Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Informatik

Secure Counter Solution

Themenbereiche:	Verteilte Datenspeicherung, Blockchain, Softwareentwicklung
Studierender:	Philipp Leu, Diego Bienz
Dozent:	Prof. Martin Jud
Experte:	Urs Gehrig
Wirtschaftspartner:	Nicht publik
Keywords:	Blockchain, Ethereum, .NET Core, ASP, Embedded Software

1. Aufgabenstellung

Der Wirtschaftspartner dieser Bachelor Diplomarbeit ist ein führender Hersteller von Maschinen in seiner Branche. Diese Maschinen verfügen über einen Stückzähler, welcher die Anzahl produzierten Produkte zählt und damit zulässt, das Alter bzw. die Abnutzung der Maschine zu schätzen. Dieser Stückzähler funktionierte bisher mechanisch und verursachte Fixkosten für jede produzierte Maschine. Innerhalb dieser Projektarbeit soll dieser mechanische Stückzähler durch eine Softwarelösung ersetzt werden. Der neue Stückzähler darf nicht mehr Fixkosten verursachen und soll die bisherigen Funktionalitäten erweitern. Die Software muss sich dabei auf die Integrität und den Schutz des Zählerstandes konzentrieren und ein Vertrauen in den generierten Wert schaffen. Es wird zusätzlich gewünscht, dass bei den Lösungsvarianten der Einsatz von Blockchain-Technologien geprüft wird.

2. Ergebnisse

Im Rahmen der Bachelor Diplomarbeit werden folgende Ergebnisse erarbeitet:

- **Ethereum Blockchain:** Für die gewählte Softwarearchitektur ist eine Blockchain notwendig. Dazu wurde eine Ethereum Blockchain aufgesetzt und konfiguriert.
- **Smart Contract:** Für die Ausführung von Code innerhalb der Ethereum Blockchain wird ein Smart Contract benötigt. Daher wurde für den Betrieb der Secure Counter Solution in Kombination mit der Blockchain ein Smart Contract implementiert und in der Blockchain veröffentlicht.
- **SCS Client:** Der Secure Counter Solution (SCS) Client bildet die Client Applikation, die auf jeder Maschine betrieben wird. Diese Software zählt die produzierten Stücke, sichert die Integrität der Daten und kommuniziert mit der Ethereum Blockchain.
- **SCS Web Management:** Zur Administration und zur Einsicht der Daten wurde eine Webapplikation implementiert. Das SCS Web Management lässt alle nötigen Funktionen für den Betrieb der Lösung zu.

3. Lösungskonzept

Zu Beginn des Projekts wurden verschiedene Lösungsvarianten zur Softwarearchitektur untersucht. Mit dabei waren verschiedene Blockchain-Technologien und ein typisches Server-Client-Modell. In Abbildung 1 ist die Softwarearchitektur des endgültigen Entscheids zu sehen. Die Maschinen sind unabhängig voneinander über mehrere Standorte verteilt. Auf der Maschine wird der SCS Client betrieben. Die Ethereum Blockchain und das SCS Web Management laufen zentral in einer Cloud-Umgebung. Diese Komponenten werden folgend beschrieben.

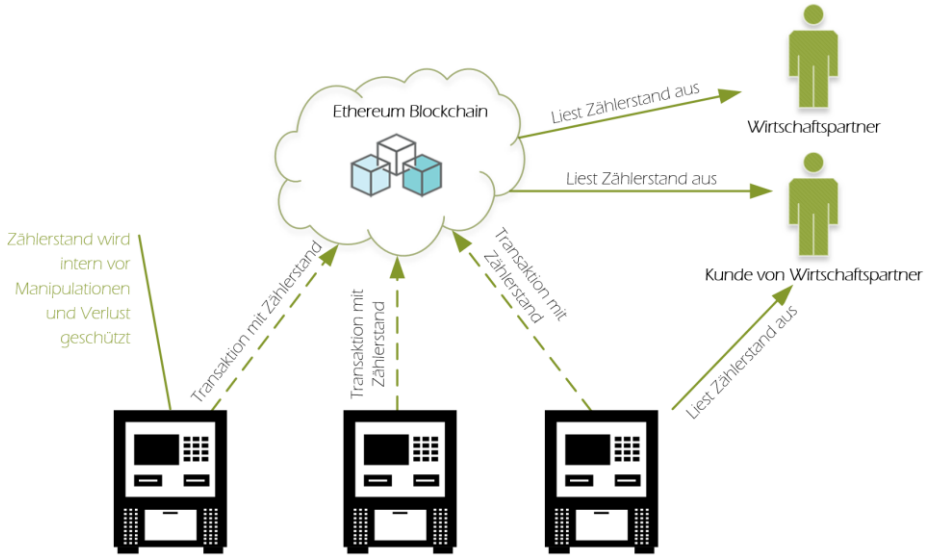

Abbildung 1 - Softwarearchitektur

SCS Client

Die lokale Verarbeitung des Zählerstandes erfolgt durch den SCS Client. Dieser ist in .NET Core implementiert. Dabei werden die produzierten Daten durch den SCS Client mit verschiedenen Methoden vor Verlust und Manipulation geschützt und in der Maschine auf mehreren Komponenten verteilt gespeichert. Um die Kommunikation mit der Ethereum Blockchain zu vereinfachen, wird die C# Open Source Bibliothek namens Nethereum eingesetzt. Der Zählerstand wird in regelmässigen Abständen an die Blockchain gesendet.

Ethereum Blockchain

Als Blockchain wird eine private Ethereum Blockchain eingesetzt. Für die Interaktionen und die Funktionen innerhalb der Blockchain wurde ein Smart Contract in Solidity implementiert. Dieser stellt zahlreiche Methoden zur Verfügung und verbessert mit den integrierten Funktionalitäten von Solidity die Datenintegrität bzw. -sicherheit. Der Smart Contract behandelt die Zählerstände und den gesamten Zählerverlauf von jeder Maschine im System.

SCS Web Management

Um die Blockchain sowie den Smart Contract zu administrieren, wurde eine Web-Applikation entwickelt. Diese ist in ASP .NET Core implementiert und in der Cloud veröffentlicht. Sie ermöglicht es, den Zählerstand oder den Zählerverlauf von der Blockchain abzufragen und den Smart Contract und die Ethereum Accounts zu verwalten.

4. Spezielle Herausforderungen

Der Entscheid für die Softwarearchitektur bedurfte viel Recherche und Zeit. Blockchain basiert zwar auf bewährten Verschlüsselungsmethoden, ist aber eine sehr junge Technologie. Es existieren verschiedene Projekte, viele davon sind jedoch in einer frühen Entwicklungsphase und zusätzlich sehr komplex. Bevor der Entscheid auf Ethereum fiel, wurden noch einige andere Blockchain Technologien ausprobiert und getestet.

Eine weitere Herausforderung war das Zusammenspiel von Hardware, Software und Cloud. Während die Hardware bereits bei Projektbeginn klar definiert war, wurde noch über die Softwarearchitektur entscheiden. Damit die Entwicklung möglichst unabhängig von Komponenten und deren Standort durchgeführt werden konnte, wurden frühzeitig Interfaces definiert. Diese Interfaces erlauben es ausserdem, die Software nach dem Projekt entsprechend zu ändern oder zu erweitern.

5. Ausblick

Die umgesetzte Lösung ist eine umfangreiche Basis für eine sichere Stückzähler-Software. Der SCS Client ist getestet und verfügt über alle nötigen Funktionalitäten, um in einer produktiven Umgebung integriert werden zu können. Das SCS Web Management und einige Einstellungen in der Blockchain müssen jedoch vor einer kompletten Integration in die produktiven Maschinen noch überarbeitet werden.

Die Lösung zeigt einen sinnvollen Einsatz einer Blockchain. Auf dieser Arbeit kann nun aufgebaut werden und neue Lösungen können in Zukunft mit anderen Smart Contracts in die private Ethereum Blockchain integriert werden. Die Softwarearchitektur bietet viel Potential und die Bachelor Diplomarbeit kann als Fundament für zukünftige Blockchain-Services desselben Wirtschaftspartners angesehen werden.