TECHNISCHE UNIVERSITÄT BERLIN

Institut für Werkzeugmaschinen und Fabrikbetrieb
Fachgebiet Industrielle Automatisierungstechnik
Prof. Dr.-Ing. Jörg Krüger

Automatisierungstechnisches Projekt

Blockchain für die vernetzte Automatisierungstechnik

Gruppe 12

Exposé

Reeder, Jörg Michael	341148	joerg.m.reeder@campus.tu-berlin.de
Loi, Justin Bryan	450377	j.loi@campus.tu-berlin.de
Rusli, Eric	407066	eric.rusli@campus.tu-berlin.de

Betreuer: Axel Vick

Inhaltsverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

CAV Connected and Autonomous Vehicles.

PoS Proof of Stake.

PoW Proof of Work.

1 Einleitung

1.1 Motivation

Sicherheit ist ein wichtiges Thema in der Industrie, insbesondere in der Automatisierungstechnik. Durch die fortschreitende Vernetzung und Nutzung Cloud-basierter Dienste, werden die sicheren Netzwerkgrenzen überschritten und es entstehen Angriffspunkte für Cyberattacken. Ein Beispiel sind Cyberangriffe auf vernetzte und autonome Fahrzeuge (CAVs). Ein Cyberangriff auf ein CAV wurde in einer kontrollierten Umgebung demonstriert, als ein bekannter Hack eines Jeep Cherokee im Juli 2015 durch zwei Forscher dazu führte, dass ein Reporter von WIRED unter einer Autobahnüberführung feststeckte und nicht in der Lage war, die Kontrolle über das Fahrzeug zu übernehmen[2].

Fahrzeugsensoren sind mögliche Angriffsvektoren, aber auch unsichere Netzwerkverbindungen ermöglichen Hackern den Zugang zu CAV-Computern. Um die Sicherheit vernetzter Anlagen zu gewährleisten müssen kryptographische Methoden eingesetzt werden. Eine solche Methode die schnell an Popularität gewinnt, ist die Blockchain-Technologie. Die Nutzung dieser Technologie soll in diesem Projekt untersucht werden.

1.2 Blockchain

Die Blockchain ist ein verteiltes gemeinsames Kontobuch und eine Datenbank mit Eigenschaften wie Dezentralität und Freiheit[3]. Am besten bekannt sind sie als Grundlage von Kryptowährungssystemen wie Bitcoin oder Ethereum, um eine sichere und dezentrale Aufzeichnung von Transaktionen zu führen. Die Innovation der Blockchain besteht darin, dass sie die Vertrauenswürdigkeit und Sicherheit eines Datensatzes garantiert, ohne dass ein vertrauenswürdiger Dritter benötigt wird.

Ein wesentlicher Unterschied zwischen einer typischen Datenbank und einer Blockchain ist die Art und Weise, wie die Daten strukturiert sind. Eine Blockchain sammelt Informationen in Gruppen, die als „Blöcke“ bezeichnet werden und Informationen enthalten. Blöcke haben bestimmte Speicherkapazitäten und werden, wenn sie gefüllt sind, geschlossen und mit dem zuvor gefüllten Block verknüpft, wodurch eine Datenkette gebildet wird, daher der Name „Blockchain“. Ein neuer Block wird von den Teilnehmern der Blockchain validiert und es wird mit einem Konsens-Algorithmus entschieden ob der Block angehängt wird. Da jeder Block Informationen über den vorherigen Block enthält ist es praktisch unmöglich die Blöcke zu verändern ohne das die anderen Teilnehmer etwas davon merken.

1.3 Smart Contract

Ein Smart Contract ist ein sich selbst ausführender Vertrag, bei dem die Bedingungen der Vereinbarung zwischen Käufer und Verkäufer direkt, als Code, in einer Blockchain hinterlegt ist[1]. Der Code und die darin enthaltenen Vereinbarungen sind dadurch dauerhaft und unveränderlich gesichert. Der Smart Contract steuert die Ausführung von Transaktionen abhängig von den enthaltenen Bedingungen und diese sind nachverfolgbar und irreversibel. Außerdem ermöglichen Smart Contracts die Durchführung vertrauenswürdiger Transaktionen und Vereinbarungen zwischen unterschiedlichen, anonymen Parteien, ohne dass eine zentrale Behörde, ein Rechtssystem oder ein externer Durchsetzungsmechanismus erforderlich ist.

2 Projekt und Zielsetzung

2.1 Spezifizierung des Projektziels

Ziel des Projekts ist ein Informationsgewinn darüber, ob und wie Blockchain Technologie genutzt werden kann, um die Kommunikation und Datenübertragung von vernetzten Teilnehmern in einem automatisierungstechnischen-Umfeld kryptografisch abzusichern. Dazu soll möglichst ein für die Rahmenbedingungen der Automatisierungstechnik geeigneter Blockchain Algorithmus ausgewählt, und eine Kommunikation zwischen mehreren Endpunkten anhand eines Beispiels Implementiert werden. Es soll außerdem ein Smart Contract entwickelt werden, der einen einfachen Steuerungsalgorithmus implementiert.
Probleme, die es zu lösen gilt, sind die Integration von Smart Contracts als Eingabe des Nutzers, die interne Kommunikation im Blockchain-basierten System, entweder als Speichersystem oder Kommunikationsmethode. Das Finden und Implementieren der am besten geeigneten Methode zur Konsensbildung ist ebenfalls eine der Herausforderungen in diesem Projekt.
Das Ergebnis soll hinsichtlich der üblichen Rahmenbedingungen in der Automatisierungstechnik ausgewertet werden. Dabei sollen die Machbarkeit, Sicherheit und Geschwindigkeit des Kommunikationssystems vor diesem Hintergrund aufgezeigt werden.

2.2 Betreuung und Organisation

Die Betreuung dieses Projekts übernimmt Axel Vick, der gleichzeitig als der Auftraggeber fungiert. Kommunikation mit dem Betreuer und der Projektorganisation und -koordination wird ein Projektleiter gewählt. Diese Verantwortung wird immer für vier Wochen übertragen, um die Aufwände der Gruppenmitglieder vergleichbar zu gestalten. Die Rotation wird dabei wie folgt festgelegt:
Michael – Justin – Eric.
Darüber hinaus wird für jedes Arbeitspaket ein Verantwortlicher bestimmt, der die Bearbeitung dessen koordiniert. Außerdem finden jede Woche folgende Meetings statt:

- Sprechstunden mit dem Betreuer: Donnerstag 10:00 Uhr
- Gruppen-Meeting: Montag 18:00 Uhr

2.3 Arbeitspakete

1. **Literaturrecherche**
   Die Projektgruppe muss sich mit dem Stand der Technik und eventuellen Vorarbeiten vertraut machen. Thematische Schwerpunkte sind:
   - Blockchain
   - Sichere Kommunikation
   - Smart Contracts
   - Kommunikation in der Automatisierungstechnik

   Alle Gruppenmitglieder sollen an der Literaturrecherche teilnehmen und die Zusammenhänge nachvollziehen können.

2. **Analyse der Problemstellung**
   Um die Rahmenbedingungen für die spätere Konzeption festzulegen, sollen übliche Infrastrukturen in der Automatisierungstechnik sowie Konzepte und Implementierungen der Blockchain Technologie analysiert werden. Dies soll insbesondere dazu dienen eine geeignete Blockchain Infrastruktur für das Projekt zu ermitteln. Das Arbeitspaket lässt sich in folgende Unterpakete aufteilen:

   - Automatisierungstechnische Komponenten
     Hier geht es um die Eigenschaften und Einschränkungen der üblichen automatisierungstechnischen Komponenten. Es soll analysiert werden, welche Komponenten an eine Blockchain angebunden werden können und welche gegebenenfalls als "Mining Node" eingesetzt werden könnten. Es kann hier auch ein Setup für eine beispielhafte Simulations- oder Hardwareumgebung vorgeschlagen werden.
   - Ausführungsumgebungen und Kommunikationsinfrastrukturen
     Automatisierungstechnische Komponenten sind in unterschiedlichen Netzwerken angebunden und laufen mit verschiedenen Anwendungsumgebungen. Es gilt festzustellen, welche Netzwerke und Ausführungsumgebungen üblich sind und welche Eigenschaften und Rahmenbedingungen sie für die Implementierung einer Blockchain Kommunikation mitbringen.
   - Gegenüberstellung von Algorithmen zur Konsensbildung und Dokumentation
     Die Protokolle zur Konsensbildung werden in diesem Abschnitt weiter untersucht, zum Beispiel PoW und PoS. Dies schließt auch die Ausführung von Smart Contracts für den erwähnten Konsens ein. Des Weiteren werden die Protokolle im Hinblick auf ihre Eignung für dieses Projekt miteinander verglichen.

3. **Konzeption eines Kommunikationsprotokolls basierend auf Blockchain**
   Nachdem die Rahmenbedingungen geklärt und ein geeigneter Algorithmus ausgewählt ist, wird ein Konzept erstellt, dass den Kommunikationsablauf und alle nötigen Komponenten spezifiziert. Die Auswahl der Entwicklungsplattform für Blockchain wird ein Teil davon. Dazu sollen Diagramme und gegebenenfalls schriftliche Spezifikationen erstellt werden, auf deren Basis eine spätere Implementierung stattfinden kann.

4. **Implementierung einer abgesicherten Kommunikation**
   Es soll das spezifizierte Kommunikationsprotokoll an einem Beispiel implementiert werden. Gegebenenfalls sollen Implementierungen für verschiedene Ausführungsumgebungen geschrieben werden und wenn möglich an echter Hardware getestet werden.

5. **Evaluation**
   Die Machbarkeit, Aufwände und Zuverlässigkeit der erarbeiteten Lösung für den Einsatz in der Automatisierungstechnik soll erörtert und im Projektbericht festgehalten werden, um einen Ausblick und/oder einen Anhaltspunkt für weiterführende Projekte und Arbeiten zu bieten.

6. **Dokumentation**
   Alle Ergebnisse der vorherigen Arbeitspakete sollen möglichst parallel zu den Tätigkeiten in einem Dokument zusammengefasst werden. Dieses soll dann als Projektbericht abschließend

überarbeitet werden. Zusätzlich müssen die Präsentationen für die Zwischen- und Abschlusspräsentation erstellt werden.

2.4 Meilensteinplan

Dazu soll folgender Meilensteinplan erreicht werden:

1. Festlegung des Zeitplans
2. Konzept einer Kommunikation mittels Smart Contract auf der Blockchain
3. Implementierung der Kommunikation anhand eines Beispiels
4. Fertigstellung des Projektberichts

zur Zeitplanung wird ein Gantt-Diagramm erstellt, das in Abbildung 1 dargestellt ist. Die Zwischenpräsentation ist für den 7. Januar 2022 geplant. Der im Gantt-Diagramm anvisierte Termin für die Abschlusspräsentation entspricht der derzeitigen Planung und soll mit der Zwischenpräsentation endgültig festgelegt werden.

IAT Projekt – Blockchain

E: Eric
M: Michael
J: Justin

08/11/21

1

TASK	ASSIGNED TO	START	END
Exposé	**Alle**	08/11/21	19/11/21
Literaturrecherche	**Alle**	08/11/21	17/12/21
Analyse der Problemstellung		22/11/21	17/12/21
Automatisierungstechnische Komponenten	M	22/11/21	17/12/21
Ausführumgebungen und Kommunikationsinfrastrukturen	J	22/11/21	17/12/21
Blockchain Algorithmen	E	22/11/21	17/12/21
Dokumentation	**Alle**	08/11/21	31/03/22

8/ Nov 2021 | 15/ Nov 2021 | 22/ Nov 2021 | 29/ Nov 2021 | 6/ Dec 2021 | 13/ Dec 2021

8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19

M T W T F S S M T W T F S S M T W T F S S M T W T F S S M T W T F S S M T W T F S S

M: 10, E: 10, J: 10
M: 30, E: 30, J: 30
M: 30
J: 30
E: 30
M: 4, E: 4, J: 4

TASK	ASSIGNED TO	START	END
Erstellung der Zwischenpräsentation	**Alle**	03/12/21	06/01/21
Konzeption der Kommunikation	**J**	03/01/22	21/01/22
Implementierung	**M**	24/01/22	18/02/22
Dokumentation	**Alle**	08/11/21	31/03/22
zwischen präsentation am 7.Januar 2021			

3/ Jan 2022 | 10/ Jan 2022 | 17/ Jan 2022 | 24/ Jan 2022 | 31/ Jan 2022 | 7/ Feb 2022

3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 1 2 3 4 5 6 7 8 9 10 11 12 13

M T W T F S S M T W T F S S M T W T F S S M T W T F S S M T W T F S S M T W T F S S

M: 10, E: 10, J: 10
J:25
M:25
M: 4, E: 4, J: 4

TASK	ASSIGNED TO	START	END
Implementierung	**M**	24/01/22	18/02/22
Test und Auswertung	**E**	19/02/22	10/03/22
Erstellung der Abschlusspräsentation	**Alle**		
Dokumentation	**Alle**	08/11/21	31/03/22
Abschluss präsentation am 21 März 2021			

Feb 14, 2022 | Feb 21, 2022 | Feb 28, 2022 | Mar 7, 2022 | Mar 14, 2022 | Mar 21, 2022

14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27

M T W T F S S M T W T F S S M T W T F S S M T W T F S S M T W T F S S M T W T F S S

E: 25
M: 10, E: 10, J: 10
M: 8, E: 8, J: 8

Abbildung 1: Zeitplanung

Literatur

[1] Jake Frankenfield. Smart contracts. https://www.investopedia.com/terms/s/smart-contracts.asp, 2021. Abgerufen am 12 November 2021.

[2] Andy Greenberg. Hackers remotely kill a jeep on the highway—with me in it. HackersRemotelyKillaJeepontheHighway\T1\textemdashWithMeinIt, 2015. Abgerufen am 12 November 2021.

[3] Michael J.W. Rennock, Alan Cohn, and Jared R. Butcher. Blockchain technology and regulatory investigations. 2018.