



Institut für Informatik
Lehrstuhl für Organic Computing
Prof. Dr. rer. nat. Jörg Hähner

Masterarbeit

**Learning drinking patterns with
Q-Learning and Feature Selection on an
Ethereum Blockchain**

Fabian Pieringer

Erstprüfer: Prof. Dr. rer. nat. Jörg Hähner

Zweitprüfer: Prof. Dr. Albert Einstein

Betreuer: Betreuer am Lehrstuhl, M.Sc.

Matrikelnummer: 150886

Studiengang: Informatik (Master)

Eingereicht am: 19. Mai 2019

Abstract

In dieser Masterarbeit ...

Inhaltsverzeichnis

Abstract	i
1 Einleitung	1
1.1 Aufbau dieser Arbeit	1
1.2 Problemstellung	1
1.3 Related Work	2
2 Stand der Technik	3
2.1 Blockchain	3
2.1.1 Funktionsweise & Konzepte	3
2.1.2 Ethereum	5
2.2 Machine Learning	7
2.2.1 Überblick	7
2.2.2 Reinforcement-Learning	7
3 System Architektur	9
3.1 Überblick	9
3.1.1 Architektur	9
3.1.2 Workflow	15
3.1.3 Entwicklungsprozess	21
3.2 Blockchain	25
3.2.1 Genesis Block	25
3.2.2 CoffeeCoin	28
3.2.3 Beverage-List	30
3.3 Learner	31
3.3.1 Modellierung	31

Inhaltsverzeichnis

3.3.2	Q-Learning	33
3.3.3	Lernprozess & Ablauf	33
3.4	Tablet-App	35
3.4.1	Interface	35
3.4.2	Internal Workflow	40
4	Studie	43
4.1	Testphase	43
4.2	Evaluation	43
5	Zusammenfassung	45
5.1	Weiterführende Forschungsfragen	45
5.2	Ausblick	45
	Literaturverzeichnis	I
	Abbildungsverzeichnis	III
	Tabellenverzeichnis	V
A	Anhang A	VII
B	Anhang B	IX

1 Einleitung

1.1 Aufbau dieser Arbeit

1.2 Problemstellung

Im heutigen Zeitalter des Smartphones in dem die Überstimulation der Sinne durch Informationen von den unterschiedlichsten Kanälen (z.B. Social Media, Push-Notifications etc.) zum Alltag vieler gehört, ist es mittlerweile unabdingbar geworden neben Werbeanzeigen, auch Apps, Plattformen, Systeme zu personalisieren. Dabei soll dem Nutzer eine User-Experience geboten werden, welche ihn einerseits vor dieser Überstimulation durch irrelevante Informationen bewahrt und andererseits eine möglichst lange Interaktion mit der App, Website, Plattform gewährleistet.

Dahingehend ist der erste Schritt, wie auch bei den maßgeschneiderten Werbeanzeigen auf den Social-Media Plattformen, das Verhalten der User zu erlernen und anhand dieses Wissens App-Interfaces oder auch Hintergrundprozesse anzupassen, sodass für jeden Nutzer eine optimale User-Experience sichergestellt werden kann. Hierbei kann auch von sog. virtuellen Assistenten gesprochen werden, welche durch die direkte Interaktion mit dem User oder durch das Beobachten des Users, dessen Verhalten und Gewohnheiten versucht zu erlernen. Die Problematik die diesen Anwendungen anhaftet, ist die Weitergabe der privaten Nutzerdaten an die Plattform- bzw. App-Server, auf welchen die Informationen abgespeichert und die Assistenten trainiert werden, da vor allem bei mobilen Endgeräten die Kapazitäten und die Rechenleistungen dafür nicht

1 Einleitung

ausreichen.

Eine Möglichkeit diese Weitergabe zu vermeiden besteht in der Blockchain-Technologie. Hierbei werden die Daten nicht mehr zentral bei einem Knoten im Netzwerk abgespeichert, sondern dezentral in einer verteilten Datenbank, in der die Sicherheit der Daten und Privatsphäre der Nutzer gewährleistet ist. Aufgrund dieser Dezentralität können virtuelle Assistenten auch lokal gehostet und trainiert werden, ohne dabei die Daten nach außen geben zu müssen. Durch diesen Ansatz entstehen jedoch bestimmte Problemstellungen, für die es in der Form noch keine standardisierten Lösungen gibt und erst zu eruieren gilt.

So lautet die Grundsatzfrage: wie gut lässt sich Blockchain mit Machine Learning verbinden? Also ist möglich virtuelle Assistenten mit den Daten von einer Blockchain zu versorgen, um damit das Verhalten eines Users zu erlernen. Gerade im Bezug auf das Erlernen des Nutzerverhaltens ist dies ein noch sehr unerforschtes Gebiet.

Eine weitere Frage welche aus dieser Problemstellung resultiert ist: wie eine notwendige "Feature Selection" auf einer Blockchain aussieht?

Um dies zu erforschen und abzubilden, wird in dieser Arbeit ein System vorgestellt, welches sich den gerade eben geschilderten Problemstellungen annimmt. Hierbei wird eine Getränkeliste an einem Lehrstuhl durch eine Tablet-App ersetzt, in welcher die konsumierten Getränke (Kaffee, Club Mate, Wasser) eingegeben werden. Die kontextuellen Daten werden daraufhin auf eine private Blockchain gespeichert und das Getränk zudem mit einem Blockchain basierten Token bezahlt. Ein lokal gehosteter Machine Learning Algorithmus liest die Informationen von der Blockchain aus und lernt für jeden Nutzer ein Modell, welches dessen Kaffeetrinkverhalten abbildet.

zum einen private Blockchain aufgesetzt, welche einerseits für Dabei soll ein lokal gehosteter Machine Learning Algorithmus

1.3 Related Work

2 Stand der Technik

2.1 Blockchain

Der folgende Abschnitt basiert auf den Inhalten dieser Literatur: ??, ??, ?? und ??.

2.1.1 Funktionsweise & Konzepte

Damit das Verständnis für die Blockchain Technologie geschaffen werden kann, sollte zuerst die darunter liegende Technologie betrachtet werden. So wird der Begriff der Blockchain oft auch mit dem des *distributed ledger* gleichgesetzt. Ein *distributed ledger* ist eine *verteilte Datenbank*, welche im Kontext einer Blockchain auch als “verteiltetes Konto” bzw. “dezentral geführtes Kontobuch” [Lui15] verstanden wird, in welchem jegliche Transaktionen abgespeichert werden.

Allerdings ist diese Gleichsetzung nicht ganz korrekt, denn eine Blockchain ist nur ein spezieller Typus eines *distributed ledgers*. So kann nämlich dieser neben Transaktionen auch aus weiteren Daten bestehen, wohingegen bei einer Blockchain die Blöcke stets Transaktionen beinhalten.

Somit stellt ein *distributed ledger* die technologische Grundlage aller virtuellen Währungen dar und ist dadurch auch einer der Hauptgründe weshalb Kryptowährungen auf einer Blockchain basieren.

Grundsätzlich steht Blockchain für eine Verkettung von geordneten Blöcken,

2 Stand der Technik

welche in sich eine oder mehrere Transaktionen beinhalten. Zu den Transaktionsdaten wird zudem ein Hashwert des Vorgängerblocks und ein Zeitstempel mit im Block abgespeichert. Erst aufgrund der Berücksichtigung des Hashwerts des vorherigen Blocks werden die Blöcke miteinander verknüpft und bilden somit eine chronologisch geordnete Kette.

Eine weitere Beschaffenheit einer Blockchain ist die Dezentralität durch das aufgespannte *Peer-to-Peer* Netzwerk. Der Vorteil dieser Topologie besteht in der Vakanz eines zentralen Knotens, welcher für das Abspeichern und Bereitstellen aller bestehenden Daten eines Netzwerks zuständig ist. Denn jeder Knoten in einem solchem Netzwerk ist sowohl Sender als auch Empfänger, sodass jeder Teilnehmer eine Kopie des Datenbestandes besitzt, was einen “Single Point of Failure” völlig ausschließt. Aus diesem Grund sind Daten einer Blockchain nie nur bei einem Knoten abgespeichert, sondern jede Node besitzt eine Kopie der aktuellen Blockchain.

Welche Daten schließlich auf die Blockchain geschrieben werden dürfen oder genauer gesagt ob eine Transaktion durchgeführt werden darf, erfolgt stets in abetracht des Konsens aller Parteien im Netzwerk. Diese Eigenschaft wird als *distributed consensus* bezeichnet und ist das Fundament einer jeder Blockchain. Durch die Einbeziehung eines jeden Teilnehmers in der Entscheidungsfindung wird die Notwendigkeit einer zentralen Entscheidungsinstanz obsolet.

Der Mechanismus welcher dafür zuständig ist diesen Konsens herbeizuführen, ist je nach Implementierung des Blockchainprotokolls unterschiedlich. Eine beliebte Methodik, welche unter anderem von Bitcoin und Ethereum verwendet wird, ist der *Proof-of-Work* Ansatz. Hierbei werden von den sog. “Minern” Iterationen an aufwändigen und komplexen Berechnungen durchgeführt, die sicherstellen sollen, dass die benötigten kryptographischen Berechnungen für eine Transaktion durchgeführt und die Daten einer Transaktion validiert werden.

Eine weitere Besonderheit einer Blockchain ist die Unveränderbarkeit der darauf gespeicherten Daten. So gibt es, im Gegensatz zu den bekannten CRUD-Operationen ¹, welche zur Kommunikation zwischen Client und Server verwendet werden, um Daten zu schreiben, zu downloaden, zu löschen und zu

¹CRUD:Wiki

editieren, bei einer Blockchain lediglich eine Schreib- und eine Leseoperation. Weswegen im Zusammenspiel mit dem Konsensverfahren Transaktionen auf einer Blockchain einzig hinzugefügt und gelesen, jedoch nie zu einem späteren Zeitpunkt gelöscht oder editiert werden können.

Dabei sind die gespeicherten Daten (unverschlüsselt oder auch verschlüsselt) für alle im Netzwerk einsehbar und bedeutet somit volle Transparenz für jeden User.

Die gerade geschilderten Eigenschaften sind einer jeden Blockchain inhärent bzw. in einer abgeänderten Form (z.B. *Proof-of-Stake*² anstatt *Proof-of-Work*) vorhanden. Was jedoch erst in neueren Blockchains (Blockchain 2.0) vorzufinden ist, sind die *Smart Contracts*.

Smart Contracts sind Programme welche auf einer Blockchain installiert werden können.

Diese Programme können z.B. Business Logiken abbilden und ausführen oder auch Verpflichtungen und Vereinbarungen im rechtlichen Sinne durchsetzen, ohne der Notwendigkeit eines Mittelmanns, welcher das Vertrauen aller beteiligten Parteien inne hat. Diese "Trust-Komponente" wird durch die Anerkennung aller Parteien von dem Smart Contract übernommen.

Das erste mal in Erscheinung getreten sind Smart Contracts mit der Veröffentlichung der Ethereum Blockchain, welche nun im Anschluss genauer betrachtet wird.

2.1.2 Ethereum

Die Ethereum Blockchain wurde 2015 in Betrieb genommen, mit dem Ziel nicht nur eine Kryptowährung zu schaffen, sondern eine Plattform zu entwickeln auf welcher sog. Dapps (Decentralized Apps) betrieben werden können. So wird Ethereum im Vergleich zu Bitcoin auch als Blockchain 2.0 bezeichnet, da es eben nicht nur eine Kryptowährung umfasst, sondern es aufgrund der Smart Contracts es möglich ist Software auf einer Blockchain zu installieren.

²Konsensalgorithmus welcher anstatt von Rechenleistung einen bestimmten Betrag an Ether als Pfand erwartet. Je höher dieser Wert desto wahrscheinlicher ist es, dass der Nutzer die Transaktion als neuen Block bestätigt [btc, Wikib]

2 Stand der Technik

Als Ethereum wird genauer genommen das Protokoll tituliert welches die Blockchain implimentiert. Die Kryptowährung die auf der Blockchain basiert wird als *Ether* bezeichnet und fungiert zudem als Zahlungsmittel im Kontext der Smart Contracts. So ist bzw. war das Bestreben der Gründer nicht eine weitere Kryptowährung zu schaffen, sondern einen Art “Supercomputer”, welcher immer online ist und aus Millionen von Computern im Netzwerk besteht, die ihre Rechenleistung zur Verfügung stellen und als Gegenleistung bzw. Anreiz in Form von Ether vergütet werden.

Dabei können zwar, wie bei einer Kryptowährung, Transaktionen durchgeführt und Ether von einem Konto auf ein anderes transferiert werden. Jedoch liegt der eigentliche Fokus auf den Smart Contracts und den Dapps.

Dazu wurde die EVM (Ethereum Virtual Machine) entwickelt, in welcher letztlich die Smart Contracts bzw. Dapps gehostet und ausgeführt werden. Dabei stellt die Virtual Machine eine Abstraktionsebene zur physischen Schicht der Blockchain dar und ermöglicht es dadurch den Smart Contracts Daten auf die Blockchain zu speichern und bietet gleichzeitig eine Laufzeitumgebung in der die Anwendungen ausgeführt werden können.

Die Implementierung der Smart Contracts erfolgt stets in der eigens entwickelten Programmiersprache Solidity. Diese folgt dem Prinzip der Objekt Orientierung, ist der Sprache Javascript angelehnt und ist zudem Turing-Vollständig, was im Bezug auf die Entwicklung von Apps und eine hohe Bandbreite an Anwendungsfällen eröffnet.

Damit die Funktionen der Smart Contracts überhaupt genutzt werden können, muss einem jedem Methodenaufruf bzw. jeder Transaktion Ether - im Kontext der Smart Contracts als “Gas” bezeichnet - mitgegeben werden, um die Miner für ihre zur Verfügung gestellte Rechenleistung zu entlohnen. Das bedeutet um Daten auf die Blockchain zu speichern, wird je nach Transaktion eine bestimmte, Menge an Gas benötigt, welches im Endeffekt den Minern als Anreiz und Belohnung zur Bereitstellung von Rechenleistung übertragen wird.

Wie das Mining bereits impliziert, basiert der Konsensalgorithmus der Ethereum Blockchain auf dem Proof of Work Konzept. Da dieser Ansatz jedoch einige Nachteile mit sich bringt, was Energieeffizienz und Transaktionen pro Sekunde betrifft, wird voraussichtlich im Juni 2019 der Wechsel auf einen Pro-

of of Stake Konsensalgorithmus erfolgen.

Die große Community, der Opensource Ansatz, die Verfügbarkeit von Libraries in verschiedenen Programmiersprachen und Kommandozeilenanwendungen, sowie die Möglichkeit Smart Contracts bzw. Dapps auf der Blockchain zu betreiben, sind eine der Hauptgründe, weshalb die Wahl bei dieser Arbeit auf Ethereum gefallen ist.

2.2 Machine Learning

2.2.1 Überblick

2.2.2 Reinforcement-Learning

- kein Lehrer dafür sensomotorische Verbindung zur Umgebung
- Lernen von Information über Ursache und Wirkung, Konsequenzen
- lernen der benötigten Schritte zum Erreichen des Ziels

Das Grundprinzip des Reinforcement-Learning besteht darin bestimmte Situationen auf Aktionen zu projizieren, um dabei den numerischen Reward des Agenten zu maximieren. Diese Aktionen werden dem Agenten jedoch nicht durch eine “Supervisor-Instanz” mitgeteilt, sondern dieser versucht durch die “Trial and Error” Methodik herauszufinden, welche Aktion in welchem Zustand den größten Reward zur Folge hat. Dabei können diese Aktionen nicht nur die Belohnung des Agenten beeinflussen, sondern zudem die Umgebung in der er sich bewegt und dadurch auch den Folgezustand.

Diese Konzept der Reward-Maximierung resultiert in dem Tradeoff zwischen *Exploration* und *Exploitation*. *Exploration* beschreibt den Versuch mehr Information über die Umgebung zu erlangen, indem die Reward-Maximierung außer Acht gelassen und eine Aktion zufällig ausgewählt wird, in der Hoffnung

2 Stand der Technik

den bisherigen Reward zu übertreffen. Im Gegenteil dazu spezifiziert *Exploitation* die Maximierung des Rewards, indem der Agent stets auf die, in einem bestimmten Zustand, bestbewertete Aktion zurückgreift. Je nach Algorithmus und Lernproblem variiert das Verhältnis der beiden, welches durch eine (iterative) Justierung der Parameter anpassen zu gilt.

Durch die Wechselwirkung der beiden ist es die Aufgabe des Agenten eine Strategie zu finden die letztlich den maximalen Reward garantiert, indem es sein Verhalten in den jeweiligen Zuständen bereits vorgibt.

Dabei gilt es vor allem zu beachten ob es sich bei dem Lernproblem um ein deterministisches oder nichtdeterministisches handelt. Deterministisch bedeutet, es wird stets die gleiche Aktion in einem bestimmten Zustand gewählt, wohingegen nichtdeterministisch lediglich eine Wahrscheinlichkeitsverteilung beschreibt, anhand der Agent in einem Zustand entscheidet, welche Aktion auszuwählen ist. //TODO: Elemente des Bestärkenden Lernen

- learn how to map situations to actions → maximize numerischen Reward
- learner not told which actions to take
- discover which actions yield the most reward
- action not only affect reward also next situation
- trial and error search and delayed reward
- optimal control of incompletely-known markov decision processes
- agent must have a goal relating to the state of env
- sensation, action, goal

From the preceding discussion, it should be clear that reinforcement learning relies heavily on the concept of state

3 System Architektur

3.1 Überblick

Im folgenden wird nun die System Architektur und der Workflow erläutert, welche als Grundlage für die Studie dienen, um die in 1.2 geschilderte Problemstellung abzubilden und letztendlich zu lösen.

3.1.1 Architektur

Um ein besseres Bild davon zu bekommen, wie die einzelnen Komponenten zusammenhängen bzw. welche Aufgaben diese in Wechselwirkung zu anderen Instanzen übernehmen und ausführen, wird zunächst die Architektur des Systems erläutert. Als Basis soll dabei die Abbildung 3.3 dienen, anhand jener vorrangig die jeweiligen Komponenten bezüglich ihrer Funktionsweise beschrieben werden. Das Zusammenspiel der Anwendungen wird im Anschluss unter 3.1.2 detailliert beleuchtet.

3 System Architektur

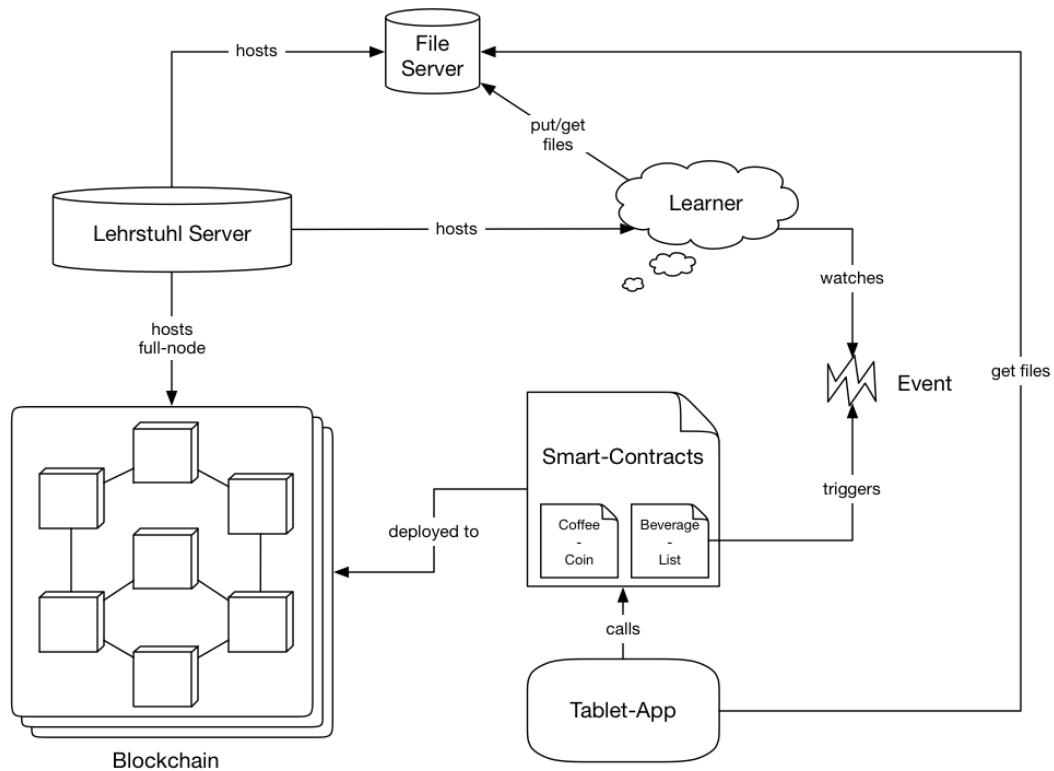


ABBILDUNG 3.1: Systemarchitektur

Lehrstuhl Server

Der Lehrstuhlserver ist dafür zuständig einen Großteil der Anwendungen zu hosten bzw. zu starten. Dies gilt sowohl für den HTTP-Fileserver als auch für die Learner-Anwendung, welche dessen Betriebssystem als Plattform nutzen. Auch die Blockchain wird auf dem Server gestartet und verwendet diesen zudem als full-node, um Transaktionen zu minen. Der Server ist im Grunde der Anwendungen, dessen primäre Funktionsweise darin besteht jenen eine Plattform zu bieten und mit Rechenleistung zu versorgen.

Learner

Der sogenannte “Learner” ist eine in Golang implementierte Softwareanwendung, dessen Hauptaufgabe darin besteht, das Kaffeetrinkverhalten der Nutzer zu erlernen - wovon auch die Namensgebung der Anwendung stammt. Um dies

zu erreichen, wurde die Anwendung in Submodule unterteilt, welche einen dedizierten Aufgabenbereich abdecken und diesen eigenständig bearbeiten. Auch wenn jene für sich autark agieren können, kann das Trinkverhalten letztendlich erst in der gegenseitigen Wechselwirkung jener erlernt werden.

Die Submodule lauten wie folgt:

- Q-Learning
- Worker
- Watcher
- (Smart Contract Deployment Skript)

Das **Q-Learning** ist, wie der Name bereits impliziert, für das eigentliche Erlernen des Trinkverhaltens zuständig. Es ist im Grunde die Implementierung des Q-Learning Algorithmus, sowie die damit einhergehende Zustandsraummodiellerung, welches aber unter `refsubsec:ql` genauer erläutert wird.

Der **Worker** ist einerseits für die Userverwaltung und andererseits für die, in einem festgelegten Intervall, Ausführung des Q-Learning Algorithmus, zuständig. (vgl. Kap. 3.3.3)

Der **Watcher** beobachtet Events, die vom Smart-Contract “Beveragelist” ausgelöst wurden. Die Daten, welches das Event beinhaltet, werden daraufhin verwendet um den Q-Learning Algorithmus zu befüllen und aufgrund diesen das Trinkverhalten zu erlernen.

Das **Smart Contract Deployment Skript**, ist in der Form zwar nicht in der Systemarchitektur vorhanden, da es aber auch ein Submodul des Learners und für das gesamte Konstrukt dahingehend essentiell ist, da es die Smart Contracts auf der Blockchain installiert und im Zuge dessen erst die Verbindung zwischen Blockchain und Learner ermöglicht, wird es in dieser Auflistung trotzdem aufgeführt.

Fileserver

Der Fileserver ist eine Go-Anwendung, welche eine rudimentäre REST [Wike] Api [Wika] zur Verfügung stellt. Von den sogenannten CRUD [Wikd] Operationen, welche als grundlegend für alle persistenten Datenspeicher angesehen werden können, implementiert dieser nur das “GET” und das “PUT”. Sowohl die “PATCH” als auch die “DELETE” Operation bieten keinen Mehrwert für die Gesamtarchitektur bzw. den Workflow und sind in Anbetracht dessen nicht implementiert.

Das bedeutet die Hauptaufgabe des Fileservers besteht darin, Dateien zu empfangen und zu speichern (PUT) und diese auf Anfrage (GET) an einen Antragsteller wieder zu versenden.

Außerdem bietet die Anwendung zusätzlich zur Api einen UDP-Broadcast, welcher v.a. beim Testing und beim Setup eine große Erleichterung darstellt. Dieser Broadcast versendet in seinen Nachrichten lediglich die IP-Adresse des Lehrstuhl-Servers und somit auch seine eigene und die der Blockchain. Da die IP-Adresse und der Port des Broadcasts stets gleich bleiben, sich aber die Host-IP der Blockchain und des Fileservers je nach Deployment theoretisch ändern können - was in der Entwicklungsphase sehr oft der Fall war. Müssen sich sowohl der Learner als auch die Tablet-App lediglich auf den Broadcast “subscriben” und können dadurch die IP der Blockchain und des Fileservers erfahren. Durch diese dynamische Zuweisung der IP-Adresse, müssen keine Updates beim Learner und der App durchgeführt werden, sollte die Blockchain und der Fileserver auf einem anderen Host deployed werden.

Aufgrund der Tatsache, dass sich die IP-Adresse des Lehrstuhl-Servers während der Studie nicht ändert, ist der UDP-Broadcast auch nicht in der Abbildung 3.1 der Systemarchitektur berücksichtigt worden. Der Anwendungsbereich ist trotz alledem im Bereich der Testphase und auch für die künftige Projekte, bei denen das System Verwendung findet, definitiv vorhanden.

Blockchain

Die Blockchain ist eine private, eigens für die Studie erstellte Ethereum-Blockchain, dessen “Genesis-Block” aus dem JSON-File (vgl. Abbildung ??) generiert wird. Die Erläuterungen zu den jeweiligen Key-Value-Pairs sind unter Kap. 3.2.1 zu finden. Das Generieren und das Starten der Blockchain erfolgt auf dem Lehrstuhlserver. Dabei hostet der Server zudem eine sogenannte “full-node” (auch “miner” genannt) der Blockchain, welche dafür zuständig ist Transaktionen zu berechnen und zu bestätigen. Aus Ressourcengründen ist dieser “miner” der einzige im Gesamtsystem, was aus theoretischer Sicht einen “Single Point of Failure” [Wikf] als Nachteil mit sich zieht. Das bedeutet sollte diese “full-node” ausfallen, würden keine Transaktionen mehr bestätigt werden. Da es weder während der Entwicklungsphase noch während der Studie zu einem einzigen Ausfall kam, ist dieser Nachteil als sehr klein einzuschätzen, weswegen auch keine weitere “full-node” zum System hinzugefügt wurde. Der große Vorteil besteht allerdings darin, dass Transaktionen sehr schnell bestätigt werden, da es keine weiteren “node’s” gibt, die um die Berechnung eines Block’s konkurrieren. Was vor allem aus Sicht der User-Experience [Wikg] einen großen Mehrwert darstellt, da dieser in wenigen Sekunden erfährt, ob seine Transaktion erfolgreich durchgeführt wurde. Dies kann bei anderen Blockchains wie z.B. Bitcoin bis zu 10 Minuten dauern [Rap09], was im Kontext der Systemarchitektur nicht tragbar wäre.

Um letztendlich mit der Blockchain kommunizieren und dessen Potential in voller Gänze ausschöpfen zu können, werden auf diese sogenannte Smart-Contracts [Dav15] deployed. Im Rahmen der Systemarchitektur sind es zwei dedizierte Smart-Contracts (*Coffe-Coin*, *Beverage-List*), welche komplett unabhängig voneinander agieren.

Smart Contracts

Die beiden Smart Contracts welche auf die Blockchain deployed werden, werden mit *Coffe-Coin* und *Beverage-List* betitelt. Diese decken zwei völlig unterschiedliche Aufgabenbereiche ab, weswegen sie keinen Einfluss aufeinander haben und deswegen unabhängig voneinander operieren. So löst nur der *Beverage-List Contract* ein Event aus, sobald eine bestimmte Funktion dessen aufgerufen wird.

Die Ausführung (*call*) beider erfolgt jedoch stets von Seiten der *Tablet-App*. Diese ist auch die einzige Instanz, welche in Form von Transaktionen mit der Blockchain interagiert.

Tablet-App

Die *Tablet-App* ist eine mit React-Native [RN:] erstellte Crossplattform App [Wikc], welche auf einem Android Tablet installiert ist. Die Hauptaufgabe der App ist es Funktionen der beiden Smart Contracts aufzurufen, in dem es die benötigten Daten an den Smart Contract übergibt, um schlussendlich Transaktionen auszulösen.

Damit eine Kommunikation mit einem Smart Contract überhaupt zustande kommt, schickt die App einen Request an den Fileserver, welcher mit den angefragten Smart Contract Daten in Form einer Datei antwortet.

Event

Das Event beschreibt im Grunde die indirekte Kommunikation zwischen dem *Learner* und der *Tablet-App* mit dem Smart Contract *Beverage-List* als Mittelsmann. So wird jenes im Zuge eines Funktionsaufrufs des Smart Contracts von Seiten der App ausgelöst und vom *Learner* detektiert und der Inhalt zum Erlernen des Kaffeetrinkverhaltens verwendet.

3.1.2 Workflow

Die unter Kap. 3.1.1 beschriebene Architektur wird im folgenden unter dem Gesichtspunkt des Workflows, also dem Zusammenspiel der einzelnen Komponenten und dem Gesamtablauf, näher betrachtet. Dabei beschreibt der Gesamtablauf die einzelnen Schritte startend beim Setup der Komponenten hin zum eigentlichen Durchlauf der einzelnen Softwareanwendungen, was letztlich im Erlernen des Kaffeetrinkverhaltens resultiert. Im Zuge dessen werden auch einzelne Algorithmen der Instanzen und Kommandos kurz erläutert, um ein besseres Verständnis für die Funktionsweise der Anwendungen zu bekommen.

Der Workflow lässt sich in zwei Phasen unterteilen. In der ersten werden die einzelnen Komponenten konfiguriert und gestartet und die zweite beschreibt den eigentlichen Ablauf und das Zusammenwirken der Instanzen.

Setup

1. Blockchain
 - 1.1. erstellen & konfigurieren
 - 1.2. starten
2. Fileserver
 - 2.1. REST Api starten
 - 2.2. UDP Broadcast starten
3. Smart Contracts
 - 3.1. deploy Beveragelist Smart Contract und sende JSON-File mit ABI und Adresse an Fileserver
 - 3.2. deploy CoffeeCoin Smart Contract und sende JSON-File mit ABI und Adresse an Fileserver

3 System Architektur

4. Learner

4.1. Worker starten

4.2. Watcher starten

5. Tablet App

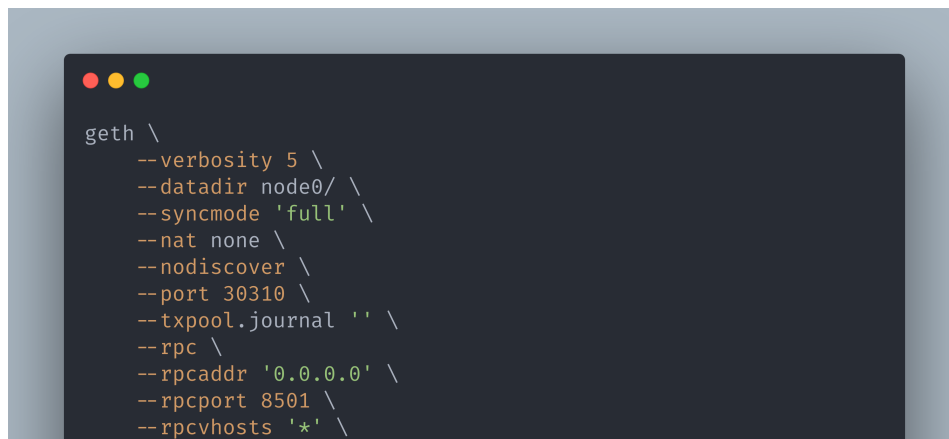
5.1. installieren

5.2. starten

Die Punkte 1. und 2. sowie 4. und 5. können auch parallel ausgeführt bzw. deren Reihenfolge vertauscht werden.

Im ersten Schritt muss die private Blockchain erstellt werden. Dabei müssen zuerst die benötigten Accounts generiert und daraufhin die Blockchain erzeugt werden. Sollte 1a) zu einem früheren Zeitpunkt bereits durchgeführt worden sein, kann dieser Punkt übersprungen und gleich mit 1b) begonnen werden. Sobald 1a) einmal durchgeführt wurde, kann die Blockchain gestartet werden.

Dies geschieht mit folgendem Befehl:

A screenshot of a terminal window with a dark background and light-colored text. The terminal shows the command to start a private Ethereum node using the 'geth' command. The command is split across multiple lines, with each line starting with a backslash to indicate it's a single command. The options include verbosity, data directory, sync mode, NAT, node discovery, port, transaction pool journal, RPC, RPC address, RPC port, and RPC allowed hosts.

```
geth \  
  --verbosity 5 \  
  --datadir node0/ \  
  --syncmode 'full' \  
  --nat none \  
  --nodiscover \  
  --port 30310 \  
  --txpool.journal '' \  
  --rpc \  
  --rpcaddr '0.0.0.0' \  
  --rpcport 8501 \  
  --rpcvhosts '*' \  

```

```

--rpcapi 'personal,db,eth,net,web3,txpool,miner,debug' \
--ws \
--wsaddr '0.0.0.0' \
--wsport 8546 \
--wsorigins '*' \
--wsapi 'personal,db,eth,net,web3,txpool,miner,debug' \
--networkid 50 \
--gasprice '2000000000' \
--targetgaslimit '0x4c4b400000' \
--mine \
--etherbase '0xe8816898d851d5b61b7f950627d04d794c07ca37' \
--unlock '0x02e9f84165314bb8c255d8d3303b563b7375eb61, ...' \
--password=node0/password.txt

```

ABBILDUNG 3.2: geth Befehl zum starten der Blockchain

Dieser Befehl setzt zum einen weitere Konfigurationsparameter der Blockchain. So wird z.B. festgelegt unter welcher IP-Adresse und Port (*--rpcaddr*, *--rpcport*, *--wsaddr*, *--wsport*) die Blockchain erreichbar ist und welche Api-Befehle unter dieser Schnittstelle ausgeführt werden dürfen (*--rpcapi*, *--wsapi*). Zum anderen wird aber zugleich auch eine sogenannte *full node* gestartet (*--syncmode*), die durch das “Flag” *--mine* sofort zum “minen” beginnt. Desweiteren werden alle Accounts entsperrt die unter (*--unlock*) gelistet sind und deren Passwörter in der angegebenen Textdatei bei (*--password*) hinterlegt sind.

Damit eine *Node* Daten speichern kann, muss ein Verzeichnis angegeben werden (*--datadir*), in dem Dateien abgelegt werden können. Hier werden z.B. die Daten der Accounts oder auch die Textdatei mit den Passwörtern (*--password*) gespeichert.

Wurde die Blockchain in Betrieb genommen, wird im nächsten Schritt die REST Api und der UDP Broadcast des Fileservers gestartet. Daraufhin ist es möglich die beiden Smart Contracts zu deployen. Dabei wird jeweils für 3a) und 3b) das identische Bash-Skript mit unterschiedlichen Eingabeparametern ausgeführt. Dieses Skript liest zuerst die Datei des angegebenen Smart Contracts ein und erzeugt daraufhin die Binaries und die ABI, welche schlussendlich dazu verwendet werden ein Go Bindingsfile zu generieren.

3 System Architektur

Im Anschluss wird dann ein Go-Skript ausgeführt, welches auf Grundlage des Bindingsfiles den Smart Contract auf der Blockchain installiert und die zurückgelieferte Adresse und die bereits bekannte ABI ein JSON-File packt und an den Fileserver schickt.

Wurden die Smart-Contracts erfolgreich deployed, kann der Learner gestartet werden. Dieser “subscribed” sich im ersten Schritt auf den UDP Broadcast und extrahiert aus den Nachrichten die IP-Adresse der Blockchain und des Fileservers. Daraufhin werden sowohl der Worker als auch der Watcher in Form von “Goroutines” aktiviert. Der Worker iteriert über die Liste aller User und kontaktiert jeweils den Fileserver ob bereits gelernte Daten für diesen Usern vorhanden sind. Sollte das Fall sein, initialisiert er damit die Parameter des Q-Learning Algorithmus des Users.

Der Watcher schickt ebenfalls eine Anfrage an den Fileserver und bekommt als Antwort die Daten der Smart Contracts. Daraufhin kann er sich mit der Blockchain verbinden und sich auf die Events des Beveragelist Smart Contracts “subscriben”.

Abschließend wird die App auf dem Tablet installiert, sollte sich diese noch nicht auf dem Tablet befinden und daraufhin gestartet. Die Initialisierung erfolgt hierbei nach dem selben Prinzip wie beim Learner. Zuerst wird der UDP Broadcast nach der Server Adresse abgefragt, mit welcher anschließend der Request an den Fileserver geschickt wird, um die benötigten Smart Contract Daten zu bekommen. Welche im Anschluss dazu verwendet werden eine Verbindung zur Blockchain bzw. zu den Smart Contracts herzustellen.

Erfolgte eine fehlerlose Abarbeitung dieser Schritte, kann zum eigentlichen Workflow übergegangen werden.

Workflow

1. App
 - 1.1. User wählt Getränk aus
 - 1.2. *call* CoffeeCoin
 - 1.3. *call* Beveragelist
2. Smart Contracts
 - 2.1. Beveragelist *triggers* Event
3. Learner
 - 3.1. Watcher:
 - 3.1.1. detektiert Event
 - 3.1.2. extrahiert Daten aus Event
 - 3.1.3. befüllt Q-Learning Algorithmus mit den Event-Daten (evaluate & predict)
 - 3.2. Worker (periodisch alle 3h)
 - 3.2.1. “triggers” Q-Learning Algorithmus (evaluate & predict)
 - 3.2.2. sendet gelernte Daten (vgl. Abbildung 3.3) an Fileserver

Diese Auflistung beschreibt einen synchronen, erfolgreichen Durchlauf der Systemarchitektur - die Asynchronität des Workers 3b) außer Acht gelassen. Alternative Abläufe sowie Zustände die aus Fehlern resultieren, werden bei den einzelnen Komponenten nochmals genauer betrachtet.

Der Workflow wird durch den User gestartet indem dieser auf Tablet ein Getränk auswählt und eine Transaktion auslöst. Zuerst wird dabei der CoffeeCoin Contract aufgerufen und das ausgewählte Getränk bezahlt. Nachdem

3 System Architektur

diese Transaktion erfolgreich bestätigt wurde, wird als nächstes der Beverage-list Contract ausgeführt. Die dabei aufgerufene Funktion des Smart Contracts verwendet die übergebenen Daten (Zeit, Getränk, Wochentag, Eth-Adresse) und löst damit ein Event aus.

Dieses Event wird vom Watcher detektiert und die Daten (Zeit, Getränk, Wochentag, Eth-Adresse) daraus extrahiert. Daraufhin wird die *Learn-Methode* des Q-Learning Algorithmus aufgerufen, bei der zuerst die vorherige “Prediction” evaluiert und basierend auf dem aktuellen Zustand eine neue “Prediction” gemacht wird.

Zu diesem synchronen Durchlauf führt der Worker am Ende jedes Timeslots (alle 3h) die *Learn-Methode* für jeden bekannten User aus. Das heißt es werden wie auch beim Watcher die “Predictions” des vorangegangenen Timeslots evaluiert, neue “Predictions” für den kommenden Timeslot erstellt und die gelernten Daten als Datei an den Fileserver gesendet.

3.1.3 Entwicklungsprozess

Abschließend wird der Prozess der Entwicklung geschildert, aus welchem schließlich die finale Version der Systemarchitektur resultierte.

Der Entwicklungsprozess beinhaltete mehrere Iterationen der einzelnen Komponenten bis hin zum derzeitigen Stand. Das Konzept sah primär die Entwicklung von drei dedizierten Software Anwendungen vor, welche aber im Zuge der Iterationen nochmal in kleinere Module aufgeteilt und ausgelagert wurden. Zudem wurden, um den Workflow und das Testen während der Entwicklungsphase zu erleichtern, Anwendungen entwickelt, welche während der Konzeption in der Art nicht vorgesehen waren, aber partiell Bestandteil der Systemarchitektur wurden.

So wurde mit zwei separaten Repos gestartet, einerseits für den Learning-Part, welcher anfänglich auch die Smart Contracts umfasste, und andererseits eines für die Tablet-App, welches bereits vor der eigentlichen Konzeption erstellt wurde, um in erster Linie bestehende Crossplattform Frameworks, auf Basis der Kompatibilität und Funktionstüchtigkeit mit Libraries, welche die Kommunikation mit der Blockchain ermöglichen, zu evaluieren.

Die Wahl fiel letztendlich auf React-Native, welches zwar nur bis zu einer bestimmten Versionsnummer der Web3.js Library von Ethereum vollends kompatibel ist und nur mit einem kleinen Workaround zum Laufen gebracht werden konnte. Jedoch im Vergleich zu anderen Frameworks (z.B. Nativescript) die beste Development-Experience (geringe Lernkurve, gute Dokumentation, CLI) bot und v.a. hinsichtlich der Requirements alle Aufgaben komplett erfüllen konnte, welche die anderen Frameworks in dieser Gänze nicht replizieren konnten.

Nachdem die erste rudimentäre Version der Tablet-App, welche lediglich eine funktionierende Kommunikation (read/write) mit einem bereits bestehenden Smart-Contract auf einer lokal gehosteten Blockchain bestätigte, erstellt wurde, kam im nächsten Schritt der Learning-Part zum Zuge.

In Anbetracht der kompletten Implementierung des Ethereum Protokolls in Golang und der Schwierigkeiten mit der Javascript Library Web3.js, v.a. im

3 System Architektur

Bezug auf das deployen der Smart-Contracts, aus einem vorangegangenen Projekt, fiel die Wahl für diese Instanz auf Golang.

Zuerst wurde der Q-Learning Algorithmus, welcher für das Erlernen des Kaffee Trinkverhalten zuständig ist, implementiert. Die Problematik bestand zum einen darin mit einer neuen Programmiersprache vertraut zu werden und zum anderen den Workflow hinsichtlich der Problemstellung und des daraus resultierenden Zustandsraums vollends abzubilden. Die Umsetzung des Algorithmus in der Programmiersprache ging relativ einfach von der Hand, was jedoch Probleme bereitete war die Simulation des Workflows, um die Algorithmus Parameter zu justieren und dessen Tauglichkeit bezüglich das Erlernen des Nutzerverhaltens zu testen.

Im Anschluss wurde ein erster Smart-Contract erstellt und via dem “go-ethereum” package deployed, woraus das erste Smart-Contract Bindingsfile resultierte, welches für die Kommunikation mit dem Smart Contract vonnöten ist. Da mit jedem neuem Deployment eines Smart Contracts eine neue Smart Contract Adresse und eine neue ABI hervorgeht, welche wiederum beide im Source Code für die Kommunikation mit dem Smart Contract, über alle Instanzen hinweg, die mit einem Smart Contract interagieren wollen, hinterlegt sein müssen, wurde ein kleiner HTTP-Fileserver entwickelt, auf dem diese Informationen gespeichert und gelesen werden können.

Bei jedem neuen Deployment werden daraufhin die Smart-Contract Adresse und die generierte ABI in ein JSON-File gepackt und an den Server geschickt. So konnte während der Entwicklung enorm an Zeit gespart werden, da sich sowohl die Learning-Instanz als auch die App, die benötigten Daten vom Server holen und somit ein ständiges “Hardcodieren” dieser Daten vermieden werden konnte.

Aus diesem Grund findet der Fileserver auch Einzug in die finale Systemarchitektur, da er als persistente Datenquelle eine enorme Erleichterung nicht nur im Entwicklungsprozess, sondern auch im “Live-System” darstellt.

Zudem wird der Fileserver auch für die Verwaltung der Algorithmus-Daten verwendet. Dabei wird bei jedem Worker-Durchlauf (vgl. Kap. 3.3.3) für jeden

Nutzer ein JSON-File erzeugt, welches folgende Key-Value-Pairs beinhaltet (vgl. Kap. Abbildung 3.3):

- qt: die aktuelle Q-Tabelle des Users
- ep: der aktuelle Epsilon-Wert
- negs: Anzahl der falschen Predictions in der aktuellen Woche
- Wk_negs: Array von negs über alle Wochen hinweg

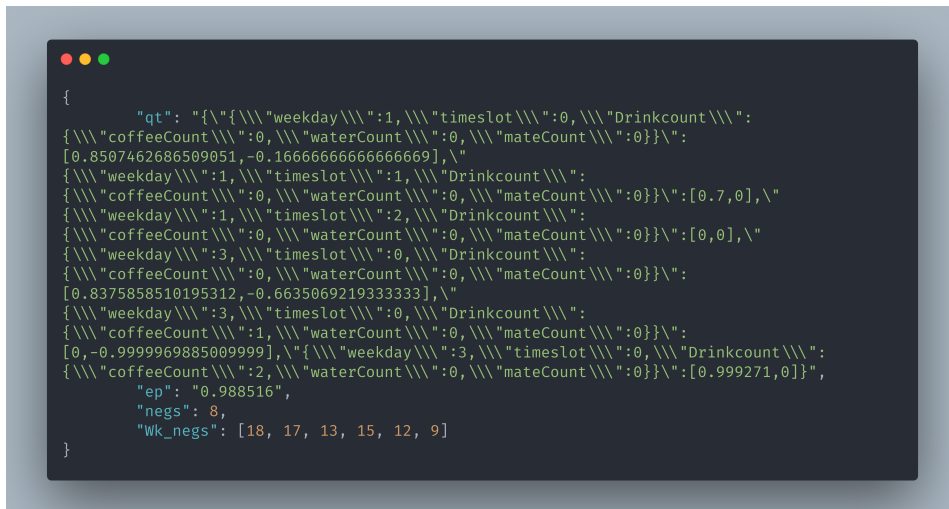


ABBILDUNG 3.3: 0x6ecbe1db9ef729cbe972c83fb886247691fb6beb-ql.json
Der Name des JSON-Files setzt sich aus der Ethereum-Adresse des Users und der Abkürzung "ql", welches für Q-Learning steht, zusammenhängen.

Der Vorteil liegt in der Möglichkeit den Learner jederzeit upzudaten ohne die gelernten Daten zu verlieren. Denn wird der Learner gestartet, holt sich dieser zuerst die Files vom Server, liest die Daten aus und initialisiert schon im Vorab die Q-Tabelle und das Epsilon eines jeden Users.

Sollte der Learner aus unbestimmten Gründen abstürzen, ist durch den eben beschriebenen Algorithmus die Erhaltung des Lernfortschrittes trotzdem sichergestellt.

Als letztes Modul wurde ein kleiner Node-Server entwickelt, dessen Aufgaben darin bestand die Smart-Contracts zu testen und als primitiver Ersatz

3 System Architektur

für die App zu fungieren. Hierbei erzeugte er in einem festgelegten Intervall (7sek) Events mit einem zufällig generierten Daten (User & Getränk) auf der Blockchain, um letztendlich die Event-Erkennung (“Watcher”) des “Learners” zu testen. Dabei wurde sowohl für den “Beverage-List Contract” als auch für den “CoffeeCoin-Contract” eine entsprechende Implementierung angefertigt.

In diesen Fällen wurde das Q-Learning-Submodul des Learners gar nicht erst gestartet, da lediglich die Funktionsweise des Watchers getestet werden sollte. Besonders hier zeigte sich die Nützlichkeit des Fileservers, da gerade in der Entwicklungsphase die Smart-Contracts noch häufigen Änderungen unterlagen und dahingehend sehr oft neu deployed werden mussten, was ohne den Fileserver dazu geführt hätte die Smart Contract Daten bei jeder Iteration neu im Sourcecode zu hinterlegen.

Nach einer längeren Testphase, in der eine einwandfreie Kommunikation mit den beiden Smart Contracts attestiert werden konnte, wurde mit der eigentlichen Entwicklung der App begonnen, für jene auch Teile der Node-Server Implementierung übernommen werden konnten.

Schwierigkeiten traten dabei erst in der Testphase auf, in der festgestellt wurde, dass zu wenig Events vom Learner detektiert werden. Die Ursache dafür lag an der sehr alten Android Version des Tablets, die nicht ermöglichte eine direkte Verbindung zum Uni-Netzwerk herzustellen. Dies gelang nur mit einem Workaround, bei dem sich das Tablet mit einem öffentlichen Wlan-Netzwerk verband und sich daraufhin über eine VPN-Verbindung in das Uni-Netzwerk einwählen konnte.

Das führte jedoch dazu, dass die Verbindung zum Wlan-Netzwerk in unregelmäßigen Abständen abbrach und dadurch auch zur Blockchain. Da so ein unvorhergesehenes Verhalten wurde in der ersten Implementierung der App nicht vorgesehen war, musste dies in einem Update der App berücksichtigt werden (vgl. Kap. 3.4), sodass keine Daten verloren gingen, sollte die Verbindung abbrechen.

Schlussendlich waren es sechs dedizierte Software Anwendungen, welche jeweils in eigenen Git-Repositories gehostet werden. Dazu zählten:

- Learner

- Tablet-App
- Go Fileserver
- Smart Contracts: Beverage-List, CoffeeCoin
- Web3 Node-Server
- Dockerimage für die Blockchain

Das Dockerimage fand in der Hinsicht keine größere Erwähnung, da es nur zu Test- und Weiterbildungszwecken entwickelt wurde und auch keine Verwendung in der finalen Architektur fand.

3.2 Blockchain

Das folgende Kapitel erläutert im Detail den Setup der privaten Blockchain, sowie die beiden Smart Contracts welche ebenso ein Teil der Systemarchitektur darstellen.

3.2.1 Genesis Block

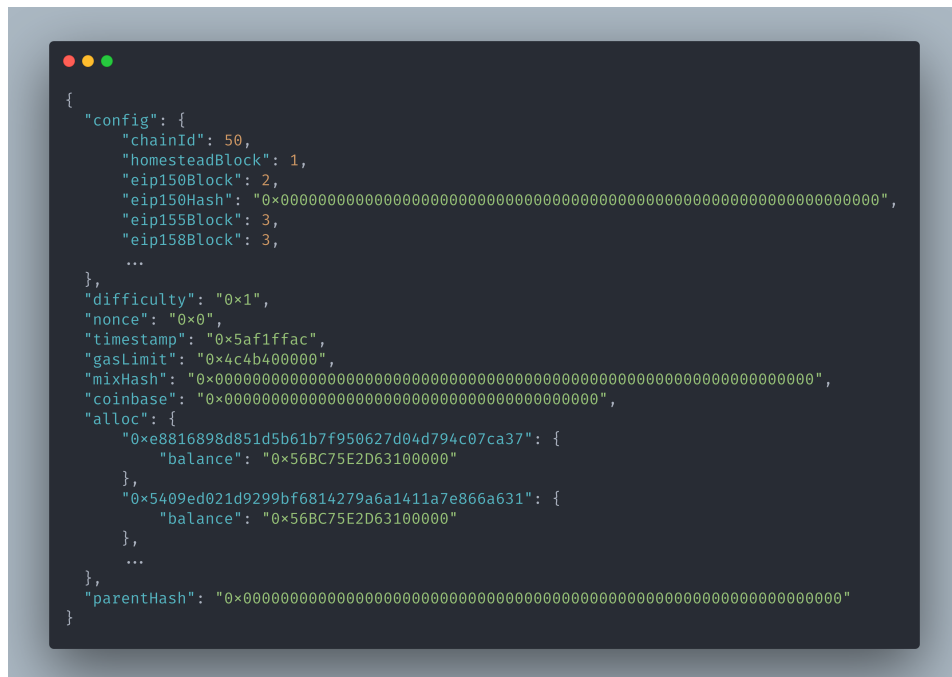
Der große Vorteil einer privaten (Ethereum) Blockchain gegenüber einer öffentlichen, ist die Möglichkeit die Blockchain nach den eigenen Vorstellungen und Anwendungszwecken zu konfigurieren. So können, wie auch bei einer öffentlichen Blockchain, Smart Contracts erstellt und Transaktionen durchgeführt werden, allerdings ohne dabei wirkliches Ether zu besitzen. Denn eine Besonderheit eines sogenannten “Testnet’s” ist das Erzeugen von “privatem” Ether, welcher Accounts zugeordnet und somit Transaktionen durchgeführt werden können.

Die Konfiguration dessen erfolgt durch ein sog. “genesis.json file” (3.5). Diese Datei ist die Grundlage für den *Genesis Block* der zu erstellenden Blockchain,

3 System Architektur

welcher der erste Block in der Kette ist und somit auch keinen Vorgänger besitzt.

Das in 3.5 abgebildete JSON Objekt zeigt die in der Systemarchitektur verwendete Datei einen solchen *Genesis Block* zu erzeugen. Nicht alle “properties” bedingen einer Erklärung, die essentiellen werden allerdings kurz erläutert:

A screenshot of a code editor with a dark background and light-colored text. The editor shows a JSON object representing a Genesis Block. The object has several properties: 'config' (an object with 'chainId', 'homesteadBlock', 'eip150Block', 'eip150Hash', 'eip155Block', and 'eip158Block'), 'difficulty', 'nonce', 'timestamp', 'gasLimit', 'mixHash', 'coinbase', 'alloc' (an object with two entries for addresses and their balances), and 'parentHash'. The 'parentHash' is a long string of zeros. The 'alloc' section shows two addresses with their respective balances in ether.

```
{
  "config": {
    "chainId": 50,
    "homesteadBlock": 1,
    "eip150Block": 2,
    "eip150Hash": "0x0000000000000000000000000000000000000000000000000000000000000000",
    "eip155Block": 3,
    "eip158Block": 3,
    ...
  },
  "difficulty": "0x1",
  "nonce": "0x0",
  "timestamp": "0x5af1ffac",
  "gasLimit": "0x4c4b400000",
  "mixHash": "0x0000000000000000000000000000000000000000000000000000000000000000",
  "coinbase": "0x0000000000000000000000000000000000000000000000000000000000000000",
  "alloc": {
    "0xe8816898d851d5b61b7f950627d04d794c07ca37": {
      "balance": "0x56BC75E2D63100000"
    },
    "0x5409ed021d9299bf6814279a6a1411a7e866a631": {
      "balance": "0x56BC75E2D63100000"
    },
    ...
  },
  "parentHash": "0x0000000000000000000000000000000000000000000000000000000000000000"
}
```

ABBILDUNG 3.4: genesis.json
JSON-File welches zur Erstellung des Genesis Blocks verwendet wurde.

- chainId: ist eine einzigartige Id für die private Blockchain
- eip150Block/eip155Block/eip158Block: eip steht für “Ethereum Improvement Proposal”. Diese drei Community getriebenen “Proposals” beschreiben sog. “hard forks”, welche dafür sorgen sollten Fehler im Protokoll zu beheben.
- homesteadBlock: Homestead ist die zweite “major version” von Ethereum, welche einige Änderungen an dem Protokoll vornahm

- difficulty: beschreibt die Schwierigkeitsstufe für einen Miner einen validen Block zu finden. Das heißt je höher der Wert desto mehr Berechnungen müssen statisch durchgeführt werden und desto mehr Zeit wird benötigt, um eine Transaktion zu bestätigen. Im Falle eines Testnets ist es deshalb ratsam einen sehr niedrigen Wert zu wählen
- gasLimit: beschreibt das Limit für eine Transaktion wie viel an Gas verbraucht werden darf.
- alloc: hier können Accounts schon im Voraus mit “fake ether” befüllt werden.
- nonce: ist ein Zähler für die Anzahl der durchgeführten Transaktionen einer Adresse

Sobald die genesis.json Datei fertiggestellt ist, kann die Blockchain mit folgendem Befehl erstellt werden:



Das Flag `--datadir` ist mit dem aus Abbildung 3.2 identisch. Das bedeutet das Verzeichnis welches hier im Befehl angegeben ist, muss beim Kommandozeilenbefehl in Abbildung 3.2 exakt gleich sein. Andernfalls ist es nicht möglich die Blockchain zu starten.

Nachdem der Setup der privaten Blockchain abgeschlossen ist, kann mit der Entwicklung eines Smart Contracts begonnen werden.

Die nächsten beiden Unterkapitel befassen sich mit den Smart Contracts, welche im Zuge dieser Arbeit entwickelt wurden.

3.2.2 CoffeeCoin

Der Smart Contract “CoffeeCoin” stellt einen sogenannten ERC-20 Token mit gewissen Abwandlungen dar. Dabei ist ein Token im Grunde eine zusätzliche Währung zur eigentlichen Währung von Ethereum dem Ether. Das bedeutet Smart Contracts können somit eine eigenständige Währung abbilden. Für solche Smart Contracts gibt es mittlerweile einige Standardisierungen, die Vorschreiben welche Methoden und Datenstruktur ein Smart Contract zu implementieren hat. Der am weit verbreitetste Standard ist der ERC-20, bei welchem es folgende Funktionen und Events zu implementieren gilt:



```
contract ERC20Interface {
    function totalSupply() public view returns (uint);
    function balanceOf(address tokenOwner) public view returns (uint balance);
    function allowance(address tokenOwner, address spender) public view returns (uint
remaining);
    function transfer(address to, uint tokens) public returns (bool success);
    function approve(address spender, uint tokens) public returns (bool success);
    function transferFrom(address from, address to, uint tokens) public returns (bool success);

    event Transfer(address indexed from, address indexed to, uint tokens);
    event Approval(address indexed tokenOwner, address indexed spender, uint tokens);
}
```

ABBILDUNG 3.5: ERC-20 Interface

- `totalSupply`: Gesamtanzahl der existierenden Tokens
- `balanceOf`: Anzahl der Tokens eines bestimmten Users
- `allowance`: besagt wie viele Tokens eines bestimmten Users durch einen bestimmten “spender” abgehoben werden dürfen
- `transfer`: transferiert die Inputanzahl an Tokens des “senders” (Adresse welche diese Funktion aufgerufen hat) an die angegebene Adresse
- `approve`: Erlaubniserteilung an den “spender” die in *allowance* festgelegte Anzahl an Tokens abzubuchen
- `transferFrom`: transferiert die angegebene Anzahl von Tokens von der “from Adresse” zur “to Adresse”

- event Transfer: wird von den beiden *transfer* Funktionen ausgelöst
- event Approval: wird von der *approve* Funktion ausgelöst

Der eben erläuterte Token Standard wurde im Falle des CoffeeCoin Smart Contracts um zusätzliche Funktionen und Datenstrukturen erweitert. Diese Erweiterungen stellen eine gesonderte Abstraktionsebene nach außen hin da, um die Kommunikation seitens der Tablet-App zu erleichtern und einfacher zu gestalten.

So werden schon beim Deployment die einzelnen Preise der Getränke und die Adresse, zu jener die Tokens beim Bezahlen eines Getränks überwiesen werden, gesetzt.

Dies ermöglicht die Implementierung folgender Funktionen:



```

contract CoffeeCoinInterface {
    function payCoffee() public returns (bool success);
    function payWater() public returns (bool success);
    function payMate() public returns (bool success);
    ...
}

```

ABBILDUNG 3.6: CoffeeCoin Interface Auszug

Diese Funktionen bieten eine Abstraktionsebene zur ERC-20 Funktion *transferFrom*. Da bereits beim Deployment die Parameter für die Getränke und die Zieladresse gesetzt werden, benötigen diese Funktionen keine weiteren Daten von der Seite der User (Tablet-App). Somit kann nach Auswahl des Getränks die entsprechende Funktion aufgerufen werden, ohne sich dabei mit den Details der Transaktion beschäftigen zu müssen.

Desweiteren wird einem User, beim ersten Aufruf einer jener Funktionen (erste ausgelöste Transaktion des Users), eine festgelegte Anzahl an Tokens als “Startguthaben” überwiesen, sodass dieser stets über genügend Token verfügt

und jederzeit Transaktionen durchführen kann.

Im Kontext der Problemstellung liegt die Zweckmäßigkeit des Smart Contracts grundsätzlich in der Bezahlung der Getränke in Form des Tokens. Dabei soll vor allem die Möglichkeit einer solchen Bezahlmethode aufgezeigt werden, weswegen die Transaktionen lediglich auf exemplarischer Ebene durchgeführt werden. Das bedeutet, den Usern wird, wie gerade beschrieben, eine nahezu unendliche Menge an Tokens zugewiesen ohne eine Gegenleistung zu fordern.

Der Sourcecode ist im Anhang unter REF SO UND SO zu finden.

3.2.3 Beverage-List

Im Gegensatz zur CoffeeCoin basiert der Beveragelist Contract auf keinem festgelegten Standard, sondern ist in voller Gänze an die Problemstellung angepasst.

Dessen Zweck besteht im Grunde darin eine Getränkliste abzubilden, in welcher jede Getränktransaktion eines Users vorzufinden ist. Dabei wird pro Transaktion nicht nur das Getränk, sondern auch das aktuelle Datum inklusive Uhrzeit und der aktuelle Wochentag, gespeichert. Diese Daten sollen es dem Learner schlussendlich ermöglichen das Kaffeetrinkverhalten des Users zu erlernen. Damit der Learner ohne großen Aufwand auf diese Informationen zugreifen kann, löst der Smart Contract, mit den eben genannten Daten beinhaltend, ein Event aus, sobald seine Methode “setDrinkData” aufgerufen wird. Diese Funktion hinterlegt die übergebenen Daten (Eth-Adress, Zeit, Wochentag, Getränk) in festgelegten Datenstruktur und löst zugleich das Event für den Learner aus.

Dieser Smart Contract umfasst noch weitere Funktionen, welche aber vor allem zu Testzwecken implementiert wurden und in der finalen Systemarchitektur keine Verwendung finden.

3.3 Learner

Als nächstes wird der sogenannte “Learner” detailliert betrachtet. Dabei wird zuerst die Problemstellung hinsichtlich des Reinforcement-Learnings modelliert und im Anschluss der verwendete Algorithmus (Q-Learning) allgemein und im Kontext der Problemstellung erläutert.

3.3.1 Modellierung

Die Modellierung eines Lernproblems im Hinblick auf einen Reinforcement-Algorithmus erfolgt in der Regel stets nach der selben Systematik.

Dabei werden zuerst der Zustandsraum, also alle möglichen Zustände, alle Aktionen des “Agenten” und der Reward für ausgeführte Aktionen eruiert. Hier in diesem Fall ist der Agent der Learner, welcher das Kaffeetrinkverhalten der User zu erlernen versucht.

Die Modellierung sieht wie folgt aus:

Zustandsraum

- Wochentag: Montag, Dienstag, Mittwoch, Donnerstag, Freitag
- Timeslot:
 - 7-9 Uhr (T0)
 - 10-12 Uhr (T1)
 - 13-15 Uhr (T2)
 - 16-18 Uhr (T3)
 - 19-6 Uhr (T4)
- Kafee-Anzahl: $n * \text{Kaffee}$ ($n = \text{Anzahl pro Tag}$)

Aktionen

- Kaffee
- Nothing

Reward

- +1 bei richtiger Prediction
- -1 bei falscher Prediction

Daraus lässt sich folgender exemplarischer Zustand konstruieren:

`< Wochentag: Montag; Timeslot: 2; Kaffee-Anzahl: 3 >`

Das bedeutet konkret: an einem Montag wurden einschließlich des 2. Timeslots (13-15 Uhr) 3 Kaffee getrunken. Dieser Status gibt jedoch keinen Aufschluss darüber, welcher sein Vorgänger war und welcher sein Nachfolger sein wird. So können einerseits alle Kaffee's nur in Timeslot 2 getrunken worden sein oder in jedem Timeslot (0,1,2) jeweils einen. Andererseits besteht auch die Möglichkeit, dass im Timeslot 2 nochmals ein Kaffee konsumiert wird oder eben erst in einem nachfolgendem Timeslot.

Dieses Lernproblem ist auch als "Multi-Armed Bandit Problem" bekannt und wird in Kap. 3.3.2 erläutert.

Der erste Modellierungsansatz sah anstatt der Kaffee-Anzahl eine Getränkeanzahl vor, bei der zum Kaffee auch die Quantität der getrunkenen "Clube Mate" und "Wasser" berücksichtigt werden sollten. Der Grund dafür liegt in dem erheblichen Einfluss des Konsums weiterer Getränke auf das Kaffeetrinkverhalten, wodurch mit solch einer granulareren Modellierung genauere Predictions zu erwarten sind. Jedoch steigt somit auch die Anzahl der zu durchlaufenden Zustände und einhergehend damit die zu erlernenden optimalen Aktionen für die Zustandsübergänge. Letzlich resultiert dies in der längeren Trainingsphase des Algorithmus, was aber aufgrund des zeitlich begrenzten Rahmen dieser

Arbeit nicht durchführbar war und deshalb der Ansatz mit lediglich der Kaffee-Anzahl gewählt wurde.

TO-DO: feature selection to add user versteht zu jeder warum algorithmus so handelt

3.3.2 Q-Learning

Im folgenden wird der implementierte Q-learning Algorithmus zuerst allgemein und anschließend im Bezug auf die Problemstellung erläutert.

TO-DO: Alles!!!!

3.3.3 Lernprozess & Ablauf

Aufgrund der Modellierung eines Zustandes ergeben sich zwei Arten bei denen eine Änderung dessen hervorgerufen wird:

- durch eine zeitliche Komponente, bei der sich entweder der Timeslot oder der Tag ändert
- durch den User indem er eine Transaktion auslöst

Das ist in der Hinsicht von großer Bedeutung, da für diese Übergänge ein Feedback für den Agenten notwendig ist, um jeweils die optimale Aktion dafür zu erlernen.

So wird das Feedback einerseits von Seiten des Users in Form einer bestätigten Transaktion generiert, was bedeutet Aktion “Kaffee” wurde ausgeführt. Oder andererseits als Folge einer fehlenden Rückmeldung des Nutzers, welche “Nothing” als optimale Aktion impliziert.

Das heißt erfolgt eine Zustandsänderung durch den User, so ist stets “Kaffee” die zu erlernende, beste Aktion. Wird eine Zustandsänderung durch einen Timeslotwechsel bewirkt, so ist das Feedback der Umgebung immerfort die

3 System Architektur

Aktion “Nothing”.

Um dem Agenten bzw. dem Q-Learning Algorithmus stets das nötige Feedback zu geben und Zustandsübergänge herbeizuführen, werden im Learner die Komponenten “Watcher” und “Worker” verwendet.

Der “Watcher” ist dafür zuständig das Feedback des Users durch das Beveragelist-Event zu detektieren und die darin enthaltenen Daten dem Algorithmus zur Verfügung zu stellen.

Der “Worker” wird für die zeitliche Komponente verwendet, indem er am Ende jedes Timeslots aktiv wird, die Zustandsänderung durchführt und dem Agenten die Aktion “Nothing” als Feedback gibt.

Auf Basis dieser Feedbacks wird es dem Q-Learning Algorithmus ermöglicht die optimalen Aktionen zu erlernen. Hierbei wird die Prediction, also die aus Sicht des Agenten beste Aktion für den Zustandsübergang, anhand der Rückmeldung, sei es durch den Watcher oder Worker, evaluiert und für den nächsten Übergang eine neue Aktion eruiert.

Dieses Prinzip der Evaluierung und Vorhersage der Aktion kann im Kontext des Lernproblems jedoch nicht kontinuierlich angewendet werden. So bedingen bestimmte Zustände nur eine Evaluierung oder nur eine Vorhersage, indes nie beides. Der Grund hierfür liegt in der Abgeschlossenheit der Tage als Lernabschnitt, welche komplett unabhängig voneinander agieren.

Zudem werden die Uhrzeiten zwischen 19 und 6 Uhr (T4) nicht in der Zustandsraummodellierung berücksichtigt, da in diesem Zeitraum keine Aktion durch den User zu erwarten ist.

Dies hat für den “Worker” zur Folge, dass zum einen am Anfang jedes Tages bzw. beim Wechsel von T4 auf T0, lediglich eine Vorhersage für den nächsten Zustandsübergang gemacht und zum anderen am Ende von T3 einzig die letzte Vorhersage evaluiert werden muss.

Dies lässt sich veranschaulicht folgendermaßen darstellen:

- Evaluierung & Vorhersage:
 - User führt Transaktion durch

- Timeslot wechselt
- Evaluierung:
 - am Ende von T3
- Vorhersage:
 - am Anfang von T0

3.4 Tablet-App

Das folgende Unterkapitel befasst sich mit dem Aufbau und der Funktionsweise der App und schildert zudem den verwendeten Algorithmus, welcher die Getränk- und Userdaten auf die Blockchain schreibt.

Die entwickelte App basiert auf dem Crossplattform Framework “React Native” [RN:], dieses erlaubt es mit einer einzigen Codebasis Apps für unterschiedliche Plattformen (z.B. iOS, Android) zu entwickeln. Der wesentliche Vorteil allerdings liegt in der Verfügbarkeit einer offiziellen Library, mit der es erst möglich ist eine Verbindung zur Blockchain bzw. den Smart Contracts herzustellen. Diese Library (Web3.js) wurde von Ethereum dafür entwickelt, um sog. DApp’s (“decentralized apps”) [DApp] auf Basis von Javascript erstellen zu können.

So ist die Entwicklung einer DApp in einer nativen Programmiersprache (Java/Kotlin/Swift) bisher nur mit “third-party libraries” möglich, weswegen die Umsetzung letztlich mit ReactNative erfolgte.

3.4.1 Interface

Eine essentielle Eigenschaft von ReactNative ist der komponentenbasierte Ansatz. Dabei setzt sich eine App aus vielen einzelnen Komponenten zusammen, welche jeweils einen dedizierten Aufgabenbereich abdecken.

3 System Architektur

Im Falle der entwickelten App existieren jeweils zwei “page components”, die wiederum mehrere kleine Komponenten in sich vereinen. Da es aber den Rahmen dieser Arbeit sprengen würde auf jede einzelne Komponente und deren Funktionsweise einzugehen, werden nur die Hauptkomponenten anhand ihrer Funktion und Bedienung geschildert.

Wird die App gestartet und es besteht eine Verbindung zum Internet bzw. zur Blockchain, so findet der User folgende Startseite vor:

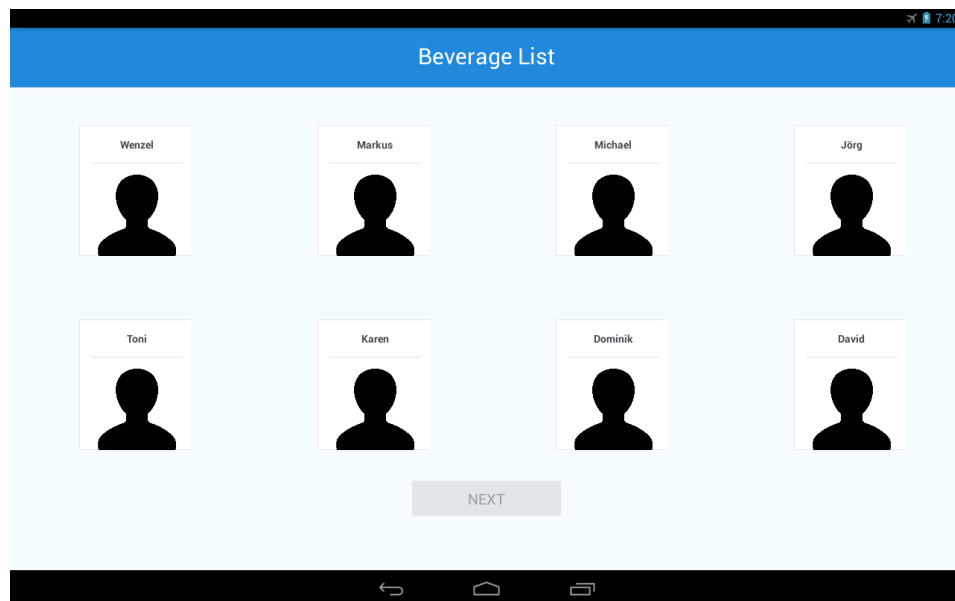


ABBILDUNG 3.7: Mitarbeiter Page: kein Mitarbeiter ausgewählt

Hier kann der User seinen Avatar selektieren und deselektieren. Ist ein Avatar ausgewählt wird der “NEXT” Button aktiviert (vgl. Abbildung 3.8) und durch dessen Betätigung gelangt der User zur nächsten Seite:

Hier besteht eine Auswahl aus folgenden Getränken: Club Mate, Wasser und Kaffee. Ausgewählt kann jedoch immer nur eines werden (vgl. Abbildung 3.12). Das Prinzip der Selektion und Deselektion ist identisch mit dem der vorherigen Seite. So wird der “SUBMIT” Button aktiv, sobald ein Getränk ausgewählt ist und inaktiv wenn das Getränk wieder deselektiert wird (vgl. Abbildung 3.9).

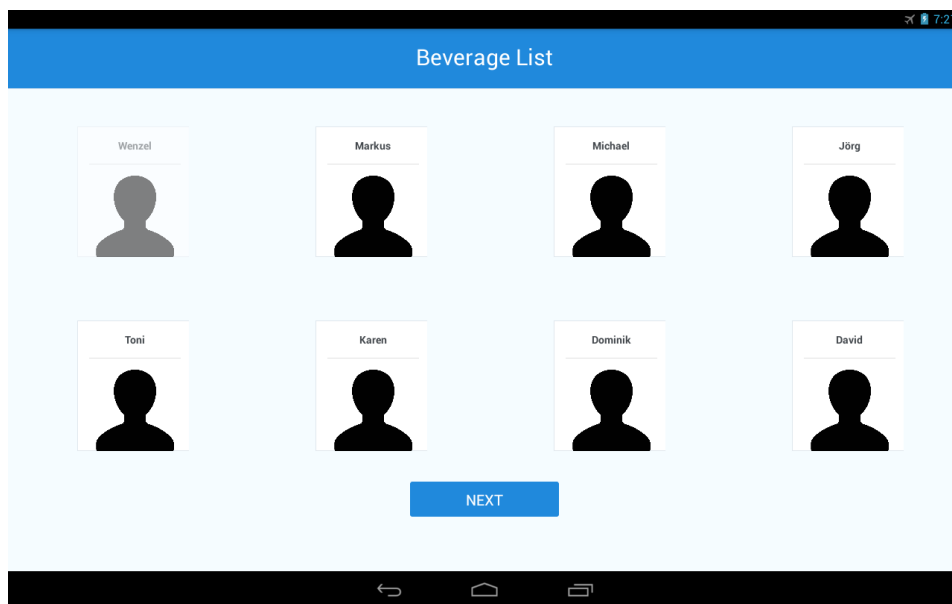


ABBILDUNG 3.8: Mitarbeiter Page: Mitarbeiter ausgewählt

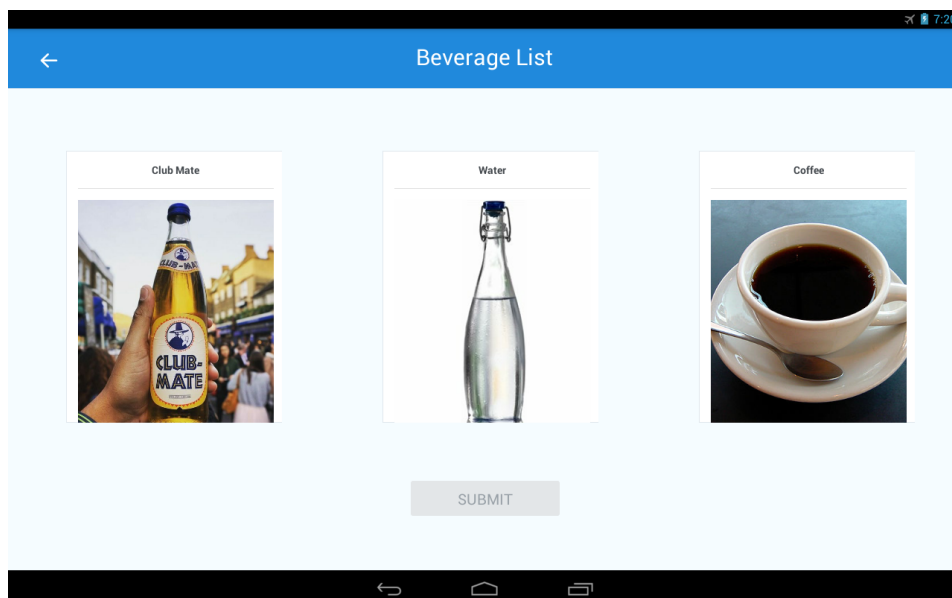


ABBILDUNG 3.9: Drinks Page: kein Getränk ausgewählt

Wird schließlich der "SUBMIT" Button gedrückt und die Transaktion als erfolgreich bestätigt erscheint folgendes Overlay:

3 System Architektur

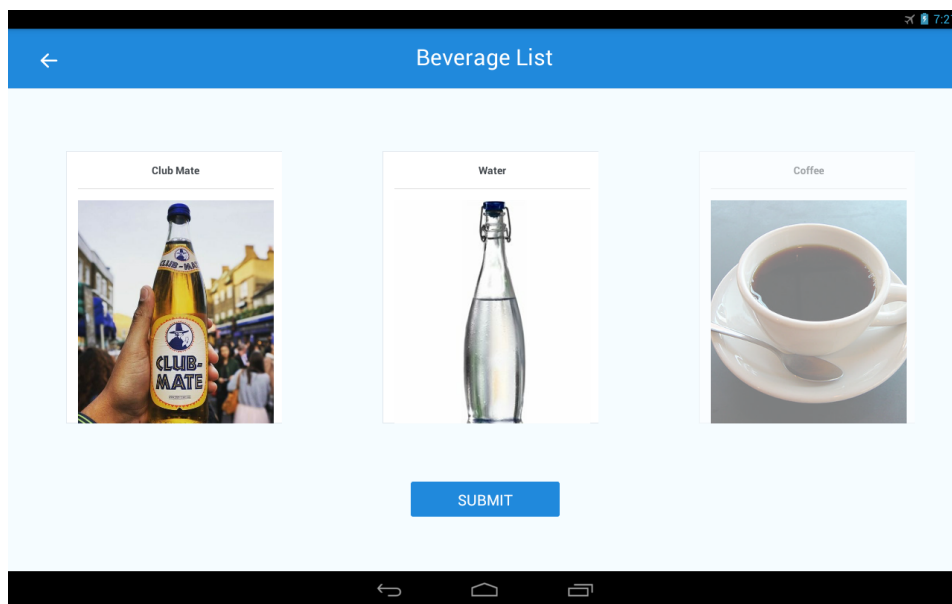


ABBILDUNG 3.10: Drinks Page: Getränk ausgewählt

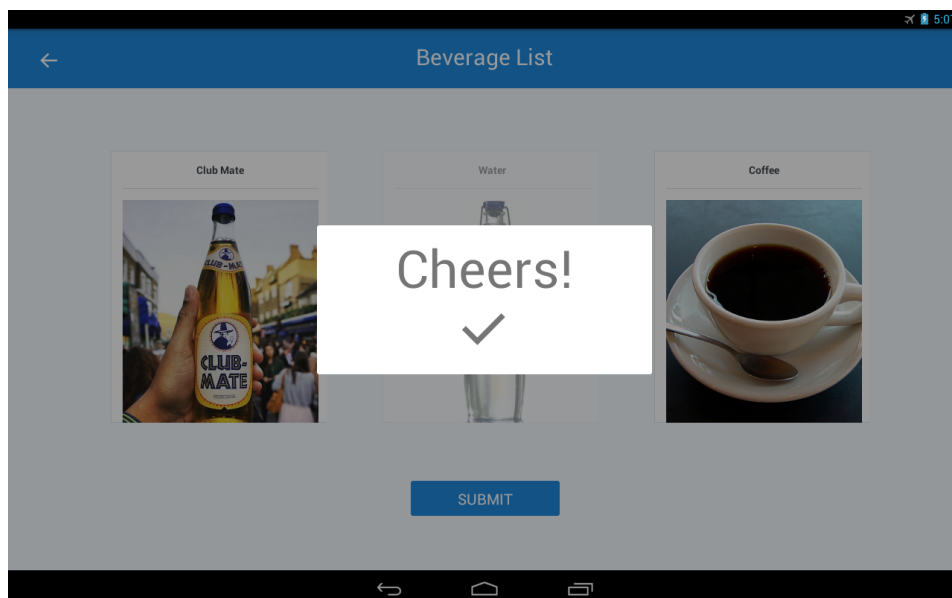


ABBILDUNG 3.11

Nach 4 Sekunden wird dieses Overlay wieder ausgeblendet und automatisch zur Startseite (vgl. Abbildung 3.7) navigiert, wodurch der Workflow von neuem startet.

Aufgrund der Tatsache, dass die Verbindung zum Uni-Netzwerk (eduroam) nur über einen Workaround hergestellt werden konnte, bei dem die Verbindung zum Netzwerk trotzdem nach einer unbestimmten Zeit immer wieder abgebrochen ist, wurde eine weitere Komponente entwickelt.

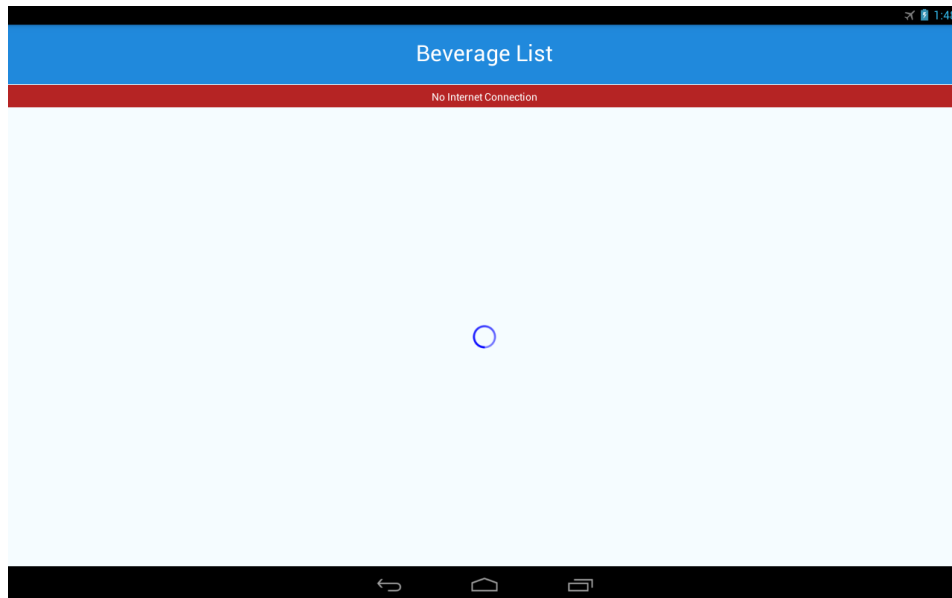


ABBILDUNG 3.12

Diese wird sofort eingeblendet sobald die Verbindung zum Internet unterbrochen ist, allerdings nur wenn sich der User auf der Startseite befindet. Wird die Seite mit den Getränken angezeigt, so wird dem User die Möglichkeit gegeben seine Transaktion abzuschließen. Da in diesem Moment jedoch keine Verbindung zur Blockchain hergestellt werden kann, werden die Transaktionsdaten zwischengespeichert und diese durchgeführt sobald wieder eine Verbindung zum Netzwerk besteht (vgl. Kap. 3.4.2). Die Loading Animation sowie das “No Internet Connection” Label werden wieder ausgeblendet sobald die App eine erneute Verbindung zum Uni-Netzwerk detektiert.

3.4.2 Internal Workflow

Basierend auf der Problematik eines unerwarteten Verbindungsabbruch und dem einhergehenden Verlust von essentiellen Lerndaten, wird im folgenden der implementierte Algorithmus geschildert, der dieser Komplikation entgegenwirkt.

1. Initialisierungsphase:
 - 1.1. “GET” Smart Contract Daten von Fileserver
 - 1.2. Initialisierung Web3.js
 - 1.3. Wiederhole für jedes Transaktionsfile:
 - 1.3.1. Transaktion durchführen
 - 1.3.2. bei “Success” Transaktionsdatei löschen
2. Warten auf Usereingabe:
 - 2.1. User ausgewählt → Ethereum-Adresse
 - 2.2. Getränk ausgewählt → Getränk
 - 2.3. Submit → (Getränk & Ethereum-Adresse)
3. Wiederhole für jedes User-Transaktionsfile:
 - 3.1. Transaktion durchführen
 - 3.2. bei “Success” Transaktionsdatei löschen
4. Generierung Transaktionsdaten:
 - Gas Estimate
 - Datum (inkl. Zeit)
 - Wochentag
 - Ethereum-Adresse & Getränk aus 2.3

5. Transaktion starten:

5.1. Erstellung der Transaktionsdatei

5.2. Transaktion durchführen

5.3. bei “Success” Transaktionsdatei löschen

5.4. gehe zu 1.

Der interne Workflow beginnt mit der Initialisierungsphase, dabei werden zuerst die Smart Contract Files vom Fileserver runtergeladen und mit den beinhaltenden Daten das Web3.js Modul initialisiert. Damit steht Verbindung und die Kommunikation mit den Smart Contracts und es wird im Anschluss über alle vorhandenen Transaktion Files iteriert. Dabei wird zuerst der CoffeeCoin Contract und dann der Beveragelist Contract aufgerufen. Wenn beide ihre Transaktionen bestätigt haben, wird die Datei gelöscht, andernfalls bleibt diese bestehen. Dies geschieht noch bevor der User das Interface zu Gesicht bekommt.

Nachdem 1. abgeschlossen ist wird auf die Eingabe des Users gewartet. Wählt dieser einen Avatar aus klickt “NEXT” wird seine hinterlegte Ethereum-Adresse temporär gespeichert. Wird dann im Anschluss ein Getränk selektiert und “SUBMIT” gedrückt, werden die Ethereum-Adresse und das Getränk an das interne Blockchain-Modul weitergereicht und die Transaktion gestartet.

Dabei wird erneut über die Transaktionsdaten iteriert, allerdings nur über die des Users. Damit soll stets die richtige Reihenfolge der getrunkenen Getränke sichergestellt werden, da dies ansonsten auf Seiten des Q-Learning Algorithmus zu falschen Lerneffekten führen würde.

Daraufhin kann mit der Generierung der fehlenden Transaktionsdaten angefangen werden. Es wird zuerst ein “Gas Estimate” für beide Smart Contract Transaktionen durchgeführt. Ein “Gas Estimate” ist, wie der Name bereits impliziert, eine grobe Schätzung wie viel Gas beim Funktionsaufruf eines Smart

3 System Architektur

Contracts benötigt wird. Abschließend werden das Datum (inkl. Zeit in Sekunden) und der Wochentag ermittelt und alle benötigten Daten an die jeweiligen Smart Contract Funktionsaufrufe übergeben. Im Falle des Smart Contracts Beveragelist: *Gas-Estimate*, *Datum*, *Wochentag*, *Ethereum-Adresse*, *Getränk*. Bei CoffeeCoin wird anhand des Getränks die entsprechende Smart Contract Funktion ausgewählt und lediglich das *Gas-Estimate* und die *Ethereum-Adresse* des Users übergeben.

Bevor jedoch beide Transaktionen durchgeführt werden, wird ein Transaktionsfile mit dem Namen “«ethereum-adresse»-«datum».json” und den Daten *Datum*, *Wochentag*, *Ethereum-Adresse*, *Getränk* gespeichert. Sogleich werden beide Funktionsaufrufe getätigt und bei erfolgreicher Bestätigung beider Transaktionen wird das gerade erstellte File wieder gelöscht. Somit soll sichergestellt werden, dass keine Transaktionen aufgrund von Verbindungsabbrüchen verloren gehen.

Anschließend erfolgt eine “Pseudo-Reload” der App und der Ablauf beginnt wieder bei 1.

4 Studie

4.1 Testphase

4.2 Evaluation

5 Zusammenfassung

5.1 Weiterführende Forschungsfragen

- anderer algorithmus sarsa
- Decision Trees besseres ergebnis?
- offline learning from bchain logs -> reinforcement oder unsupervised
- algorithmus daten auch auf bchain speichern -> transparenz
-

5.2 Ausblick

Literaturverzeichnis

- [btc] btc-echo. Was ist proof-of-stake?
- [DAp] Dapp.
- [Dav15] David Tuesta. Smart contracts: the ultimate automation of trust?, 2015-10-15.
- [Lui15] Luisa Geiling. Distributed ledger: Die technologie hinter den virtuellen währungen am beispiel der blockchain, 2016-02-15.
- [Rap09] Raphael Honig. So lange dauert mining bei bitcoins | kryptopedia, 2018-04-09.
- [RN:] React native.
- [Wika] Wikipedia. Application programming interface - wikipedia.
- [Wikb] Wikipedia. Cross-platform software - wikipedia.
- [Wike] Wikipedia. Cross-platform software - wikipedia.
- [Wikd] Wikipedia. Crud - wikipedia.
- [Wike] Wikipedia. Representational state transfer - wikipedia.
- [Wikf] Wikipedia. Single point of failure - wikipedia.
- [Wikg] Wikipedia. User experience - wikipedia.

Abbildungsverzeichnis

3.1	Systemarchitektur	10
3.2	geth Befehl zum starten der Blockchain	17
3.3	0x6ecbe1db9ef729cbe972c83fb886247691fb6beb-ql.json Der Name des JSON-Files setzt sich aus der Ethereum-Adresse des Users und der Abkürzung "ql", welches für Q-Learning steht, zusammenhängen.	23
3.4	genesis.json JSON-File welches zur Erstellung des Genesis Blocks verwendet wurde.	26
3.5	ERC-20 Interface	28
3.6	CoffeeCoin Interface Auszug	29
3.7	Mitarbeiter Page: kein Mitarbeiter ausgewählt	36
3.8	Mitarbeiter Page: Mitarbeiter ausgewählt	37
3.9	Drinks Page: kein Getränk ausgewählt	37
3.10	Drinks Page: Getränk ausgewählt	38
3.11	38
3.12	39

Tabellenverzeichnis

A Anhang A

B Anhang B