Proof-of-Trust

ISACA Germany Chapter

Digital Trust am Beispiel der Kryptoverwahrung

Die Geschehnisse um den Krypto-Handelsplatz „FTX.com" zeigen die Notwendigkeit, vertrauenswürdige Nachweise über die Sicherheit von treuhänderisch verwahrten Kunden-Guthaben zu erbringen. Wenn Krypto-Handelsplätze bzw. die eingebundenen Kryptoverwahrer derzeit noch nicht über ein „Proof-of-Reserves" (PoR) verfügen, können derartige Verfahren im Sinne der Begünstigung von Vertrauen nützlich sein. PoR ist ein kryptografisches Überprüfungsverfahren, um Existenz, Vollständigkeit und Unversehrtheit von Kryptowerten nachzuweisen. Bezweckt wird die Vertrauenssteigerung in die Auszahlungsfähigkeit des Intermediärs aus Sicht der Kunden. Der Beitrag skizziert das Konzept von PoR und zeigt zudem Lösungsmöglichkeiten im Hinblick auf die Grenzen der Aussagefähigkeit von PoR als Maßnahme zur Vertrauenssteigerung. Das Zusammenspiel aus PoR und ISACA Digital Trust wird hier als Proof-of-Trust bezeichnet.

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Einleitung

Die Krypto-Industrie blickt auf spektakuläre Insolvenzen von einst bedeutsamen Instituten und Dienstleistern zurück. Ende 2022 wurde bekannt, dass die drei Jahre zuvor gegründete Organisation hinter dem Krypto-Handelsplatz FTX.com zusammen mit ihrer Partnerorganisation "Alameda Research" irreguläre Transaktionen durchgeführt hatte, welche für traditionelle Finanzinstitutionen illegal gewesen wären. Zentral in diesem Fall war die fehlende Vermögenstrennung zwischen Kunden-Guthaben und eigenem Vermögen. FTX unterlag einem "Bank-Run", was zu einem Kursverfall des eigenen Kryptowerts führte und mit weiteren Kaskadeneffekten inklusive Insolvenzen anderer Unternehmen endete. Insgesamt zählt der Fall von FTX zu einem der größten finanziellen Betrugsfälle der Welt. Entsprechend angespannt erscheinen verschiedene Finanzaufsichtsbehörden in der Sache Krypto-Dienstleistungen und deren Regulierung. Eine zentrale Rolle spielt hierbei die Sicherheit der Verwahrung von Kryptowerten durch Unternehmen für Kunden.

Kryptowerte können auf zwei Arten verwahrt werden: einerseits können diese von Besitzern oder Nutzern selbst aufbewahrt werden. Hier liegt es dann in der Verantwortung des Einzelnen, Werte sicher aufzubewahren. Andererseits können Kryptowerte durch einen Verwahrer als Dienstleister fremdverwahrt werden, was diesen Akteuren vollständige Kontrolle über die Assets verleiht. Nicht nur Unternehmen entscheiden sich risikobezogen für Letzteres. Mit Blick auf die FTX-Saga ist zu erwarten, dass nicht nur Anleger, sondern auch deutsche Aufsichtsbehörden fortan den **Fokus auf die Sicherheit** und die nachweisbare Existenz sowie Kontrolle der von Kryptoverwahrern gehaltenen Kryptowerte legen werden (vgl. [Trautmann 2023]). Vor diesem Hintergrund entstand in der Krypto-Branche der Begriff "**Proof-of-Reserves**" als Maßnahme zur Vertrauensbildung/-steigerung, welche kryptografisch die Vorhaltung bestimmter Assets nachweisen kann.

Allerdings ist es hier – wie so oft – wichtig, die Möglichkeiten und Grenzen eines solchen Ansatzes zu verstehen. Dahingehend hat sich das Public Company Accounting Oversight Board (PCAOB) – eine Aufsichtsbehörde zur Überwachung der Abschlussprüfungen bei Unternehmen von öffentlichem Interesse in den Vereinigten Staaten – am 8. März 2023 wie folgt geäußert (vgl. [PCAOB 2023]): "*Importantly, investors should note that PoR engagements are not audits and, consequently, the related reports do not provide any meaningful assurance to investors or the public.*" Jüngst zeichnete sich auch in den USA ein zunehmend strikteres Vorgehen der Aufsichtsbehörde SEC gegenüber Krypto-Dienstleistern ab (vgl. [Reuters 2023]). Zugleich beantragen bedeutsame Vermögensverwalter die regulatorische Zulassung eines handelbaren Bitcoin-Spot-ETFs. Als Kryptoverwahrer wurde bei den Anträgen das seinerseits von der SEC angeklagte amerikanische Unternehmen Coinbase Inc. angegeben (vgl. [Bloomberg 2023]).

In diesem Beitrag erläutern wir als Fachgruppe Digital Trust, warum Institutionen mit diesem Begriff werben. Die anschließende konzeptionelle Darstellung bildet die Basis, um zugleich die Grenzen von Proof-of-Reserves zu verstehen. Der Beitrag schlägt unter Heranziehung des Konzepts von Digital Trust Lösungsmöglichkeiten zur Überwindung dieser Grenzen vor.

Konzeption von Vertrauen

Im Bereich der Informationssysteme wurde Vertrauen verstärkt in Bezug auf das Vertrauen in Menschen untersucht und definiert, ohne Berücksichtigung des Vertrauens in die Technologie selbst. Die IS-Vertrauensforschung hatte zunächst in erster Linie untersucht, wie sich das Vertrauen in Menschen auf die IT-Akzeptanz auswirkt. Vergleichsweise wenig Forschung hatte das Vertrauen in eine Technologie, d.h. in ein IT-Artefakt, direkt untersucht (vgl. [McKnight et. al. 2011]).

Demgegenüber ist das Konzept von Proof-of-Reserves ein technischer Versuch zur Vertrauenssteigerung. Eine detaillierte Beschreibung des PoR-Konzepts ist im späteren Abschnitt „Konzept von Proof-of-Reserves (PoR)“ aufgeführt.

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Das Konzept des **Vertrauens** wurde von verschiedenen Forschern untersucht und definiert. Für diesen Artikel ist folgende Definition von Simmel von Interesse (vgl. [Simmel 1968]):

"*Vertrauen, als die Hypothese künftigen Verhaltens, die sicher genug ist, um praktisches Handeln darauf zu gründen, ist als Hypothese ein mittlerer Zustand zwischen Wissen und Nichtwissen um den Menschen. Der völlig Wissende braucht nicht zu vertrauen, der völlig Nichtwissende kann vernünftigerweise nicht einmal vertrauen.*"

Laut dieser Definition ist Vertrauen eine rational begründete Annahme, welches die Wahrscheinlichkeit des Einlösens einer zukünftigen, versprochenen Handlung abbildet. Nach dieser Konzeption ergibt sich im Kontext der Kryptoverwahrung folgende Konstellation:

Der Investor oder Nutzer der Plattform ist hier der Akteur, welcher entscheiden muss, ob einem Anbieter vertraut werden soll. Um diese Entscheidung zu treffen, verlässt sich diese Person oder Organisation auf Signale und Zeichen, welche vom Anbieter absichtlich oder unabsichtlich ausgesandt werden. Im täglichen Leben werden viele solche Vertrauensentscheidungen innerhalb von wenigen Minuten oder sogar Sekunden getroffen. In solchen Fällen wird ein Akteur eher auf das aktuelle Verhalten des Gegenübers oder die präsente Situation achten, z.B. steigt man in ein Taxi ein, welchen Anruf stellt man zum Chef durch, etc. (vgl. [Hamill et. al. 2005]).

Im Falle eines Krypto-Anbieters kann man davon ausgehen, dass Investorin Alice sich nicht innerhalb von wenigen Minuten für oder gegen einen Anbieter entscheiden muss und zumindest die Möglichkeit hat, sich über verschiedene Optionen zu informieren. Absichtliche **Signale** des Anbieters wären z.B. Marketingmaterialien oder die Resultate freiwilliger Audits und Penetrationstests. Unbeabsichtigte Zeichen wären z.B. Zeitungsberichte, Gerichtsunterlagen, öffentlich verfügbare Daten oder Berichte über Security Breaches. Für Investorin Alice ist es relevant herauszufinden, ob Anbieter Bob und Charlie in der Lage sind, ihre „Einlagen" technisch und organisatorisch zu schützen (ability), ob die Anbieter tatsächlich ihren Kunden gegenüber wohlwollend und ehrlich (benevolence) sind (und kein Crypto-Scam) und ob die Anbieter den Anschein erwecken, dass sie ihre Versprechungen über Zeit einhalten können (integrity).

Spieltheoretisch betrachtet ist diese Situation ein "**Signaling Game**" (vgl. [Ostrom/Walker 2003]): Kryptoverwahrer Bob und Charlie wollen Alice überzeugen, mit ihnen zusammenzuarbeiten. In diesem rein fiktiven Fall ist Bob legitim und versucht somit Alice davon zu überzeugen, dass ihn versteckte (oder zumindest schwer demonstrierbare) Eigenschaften auszeichnen, die er auch tatsächlich besitzt. Dies ist nicht immer einfach, z.B. wenn ein Spieler (Anbieter oder Konsument) neu zum Spiel hinzukommt und keine Historie vorweisen kann, nicht die Ressourcen hat, sich unabhängig prüfen zu lassen, oder generell in Märkten, in denen die Nichteinhaltung von Versprechen (ob absichtlich oder nicht) regelmäßig vorkommt. Im Gegensatz dazu ist Charlie in unserem Beispiel ein Spieler, der den Anschein einer legitimen Institution erwecken will, aber faktisch keine ist. Basierend auf den verfügbaren Informationen entscheidet sich Investorin Alice, ob sie Anbieter Bob oder Anbieter Charlie vertrauen möchte und somit dort ihre Kryptogeschäfte abzuwickeln gedenkt.

In diesem Fall wäre es möglich, dass Bob und Charlie beide die technischen Möglichkeiten zur Sicherung der "Einlagen" besitzen, aber dass Bob größere Benevolenz und Integrität signalisiert, z.B. durch Audits und Assurance, Abwesenheit von Skandalen, belegter Kundenfreundlichkeit, etc. (vgl. [Mayer et. al. 1995]). In unserem Beispiel ist dies Charlie nicht im gleichen Umfang möglich, weil er teure Signale (wie Audits und Assurance) nicht durchführen kann; das Risiko des "Entdecktwerdens" ist für ihn zu groß.

Allerdings sind empirisch innerhalb als auch außerhalb der Krypto-Industrie viele Fälle bekannt, in denen es nicht-vertrauenswürdigen Organisationen gelungen ist, Investoren, Regulatoren und Kunden zu täuschen. Der Niedergang und Betrugsfall von FTX stellt einen solchen Fall dar, aber andere aktuelle Fälle wie Theranos (Elizabeth Holmes) oder Frank (Charlie Javice) zeigen auf, dass solche Vorkommnisse nicht ausschließlich im Bereich Krypto zu verorten sind.

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Generell lässt sich feststellen, dass PoR aus technischer Perspektive nützlich und vertrauenswürdig sein kann, sofern das Verfahren korrekt und sicher implementiert ist. Allerdings stellt sich die Frage des Vertrauens, wie so oft, in einem nicht komplett technischen Kontext. Hier besteht theoretisch betrachtet eine wesentlich höhere Komplexität, weil nicht nur eine isolierte Technologie, sondern auch deren Implementierung, relevante Prozesse und oftmals eine ganze Organisation der Analyse bedürfen. Wie bereits in der Einleitung angerissen, lässt sich ausschließlich basierend auf der Technologie PoR keine belastbare Aussage über Verwahrer treffen, was allerdings nicht der Technik von PoR anzulasten ist. Praktisch kommt weiterhin hinzu, dass eine solche Prüfung nicht nur die meisten Kunden, sondern auch Auditoren schnell überfordern wird. Um PoR tatsächlich "End-to-End" zu prüfen, werden fast immer ein Expertenteam und viel Zeit benötigt werden. Besonders in einem Nischenbereich wie dem Kryptoverwahrgschäft mit seinen speziellen Anforderungen und wenigen Spezialisten verkompliziert sich deswegen die Beauftragung von befähigten und gleichzeitig unabhängigen Prüfern.

Weiterhin sind in diesem "Signaling Game" andere Spieler durchaus denkbar und in ähnlichen Bereichen wichtige Akteure. Der Staat und andere Regulatoren seien hier genannt, welche zumeist an einem stabilen Markt (bspw. Finanzstabilität) oder dem Verbraucherschutz interessiert sind. Diese können, je nach Gesetzeslage, gewisse Kontrollen, Prüfungen, Versicherungen und andere Maßnahmen vorschlagen oder anordnen. In diesem Fall sind die Prüfer vom Geprüften unabhängiger. Zu welchem Ausmaß deren Signale und Urteile allerdings für Kunden relevant, verständlich oder nützlich sind, hängt von Umfang, Tiefe und Ausrichtung der vorgeschriebenen Prüfungen ab.

Kryptoverwahrgeschäft in Deutschland

Das vom deutschen Gesetzgeber aufsichtlich regulierte Kryptoverwahrgeschäft erhielt per Umsetzung der Änderungsrichtlinie zur Vierten EU-Geldwäscherichtlinie Einzug in das Kreditwesengesetz (KWG), § 1 Abs. 1a Satz 2 Nr. 12 KWG. Für den Geschäftsbetrieb ist seitdem eine Erlaubnis der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) nach Maßgabe des § 32 KWG notwendig. Zum 21. Juni 2021 hatten 27 Interessenten bei der BaFin einen Erlaubnisantrag eingereicht. Demgegenüber gibt es zum 1.2.2024 zehn Verwahrer mit einer finalen rechtskräftigen Erlaubnis (vgl. [BaFin 2023]). Die erste Erlaubnis für den deutschen Markt wurde der US-amerikanischen Coinbase Germany GmbH erteilt. Nicht lange dauerte es, bis bei einer Jahresabschlussprüfung bei diesem Institut organisatorische Mängel festgestellt wurden. Die BaFin hat in der Folge die Sicherstellung einer ordnungsgemäßen Geschäftsorganisation nach § 25a Absatz 2 Satz 2 KWG angeordnet (vgl. [BaFin 2022]).

Kryptowerte sind grundsätzlich nicht durch Einlagensicherung oder Anlegerschutz geschützt. Eine Absicherung kann vorliegen, wenn der Kryptowert selbst als Wertpapier eingestuft wird oder es sich beispielsweise um Anteile eines Fonds handelt, der in Kryptowerte investiert. Dieser Umstand erfordert ein besonderes Maß an Vertrauen in das Krypto-Ökosystem. Der Fall "FTX" führte dazu, dass erste Krypto-Handelsplätze bzw. ihre Verwahrer öffentlich werben, dass ihre Verwahrungsprozesse in Echtzeit verifiziert werden können: "Proof-of-Reserves".

Funktionsweise von Krypto-Handelsplätzen

Eine angemessene Einschätzung der Risiken, die bei einer Fremdverwahrung von Kryptowerten bestehen, setzt ein Grundverständnis über die Funktionsweise von Krypto-Handelsplätzen, insbesondere der Dienstleister-Kette, voraus. Wie bereits beschrieben kommen Kryptoverwahrer vornehmlich in zwei Szenarien zum Einsatz: Institutionelle Anleger investieren über einen Handelsplatz in Kryptowerte und möchten diese sicher verwahren. Zu diesem Zweck schließen sie entweder direkt einen Vertrag mit einem Verwahrer ab oder der Handelsplatz stellt eine Treuhandverwahrung zur Verfügung. Das Vertrauen in die Sicherheit der Verwahrlösung geht mit einem Vertrauen sowohl in eine wirksame Finanzaufsicht als auch in eine wirksame und ordnungsgemäße Abschlussprüfung einher. Hier ist also anzunehmen, dass sich Anleger auf verschiedene Nachweise hinsichtlich Informationssicherheit, Buchführung, sowie Prozessmanagement auf der einen Seite und die staatliche Aufsicht und Kontrolle auf der anderen Seite, verlassen.

Auch **Verbraucher** kommen mit Verwahrern in Berührung, wenn sie über Kryptowerte bei einem Handelsplatz verfügen, vor allem wenn sie ihre Werte nicht selbst verwahren. Ein Kryptoverwahrer kann Teil des Dienstleistungsgeflechts eines Krypto-Handelsplatzes sein, wie in der nachfolgenden Abbildung illustriert wird (vgl. Abbildung 1). Es kann sich dabei entweder um einen externen oder einen an den Handelsplatz gebundenen Verwahrer handeln.

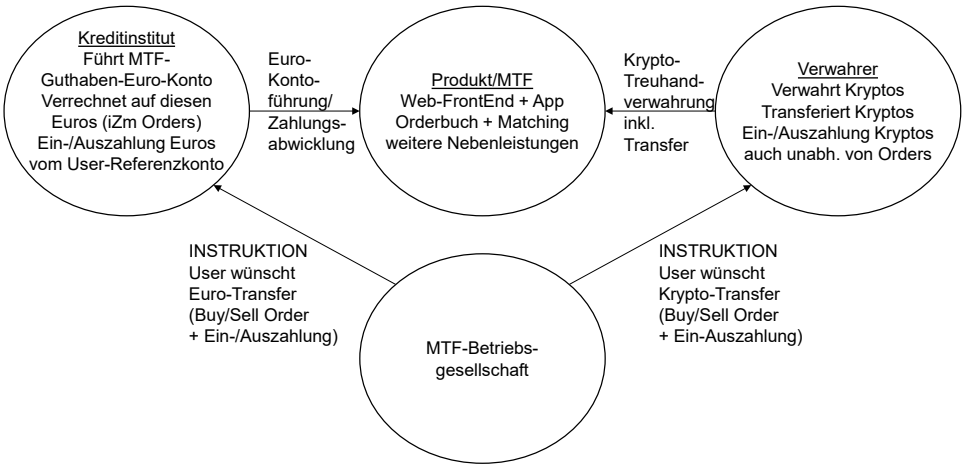

Abbildung 1 – Funktionsweise eines Krypto-MTF, eigene Darstellung

Kryptowerte können online bei einem **Intermediär** gehandelt werden. In Deutschland kann dieser bspw. als multilaterales Handelssystem (Multilateral Trading Facility – MTF) organisiert sein. Vom europäischen Pass abgesehen, bedarf der Betrieb aufgrund des Inlandsprinzips einer Genehmigung der Aufsichtsbehörde gemäß § 32 Abs. 1 Satz 1 KWG.

Ein solcher **Krypto-MTF** bringt – dem Wortlaut des § 1 Abs. 1a Satz 2 Nr. 1b KWG nach – die Interessen einer Vielzahl von Personen (Multilateralität) hinsichtlich des Kaufs und Verkaufs von Kryptowerten innerhalb des Systems und nach festgelegten Bestimmungen derart zusammen, dass ein Kaufvertrag über diese Kryptowerte geschlossen wird. Kryptowerte sind im Katalog der Finanzinstrumente erfasst, vgl. § 1 Abs. 11 Satz 4 KWG.

Das Zusammenführen der Parteien erfolgt IT-gestützt (algorithmenbasiert). Handelsteilnehmer als Endkunden des MTF haben bspw. über Bedienelemente im User Interface des webbasierten MTF-Frontends die Möglichkeit, elektronische Orderaufträge gegenüber dem MTF zu erteilen. Der MTF führt diese Kauf- und Verkaufsaufträge im weiteren Verlauf algorithmenbasiert zusammen. Die Liquidität MTF-gehandelter Finanzinstrumente kann durch eine verpflichtende Partizipation institutioneller Teilnehmer gestärkt werden.

Handelsteilnehmer vieler MTFs müssen in der Praxis regelmäßig auf Basis von allgemeinen Geschäftsbeziehungen diverse Verträge mit jeweils gesonderten Vertragspartnern abschließen. Aus diesen Verträgen ergibt sich, dass der Endkunde jeweils eine direkte Vertragsbeziehung hinsichtlich einer konkreten (sektoralen) Dienstleistung abschließt. Als denkbare Vertragsbeziehungen kommen infrage:

- Vertragsabschluss mit der MTF-Betreibergesellschaft im Hinblick auf den autorisierten Zugriff des Endkunden auf den Handelsplatz,
- Vertragsabschluss mit einem Kreditinstitut hinsichtlich der Führung eines Euro-Guthabenkontos zu Abrechnungszwecken,
- Vertragsabschluss mit einem Verwahrer hinsichtlich der Treuhandverwahrung handelbarer Kryptowerte.

Weitere vertragliche Ausgestaltungsvarianten sind denkbar.

Der Kryptoverwahrer hält die Kryptowerte von Krypto-Handelsplätzen regelmäßig im Namen und auf Rechnung der Endkunden. Folgendes Beispiel betrachtet eine Verkaufsorder im Rahmen eines fiktiven MTFs aus prozessualer Sicht:

Ein Handelsteilnehmer des MTF möchte einen Kryptowert verkaufen. Hierzu gibt er im MTF-Frontend eine Verkaufsorder ab. Die Abgabe einer Verkaufsorder triggert zwei parallel ablaufende Anweisungen. Der Verwahrer wird angewiesen, den zu verkaufenden Kryptowert betragsmäßig zu "reservieren". Daneben wird der Führer des Euro-Referenzkontos/Zahlungsabwickler angewiesen, den für die Order-Ausführung erforderlichen Euro-Betrag zu "sperren". Anschließend folgt die Einstellung der Verkaufsorder in das Orderbuch des MTF. Dieser sucht algorithmenbasiert nach einer korrespondierenden Kauforder. Sofern Verkauf- und Kauforder korrespondieren, werden diese gegeneinander (teil-)ausgeführt. Anschließend erfolgt die buch- und wertmäßige Verrechnung auf den "Konten" (Verrechnungskonto, verfügbar im Mitgliedsbereich und zugehörig zu einem Handelsteilnehmer) der betroffenen Handelsteilnehmer: Die Kryptowert-Übertragungsanweisung wird von Seiten des Verwahrers, die Zahlungsanweisung von Seiten des Euro-Kontoführers/Zahlungsabwicklers, jeweils im Auftrag des Handelsteilnehmers, ausgeführt: Der reservierte Kryptowert-Bestand wird durch den Verwahrer für den Verkäufer entsprechend als Auslieferung und beim Käufer als Einlieferung verbucht. Der gesperrte Euro-Betrag wird durch das Kreditinstitut für den Verkäufer entsprechend als Einzahlung und beim Käufer als Auszahlung verbucht.

Eine wichtige Aufgabe eines Krypto-Handelsplatzes bzw. eines Verwahrers ist der Schutz der Kryptowerte vor Verlust, Missbrauch, Unterschlagung oder Diebstahl durch Insider oder unbefugte Dritte. Diese Unternehmen stehen diesbezüglich vor besonderen Sicherheitsherausforderungen, die sich zum einen aus der Rolle dieser Organisationen und den resultierenden Risiken und zum anderen aus den technologischen Gegebenheiten im Krypto-Bereich ergeben.[1] Deshalb müssen Verwahrer und auch Handelsplätze Zeit, Ressourcen und Fachwissen auf die Erfüllung dieser Kernaufgabe konzentrieren.

Kryptoverwahrer berücksichtigen im Hinblick auf die Ausgestaltung ihrer Verwahrinfrastruktur vor allem zwei bedeutsame Erfordernisse: Sicherheit und Liquidität. So entscheiden sich manche Verwahrer für eine Kombination aus "Cold-" (Offline) und "Hot-"Wallets (Online/schnell verfügbarer Bestand zur Sicherstellung der Erfüllung von Kunden-Auslieferungswünschen), um die nötige Liquidität für jede Transaktionsanfrage in Echtzeit gewährleisten und gleichzeitig potenzielle Sicherheitsbedrohungen mitigieren zu können.

Im Fall von FTX wurden, laut eines Berichts des Insolvenzverwalters, Kryptowerte auf cloudbasierten Hot-Wallets verwahrt. Teilweise wurden die privaten Schlüssel, die die Verfügungsgewalt ermöglichen, unverschlüsselt (in Klartext) und ohne Wiederherstellungsmöglichkeiten in einer Cloud-Umgebung ohne angemessene interne Kontrollen (insbesondere Access-Identity-Management und User-Endpoint-Controls), aufbewahrt (vgl. [Ray 2023]). in diesem "Dunstkreis" sind die Vermögenswerte der Kunden durch den Kryptodienstleister FTX völlig unzureichend geschützt worden.

Eine Multilateral Trading Facility (MTF) "verschiebt" regelmäßig die Kryptowerte, die sich in den Kunden-Guthaben-Wallets befinden, in Hot-Wallets ("Konsolidierung"). Die IT-basierte Kryptoverwahrung muss also interoperabel zu den Accounting-Prozessen des Anbieters sein, so dass jede Transaktion dem jeweiligen Nutzer korrekt und vollständig zugeordnet werden kann. Ferner müssen für alle Transaktionen compliancebasierte Aufzeichnungen erstellt und revisionssicher aufbewahrt werden können. Nicht zuletzt lehrte der FTX-Fall, dass die Vermögenstrennung zwischen einzelnen Kunden-Assets und Unternehmens-Assets zu den Grundsätzen einer angemessenen Kryptoverwahrung zählt (Asset Segregation). Die dargestellten Grundzüge der Kryptoverwahrung helfen, die Technik von PoR besser zu verstehen.

[1] Beispielweise gestaltet sich die Rückholung gestohlener oder anderweitig kriminell akquirierter Werte oftmals schwierig bis unmöglich.

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Konzept von Proof-of-Reserves (PoR)

Aufgrund des zunehmenden Misstrauens, das durch die jüngste Schieflage um den Handelsplatz FTX verstärkt wurde, werben manche Krypto-Handelsplätze bzw. Kryptoverwahrer mit "Proof-of-Reserves" (kurz: PoR). Bezweckt wird die Herstellung manipulationsfreier Transparenz über Existenz, Vollständigkeit und Unversehrtheit der für die Kunden verwahrten Kryptowerte. Es handelt sich um einen Versuch der Selbst-Regulierung.[2]

Ein PoR ist ein von einer unabhängigen externen Partei durchgeführter Auftrag. Ziel ist es sicherzustellen, dass ein Verwahrer auch die Vermögenswerte hält, die dieser im Namen der Kunden zu halten behauptet. Kunden können hierdurch überprüfen, dass ihre Kryptowerte tatsächlich im Bestand des Handelsplatzes bzw. des Verwahrers sind – und folglich nicht anderweitig über diese verfügt worden ist (Vermögenstrennung).

Aus technischer Sicht fasst der PoR-Prüfer die zu prüfenden Assets zu einem sog. Merkle-Baum zusammen, einer datenschutzkonformen Struktur, die alle Kunden-Guthaben in Form von Kryptowerten umfasst. Diese Struktur basiert auf der Konsolidierung großer Datenmengen mithilfe sog. kryptografischer Hashfunktionen. Eine solche Funktion H ist eine Abbildung, die jedem beliebigen Input $\mathbf{x}$ einen eindeutigen Hashwert h zuweist, so dass $\mathbf{H(x) = h}$ gilt. Der Hashwert kann als eine Art Fingerabdruck aufgefasst werden. Es ist nicht möglich, Rückschlüsse vom Hashwert auf den Input zu ziehen oder einen identischen Hashwert durch einen anderen Input herbeizuführen. Veränderungen (Manipulationen) werden sichtbar, wie das folgende Beispiel[3] zeigt. Dieses Beispiel kann mithilfe des aufgeführten Inputwerts und eines frei verfügbaren Online-Tools (Aufruf per Webbrowser) ohne Mühe nachvollzogen werden.

```
x = User 1: 0,69 BTC

h = 9fa265cd0090918272d9f476224e7fedc14261cd8bb13e8edc462a7e16502284

x = User 2: 0,96 BTC

h = 13d25a06f05cb2aa624965af50e6851cd111915589d703f4e79c197713c5eb95
```

Mithilfe dieser Technik erhält der PoR-Prüfer die sog. Merkle-Wurzel (vgl. Abbildung 2). Dies ist eine Art kryptografischer Fingerabdruck, der die Kombination der einzelnen Kunden-Guthaben eines Handelsplatzes zu einem bestimmten Zeitpunkt (Erstellung eines sog. Snapshots) eindeutig identifiziert.

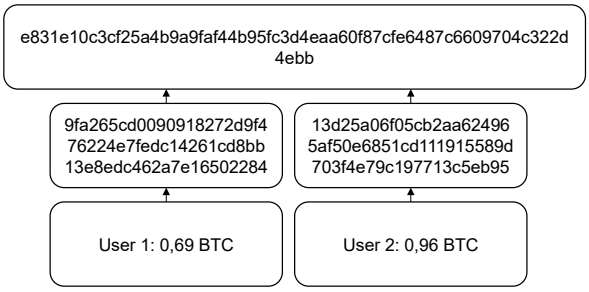

Abbildung 2 – Datenstruktur eines Merkle-Baums, eigene Darstellung

[2] Unter Selbstregulierung wird der Umstand verstanden, dass Mitglieder einer Branche die Einhaltung rechtlicher, ethischer oder sicherheitstechnischer Standards selbst überwachen, anstatt diese Standards von einer externen Instanz, bspw. einer staatlichen Aufsichtsbehörde, überwachen und durchsetzen zu lassen.

[3] Bei der International Bank Account Number (IBAN) werden Hashfunktionen als Prüfsumme genutzt. Die Gültigkeit einer Kontonummer kann mittels der Prüfsumme bestimmt werden. Das nachfolgend aufgeführte Beispiel basiert auf dem Secure Hash Algorithm mit Bit-Länge 256 (SHA-256).
(Tool: https://emn178.github.io/online-tools/sha256.html; Abruf: 5. März 2023).

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Der PoR-Prüfer verifiziert die Kunden-Guthaben anhand der vom Handelsplatz erstellten digitalen Signaturen über die auf der Blockchain verzeichneten digitalen Vermögenswerte und der öffentlich zugänglichen Blockchain-Daten. Hierzu vergleicht der PoR-Prüfer die Meldedaten mit den im Merkle-Baum dargestellten Kunden-Guthaben auf Übereinstimmung (Nachweis der Existenz, Vollständigkeit und Unversehrtheit).

Optional kann jeder Kunde in seinem Handelskonto überprüfen, ob sein Guthaben (identifiziert anhand des Hashwerts) in die PoR-Prüfung einbezogen worden ist. Die Datenstruktur stellt im Normalfall sicher, dass sich jede Änderung an den Daten auf die Merkle-Wurzel auswirkt, so dass Manipulationen offensichtlich werden.

Wie bei allen Anwendungen von Hashfunktionen, ist es aber möglich, dass es zu so genannten Kollisionen kommt, was bedeutet, dass zwei unterschiedliche Inputs zum gleichen Output führen. Dies liegt darin begründet, dass eine (nahezu) unendliche Anzahl von Eingabemöglichkeiten durch eine beschränkte Menge von Bits repräsentiert wird. Solche Kollisionen können zufällig zustande kommen oder von Angreifern absichtlich herbeigeführt werden. Aus diesem Grund ist die Wahl des oder der[4] Hashverfahren zentral. Während der im obigen Beispiel verwendete Algorithmus SHA-256 nach heutigem Kenntnisstand als kryptografisch stark gilt, ist dies nicht bei allen Kryptoverfahren mangels breiter untersuchter oder unabhängig verifizierter Sicherheitsaussagen der Fall (vgl. [Gebhardt et. al. 2006]). Weiterhin verändert sich die relative Sicherheit von Algorithmen ständig: immer höhere Rechenleistungen machen Angriffe per se einfacher, während die sich ständig weiter entwickelnde kryptologische Forschung immer neue Verwundbarkeiten identifiziert.

Verlässliche Prüfungsurteile lassen sich also nur ableiten, wenn zum Zeitpunkt der Prüfung sichere Algorithmen eingesetzt wurden. Das bedeutet, dass die Wahl des Hashing-Algorithmus mindestens der technischen Richtlinie des BSI bzw. den Empfehlungen und Vorgaben für sichere kryptografische Verfahren auf Basis internationaler Standards zur Kryptografie (z.B. von NIST, ISO/IEC) genügen sollte.

PoR liefert analog einer Bankbestätigung, die als klassische Nachweisunterlage im Rahmen von Abschlussprüfungen eingesetzt wird, eine unabhängige Bestätigung einer dritten Partei über die Existenz und Vollständigkeit von Wertguthaben, hier jedoch über die Existenz und Vollständigkeit von digitalen Vermögenswerten. Zudem wird auf Basis manipulationssicherer Kryptografie verifiziert, dass die Kunden-Guthaben unversehrt sind. Hier stößt eine isolierte Suchabfrage von Wallet-Beständen mittels Blockchain-Explorer (API- und webbasiertes Query-Tool für Blockchain-Daten) an Grenzen.

Herausforderungen bei PoR-Prüfungen

Sollen Existenz, Vollständigkeit und Unversehrtheit von Kunden-Guthaben in Form von Kryptowerten auf Basis des oben beschriebenen PoR-Verfahrens geprüft werden, so ist aufgrund der bisher mangelnden empirischen Erfahrung mit Prüfungen in der Krypto-Industrie Vorsicht geboten. Auf drei Besonderheiten wird im Folgenden hingewiesen: fehlende verbindliche Regelungen und Standards, die Transaktionshistorie sowie Grenzen isolierter Aussagen.

Fehlende verbindliche Regelungen oder Standards

Es ist naheliegend, dass PoR-Prüfungen von Prüfungsgesellschaften auf Grundlage anerkannter Prüfungsstandards nebst Berichterstattung in berufsüblicher Art erbracht werden. Dabei wird die Einhaltung von Regeln geprüft. Derzeit bestehen jedoch keine verbindlichen Regelungen oder Standards, die Prüfungsleistungen im Umfeld von Kryptowerten thematisieren. Folglich können derzeit nur allgemeine Prüfungsgrundsätze ohne konkreten Branchenbezug als Orientierungshilfe herangezogen werden. Allerdings erfordert eine Prüfung auf der Basis von PoR-Konzepten spezifisches, technisches Fachwissen.

[4] Zum Beispiel ist es möglich, zwei oder mehrere Hashverfahren gleichzeitig zu nutzen und beide Digests zu publizieren, was das Finden von Kollisionen erschwert.

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Der aufsichtsrechtlich zu erwartende Fokus auf die (IT-)Sicherheit der Kundenwerte kann jedoch im Prüfungsauftrag explizit berücksichtigt werden.

Erste öffentlich zugängliche Berichterstattungen zu PoR-Prüfungen stammen von den Wirtschaftsprüfungsgesellschaften "Mazars, Südafrika" und "BDO, Italien".

Der Bericht "BINANCE CAPITAL MANAGEMENT CO. LTD. ("BINANCE") – PROOF OF RESERVE (POR -) REPORT" der Wirtschaftsprüfungsgesellschaft "Mazars, Südafrika", datiert vom 7. Dezember 2022 (vgl. [Binance 2022]).

Binance ist der weltweit führende Krypto-Handelsplatz nach wöchentlichen Webpage-Aufrufen, Liquidität und Handelsvolumen (vgl. [CoinMarketCap 2023]). Prüfungsgegenstand war die vom Krypto-Handelsplatz vorgelegte Dokumentation über die Kunden-Guthaben (Asset Balance Reports for the In-Scope Assets) sowie die Verbindlichkeiten gegenüber Kunden (Customer Liability Report). Diese umfassten die Kunden-Guthaben der Handelsplattform am 22. November 2022 um 23:59:59 (UTC). Ziel der Prüfung war die Aussage, ob die in Kryptowerten bestehenden Kunden-Guthaben gedeckt sind, auf der Blockchain existieren und unter der Kontrolle der Handelsplattform Binance stehen. Die Prüfung erfolgte nach den Maßgaben des vom IAASB veröffentlichten International Standard on Related Services (ISRS) 4400 (Revised) "Agreed-Upon Procedures Engagements" (AuP). Hierbei handelt es sich um einen international anerkannten Prüfungsstandard für die Durchführung vereinbarter Untersuchungshandlungen. Es wird nur über festgestellte Tatsachen berichtet, ohne eine eigene Beurteilung abzugeben.

Die Besonderheit bei AuP-Prüfungen liegt darin, dass Art und Umfang der Prüfungshandlungen zwischen dem Prüfer und der zu prüfenden Einheit abgestimmt und individuell vereinbart werden. Die Prüfungsergebnisse werden einzeln dargestellt, ohne eine zusammenfassende Gesamtwürdigung der Prüfung vorzunehmen. Eine Allgemeingültigkeit der Prüfung ist nur selten gegeben.

AuP-Aufträge bergen somit die Gefahr, dass neben einem allgemeinen Prüfungsrisiko die gezielte Ausgestaltung von Prüfungshandlungen die Entdeckung von Prozess- und Ablaufschwächen erschwert bzw. verhindert und bei den Berichtsadressaten eine trügerische Sicherheit erzeugt. Allerdings sind solche individualisierten Prüfungen im Moment die einzig mögliche Herangehensweise, weil eben keine Standards für derartige Prüfungen existieren.

Die Mazars-Gruppe gab im Dezember 2022 bekannt, alle Arbeiten mit Krypto-Kunden, darunter Binance, zu suspendieren. Das WP-Netzwerk äußerte sich besorgt hinsichtlich der Wahrnehmung von öffentlich zugänglichen PoR-Berichten (vgl. [CNBC 2022]).

Der Bericht "INDEPENDENT AUDITORS' REPORT ON THE CONSOLIDATED RESERVES REPORT" der Wirtschaftsprüfungsgesellschaft BDO, Italien, datiert vom 10. November 2022 (vgl. [Tether 2022]).

Prüfungsgegenstand ist der "Consolidated Reserves Report" (kurz: CRR) der Tether Holdings Limited, der zum Stichtag 30. September 2022 aufgestellt worden ist. Neben der Tether Holdings Limited sind weitere Tochtergesellschaften im Scope dieser Prüfung. Der durch die geprüfte Gesellschaft emittierte Tether (USDT) ist ein Stablecoin bzw. ein sogenannter wertreferenzierter Token.[5] Ziel der Prüfung war die Aussage, ob der "Consolidated Reserves Report" frei von wesentlichen Fehlern aufgestellt und veröffentlicht worden ist. Die Prüfung erfolgte nach den Maßgaben des vom International Auditing and Assurance Standards Board (IAASB) veröffentlichten International Standard on Assurance Engagements 3000 (Revised) "Assurance Engagements Other than Audits or Reviews of Historical Financial Information" (kurz: ISAE 3000 Revised). Hierbei handelt es sich um einen international anerkannten Prüfungsstandard für sonstige betriebswirtschaftliche Prüfungen im Bereich der nichtfinanziellen Berichterstattung. Der ISAE 3000 (Revised) dient ebenfalls als Grundlage für den vom Institut der Wirtschaftsprüfer in Deutschland e. V. (IDW) entwickelten Prüfungsstandard: IT-Prüfung außerhalb der Abschlussprüfung (IDW PS 860, Stand:

[5] Ein Stablecoin ist eine digitale Darstellung einer Fiat-Währung, die in einem öffentlichen Blockchain-Netzwerk eingesetzt wird. Diese wertreferenzierten Token sind an Vermögenswerte wie US-Dollar oder Sachgegenstände gebunden.

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

2. März 2018).[6] Eine Prüfung nach ISAE 3000 (Revised) kann nach zwei Arten erfolgen. Dies erste Variante prüft das Sollkonzept des zugrundeliegenden IT-Systems auf Angemessenheit. Diese Variante erlaubt noch keine Aussage über den tatsächlichen Zustand des IT-Systems (Ist-Zustand). Daher erweitert die zweite Variante den Prüfungsgegenstand auf die Wirksamkeit des IT-Systems für einen definierten historischen Beobachtungszeitraum. Bei der zweiten Variante ist die Aussagekraft des Prüfungsurteils wesentlich erweitert.

Im Gegensatz zu AuP-Aufträgen fordert eine Prüfung nach ISAE 3000 bzw. IDW PS 860 zunächst die eindeutige Festlegung des Prüfungsgegenstands.[7] Dies geschieht bspw. dadurch, dass die zu prüfende Einheit eine Prozessbeschreibung des zugrundeliegenden IT-Systems bzw. IT-Verfahrens (als Beschreibung des SOLL-Zustands) fertigt und bereitstellt. Der Prüfer konzipiert im Anschluss eine Prüfungsstrategie mit dem Ziel, eine Aussage (mit hinreichender oder begrenzter Sicherheit) über die Angemessenheit des SOLL-Zustands und ggfs. den tatsächlichen Umsetzungsgrad des IST-Zustands (Gap zum SOLL-Zustand) treffen zu können.

Das Prüfungsurteil wird in Form einer Gesamtwürdigung dargereicht und ist somit für den Adressaten unmittelbar verständlich. Hierin liegt ein großer Vorteil im Vergleich zur Berichterstattung einer AuP-Prüfung. Grenzen von Prüfungsleistungen nach ISAE 3000 bestehen in der Stichtagsbezogenheit des Berichtsurteils. Schlussfolgerungen für künftige Entwicklungen sind nur äußerst begrenzt möglich und verbleiben ausschließlich beim Berichtsadressaten.

Transaktionshistorie

Zur Begrenzung des Prüfungsrisikos liegt es nahe, dass ein Prüfer die Transaktionshistorie analysiert. Hierbei sind insbesondere zeitliche Aspekte zu beachten. Der Handelsplatz könnte sich kurz vor Durchführung einer Prüfung Kryptowerte leihen, um die zu verifizierende Höhe an Kryptowerten vorzutäuschen. Um dieser missbräuchlichen Gestaltung vorzubeugen, sollte zwingend eine Bestandsaufnahme der mit der Verwahrung assoziierten Wallets erfolgen. Hierbei ist eine Einsichtnahme in den Transaktionslog unerlässlich, um vor allem auffällige Transaktionen in Stichtagsnähe zu identifizieren und zu analysieren. Der Prüfer muss folglich mit dem Einsatz von Analytics-Techniken vertraut sein (vgl. [Trautmann/Ewel 2022]). Hieraus ersichtlich ist, dass sich aussagekräftige Prüfungen zumindest auf einen Teil der Prozesse und Kontrollen des Verwahrers erstrecken müssen, um belastbare Aussagen treffen zu können. Dies ist bspw. im Bereich der SOX-Compliance auch üblich.

Blockchain-Analytics-Tools bieten Funktionen zur Untersuchung, Klassifizierung, Risikobewertung und Überwachung von Blockchain-Adressen und Netzwerkinformationen. Die Kernidee besteht darin, Blockchain-Adressen mit realen Identitäten zu verknüpfen und Tools zur Analyse der Transaktions- und Netzwerkinformationen bereitzustellen. Diese Methodiken und Tools ermöglichen die zielgerichtete Analyse Wallet-bezogener ein- und ausgehender Transaktionen, sollten aber idealerweise selbst standardisiert und entsprechend überprüft werden. Trotz alldem ist eine PoR-Prüfung immer eine Momentaufnahme, die ausschließlich Aussagen bis zu einem definierten Zeitpunkt treffen kann.

Grenzen isolierter Aussagen

Isolierte Aussagen, wie etwa über die Auszahlungsfähigkeit eines Krypto-Handelsplatzes einzig anhand einer PoR-Prüfung zu treffen, sind nicht zielführend und daher präventiv zu vermeiden.

Nicht alle in der Praxis auftretenden Krypto-Handelsplätze oder Kryptoverwahrer unterliegen der gesetzlichen Verpflichtung zur Abschlussprüfung. Ferner liefert eine PoR-Prüfung keine Aussage über die Zahlungsfähigkeit der geprüften Einheit, da weder Zahlungsverpflichtungen oder -beschränkungen (bspw. gem. § 17 InsO) Bestandteil einer solchen Prüfung sind.

[6] Vgl. IDW PS 860 Tz. 8.
[7] Vgl. ISAE 3000 Tz 12 (a); IDW PW 860 Tz. 5.

Zudem können PoR-Prüfungen nicht bei sogenannten "Cold-Wallets" und bei Fiat-Währungsbeständen angewendet werden. Es ist zum Beispiel denkbar, dass die Verfügungsgewalt über die Wallets, in denen die Kryptowerte verwaltet werden, seit der letzten Prüfung verloren ging oder Kryptobestände gestohlen wurden. Prüfungshandlungen beziehen sich auch außerhalb dieses spezifischen Bereichs fast immer auf einen Zeitpunkt bzw. einen Zeitraum. Jede Übertragung von Prüfungsergebnissen auf einen künftigen Zeitpunkt birgt die Gefahr, dass aufgrund zwischenzeitlicher Änderungen oder externer Einflüsse falsche Schlussfolgerungen gezogen werden.

Zur Erlangung eines ausreichenden Maßes an Prüfungssicherheit bedarf es eines schlüssigen Konzepts, das vertrauensbildende und -steigernde Maßnahmen bündelt und nicht nur isolierte technische Aussagen trifft, welche allein nicht in der Lage sind, die Fragen von Anlegern und Regulatoren zu beantworten.

Deswegen beschäftigen wir uns auch im Folgenden mit etablierten Prüfungsformen durch qualifizierte Dritte. Hierunter zählen neben der Abschlussprüfung auch normierte IT-Prüfungen, wie bspw. eine Zertifizierungsprüfung des Informationssicherheitsmanagements anhand der Normenreihe ISO/IEC 27001. Das folgende Kapitel skizziert mögliche Bausteine eines solchen Konzepts.

Vertrauensbildende unabhängige Prüfungen ("Proof-of-Trust")

Die Nutzung moderner Technologien kann zur Erweiterung des bisher vorliegenden Risikospektrums führen. Wie bspw. kann sich ein Krypto-Nutzer sicher sein, dass seine von einem Krypto-Handelsplatz verwahrten Kryptowerte sicher sind und jederzeit ausgezahlt werden können? Eine nicht adäquat gesicherte Aufbewahrung führt zu einer Schadensanfälligkeit, bei der beispielsweise die in Kryptowerten verbrieften Rechte irreversibel verloren gehen bzw. nicht mehr ausgeübt werden können. An diesem Wurzelrisiko setzt die professionelle Dienstleistung des Kryptoverwahrgeschäfts an (vgl. [Trautmann/Ewel 2020]). Wie bereits dargelegt, lässt sich Vertrauen in einen Dienstleister jedoch nicht einzig durch PoR-Maßnahmen herstellen. Es bedarf eines **schlüssigen Konzepts**, das ganzheitlich auf Prozesse, Menschen und Technologie ausgerichtet ist.

Eine Prüfung dieses Konzepts durch eine unabhängige Instanz kann als **vertrauensbildende Maßnahme** aufgefasst werden. Die Prüfungsurteile sind im positiven Fall konfirmativer Natur, da sie einen Status belegen.

Ein nächster Schritt könnte eine Zertifizierung darstellen, also ein Prozess zur Gewinnung eines vertrauenswürdigen Urteils, welches sich immer auf Grundlagen stützen muss (z.B. Control Objectives, Assertions, Standards). Durch den Vergleich eines vom Prüfer nicht selbst herbeigeführten Ist-Objektes mit einem vorgegebenen oder zu ermittelnden Soll-Objekt wird das Urteil abgeleitet. Zertifizierungen richten sich an diejenigen, die auf dieser Grundlage weitreichende Entscheidungen zu treffen haben (vgl. [Marten et. al. 2003]).

Im Krypto-Umfeld fehlen zurzeit noch die Grundlagen, an denen sich Prüfungen belastbar ausrichten können.

Im Rahmen von (Assurance-) Prüfungen werden Gesetze, behördliche Verwaltungsauffassungen, nationale und internationale Normen und Standards als Prüfungskriterien herangezogen, deren Einhaltung als Prüfungsobjekt zwischen Prüfer und zu prüfender rechtlicher Einheit festgelegt wird. Für Prüfungen im Umfeld von „Digital Trust“ bieten sich u. a. die Normenreihe ISO/IEC 27000 (Information Security Management Systems), ISO/IEC 20000 (IT Service Management) sowie die Information Technology Infrastructure Library (ITIL), Control Objectives for Information and Related Technology (COBIT), ISO 31000 (Risk Management) und die EU-Datenschutz-Grundverordnung (EU-DSGVO) an.

Für verwahrende Institute im deutschen regulierten Finanzumfeld sind insbesondere das Kreditwesengesetz (KWG), die Mindestanforderungen an das Risikomanagement (MaRisk) und die Bankaufsichtlichen Anforderungen an die IT (BAIT) relevant. Zusätzlich sind Standards im Hinblick auf die Prüfungsmethodologie zu beachten. Neben den ISACA-Standards, bspw. ITAF und COBIT, sind dies unter anderem

IDW-, DIIR-, IPPF- und ISAE-Standards. Diese wirken sich auf Art und Umfang des Prüfungsverfahrens aus (vgl. [ISACA 2022-2]).

Prüfungen und Digital Trust

ISACA definiert "**Digital Trust**" wie folgt: "*Digital Trust is the confidence in the integrity of the relationships, interactions and transactions among providers and consumers within an associated digital ecosystem. This includes the ability of people, organizations, processes, information, and technology to create and maintain a trustworthy digital world.*"

Digital Trust bezieht sich im Kontext eines digitalen Ökosystems auf die Bereitschaft der Akteure, sich - aufgrund positiver Erwartungen - gegenüber anderen verwundbar zu machen. Diese Definition hat zwei entscheidende Elemente. Erstens den psychologischen Zustand der Bereitschaft, verletzlich zu sein. Zweitens gibt es positive Erwartungen an eine andere Partei. Vertrauenswürdigkeit ist eine aggregierte Wahrnehmung der Eigenschaften einer anderen Partei entlang dreier Unterdimensionen: Fähigkeit, Integrität und Wohlwollen (vgl. [Lynn et. al. 2021]). Mit Fähigkeit umschreiben wir z.B. die technischen, organisatorischen Möglichkeiten, sichere Prozesse oder Architekturen aufzubauen. Integrität würde in diesem Kontext bedeuten, dass die Prozesse auch immer gelebt und befolgt werden. Das Wohlwollen beschreibt, ob ein Akteur tatsächlich gewillt ist, seine Versprechen einzulösen. Wegen ihrer besonderen Bedeutung haben wir diese drei Dimensionen bereits im Abschnitt „Konzeption von Vertrauen“ am Fallbeispiel der Investorin Alice illustriert.

Kunden, Mitarbeiter, Lieferanten und sonstige Stakeholder haben ein Interesse daran, dass ihre (digitalen) Beziehungen zu einer Organisation zuverlässig und vertrauenswürdig sind. Die Toleranz für jede Verletzung von Digital Trust tendiert gegen "Null". Digital Trust hilft Organisationen sicherzustellen, dass alles, was sie machen, dazu beiträgt, dass andere Vertrauen in sie haben (vgl. [ISACA 2023]).

Prüfungsleistungen und Zertifizierungen ermöglichen dem geprüften Unternehmen eine unabhängige Bestätigung über einen zeitpunkt- oder zeitraumbezogenen Zustand auf Basis akzeptierter Prüfungskriterien. Die Prüfungskriterien richten sich hierbei an relevanten internen Erfordernissen, Gesetzen, Regulierung und strategischen Zielen aus (vgl. [ISACA 2022-1]). Insofern können Prüfungsleistungen und Zertifizierungen der Verwirklichung von Digital Trust dienlich sein.

Abschlussprüfung ("Proof-of-State")

Der Zweck einer Abschlussprüfung besteht darin, das Maß an Vertrauen der Adressaten in den Abschluss zu erhöhen. Dies wird dadurch erreicht, dass der Abschlussprüfer ein Prüfungsurteil darüber abgibt, ob der Abschluss in allen wesentlichen Belangen in Übereinstimmung mit den maßgebenden Rechnungslegungsgrundsätzen aufgestellt wurde (vgl. [IDW 2022]).

Ziel der Abschlussprüfung ist die Feststellung, ob der zugrundeliegende Abschluss ein korrektes und vollständiges Bild der Vermögens-, Finanz- und Ertragslage des Unternehmens zeichnet.[8] Dabei sind Art, Umfang und Dokumentation der Prüfungsdurchführung von Größe, Komplexität und Risiko des Prüfungsgegenstands abhängig.

Prüfungsgegenstand sind Abschluss und ggfs. Lagebericht. Während die Bilanz als ein Bestandteil des Abschlusses stichtagsbezogen ist (bspw. zum 31. Dezember), erstreckt sich die Gewinn- und Verlustrechnung auf einen Zeitraum (bspw. vom 1. Januar bis 31. Dezember eines Jahres). Der Abschluss trifft also sowohl stichtagsbezogene (Bilanz) oder zeitraumbezogene (GuV) Aussagen über einen (finanziellen) Status der rechtlichen Einheit, daher der Begriff "Proof-of-State".

Der Abschlussprüfung fallen im Wesentlichen drei Funktionen zu, und zwar Kontrolle, Information und Beglaubigung (vgl. [IDW 2020]).

[8] Vgl. § 317 Abs. 1 HGB.

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

- Die **Kontrollfunktion** ist präventiver Natur. Die geprüfte Einheit soll durch die Abschlussprüfung aufdeckte Fehler vor Erteilung des Bestätigungsvermerks korrigieren können.
- Die **Informationsfunktion** richtet sich an alle Stakeholder. Der Prüfungsbericht ist vornehmlich für die gesetzlichen Vertreter der geprüften Einheit bestimmt und wird im Regelfall nicht offengelegt. Ausschließlich der Bestätigungsvermerk wird im Rahmen der Offenlegung der interessierten Öffentlichkeit zugänglich gemacht.
- Die **Beglaubigungsfunktion** zeigt sich in der Erteilung oder Versagung des Bestätigungsvermerks über die Vornahme und das Ergebnis der Abschlussprüfung.

(Assurance-) Leistungen außerhalb der Abschlussprüfung

Assurance-Leistungen zeichnen sich im Gegensatz zur Abschlussprüfung dadurch aus, dass der Auftraggeber und der Wirtschaftsprüfer den Prüfungsgegenstand individuell definieren. Auf Basis des abgestimmten Prüfungsgegenstands entwirft der Wirtschaftsprüfer ein geeignetes Prüfungsprogramm. Die Prüfungsergebnisse ermöglichen dem Wirtschaftsprüfer im Sinne eines Soll-Ist-Vergleichs ein "Urteil" im Hinblick auf den Prüfungsgegenstand. Je nach Beauftragung kann die Berichterstattung bspw. in Form einer Bescheinigung oder sonstigen schriftlichen Erklärung ausgestaltet sein. Zielsetzung ist die Vertrauensbildung/-steigerung der Adressaten in den vom geprüften Unternehmen dargereichten Prüfungsgegenstand. Das Urteil des Wirtschaftsprüfers soll Dritten zur Bestätigung der Verlässlichkeit von Informationen dienen. Prüfungsgegenstand von Assurance-Leistungen können neben finanziellen Informationen auch bspw. die Funktionstüchtigkeit von Applikationen oder interne Kontrollsysteme von Dienstleistern, auf die der Auftraggeber bestimmte Funktionen, Aktivitäten oder sonstigen Prozesse ausgelagert hat, sein.

Eine spezielle Ausformung dieser Assurance-Leistungen sind IT-Prüfungen außerhalb der Abschlussprüfung. Die Vorgehensweise des Prüfers ist international in der Prüfungsnorm ISAE 3000 festgeschrieben, von der sich die deutsche Prüfungsnorm IDW PS 860 ableitet.[9] Zielsetzung dieses Engagementtyps ist eine unabhängige Bewertung der zugrundeliegenden IT-Landschaft (u.a. Infrastruktur, Anwendungen, Prozesse, Daten und Organisation). Die Prüfungskriterien beziehen sich zumeist auf die Merkmale Vertraulichkeit, Integrität und Verfügbarkeit. Darüber hinaus können auch die Effektivität und Effizienz IT-basierter Geschäftsprozesse Gegenstand von IT-Prüfungen sein. Je nach konkreter Definition des Prüfungsgegenstands lassen sich die folgenden Arten von IT-Prüfungen unterscheiden:

- **Compliance-Prüfungen:** Diese Prüfungen gewährleisten, dass das zu untersuchende IT-System bzw. der IT-Prozess den gesetzlichen und regulatorischen Anforderungen entspricht, wie beispielsweise Datenschutz- und Sicherheitsvorschriften.
- **Sicherheitsaudits:** Diese Prüfungen beurteilen die Sicherheit der zugrundeliegenden IT-Systeme bzw. IT-Prozesse und helfen dabei, Schwachstellen und Risiken zu identifizieren und zu beseitigen.
- **System- und Prozessprüfungen:** Diese Prüfungen beurteilen die Effektivität und Effizienz der zugrundeliegenden IT-Systeme bzw. IT-Prozesse im Hinblick auf das Anforderungsprofil der Nutzer.
- **Risikobewertungen:** Diese Prüfungen helfen bei der Identifizierung und Bewertung von Risiken, die im Zusammenhang mit den zugrundeliegenden IT-Systemen bzw. IT-Prozessen auftreten können. Aus den Prüfungsergebnissen lassen sich anschließend risikomindernde bzw. mitigierende Maßnahmen ableiten.
- **Qualitätssicherungsprüfungen:** Diese Prüfungen unterstützen die Qualitätssicherung von IT-Produkten und IT-Dienstleistungen, indem sie die Einhaltung von Qualitätsstandards untersuchen.

Solche Audits sind üblicherweise Teil der dritten "Verteidigungslinie" im GRC-Management[10] eines Unternehmens (vgl. [IIA 2020]). Während die ersten beiden Verteidigungslinien durch unternehmensinterne

[9] Vgl. hierzu auch den Abschnitt zu den Herausforderungen bei PoR-Prüfungen.
[10] GRC steht für Governance, Risk and Compliance.

Ressourcen realisiert werden, ergänzt die dritte Verteidigungslinie das GRC-Management mittels unabhängiger und objektiver Prüfungsleistungen einer außenstehenden Partei. IT-Prüfungsaktivitäten der dritten Verteidigungslinie bezwecken eine Verbesserung des IT-Risikomanagements und des IT-Risikomanagementprozesses sowie die Verbesserung aller von der IT abhängigen Prozesse eines Unternehmens in Bezug auf Steuerungs- und Kontrollmaßnahmen zur Risikobehandlung. Das GRC-Management unterstützt damit stets auch die Erreichung der Unternehmensziele, die Verbesserung der Unternehmenssteuerung und die Einhaltung von internen und externen Regelungen (vgl. [ISACA 2022-2]).

Damit Assurance-Prüfungen im Umfeld der Kryptoverwahrung die gewünschte vertrauensbildende Wirkung (Proof of Trust) entfalten können, muss das in diesen Prüfungen angelegte Prüfungsprogramm geeignete Mindeststandards erfüllen, um eine gesicherte, qualitative Vergleichbarkeit unterschiedlicher Prüfungssubjekte zu gewährleisten. Im Besonderen müssten sich diese Standards mit technischen, prozeduralen, methodischen, rechtlichen und buchhalterischen Themen befassen und den "Scope", also die Reichweite und Breite einer ausreichend umfangreichen Prüfung definieren. Ein solches Prüfungsprogramm würde in Anlehnung an das Blockchain Framework Audit Program aus dem Jahr 2021 mindestens die folgenden Prüffelder umfassen (vgl. [ISACA 2021]):

- Governance
- Infrastruktur
- Datenmanagement
- Schlüsselmanagement und Smart Contracts.

Zusammenfassung und Ausblick

Die FTX-Causa wird nicht zum Verfall der Krypto-Industrie führen. Allerdings legt der Fall von FTX nahe, dass Krypto-Handelsplätze und Kryptoverwahrer verstärkt in den Fokus der Aufsichtsbehörden geraten werden. Dies ist auch im Hinblick auf das Vertrauen der Marktteilnehmer ein zentraler Aspekt.

Ein Prüfungsurteil über Existenz, Vollständigkeit und Unversehrtheit von Kunden-Guthaben bei einem Kryptoverwahrer ("Proof-of-Reserves") setzt technische Expertise voraus. Die Prüfungshandlungen gehen zudem in Anspruch, Durchführung, Dauer und Nachbearbeitung deutlich über das Niveau von bekannten und seit langem etablierten IT-Prüfungen hinaus. Weitere Grenzen dieses Ansatzes bestehen aktuell noch in fehlenden verbindlichen Regelungen oder Standards. Bis diese etabliert werden (können), müssen Krypto-Anbieter weiterhin intern, oder in Abstimmung mit ihren Prüfern, individuell geeignete Prüfungsverfahren erarbeiten.

Belastbare Prüfungen der Krypto-Dienstleister werden Zeit, Ressourcen und Expertise benötigen und somit mit hohen Kosten einhergehen. Weiterhin stellen sich zusätzliche technische Fragen, die spezifische Expertise in den Bereichen Kryptografie und Kryptowerte erfordern. Auch diese müssen von Experten noch diskutiert und danach folgend standardisiert werden.

Wie dargelegt lässt sich Vertrauen nicht einzig durch "Proof-of-Reserves" herstellen. Es bedarf eines schlüssigen Konzepts, das durch unabhängige Prüfungsmaßnahmen wiederkehrend bestätigt wird. Als vertrauensbildende Maßnahmen skizzierte der Beitrag neben der Abschlussprüfung ("Proof-of-State") bewährte Assurance-Leistungen. Durch eine zielgerichtete Bündelung dieser verschiedenen Maßnahmen besteht die Chance "Digital Trust" so zu etablieren, dass dem Vertrauensverfall der Krypto-Industrie wirksam begegnet werden kann, was wir als "Proof-of-Trust" bezeichneten.

Zum aktuellen Stand, Anfang Februar 2024, befindet sich die Krypto-Industrie in einer angespannten Situation. In dieses Umfeld reihen sich regulatorische Aktivitäten gegen Krypto-Dienstleister sowie erfolgreich abgeschlossener Erlaubnisverfahren bekannter Vermögensverwalter in den USA ein, während innerhalb der Europäischen Union (EU) die Anwendung eines harmonisierten Regelwerks kurz bevorsteht. Es bleibt abzuwarten, inwiefern die Erhöhung von Rechtsklarheit zur Entspannung der herrschenden Vertrauensschieflage beitragen kann.

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

Literatur

[BaFin 2022] BaFin, „Coinbase Germany GmbH: BaFin ordnet Sicherstellung einer ordnungsgemäßen Geschäftsorganisation an“, (*https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Massnahmen/60b_KWG_84_WpIG_und_57_GwG/meldung_2022_11_08_Coinbase_Germany.html*; Abruf: 8. November 2022).

[BaFin 2023] BaFin, Unternehmensdatenbank, Kategorie „Kryptoverwahrer“, (*https://portal.mvp.bafin.de/database/InstInfo/sucheForm.do*; Abruf: 30. Juni 2023).

[Barth 2022] Barth, „Verkauf des Bankhauses von der Heydt ist gescheitert“, (*https://finanzbusiness.de/nachrichten/fintech/article13879384.ece*; Abruf: 2. Dezember 2022).

[Binance 2022] Binance Capital Management Co. Ltd., „PROOF OF RESERVE (“POR”) Report“, (*https://merkle.silversixpence.io/files/Binance%20POR%20Report%207%20December%202022.pdf*; Abruf: 26. Februar 2023).

[Bloomberg 2023] Bloomberg, „Valkyrie Is Latest ETF Issuer to Refile Bitcoin Fund Application With SEC“, (*https://www.bloomberg.com/news/articles/2023-07-05/valkyrie-is-latest-etf-issuer-to-refile-bitcoin-fund-application*; Abruf: 6. Juli 2023).

[CNBC 2022] CNBC, „Mazars Group suspends all work with crypto clients including Binance, Crypto.com, citing concerns over public perception of proof of reserves“, (*https://www-cnbc-com.cdn.ampproject.org/c/s/www.cnbc.com/amp/2022/12/16/mazars-suspends-all-work-with-crypto-clients-including-binance-cryptocom.html*; Abruf: 6. Januar 2023).

[CoinMarketCap 2023] CoinMarketCap „Top Cryptocurrency Spot Exchanges“, (*https://coinmarketcap.com/rankings/exchanges/*; Abruf: 26. Februar 2023).

[Gebhardt et. al. 2006] Gebhardt / Illies / Schindler, „A Note on the Practical Value of Single Hash Collisions for Special File Formats“, in: Sicherheit 2006: Sicherheit - Schutz und Zuverlässigkeit, Beiträge der 3. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI), 2006.

[Hamill et. al. 2005] Hamill / Gambetta, „Streetwise: How Taxi Drivers Establish Customers’ Trustworthiness“, 2005.

[IDW 2020] Institut der Wirtschaftsprüfer in Deutschland e.V., WP Handbuch 2020, 17. Auflage; Düsseldorf: IDW Verlag, 2020.

[IDW 2022] Institut der Wirtschaftsprüfer in Deutschland e.V., International Standard on Auditing 200: Übergeordnete Ziele des unabhängigen Prüfers und Grundsätze einer Prüfung in Übereinstimmung mit den International Standards on Auditing (ISA DE 200), Stand: 28. September 2022.

[IIA 2020] The Institute of Internal Auditors (IIA), „The IIA’s Three Lines Model“ (Update 2020), (*https://www.theiia.org/globalassets/site/content/articles/global-knowledge-brief/2020/july/the-iias-three-lines-model/glob-three-lines-model-paper_layout-rebuild.pdf*; Abruf: 7. September 2023).

[ISACA 2021] Information Systems Audit and Control Association, Inc., „Blockchain Framework Audit Program (2021)“, (*https://www.isaca.org/blockchain-framework-audit-program*; Abruf: 23. April 2023).

[ISACA 2022-1] Information Systems Audit and Control Association, Inc., „Digital Trust Ecosystem Framework (DTEF)“, 2022.

[ISACA 2022-2] ISACA Germany Chapter e. V. / Fachgruppe IT-Revision, „Grundlagen der IT-Revision für den Einstieg in die Praxis“ (2022),

Storkower Str. 158
10407 Berlin
Germany
E: info@isaca.de
T: +49 30 37580810
W: www.isaca.de

(*https://www.isaca.de/images/Publikationen/Leitfaden/ISACA%20Leitfaden%20Grundlagen%20der%20IT-Revision%202022.pdf*; Abruf: 7. September 2023).

[ISACA 2023] Information Systems Audit and Control Association, Inc., „State of Digital Trust 2023“, (*https://www.isaca.org/resources/reports/state-of-digital-trust-2023*; Abruf: 9. Mai 2023).

[Lynn et. al. 2021] Lynn / van der Werff / Fox, „Understanding Trust and Cloud Computing: An Integrated Framework for Assurance and Accountability“, in: Theo Lynn, John G. Mooney, „Data Privacy and Trust in Cloud Computing“, Palgrave Macmillan Cham, Switzerland, 2021.

[Marten et. al. 2003] Marten / Quick / Ruhnke, „Wirtschaftsprüfung – Grundlagen des betriebswirtschaftlichen Prüfungswesens nach nationalen und internationalen Normen“, 2. Auflage; Stuttgart: Schäffer-Poeschel Verlag, 2003.

[Mayer et. al. 1995] Mayer / Davis / Schoorman, „An Integrative Model of Organizational Trust. The Academy of Management Review“, 20(3), 709–734, 1995, (*https://doi.org/10.2307/258792*; Abruf: 6. Juli 2023).

[McKnight et. al. 2011] McKnight / Carter / Thatcher / Clay, „Trust in a Specific Technology: An Investigation of Its Components and Measures“, in: ACM Transactions on Management Information Systems, Vol. 2, No. 2, Article 12 (June 2011).

[Ostrom/Walker 2003] Ostrom / Walker, „Trust in Two-Person Games: Game Structures and Linkages”, In: Trust and Reciprocity: Interdisciplinary lessons from experimental research, 2003.

[PCAOB 2023] PCAOB, „Investor Advisory: Exercise Caution With Third-Party Verification/Proof of Reserve Reports", (*https://pcaobus.org/resources/information-for-investors/investor-advisories/investor-advisory-exercise-caution-with-third-party-verification-proof-of-reserve-reports*; Abruf: 8. März 2023).

[Ray 2023] Ray III, „Chapter 11, Case No. 22-11068, in re: FTX Trading Ltd., et al.“, (*https://restructuring.ra.kroll.com/FTX/Home-DownloadPDF?id1=MTQ5MDc2OQ==&id2=-1*; Abruf: 11. April 2023).

[Reuters 2023] Reuters, „Analysis: US SEC crackdown on Coinbase, Binance puts crypto exchanges on notice“, (*https://www.reuters.com/business/finance/us-sec-coinbase-binance-crackdown-puts-crypto-exchanges-notice-2023-06-08/*; Abruf: 6. Juli 2023).

[Simmel 1968] Simmel, „Soziologie. Untersuchungen über die Formen der Vergesellschaftung.“, 5. unver. Aufl.; Berlin: Duncker & Humblot, 1968.

[Tether 2022] Tether Holdings Limited, „INDEPENDENT AUDITORS' REPORT ON THE CONSOLIDATED RESERVES REPORT“, (*https://assets.ctfassets.net/vyse88cgwfbl/1Xfu4398CIoMiuKjPhvnHM/6d1608c90bb775d2d432b7b24264da28/ESO.02_Std_ISAE_3000R_Opinion_30-9-2022_RC134792022BD0548.pdf*; Abruf: 26. Februar 2023).

[Trautmann 2023] Trautmann, „A Review of FTX’s Control Failures Considering the Upcoming European Regulatory Regime”, Journal of International Banking Law and Regulation, Vol. 8, 2023.

[Trautmann/Ewel 2020] Trautmann / Ewel, „Der RiSi2Ko-Prüfungsansatz“, in: die bank, Zeitschrift für Bankpolitik und Praxis, Juli 2020.

[Trautmann/Ewel 2022] Trautmann / Ewel, „Der Einsatz von Blockchain Analytics bei KWG-Instituten“, in: IT-Governance, Heft 35, Juni 2022.

Autorenteam

- Dirk Diefenbach (WP, StB), dhpg Wirtschaftsprüfer Rechtsanwälte Steuerberater GmbH & Co. KG
- Christian Ewel (CISA, CRISC), Flick Gocke Schaumburg Partnerschaft mbH
- Christian Schulz (CISA), Fujitsu Services GmbH
- Kilian Trautmann (CISA)
- Marc Weber (CISA, CGEIT, CRISC), selbständiger Unternehmensberater, Mitherausgeber der IT-Governance
- Dr. Laurin Weissinger (CISA, CISM, CRISC), Fresenius Digital Technology

Vorstand ISACA Germany Chapter

- Dr. Tim Sattler (Präsident)
- Thomas O. Englerth (Vizepräsident – Zertifizierungen)
- Dirk Meissner (Vizepräsident – Finanzen und Verwaltung)
- Markus Gaulke (Vizepräsident – Weiterbildung)
- Prof. Dr. Matthias Goeken (Vizepräsident – Veröffentlichungen)
- Julia Hermann (Vizepräsidentin – Kommunikation und Marketing)
- Matthias Kraft (Vizepräsident – Fachgruppen)

Möchten Sie zu diesem Positionspapier mit uns Kontakt aufnehmen. Dann schreiben Sie uns bitte an: FG_digital-trust@isaca.de

Interessieren Sie sich für weitere Veröffentlichungen des ISACA Germany Chapter? Dann besuchen Sie uns jetzt auf: http://www.isaca.de/publikationen