BLOCKCHAIN REALLABOR RHEINISCHES REVIER

# Gestohlene und verlorene Wallets

K. Wittek[1], T. Spielmann[1]
[1] Institut für Internet-Sicherheit – if(is), Westfälische Hochschule, Gelsenkirchen, Deutschland
kontakt_reallabor@fit.fraunhofer.de

## Ausgangssituation und Problemstellung

In Wallets werden im Kontext von DLT-Systemen und SSI-Systemen die eigenen persönlichen Daten aufbewahrt. Eine Wallet kann sowohl in Form von Software als auch als Hardware realisiert werden und ist vergleichbar mit der Aufbewahrung von Zeugnissen und persönlichen Dokumenten in der analogen Welt. Daher ist aus der analogen Welt ebenfalls bekannt, mit wie viel Aufwand eine verlorene oder gestohlene Brieftasche bedeutet. Der Vorteil einer digitalen Wallet ist jedoch, dass diese einfacher zu kopieren sind. Genau aus diesem Grund ist ein umfangreiches Sicherheitskonzept unerlässlich.

## Anwendungskontext

Wallets sind als Aufbewahrungsort für off-chain gespeicherte Daten von großer Bedeutung. Jedoch gibt es grob zwei Kategorien von Daten, welche in einer Wallet gespeichert werden.

*Wallet mit Rechten*

Eine Wallet für Rechte kommt in einer permissioned Blockchain zum Einsatz. Das bedeutet in dieser Wallet würde privates Schlüsselmaterial verwaltet werden, welches zum Signieren von Daten genutzt werden darf. Diese Wallet gehört zum Beispiel einer Meldebehörde, einem Prüfungsamt oder Ähnlichem. Das bedeutet, bei einem Abhandenkommen durch Verlust oder Diebstahl ist die Integrität des Systems essentiell gefährdet. Daher müssen hier dringend allgemeintaugliche Lösungen her, um dieses Risiko mitigieren zu können.

*Wallet für Daten*

Eine Wallet für Daten enthält beispielsweise Credentials über die Identität, Zeugnisse, Bankdaten, oder Ähnlichem. Diese Daten sind personenbezogen und gehören in der Regel dem Eigentümer. Sie dienen beispielsweise zum Nachweis der eigenen Identität, Bankverbindung, Zeugnisse oder Ähnlichem. Somit bedeutet ein Abhandenkommen durch Verlust oder Diebstahl zwar einen großen Aufwand für den Eigentümer, gefährdet aber die Integrität des Systems nicht erheblich. Trotzdem muss auch hier eine praxistaugliche Lösung gefunden werden, um den Verlust für den Eigentümer abzumildern. Eine Besonderheit stellt außerdem das Wallet als Zugang zu virtuellen und cyber-physischen Assets dar. Ein Verlust bedeutet hier in der Regel den Verlust der Assets.

## Lösungsansätze

Als Lösung dieser Forschungsfrage ist ein Leitfaden denkbar. Dieser soll die Anwender in die Lage versetzen sich sowohl für die richtige Wallet zu entscheiden als auch diese sicher gegen Verlust oder Diebstahl sichern zu können. Im Folgenden sind einige wichtige und grundlegende Unterscheidungen aufgezählt, welche im Rahmen dieser Forschungsfrage unbedingt wieder aufgegriffen und tiefgehend beleuchtet werden sollten.

*Hardware vs. Software Wallet*

In diesem Punkt soll die Umgebung der Wallet betrachtet werden. Unter einem Hardware-Wallet versteht man in der Regel Sicherheitstoken, USB-Sticks oder auch einen ausgedruckten QR-Code. Sie haben alle eine Sache gemeinsam: Sie sind nicht ständig aktiv, sondern werden nur während der Benutzung unter Strom gesetzt. Somit wird das Zeitfenster eines potentiellen Angriffs deutlich reduziert. Allerdings leiden hierunter die Anwenderfreundlichkeit und die Flexibilität, da eine solche Wallet unter Umständen nicht immer mitgeführt wird. Entgegengesetzt verhält es sich bei einem Software-Wallet. Hierbei handelt es sich um eine Software, welche auf einem anderen (Betriebs-)System läuft, bspw. auf einem Smartphone, Tablet oder PC. Dieser Umstand erhöht nicht nur die Flexibilität, sondern auch die Angreifbarkeit, da es ständig aktiv ist. Daher soll hier der Unterschied zwischen Hard-

und Software-Wallets deutlich gemacht werden. Dabei ist eine Schwerpunktbetrachtung der möglichen Sicherheitskonzepte dieser beiden Möglichkeiten angebracht.

*Hot vs. Cold Wallet*

Die Entscheidung zwischen Hot- und Cold-Wallet, also mit Internetverbindung oder offline, ist eine weitere wichtige Entscheidung, nicht nur aus der Sicht der Sicherheit. Hierbei wird eine Hot-Wallet meist beim Betreiber online gespeichert und verursacht so weniger Aufwand für den Eigentümer. Doch das bedeutet nicht nur Komfort, sondern auch Kontrollverlust und Angreifbarkeit. Eine Cold-Wallet kehrt die Vor- und Nachteile hingegen jeweils um. Da es sich hier um eine offline Wallet handelt, ist diese direkt beim Eigentümer gespeichert, unabhängig ob in Form von Hard- oder Software. Jedoch muss diese vor der Verwendung erst mit dem Internet verbunden bzw. die Daten aus ihr ausgelesen werden. Diese Auslesevorgang kann weitere riskante Vorgänge enthalten. Im Kontext dieser Forschungsfrage soll daher der Unterschied von Hot- und Cold-Wallets deutlich werden. Hierbei liegt der Fokus auf der Sicherheit und Benutzerfreundlichkeit der einzelnen Varianten.

*Sicherheitsstrategien bei der Nutzung von Wallets*

Auch die konkrete Nutzung einer Wallet kann zur Sicherheit und vor Allem zum Abschwächen der Folgen eines Verlustes beitragen.

Eine grundsätzliche Maßnahme gegen Datenverlust ist die Erstellung von Backups. Diese können auf demselben Gerät gespeichert werden, um die Daten schnell bei kleinen Fehlern wiederherstellen zu können. Dieses muss jedoch ebenso gut abgesichert werden, wie die Wallet selbst. Gegen einen Defekt der Wallet bzw. des Geräts mit der Wallet hilft die Speicherung eines Backups auf einem externen Gerät. Hier kann im Rahmen der Forschungsfrage ein Konzept zur Backup-Erstellung, -Speicherung und –Wiederherstellung erstellt werden.

Auch können unterschiedliche Wallet-Instanzen für Credentials unterschiedlicher Arten genutzt werden. Beispielsweise eine Wallet für tägliche Credentials wie Identität, bargeldloses Zahlen oder Ähnliches; und eine andere Wallet für nicht-alltägliche Credentials wie z.B. Zeugnisse und Bescheinigungen. Ebenfalls kann im Rahmen der Forschungsfrage eine Strategie für eine mögliche Aufteilung entwickelt werden.

Selbstverständlich kann eine Lösung auch mehrere dieser oben genannten Aspekte kombinieren. Dies ist im Sinne der Sicherheit von Wallets und als Vorbeugung vor Verlust dringend empfohlen. [3].

## Literatur

1 Norbert Pohlmann, 2019, "Cyber-Sicherheit - Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung", Kapitel 14.6 Sicherheit und Vertrauenswürdigkeit der Blockchain-Technologie

2 Sichern Sie Ihre Wallet , https://bitcoin.org/de/sichern-sie-ihre-wallet#online

3 Intro to Ethereum Wallets: https://docs.ethhub.io/using-ethereum/wallets/intro-to-ethereum-wallets/

## Forschungseinrichtungen

Zur Bearbeitung dieser Forschungsfrage sind Kompetenzen aus folgenden Bereichen erforderlich:

- Cyber-Security
- Informatik (UX)