GameChanger

Multi Blockchain Offline Verwahrung

Programm / Ausschreibung	IWI, IWI, Basisprogramm Ausschreibung 2023	**Status**	abgeschlossen
Projektstart	16.11.2022	**Projektende**	16.11.2023
Zeitraum	2022 - 2023	**Projektlaufzeit**	13 Monate
Keywords			

Projektbeschreibung

Ziel dieses Projekts ist es einen hochsicheren Crypto Safe zu entwickeln und damit die Grundvoraussetzung für die Potenziale der Blockchain Technologie zu schaffen.

Mit dem Projekt wird einerseits auf die No-Cloud-Policy traditioneller Banken und andererseits auf institutionelle prozess- und aufsichtsrechtliche Anforderungen reagiert. Die Daten der Bankkunden dürfen beispielsweise das Hoheitsgebiet der Bank nicht verlassen. Der Verwahrungsservice über eine reine Cloud-Anwendung (Webapplikation, die mit Wallet-Servern im Rechenzentrum der TMIA GmbH kommuniziert) ist aus Sicherheitsgründen untersagt. Daher wollen wir eine On-Premises-Lösung entwickeln, die in den Rechenzentren der Banken eingerichtet und gehostet werden kann, den NodeVenture GameChanger.

Ziele des Vorhabens im Überblick:
- Hochsichere und benutzerfreundliche Verwahrung der Private Keys
- Schutz vor Naturkatastrophen, Stromausfällen oder anderen externen Faktoren
- Wiederherstellbarkeit des digitalen Vermögens bei plötzlichem Tod eines Nutzers
- Ausschluss von Diebstahl und Manipulation (intern/extern)

1. Crypto Safe (mit Schutzpanzer)
Ein Private Key fungiert als eindeutig auf eine Person zugewiesener Schlüssel, eine Art persönliche digitale Signatur mittels der mit einer Blockchain sowie deren Netzwerkteilnehmern interagiert werden kann. Ohne den Private Key sind die digitalen Vermögens-werte für immer verloren. Einerseits müssen die Schlüssel rund um die Uhr zur Verfügung stehen, da ansonsten die Handlungsfähigkeit eingeschränkt wird. Andererseits dürfen die Schlüssel nicht in falsche Hände geraten. Die Offlineverwahrung von Private Keys, auf die dennoch über unsere Kommunikationstechnologie rund um die Uhr zugegriffen werden kann, ist das Herzstück des Projekts, der NodeVenture Crypto Safe.

Ergebnis: Stabiles und performantes System, das man nicht manipulieren kann und das ununterbrochen automatisiert überwacht wird (Walletserver & Schutzpanzer). Nur im Ausnahmefall der Wartung kann auf das System zugegriffen werden,

jedoch ohne die geringste Möglichkeit an sensible Informationen zu gelangen.

2. NodeVenture-Cloud

Um Transaktionen mit Kryptowährungen abzurufen, aktuelle Informationen zu Transaktionsgebühren zu erhalten, neue Transaktionen zu erstellen sowie an die Blockchain zu übermitteln, werden Full Nodes diverser Blockchains (Bitcoin, Ethereum, ...) betrieben. Die Full Nodes müssen dabei mit Offline-Wallet-Servern Informationen austauschen. Da-bei darf die Integrität der Daten (Wallet-Adressen, Transaktionsbeträge) niemals gefährdet werden. Nur wer Full Nodes betreibt, also Netzwerkknotenpunkte mit der kompletten Information einer Blockchain, kann sich der Integrität der Daten sicher sein. Außerdem werden Full Nodes betrieben, um diesbezüglich von Drittanbietern unabhängig zu sein und auch um den Schutz der Privatsphäre gewährleisten zu können. Des Weiteren setzen wir auf die Entwicklung einer eigenen Cloud-Solution, die wir in nationalen Rechenzentren hosten, um auf internationalen Cloud-Anbieter, wie AWS, Azure oder Google-Cloud verzichten zu können. Diesen Schritt gehen wir aus Datenschutz- und Transparenzgrün-den. Außerdem können wir nur unsere eigene Cloud überwachen. Sollte ein externer Cloudanbieter Probleme haben, kommen wir nicht in der für uns notwendigen Zeit an die Informationen. Ein weiteres Ziel ist es deshalb, eine NodeVenture-Cloud aufzubauen, die Full Nodes betreibt und stets valide Marktdaten zur Verfügung stellt. Es muss ein sicherer Informationsaustausch zwischen der NodeVenture-Cloud und dem Offlinesystem entwickelt werden.

Ergebnis: Die NodeVenture Cloud muss sämtliche Marktdaten für die Endkunden zu Verfügung stellen und ohne Unterbrechung mit dem Crypto Safe kommunizieren. Zudem darf die Performance keinesfalls bei Mehrauslastung sinken.

3. Überwachungs- und Kontrollzentrum

Eine weitere Herausforderung besteht in der Überwachung und Wartung der On-Premises-Lösung, insbesondere in der Echtzeitüberwachung des Offlinesystems. Ein Überwachungs- und Kontrollzentrum muss stets über den Zustand des Wallet-Servers informiert sein, um bei Unregelmäßigkeiten oder Problemen frühzeitig zu intervenieren. Nur so kann ein ununterbrochener reibungsloser Betrieb aufrechterhalten werden. Dies gilt ebenso für die Kontrolle des Schutzpanzers. Für die Überwachung eines Systems, mit dem keine Onlineverbindung besteht, gibt es nur den Weg über die patentierte Kommunikationstechnologie (Optokoppler), um Informationen über den aktuellen Zustand des Systems nach außen zu kommunizieren. Dazu müssen notwendige Parameter genauso wie Konzepte für deren Messbarkeit entwickelt werden.

Ergebnis: Durch das Monitoring sollen die Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Services sichergestellt werden, sowie missbräuchliche Verwendungen dieser erkannt werden. Verlässliche Parameter geben jederzeit Auskunft über den Zu-stand des kompletten Crypto Safes (Walletserver, Optokoppler, Schutzpanzer). Unregelmäßigkeiten und verdächtige Handlungen werden resultieren in Alarm und dementsprechende Gegenmaßnahmen werden eingeleitet.

4. Schaltzentrale

Zu guter Letzt braucht es eine Art Schaltzentrale, die den Informationsaustausch zwischen den einzelnen Komponenten durchführt und den Betrieb aufrechterhält. Zu den Bestandteilen der On-Premises-Lösung gehört auch die Anwendung durch Endnutzer (Webapplikation).

Ergebnis: Die Schaltzentrale ist verantwortlich für die Benutzerverwaltung. Sie muss bestehende Kundenlösungen einfach integrieren können. Beispielsweise eine Integration in ein bestehendes Onlinebanking. Für die Skalierbarkeit soll ein Rollout

in die Cloud mit Parallelisierung möglich sein. Weiters ist die Schaltzentrale für eine sichere Kommunikation sowohl zur NV-Cloud als auch zum Crypto Safe verantwortlich. Abschließend braucht es eine saubere Spezifikation für sämtliche Wartungsprozesse und Zugriffsrechte (inklusive Monitoring).

Projektpartner

- TMIA GmbH in Liquidation