwendung muss ein passendes Konsensfindungsverfahren, auch in Abhängigkeit der ausgewählten Berechtigungsarchitektur, ausgewählt und genutzt werden, um sicher und vertrauenswürdig arbeiten zu können.[1] Ein Validierungsalgorithmus überprüft die Hash-Werte und Signaturen der Transaktionen und auch neue Blöcke, die von der ausgewählten Node erstellt und verteilt worden sind. Zusätzlich werden aber auch die Syntax und die Semantik der Elemente überprüft, wie „Stimmt die Blockchain-Adresse?“, „Sind genug Coins vorhanden?“ etc.

Da die Blockchain-Technologie einen Vertrauensdienst anbietet, spielt die Sicherheit und Zuverlässigkeit der Software eine entscheidende Rolle. Es muss sichergestellt werden, dass die Peer-to-Peer-Mechanismen, die Vertrauenswürdigkeitsmechanismen, die verwendete Kryptografie, die Smart-Contract-Umsetzung etc. keine Schwachstellen enthalten und nur das tun, was erwartet wird.

Sicherheit der Blockchain-Anwendung

Die Blockchain-Anwendung kann aus einer Blockchain-App bestehen, die Daten von der Anwendung in Transaktionen vom Blockchain-Teilnehmer mit seiner Wallet signiert und in der Blockchain verstetigt. Außerdem werden Transaktionen in der Blockchain-App verifiziert und die Daten von der Anwendung „verarbeitet“. Die Blockchain-App nutzt das Wallet des Blockchain-Teilnehmers, die als Hardware-Sicherheitsmodule (USB-, NFC-Token, Smartcard, …) realisiert ist und in der die Schlüssel gespeichert sind. Die eigentliche Anwendung nutzt die Blockchain-Technologie (siehe Abbildung 5).

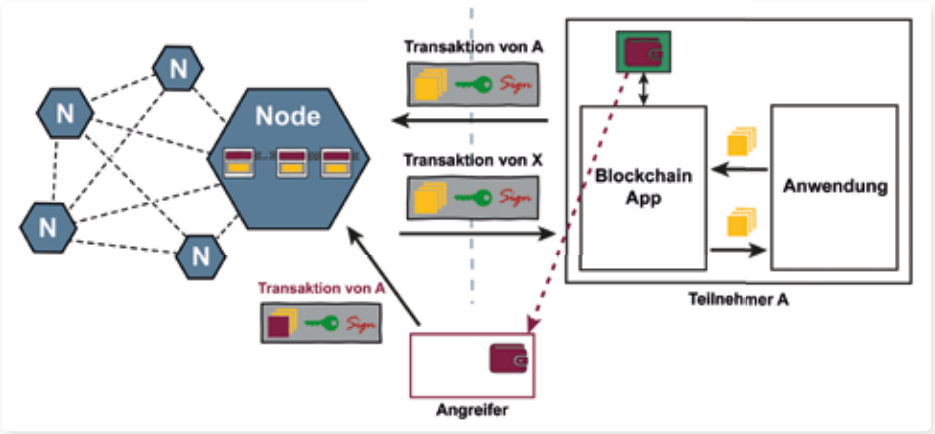

Abb. 8: Hier ist dargestellt, wie der Angreifer durch den Besitz der Wallet oder durch den unerlaubten Zugriff auf die Wallet des Teilnehmers A echte Transaktionen erstellen und damit die Blockchain manipulieren kann.

Die Sicherheit der Blockchain-Technologie hängt auch von der Geheimhaltung der privaten Schlüssel der Public-Key-Verfahren in der Wallet ab. Der private Schlüssel muss immer geheim bleiben. Wer den privaten Schlüssel einer Wallet besitzt, ist in der Lage, über die gesamten Transaktionen der Wallet zu verfügen. Ein Verlust des privaten Schlüssels bedeutet, dass sämtliche in der Blockchain-Adresse gespeicherten Transaktionen für immer „verloren“ sind. Gefahren bei nicht ausreichendem Schutz des privaten Schlüssels sind zum Beispiel:

- Das private IT-System des Blockchain-Teilnehmers wird mithilfe von Malware ausgespäht.
- Bei einem IoT-Device, zum Beispiel Auto, wird der geheime Schlüssel ausgelesen.
- Die Website der Online-Wallet wird gehackt.
- Ein nicht ausreichend gesichertes Smartphone wird gestohlen und genutzt.

Der Schutz des privaten Schlüssels in der Wallet sollte mithilfe von Hardware-Security-Modulen realisiert werden (SmartCards, Security-Token, High-Level-Sicherheitsmodule). Auch wenn der Angreifer die Schlüssel nicht auslesen kann, könnte er den Angriff so organisieren, dass er die angebotenen Sicherheitsfunktionen des Hardware-Sicherheitsmoduls unberechtigt nutzt. Dies kann zum Beispiel durch eine Malware erfolgen, die bei der Verwendung einer Smartcard oder eines USB-Sicherheitstokens nach der Aktivierung die Sicherheitsdienste unberechtigt für Angriffe nutzt. Diese unberechtigte Nutzung muss aktiv verhindert werden.

Der Angreifer ist in der Lage, valide Transaktionen für den entsprechenden Teilnehmer A zu erstellen und dadurch die Blockchain und die Blockchain-Anwendung zu manipulieren. Daher ist es besonders sicherheitsrelevant, dass das Wallet nicht gestohlen oder unberechtigt genutzt werden kann.

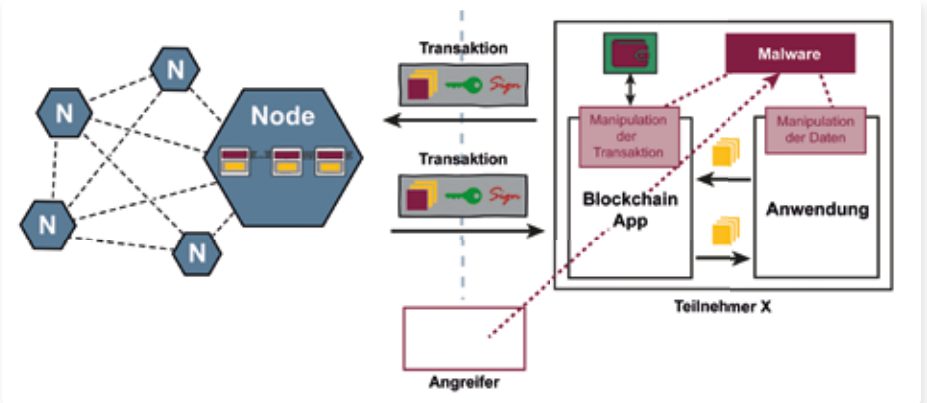

Abb. 9: Manipulation der Blockchain-Anwendung

Manipulation der Blockchain-Anwendung

Wenn die Blockchain auf der Node über ein hohes Sicherheitslevel verfügt, werden Kriminelle mit hoher Wahrscheinlichkeit versuchen, über die Blockchain-Anwendung anzugreifen. Daher muss auch die Blockchain-Anwendung manipulationssicher sein, damit keine erfolgreichen Angriffe umgesetzt werden können.

In Abbildung 9 wird gezeigt, wie ein Angreifer auf dem IT-System des Blockchain-Teilnehmers eine Malware positioniert hat und damit die Blockchain und die Anwendung manipulieren kann. Sowohl ausgehende Transaktionen des entsprechenden Teilnehmers können vor der Sendung/Weiterleitung an die Blockchain-Infrastruktur manipuliert werden als auch „eigene" Transaktionen und die von anderen Teilnehmern, die aus der Blockchain ausgelesen werden. Der Angreifer ist in der Lage, dem Teilnehmer eine falsche Realität der Blockchain vorzutäuschen. Dieser Art des Angriffes kann mithilfe einer vertrauenswürdigen Laufzeitumgebung entgegengewirkt werden. Vertrauenswürdige Laufzeitumgebungen können auf den Technologiefeldern „Trusted Computing", „Trusted Execution Environment" und „Sandboxing" umgesetzt werden.

Zusammenfassung

Die Blockchain-Technologie schafft als Vertrauensdienst eine Basis für eine verteilte und vertrauenswürdige Zusammenarbeit und stellt damit ein hohes Potenzial für neue Geschäftsmodelle und Ökosysteme dar. Die Elemente, Prinzipien und Architektur der Blockchain-Technologie zeigen den technischen Hintergrund und interessante Möglichkeiten auf, Sicherheit und Vertrauen zu erzielen. Alle IT-Sicherheits- und Vertrauensfunktionen sind inhärent als „Security-by-Design" in die Blockchain-Technologie integriert. Die Blockchain-Infrastruktur hat komplexe Kommunikations-, Sicherheits- und Vertrauenswürdigkeitsfunktionen, die im Einklang miteinander die notwendigen Sicherheits- und Vertrauenseigenschaften erbringen.

Die Blockchain-Anwendungen sind dem „realen Leben" ausgesetzt. Sie müssen daher ganz besonders für die sichere Generierung, Nutzung und Speicherung, der Schlüssel sowie für eine manipulationsfreie Laufzeitumgebung sorgen.

Für viele Unternehmen ist Blockchain eine ideale Technologie für eine vertrauenswürdige, verteilte Zusammenarbeit. Vertrauensdienste, wie die Blockchain, spielen in der Zukunft sicher eine immer wichtigere Rolle. ■

Literatur:

[1] *N. Pohlmann: „Eine vertrauenswürdige Zusammenarbeit mit Hilfe der Blockchain-Technologie", Buch: „Cybersecurity Best Practices – Lösungen zur Erhöhung der Cyberresilienz für Unternehmen und Behörden", Herausgeber: M. Bartsch, S. Frey; Springer Vieweg Verlag, Wiesbaden 2018*

[2] *C. Kammler, N. Pohlmann: „Kryptografie wird Währung – Bitcoin: Geldverkehr ohne Banken", IT-SICHERHEIT, Ausgabe 6/2013, DATAKONTEXT-Fachverlag*

PROF. DR. NORBERT POHLMANN
ist Professor für Informationssicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrusT und im Vorstand des Internetverbandes – eco.