ADRIAN KELLER
RALF HOFSTETTER
CLAUDIA HÖSLI
NICOLAS MEMMISHOFER

CRYPTO CUSTODY

Risiken und Kontrollen aus prüferischer Sicht

Kryptowährungen sind sowohl mit Chancen als auch Risken verbunden. Die Risiken, insb. während des Generierens sowie des Verwaltens der Schlüssel, müssen durch die Eignerin oder den Eigner resp. durch diese beauftragte Dritte (Crypto Custodian) mit risikoorientiert ausgestalteten Kontrollen adressiert und durch die Abschlussprüferin oder den Abschlussprüfer angemessen gewürdigt werden.

1. EINLEITUNG

In der dezentralen Blockchain-Technologie existiert keine zentrale Kontrollinstanz. Das hat zur Folge, dass alle Nutzer und Nutzerinnen ihre Rolle, die damit verbundenen Aufgaben und Verantwortlichkeiten sowie die Risiken verstehen müssen. Der private Schlüssel ist dabei das zentrale Element, mit dem Nutzer oder Nutzerinnen Transaktionen auslösen, ihre Kryptowährung und damit ihre digitalen Vermögenswerte kontrollieren. Demnach gilt: «Key management is key.» Geht der private Schlüssel verloren, gibt es keine Möglichkeit, ihn bei einer zentralen Instanz zurücksetzen zu lassen oder einen neuen privaten Schlüssel anzufordern. Das Wiederherstellen des privaten Schlüssels kann nur mithilfe einer geeigneten Backuplösung erfolgen.

Anbietende von Verwahrlösungen für Kryptowährungen (sog. Crypto-Custody-Lösungen) sind Dienstleistungsunternehmen, die sichere Speicherlösungen für Kryptowährungen anbieten. Solche werden sowohl für institutionelle als auch für private Kunden und Kundinnen entwickelt und erbracht. Hauptziel ist es dabei, die Verfügbarkeit, Vertraulichkeit und Integrität («Schutzziele») von privaten Schlüsseln und den notwendigen Informationen für deren Wiederherstellen (im Folgenden Back-ups genannt) sicherzustellen, damit die Kundschaft auf die jeweiligen Kryptowährungen zugreifen kann.

2. RISIKEN RUND UM CRYPTO CUSTODY

Private Schlüssel erlauben einem Nutzer oder einer Nutzerin den Zugriff auf seine bzw. ihre digitalen Vermögenswerte und schützen vor nicht autorisierten Zugriffen oder Transaktionen. Wurde ein privater Schlüssel kompromittiert – etwa durch Betrug oder Diebstahl –, können Dritte die digitalen Vermögenswerte kontrollieren. Aus diesem Grund sind das sichere Erstellen und Aufbewahren der privaten Schlüssel sowie deren Back-ups höchst relevant.

Erhebliche Risiken liegen insb. in der Kompromittierung und im Verlust von Vertraulichkeit, Verfügbarkeit oder Integrität der privaten Schlüssel und deren Back-ups:

→ Vertraulichkeit: Risiko, dass nicht autorisierte Personen auf den privaten Schlüssel und auf Back-ups zugreifen können und es auch tun. Ein nicht autorisierter Zugriff kann Transaktionen und den Zugriff auf die digitalen Vermögenswerte ermöglichen.

→ Verfügbarkeit: Risiko, dass die privaten Schlüssel und deren Back-ups nicht mehr oder nicht zeitnah verfügbar sind. Ein Verlust der Verfügbarkeit der privaten Schlüssel und deren Back-ups kann den Zugriff auf die digitalen Vermögenswerte verunmöglichen.

→ Integrität: Risiko, dass die privaten Schlüssel oder deren Back-ups verändert werden und damit nicht mehr lesbar sind. Ist die Integrität der privaten Schlüssel und deren Back-ups beeinträchtigt, so kann das ebenfalls den Zugriff auf die digitalen Vermögenswerte verunmöglichen.

Aus den erwähnten Hauptrisiken ergeben sich die nachfolgenden konkreten Risiken in den wesentlichen Phasen eines Lebenszyklus von privaten Schlüsseln:

→ Schlüsselzeremonie: Bei der Schlüsselzeremonie (Generierung von privaten Schlüsseln) besteht u. a. das Risiko, dass die privaten Schlüssel während der Erstellung oder beim

ADRIAN KELLER,
PARTNER, LEITER AUDIT
FÜR BLOCKCHAIN,
DIPL. WIRTSCHAFTSPRÜFER,
PWC SCHWEIZ

RALF HOFSTETTER,
DIRECTOR, TRUST &
TRANSPARENCY SOLUTIONS
LEADER, CISA, CISSP,
ISO 27001 LEAD AUDITOR,
PWC SCHWEIZ

Transport an jene Orte, an denen die privaten Schlüssel und deren Back-ups schliesslich verwahrt werden, eingesehen und z. B. kopiert werden. Das kann durch beteiligte oder unbeteiligte Personen erfolgen, die sich bspw. Zugriff auf ausgewählte technische Komponenten, z. B. Druckerspeicher, verschaffen.
→ Schlüsselverwaltung: Bei der Verwaltung der privaten Schlüssel und deren Back-ups besteht ein inhärentes Risiko, dass diese verloren gehen, gestohlen werden oder nicht mehr lesbar sind. Auch besteht ein Betrugsrisiko, falls die Aufbewahrung der privaten Schlüssel und Back-ups keiner klaren Aufgabenteilung folgt oder die mit Kontrollen und Sicherheit betrauten Personen nötige Sicherheitsstandards missachten. Zudem müssen die privaten Schlüssel und deren Backups, die an unterschiedlichen Orten gelagert werden sollten, auch gegen physische Einflüsse geschützt sein.
→ Transaktionen: Bei der Initiierung und Genehmigung von Transaktionen für digitale Vermögenswerte können ein unzureichend ausgestaltetes Kontrollsystem oder eine unzureichend ausgebildete Funktionstrennung finanzielle Risiken verursachen. In der traditionellen Bankenwelt ist bei Irrtum oder Betrug eine Rückerstattung von finanziellen Werten möglich – nicht aber in der Kryptowelt.

Ein Verlust der Kontrolle von Kryptowährungen birgt auch aus Sicht der Abschlusserstellung wesentliche Risiken:
→ Verwahrer oder Verwahrerin (Custodian): Kryptowährungen, über die der Verwahrer oder die Verwahrerin keine Kontrolle mehr hat, sind von der Aktivseite über die Erfolgsrechnung auszubuchen. Da Custodians i. d. R. das Verwahrungsrisiko tragen, bleibt in diesen Fällen weiterhin eine Verbindlichkeit gegenüber der Kundschaft bestehen. Custodians verdienen meist einen kleinen Prozentsatz der verwahrten Kryptowährungen. Deshalb ist zu erwarten, dass das Eigenkapital im Verhältnis zu den verwahrten Kryptowährungen eher gering ist. So können Custodians bei einem Teilverlust der Kryptowährungen und ohne ausreichende Versicherung des Verlustrisikos schnell in eine Überschuldungssituation geraten. Bei unmöglicher Sanierung des Verwahrers oder der Verwahrerin würde das ebenfalls bedeuten, dass die Kundschaft auf einen Teil oder die Gesamtheit ihrer Kryptowährungen Abschreibungen tätigen müsste.
→ Unternehmen mit Kryptowährungen in der Bilanz: Kryptowährungen, über die das Unternehmen keine Kontrolle mehr hat, sind von der Aktivseite über die Erfolgsrechnung auszubuchen.
→ Banken und Vermögensverwaltende mit Kryptowährungen in der Ausserbilanz: Wenn eine Bank oder Vermögensverwaltende Kryptowährungen in der Ausserbilanz ausweisen, kann ein Verlust der Kontrolle der Kryptowährungen in der Ausserbilanz zu einer Einbuchung der weiterhin bestehenden Kundenverbindlichkeit in der Bilanz führen; vorausgesetzt, die Bank oder die Vermögensverwaltenden tragen das Verwahrungsrisiko selbst. Übrigens: Ein Abschlussprüfer oder eine Abschlussprüferin muss aus diesem Grund und wegen des erhöhten Risikos über die Kryptowährungen in der Ausserbilanz die gleichen Prüfungshandlungen vornehmen wie für Kryptowährungen, die in der Bilanz erfasst sind.

Crypto Custody kann sich wesentlich auf das Unternehmen und die Abschlussprüfung auswirken. Geht die Kontrolle über digitale Vermögenswerte verloren, müssen gegebenenfalls Aktiven abgeschrieben und/oder zusätzliche Verbindlichkeiten in der Bilanz erfasst werden. Dies kann schnell zu einer Überschuldung und einer notwendigen Sanierung führen, je nach Umfang der verlorenen Kryptowährungen und der Eigenkapitalsituation.

3. ARTEN VON CRYPTO-CUSTODY-LÖSUNGEN

Der Schutz der privaten Schlüssel und Back-ups ist zentral. Insb. müssen die privaten Schlüssel und deren Back-ups getrennt voneinander aufbewahrt und vor internen wie auch externen Angreifenden geschützt werden. Hier kommen professionelle Crypto-Custody-Lösungen ins Spiel. Sie dienen dazu, die erwähnten Risiken bezüglich Vertraulichkeit, Verfügbarkeit und Integrität der privaten Schlüssel und deren Back-ups über den ganzen Lebenszyklus zu reduzieren.

Für Unternehmen stellt sich die Frage, welche Crypto-Custody-Lösung sie wählen sollen. Dabei sind zwei Aspekte zu berücksichtigen:

3.1 Soll die Crypto-Custody-Lösung intern oder extern betrieben werden?

Diese Überlegung ist strategisch und kommerziell von Bedeutung. Wird die Lösung intern betrieben, muss das Unternehmen insb. die notwendige Erfahrung und das nötige Wissen aufbauen. Bezieht es die Crypto-Custody-Lösung hingegen von einem externen Anbieterunternehmen, kann es die Aufgabe zwar an dieses delegieren, die Verantwortung – insb. über das interne Kontrollsystem – verbleibt jedoch im eigenen Haus. Zu diesem Zweck stellen professionelle Crypto-Custody-Provider sog. Kontrollberichte nach den Standards ISAE 3000 oder ISAE 3402 resp. SOC 1 oder 2 zur Verfügung. Mittels dieser lassen sich die ausgelagerten Prozesse, Risiken und Kontrollen beurteilen und überwachen.

CLAUDIA HÖSLI,
SENIOR MANAGER,
DIGITAL ASSURANCE,
PWC SCHWEIZ

NICOLAS MEMMISHOFER,
ASSISTANT MANAGER,
ASSET MANAGEMENT,
PWC SCHWEIZ

3.2 Soll die Lösung als Cold-, Warm- oder Hot-Storage-Lösung aufgebaut werden?
In der Praxis wird zwischen sog. Cold, Warm und Hot Storage unterschieden:
→ Bei Hot-Storage-Lösungen sind die Wallets permanent online. D. h., sie sind immer mit der Blockchain verbunden und Transaktionen können mit geringem Zeitverzug genehmigt und damit getätigt werden.
→ Cold-Storage-Lösungen sind sog. Offline-Wallets und entsprechend physisch von anderen Systemen abgeschottet. Sie gelten grundsätzlich als die sicherere Lösung zur Verwahrung der privaten Schlüssel. Jedoch lassen sich Transaktionen nur stark verzögert genehmigen und ausführen. Sie kommen deshalb v. a. bei der langfristigen Aufbewahrung von digitalen Vermögenswerten zum Einsatz.
→ Warm-Storage-Lösungen sollen die Vorteile der beiden Welten kombinieren.

Für Storage-Lösungen werden hauptsächlich Hardware-Sicherheitsmodule (HSM) oder Umgebungen mit sog. Multi-Party Computation (MPC) zum Schutz der privaten Schlüssel verwendet. Die Aufbewahrung der Back-ups erfolgt meist in Schliessfächern bei vertrauenswürdigen Drittparteien.

4. RISIKEN UND MASSNAHMEN AUS SICHT DES WIRTSCHAFTSPRÜFERS/DER WIRTSCHAFTSPRÜFERIN

Um den aufgezeigten Risiken zu begegnen, sollte der Abschlussprüfer oder die Abschlussprüferin die nachfolgenden Aspekte im Auge behalten. Zu prüfen ist, dass angemessene Kontrollen für die sichere Verwahrung der privaten Schlüssel und deren Back-ups implementiert sind. Dabei muss sichergestellt werden, dass die gesamte Lebensdauer der privaten Schlüssel abgedeckt wird. Deckt der Nachweis der angemessenen Kontrollen nicht den gesamten Lebenszyklus ab, besteht das Risiko, dass die privaten Schlüssel bereits in der Vergangenheit kompromittiert wurden und die digitalen Vermögenswerte jederzeit abhandenkommen können.

Dabei ist irrelevant, ob das Unternehmen die Lösung selber oder durch eine Drittfirma betreibt. Wird die Lösung eigenständig betrieben, so ist auch der Abschlussprüfer bzw. die Abschlussprüferin für die eigenständige Bewertung der Risiken und die Prüfung der Kontrollen zuständig. Ist die Lösung ausgelagert und stellt das Dienstleistungsunternehmen einen Kontrollbericht zur Verfügung, so ist ein Abstützen auf den Kontrollbericht möglich. Diesen Kontrollbericht muss der Abschlussprüfer oder die Abschlussprüferin detailliert würdigen und gegebenenfalls sog. Complementary User Entity Controls (Kontrollen, für die der Berichtsempfänger bzw. die Berichtsempfängerin zuständig ist) prüfen.

Um den ganzen Lebenszyklus der privaten Schlüssel mit genügend Evidenzen abzudecken, empfiehlt es sich, den Abschlussprüfer oder die Abschlussprüferin von Anfang an zu involvieren. In der Praxis hat es sich etabliert, dass die Abschlussprüfenden (oder andere unabhängige Dritte) an der Schlüsselzeremonie teilnehmen. So lassen sich potenzielle Risiken bereits während der Zeremonie verringern. Die Prüfbarkeit der Schlüsselzeremonie sollte durch ausreichend Unterlagen und Nachweise gewährleistet sein.

Bei der Verwahrung der privaten Schlüssel muss der Abschlussprüfer oder die Abschlussprüferin den privaten Schlüssel mit sämtlichen Backups berücksichtigen. Er bzw. sie muss prüfen, ob nicht nur die privaten Schlüssel, sondern auch deren Back-ups sicher verwahrt sind. Die Sicherheitsanforderungen an Back-ups sind gleich wie jene an die privaten Schlüssel.

Im Weiteren müssen Abschlussprüfende Sicherheit über die Umgebung zur Signierung von Transaktionen erlangen. Dabei ist zu prüfen, ob und wie das Unternehmen einen Prozess implementiert hat, der sicherstellt, dass nur zeichnungsberechtigte oder autorisierte Mitarbeitende den Verkauf der Kryptowährung veranlassen können – mindestens im 4-Augen-Prinzip. Als Basis sollte das Unternehmen dem Abschlussprüfer oder der Abschlussprüferin eine Kompetenzordnung für die Ausführung von Transaktionen auf der Blockchain vorweisen.

Wichtig aus Abschlussprüfendensicht ist es zudem, durch Prüfungshandlungen sicherzustellen, dass das Unternehmen tatsächlich Zugriff auf seine digitalen Vermögenswerte hat. Dazu besonders geeignet sind Sign-Message-Verfahren (Senden einer Nachricht über die Blockchain). Bietet die Crypto-Custody-Lösung diese Möglichkeit nicht, können Mikrotransaktionen durchgeführt werden (Simulation einer Transaktion zur Demonstration der Kontrolle über private Schlüssel).

Wie erwähnt ist wichtig, dass der Abschlussprüfer oder die Abschlussprüferin über Kryptowährungen in der Ausserbilanz einer Finanzgesellschaft, die das Verwahrungsrisiko selbst trägt, im Regelfall die gleichen Prüfungshandlungen vornimmt wie für Kryptowährungen in der Bilanz.

Bei der Abschlussprüfung sollte die Wahrscheinlichkeit des Verlusts von digitalen Vermögenswerten sorgfältig beurteilt werden, um einen allfälligen Einfluss auf die Jahresrechnung, v. a. bezüglich der Annahme der Fortführungsfähigkeit, zu evaluieren. So muss bei der Abgabe des Prüfurteils sichergestellt werden, dass aufgrund des geprüften funktionierenden Kontrollsystems faktisch keine Möglichkeit be-

steht, dass digitale Vermögenswerte innerhalb der nächsten zwölf Monate verloren gehen, falls ein Verlust dieser Vermögenswerte die Fortführungsfähigkeit der Gesellschaft gefährdet.

5. FAZIT

Die privaten Schlüssel und deren Back-ups sind zentral für den Zugriff auf und die Kontrolle von digitalen Vermögenswerten auf der Blockchain. Mit einem funktionierenden Kontrollsystem lassen sich die Risiken bezüglich der Verfügbarkeit, Vertraulichkeit und Integrität («Schutzziele») von privaten Schlüsseln und deren Back-ups reduzieren. Das ist dringend notwendig, da sich aus einem allfälligen Verlust der Kontrolle über Kryptowährungen wesentliche Risiken für das Unternehmen ergeben. Der Abschlussprüfer oder die Abschlussprüferin muss diesen Risiken mit entsprechenden Prüfhandlungen Rechnung tragen. Dazu gehört u. a. das Einfordern eines Nachweises, dass angemessene Kontrollen für die sichere Verwahrung der privaten Schlüssel und deren Back-ups über den gesamten Lebenszyklus hinweg implementiert sind. Dazu sollte der Abschlussprüfer oder die Abschlussprüferin idealerweise schon bei der Schlüsselzeremonie involviert sein, bei der die privaten Schlüssel generiert werden. Im Weiteren muss er oder sie nachvollziehen, dass nur zeichnungsberechtigte oder autorisierte Mitarbeitende den Verkauf der Kryptowährung veranlassen können und dass das Unternehmen auf seine digitalen Vermögenswerte tatsächlich zugreifen kann. Schliesslich müssen Abschlussprüfende die Wahrscheinlichkeit eines Verlusts von digitalen Vermögenswerten nach der Berichtsabgabe sorgfältig beurteilen und sicherstellen, dass das geprüfte Kontrollsystem für das kommende Geschäftsjahr keinen existenzbedrohenden Verlust zulässt. ■