Name: Andreas Roos (Matrikel-Nr: 791432)

Thema: Aufbau und Management einer Konsortial- / Sidechain auf Blockchain Basis

Semester: Abschlussarbeit (BHTB MIB 13 für SoSe19)

Betreuer: Prof. Dr. Stefan Edlich

Exposee

1. Einleitung
   Seit Anfang der 90er Jahre wurden diverse Verfahren der kryptografisch abgesicherten Verkettung einzelner Blöcke, genannt Blockchain, entwickelt und verbessert. Im Jahr 2008 wurde diese Technik als verteiltes Datenbankmanagementsystem beschrieben und 2009 als erste öffentliche verteilte Blockchain mit der Kryptowährung Bitcoin implementiert. Dabei handelt es sich um eine dezentral geführte Kontobuchtechnologie, worin die jeweils korrekten Zustände von Transaktionen dokumentiert werden.

   Während der Entwicklung der Blockchain-Technologie gab es verschiedene, teils erfolgreiche Ansätze diese Systeme auf eine bestimmte Art zu verbessern. Die Verbesserungen reichen vom Thema Sicherheit oder Performance bis hin zu den Abgrenzungen von öffentlichen, privaten und hybriden Blockchains. Zusätzlich wurden nicht nur Kryptowährungen, sondern auch Abläufe wie die Nachverfolgung von Handelslieferketten, die Sicherstellung von Urheberrechten oder sogar Spielstände in der Unterhaltungsindustrie gespeichert.

   Aufgrund der Weiterentwicklung und das größer werdende Interesse in der Öffentlichkeit, wird diese Technik auf Dauer auch für Startup's und KMU's immer interessanter.

2. Problemstellung
   Da die ursprünglichen Ansätze alles andere als ressourcenschonend und somit teuer waren, blieb die Technik nur wenigen vorbehalten. Denn je nach Implementierung wird sehr viel Rechenleistung und Speicherplatz benötigt. Neben den Nachteilen der regelrechten Ressourcenverschwendung bspw. aufgrund schnell wachsender Blockchains besteht u.a. auch die Gefahr einer Monopolisierung und steuert genau entgegengesetzt dem Grundgedanken einer dezentralisierten Umgebung bei.

3. Fragestellung
   - Sind bereits praxistaugliche Lösungen für KMU's auf dem Markt?
   - Wie kann dieses System implementiert / realisiert werden?
   - Wie umfangreich ist der Verwaltungsaufwand?
   - Wie sicher ist solch eine Lösung im Gegensatz zu einer klassischen zentralen Lösung?

4. Ziel
   Das Thema Blockchain ist ein relativ junges Thema. Aufgrund der raschen Entwicklung gibt es sehr interessante Ansätze die Implementierung und stetige Weiterentwicklung zu vereinfachen und zusätzlich die Last auf der Blockchain zu reduzieren. Ein Ansatz ist es, aus der Haupt-Blockchain heraus eine Konsortial- / Sidechain neu zu erstellen und dort nach eigenen Regeln eine Umgebung zu betreiben.

   Es soll untersucht werden, ob aktuell geeignete Produkte vorhanden sind und wie der Aufbau für KMU's realisiert werden kann. Des Weiteren soll die Verwaltung des Systems, die Absicherung / Sicherheit, der Ressourcenverbrauch und die

Möglichkeit Schnittstellen zur Anbindung von Applikationen anhand eines Beispiels betrachtet werden.

Als Beispiel soll eine Art Notariat erstellt werden. Damit es Anwendern wie bspw. Studenten möglich ist, einen bestimmten Zustand eines Dokumentes und ein Kommentar in der Blockchain zu sichern. Zusätzlich soll es dem Anwender möglich sein, Informationen eines bereits gespeicherten Eintrages abzufragen.

5. Theoriebezug
   Es werden u.a. Kenntnisse aus den folgenden Modulen verwendet:
   - Computerarchitektur und Betriebssysteme
   - Kommunikationsnetze
   - Datenbanken
   - Algorithmen und Datenstrukturen

   Hinzu können Skript- / Programmiersprachen wie bspw. HTML, CSS, JavaScript zum Einsatz kommen. Des Weiteren wird der Zyklus der Softwareentwicklung, bestehend aus Analyse, Design, Entwicklung und Testen behandelt.

6. Material
   Bisher sind keine vorher definierten Materialien vorgesehen. Diese werden sich bspw. aus den Recherchen der einzelnen Produktanbieter ergeben.

7. Gliederung
   Nachfolgend befindet sich eine erste Gliederung. Aufgrund der noch bevorstehenden, genaueren Recherchen und Analysen erfolgt diese unter Vorbehalt. Änderungen möglich.

   Deckblatt
   Inhaltsverzeichnis
   Abstract
   Abbildungsverzeichnis
   Tabellenverzeichnis
   Glossar
   Abkürzungsverzeichnis
   1. *Einleitung*
   2. *Aufgabenstellung*
   3. *Technische Grundlagen*
      - 3.1. *Wie funktioniert eine Blockchain*
      - 3.2. *Arten von Blockchains (öffentlich, privat, hybrid)*
      - 3.3. *Nodes und der Konsens*
      - 3.4. *Hashing*
      - 3.5. *Kryptographie und digitale Signaturen*
      - 3.6. *dApp (decentralized application)*
   4. *Analyse (bezogen auf die Aufgabenstellung)*
      - 4.1. *Produkte auf dem Markt*
      - 4.2. *Anforderungen*
   5. *Design (eine Gliederung erfolgt nach der Analyse)*
   6. *Implementierung*
      - 6.1. *Ein Rundgang durch das System*
      - 6.2. *Aufbau der Server (Grundinstallation)*

6.3. Aufbau der Blockchain
6.4. Implementierung von Benutzerschnittstellen (z.B. dApp)

7. Anwendung
7.1. Verwaltung der Server
7.2. Transaktionen tätigen
7.3. Benutzerschnittstellen (fertige Produkte, dApp)

8. Ergebnisse und Fazit

Literaturverzeichnis
Anhang
Eidesstattliche Erklärung

8. Literaturverzeichnis
   - Materialien aus diversen Modulen des Studiums.
   - Herstellerseiten (Produktinformationen, API's, usw.)

9. Zeitplan

Datum	Kommentar	Status
01.04.2019	- Freigabe vom Prüfungsamt mit Start- und Endtermin (Anmeldebestätigung)	
08.04.	- Erstellung / Anpassung Milestoneplan und Inhaltsverzeichnis (2 Stufen tief)	
15.04.	- Dokumentation: Einleitung, Aufgabenstellung, Technische Grundlagen	
22.04.	- Dokumentation: Analyse, Design	
29.04.	- Entwicklung: Implementierung	
06.05.	- Dokumentation: Implementierung	
13.05.	- Entwicklung: Anwendung	
20.05.	Review 1/2 - Dokumentation: Anwendung	
27.05.	- Dokumentation: Ergebnisse und Fazit, Anhang / Literaturverzeichnis - Anpassungen (aus Review 1/2)	
03.06.	Review 2/2	
10.06.	- Abschluss: letzte Anpassungen (aus Review 2/2) und Druck	
17.06.	Abgabe	
24.06.	Kolloquium	
	Prüfungstermin	