satw

Distributed Ledger Technology

Cybersecurity – Herausforderungen für die politische Schweiz

Stand der Dinge

Die Blockchain ist eine spezielle Form der Distributed Ledger Technology (DLT). Man kann sich die DLT als eine verteilte Datenbank (Ledger) vorstellen, die von jedem beteiligten Knoten in einem Netzwerk unabhängig verwaltet und aktualisiert wird. Es gibt keine zentrale Behörde, die die Datenbank pflegt und die Datensätze an die Knoten übermittelt. Stattdessen werden die Datensätze unabhängig voneinander erstellt und von jedem Knoten verwaltet. Jeder Knoten verarbeitet daher jede Transaktion und kommt zu seinem eigenen Abschluss. Ein Konsensprotokoll stellt sicher, dass jeder Knoten eine identische Kopie der Datenbank aufbewahrt.
Es gibt verschiedene Möglichkeiten, wie DLT implementiert werden kann, wobei Blockchain die bekannteste ist. Sehr oft wird Blockchain mit Kryptowährungen wie Bitcoin assoziiert. Hierbei ist zu beachten, dass die Begriffe nicht austauschbar verwendet werden sollten, da Blockchain die Technologie ist, auf der die meisten Kryptowährungen aufgebaut sind.

Vor allem in der Schweiz gibt es viele Blockchain-Startups. Ein kürzlich veröffentlichter Bericht zählt mehr als 800 Firmen mit über 4'000 Fachleuten, die im Bereich der Blockchain- und Kryptowährungstechnologie tätig und hauptsächlich im «Swiss Crypto Valley» um Zug angesiedelt sind.

Herausforderungen

Mit der Blockchain entfällt die Notwendigkeit, bei Transaktionen einer zentralen Behörde wie einer Bank, einer Versicherung oder einem Notar zu vertrauen. Der Verzicht auf eine zentrale Behörde hat aus sicherheitspolitischer Sicht Vor- und Nachteile.

Empfehlungen

Insgesamt eröffnen Blockchain und DLT neue Möglichkeiten für eine breite Palette von kommerziellen Anwendungen. Blockchain-basierte Lösungen, die Start-ups derzeit entwickeln und fördern, werden sich weiterentwickeln.

Organisationen, die den Einsatz von Blockchain-basierten Lösungen planen, wird empfohlen, eine angemessene Risikobewertung durchzuführen und sich dabei auf die Anwendung zu konzentrieren, die auf der der Blockchain zugrunde liegenden Plattform läuft.

Es gibt keinen einzigen Single Point of Failure, aber es gibt auch keinen Kontrollpunkt, der in der Lage ist, unvorhergesehene Probleme zu erkennen und darauf zu reagieren. Stattdessen muss man auf die Blockchain-Technologie selbst und die eingebaute Fehlertoleranz vertrauen.

Bisher gemeldete Blockchain-Sicherheitsprobleme beziehen sich in der Regel nicht auf die Blockchain-Plattform selbst, sondern auf die Anwendungen, die auf ihr laufen. In diesem Sinne unterscheiden sich Blockchain-Anwendungen nicht von traditionellen Anwendungen, sie sind beide mit ähnlichen Sicherheitsproblemen konfrontiert.

Aus der Sicht der Endbenutzer sind unzureichende Praktiken bei der Schlüsselverwaltung ein Hauptanliegen. Verlorene oder gestohlene Schlüssel sind ein weitverbreitetes Problem, das im Falle von Krypto-Währungen unmittelbare finanzielle Auswirkungen hat.

Handlungsbedarf

Die Blockchain-Technologie und ihre Anwendungen werden sich weiter entwickeln. Insbesondere werden eine verbesserte Leistung zur Erhöhung der Transaktionsverarbeitungs-geschwindigkeit sowie neue Sicherheits- und Datenschutzfunktionen erwarten.

Aus rechtlicher Sicht hat die Verwendung von Blockchain im Finanzsektor mehrere Fragen aufgeworfen. Der Bundesrat hat daher im November 2019 die Botschaft zur weiteren Verbesserung der rechtlichen Rahmenbedingungen für Blockchain- und DLT-basierte Anwendungen verabschiedet. Es werden Änderungen an neun Bundesgesetzen vorgeschlagen, die sowohl das Zivilrecht als auch das Finanzmarktrecht betreffen. Sie zielen darauf ab, die Rechtssicherheit zu erhöhen, Hindernisse bei der Anwendung der DLT zu beseitigen und das Missbrauchsrisiko zu verringern.

Referenzen

CV VC: The Crypto Valley's Top 50 H1 2019, July 2019.
https://cvvc.com/application/files/2115/6453/7847/CVVC-Top50-H1-2019.pdf

Swiss Federal Council: Botschaft zum Bundesgesetz zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register, Nov. 2019.
https://www.newsd.admin.ch/newsd/message/attachments/59301.pdf

Kontakt

Nicole Wettstein
Leiterin Schwerpunktprogramm Cybersecurity
+41 44 226 50 13

https://www.satw.ch/cybersecurity-herausforderungen

Impressum
Schweizerische Akademie der Technischen Wissenschaften SATW
Expertenbeiträge
Karl Aberer, EPFL | Umberto Annino, InfoGuard | Alain Beuchat, Banque Lombard Odier & Cie SA | Matthias Bossardt, KPMG | Adolf Doerig, Doerig & Partner | Stefan Frei, ETH Zürich | Roger Halbheer, Microsoft | Pascal Lamia, MELANI | Martin Leuthold, Switch | Hannes Lubich, Verwaltungsrat und Berater | Adrian Perrig, ETH Zürich | Raphael Reischuk, Zühlke Engineering AG | Riccardo Sibilia, VBS | Bernhard Tellenbach, ZHAW | Daniel Walther, Swatch Group Services | Andreas Wespi, IBM Research Lab
Redaktion und Grafik
Beatrice Huber; Claude Naville, Adrian Sulzer, Nicole Wettstein

www.satw.ch
September 2020