pwc

Handelszeitung

30. September 2021

Handelszeitung

Die privaten Schlüssel gut aufbewahren

Crypto Custody Kryptowährungen sind attraktiv, bergen jedoch besondere Risiken. Diese gilt es konsequent zu identifizieren und aktiv zu reduzieren.

ADRIAN KELLER UND RALF HOFSTETTER

Kryptowährungen basieren auf der dezentral strukturierten Blockchain-Technologie. Demnach existieren in der Blockchain keine zentralen Kontrollinstanzen wie Banken in traditionellen Finanzmärkten. Die Nutzerinnen und Nutzer können mit entsprechendem Fachwissen die digitalen Vermögenswerte selbst verwalten.

Dazu brauchen sie private Schlüssel. Mit diesen lösen sie Transaktionen aus und kontrollieren ihre digitalen Vermögenswerte. Bei Verlust der privaten Schlüssel kann ihn keine zentrale Instanz zurücksetzen oder wiederherstellen; das gelingt nur mithilfe einer geeigneten Sicherung. Die besteht aus einem Backup-Code und/oder einer Datensicherung des privaten Schlüssels, die vom privaten Schlüssel geografisch getrennt aufbewahrt werden sollten. Wer also in Kryptowährungen investiert, muss Aufgaben und Verantwortlichkeiten aller Involvierten verstehen und die Crypto-Custody-Risiken kennen und verringern.

Risiken kennen

In wenigen Jahren wird ein wesentlicher Teil der Finanzprodukte ohne zentrale Kontrollinstanz angeboten. Kryptowährungen beschleunigen nicht nur die Umsetzung digitaler Finanzprodukte aus (Kapital-)Kostenüberlegungen, sondern ermöglichen auch eine Abwicklung in Nullzeit, wodurch sich die Transaktionskosten erheblich reduzieren. Dass sowohl institutionelle als auch private Investoren diese Vorteile nutzen möchten, ist nachvollziehbar.

Allerdings sollten sie ihre Crypto-Custody-Risiken kennen. Geht nämlich der private Schlüssel und dessen Sicherung verloren oder werden diese verändert, verliert die Anlegerin den Zugriff auf ihre Kryptowährungen. Unbefugte können das ausnutzen und unautorisierte Transaktionen auslösen. Ebenso besteht ein Betrugsrisiko, wenn die Crypto Custody keiner klaren Aufgabenteilung folgt oder die Verantwortlichen Sicherheitsstandards missachten. In der traditionellen Bankenwelt ist bei Irrtum oder Betrug eine Rückerstattung von Werten möglich – nicht aber in der Welt der Kryptowährungen.

Anleger müssen die privaten Schlüssel und deren Sicherung getrennt voneinander aufbewahren und vor Angriffen schützen. Hier kommen professionelle Crypto-Custody-Angebote ins Spiel. Diese sichern die Verfügbarkeit, Vertraulichkeit und Integrität der privaten Schlüssel und ermöglichen eine Wiederherstellung. Investoren können Crypto-Custody-Lösungen eigenständig oder extern bei einem Drittanbieter betreiben, je nach vorhandener technischer Expertise. Abgestimmt auf ihren Sicherheitsanspruch führen sie ihre digitalen Geldbörsen offline, online oder in einer individuellen Kombination.

Wirtschaftsprüfer einbinden

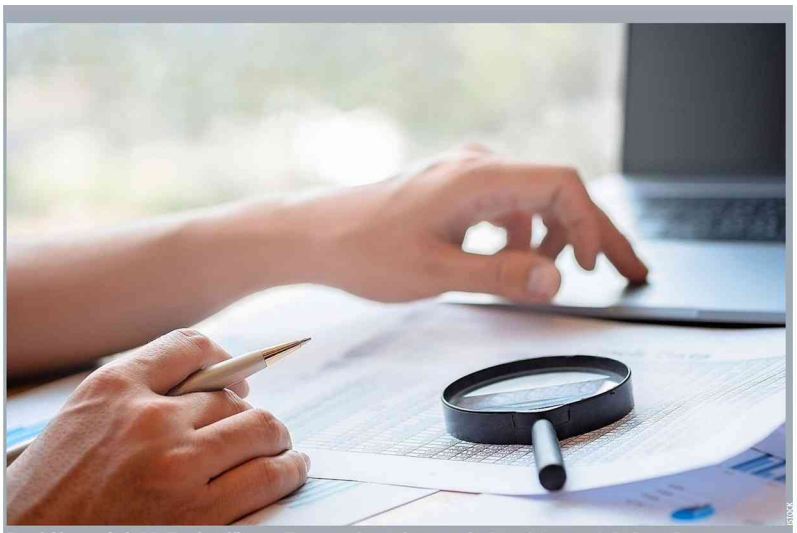
Der Wirtschaftsprüfer eines Unternehmens mit Kryptowährungen prüft, ob private Schlüssel und Sicherung angemessen verwahrt werden und entsprechende Kontrollen greifen. Mit seinen Prüfhandlungen muss er nachvollziehen können, dass das Unternehmen tatsächlich auf seine digitalen Vermögenswerte zugreifen kann und kein Unbefugter sensible Informationen zum privaten Schlüssel eingesehen oder sich sogar angeeignet hat.

Dabei muss die Wirtschaftsprüferin sicherstellen, dass die Kontrollen die gesamte Lebensdauer der privaten Schlüssel abdecken – ab Generierung der Schlüssel im Rahmen einer Schlüsselzeremonie. Andernfalls besteht das Risiko, dass die Schlüssel bereits in der Vergangenheit kompromittiert wurden und die Kryptowährungen jederzeit abhandenkommen können. Deshalb empfiehlt es sich, Wirtschaftsprüfer schon bei der Schlüsselzeremonie einzubinden.

Im Weiteren schafft die Wirtschaftsprüferin Transparenz und Sicherheit über die Freigabe von Transaktionen. Dabei prüft sie, ob und wie das Unternehmen gewährleistet, dass nur zeichnungsberechtigte oder autorisierte Mitarbeitende den Verkauf von Kryptowährungen veranlassen – mindestens im Vieraugenprinzip.

Schliesslich muss die Wirtschaftsprüferin die Wahrscheinlichkeit eines Verlusts von digitalen Vermögenswerten sorgfältig beurteilen und einen allfälligen Einfluss auf die Jahresrechnung des geprüften Unternehmens evaluieren. Aus seinem Prüfurteil soll hervorgehen, dass das Verlustrisiko mit entsprechenden Kontrollen adressiert wurde und die Weiterführung des operativen Betriebs nicht gefährdet ist.

Adrian Keller, Partner und Leiter Audit für Blockchain, Ralf Hofstetter, Director, Trust & Transparency Solutions, beide PwC Schweiz, Zürich.



Entwicklungen bei KMU-Treuhandfirmen: Eine verstärkte Verlagerung der Dienstleistungen in Richtung Beratung und es gibt vermehrte Anfragen für das Outsourcing von Dienstleistungen, vor allem Human-Resources-Themen.

KRYPTOWÄHRUNGEN

Transparenz und Vertrauen

Verantwortung Kryptowährungen spannen den Beziehungsrahmen von Unternehmen, Verwahrer und (Wirtschafts-)Prüfer neu auf (siehe Abbildung rechts). Denn damit eine sichere Aufbewahrung gewährleistet ist, müssen die involvierten Parteien ihre Verantwortung wahrnehmen und vertrauensvoll zusammenarbeiten.

• **Das Unternehmen** mit Kryptowährungen muss eine geeignete Crypto-Custody-Lösung auswählen und dabei sicherstellen, dass ein risikoorientiertes Kontrollsystem existiert. Bei einer externen Lösung ist der Verwahrer für die Durchführung der Kontrollen zuständig. Diese bleiben jedoch in der Verantwortung des Unternehmens.

• **Der Verwahrer** trägt das Verwahrungsrisiko. Er verdient meist einen kleinen Prozentsatz der verwahrten Kryptowährungen. Bei einem Teilverlust der Kryptowährungen ohne Versicherung des Verlustrisikos kann er in eine Überschuldungssituation geraten und die Bilanz des Unternehmens belasten. Er betreibt die Kontrollen und beauftragt einen Prüfer mit deren Attestierung.

• **Der Wirtschaftsprüfer** trägt dem Risiko eines Verlusts von privaten Schlüsseln mit seinen Prüfhandlungen Rechnung. Unter anderem fordert er den Nachweis ein, dass angemessene Kontrollen für die Crypto Custody über den gesamten Lebenszyklus hinweg existieren. Bei einer externen Verwahrungslösung würdigt er den Attestierungsbericht kritisch und stellt insbesondere sicher, dass relevante Risiken durch Kontrollen adressiert sind und keine signifikanten Feststellungen identifiziert wurden.

Sichere Aufbewahrung