
IP6: Blockchain Transactionmanager

Bachelorthesis

Faustina Bruno, Jurij Maïkoff

Studiengang:

- iCompetence
- Informatik

Betreuer:

- Markus Knecht
- Daniel Kröni

Auftraggeber:

Fachhochschule Nordwestschweiz
FHNW Campus Brugg-Windisch
Bahnhofstrasse 6
5210 Windisch



2019-10-01

Abstract

Contrary to popular belief, Lorem Ipsum is not simply random text. It has roots in a piece of classical Latin literature from 45 BC, making it over 2000 years old. Richard McClintock, a Latin professor at Hampden-Sydney College in Virginia, looked up one of the more obscure Latin words, consectetur, from a Lorem Ipsum passage, and going through the cites of the word in classical literature, discovered the undoubtable source. Lorem Ipsum comes from sections 1.10.32 and 1.10.33 of "de Finibus Bonorum et Malorum" (The Extremes of Good and Evil) by Cicero, written in 45 BC. This book is a treatise on the theory of ethics, very popular during the Renaissance. The first line of Lorem Ipsum, "Lorem ipsum dolor sit amet..", comes from a line in section 1.10.32.

Inhaltsverzeichnis

1	Einleitung	1
1.1	Problemstellung	1
1.2	Ziel	1
1.3	Methodik	1
1.4	Strukturierung des Berichts	2
2	Theoretische Grundlagen	3
2.1	Anwendungsbereich	3
2.2	Ethereum Client	3
2.2.1	Parity	4
2.2.2	Geprüfte Alternativen	4
2.3	Komponenten	4
2.3.1	Ethereum Blockchain	5
2.3.2	Smart Contracts	5
2.3.3	Transaktionen	6
2.3.4	Gas	7
2.3.5	Account	8
2.3.6	Blockchain Wallet	9
2.3.7	Denial of Service (DoS) Attacken	10
2.4	Lösungsansätze	11
2.4.1	Lösungsansatz 1: Smart Wallet	11
2.4.2	Lösungsansatz 2: Smart Wallet mit externen Programm nach Whitelist-Check	13
2.4.3	Lösungsansatz 3: Smart Wallet mit externen Programm vor Whitelist-Check	16
2.4.4	Lösungsansatz 4: Super Smart Wallet	18
2.5	Evaluation der Lösungsansätze	19
2.5.1	Lösungsansatz 1: Smart Wallet	20
2.5.2	Lösungsansatz 2: Smart Wallet mit externen Programm nach Whitelist-Check	20
2.5.3	Lösungsansatz 3: Smart Wallet mit externem Programm vor Whitelist-Check	21
2.5.4	Lösungsansatz 4: Super Smart Wallet	21
2.5.5	Resultat Evaluation	22

3	Praktischer Teil	23
3.1	Parity	23
3.1.1	Konfiguration der Blockchain	23
3.1.2	Whitelist	27
3.2	Schutz vor DoS Attacken	27
4	Fazit	28
5	Anhang	32
5.1	Glossar	32
5.2	Entwicklungsumgebung	32
5.2.1	Blockchain	33
5.2.2	Wallet	33
5.2.3	Smart Contracts	33
6	Ehrlichkeitserklärung	35

1 Einleitung

Dieses Kapitel liefert eine ausführliche Zusammenfassung der Bachelorthesis.

1.1 Problemstellung

Die Aufgabe beinhaltet ein Blockchain Netzwerk [1] für die Fachhochschule Nordwest Schweiz[2] (FHNW) zur Verfügung zu stellen, welches von den Studierenden zu Testzwecken genutzt werden kann. Blockchains verfügen über verschiedene Mechanismen, um sich gegen Attacks abzusichern. Eine davon ist eine Gebühr auf jeder Transaktion, der sogenannte Gas Price 2.3.4 [3]. Dadurch können Denial of Service (DoS) Attacks 2.3.7 [4], bei denen das Netzwerk mit unzähligen Transaktionen geflutet wird, effizient bekämpft werden. Der Angreifer kann die Attacke nicht aufrecht erhalten, da ihm die finanziellen Mittel zwangsläufig ausgehen. Obwohl dieser Schutzmechanismus auf einer öffentlichen Blockchain sehr effizient und elegant ist, eignet er sich nicht für eine Lernumgebung. Hier sollen Anwender die Möglichkeit haben, Transaktionen ohne anfallende Gebühren ausführen zu können. Dadurch wird jedoch die Blockchain anfällig für DoS Attacks.

1.2 Ziel

Das Ziel der Arbeit ist es ein Test Blockchain Netzwerk aufzubauen, welches für eine definierte Gruppe von Benutzern gratis Transaktionen erlaubt und trotzdem ein Schutzmechanismus gegen DoS Attacks hat.

1.3 Methodik

//TODO Kapitel besprechen und beschreiben Hier wird beschrieben wie und was gemacht wurde

!!muss besprochen überarbeitet werden Wir haben zu Beginn Meilensteine und grössere Arbeitspakete definiert. Die kleineren Arbeitspakete wurden nach neugewonnen Wissen und Arbeitsstand definiert.

Durch die erarbeiteten Lösungsansätze, der Evaluation und die Besprechung nach der Zwischenpräsentation, wurden die Meilensteine geändert und die Planung anders gestaltet.

Agiles Vorgehen, -> mit neuem Wissen weiter geplant

//TODO möglicher Text besprechen und überarbeiten Zu Beginn wurde ein provisorischer Projekt Plan mit möglichen Arbeitspaketen und Meilensteine definiert. Da die Thematik komplett unbekannt war, wurde auf ein agiles Vorgehen gesetzt, um neue Erkenntnisse in die Planung einfließen zu lassen. Nach der Einlese- und Probierphase, wurden Lösungskonzepte konzipiert, evaluiert und an der Zwischenpräsentation dem Experten und den Betreuern präsentiert. Hier wurde das weitere Vorgehen besprochen und die neuen Meilensteine definiert. Die Arbeitspakete werden alle zwei Wochen definiert.

1.4 Strukturierung des Berichts

Der Bericht ist in einen theoretischen und praktischen Teil gegliedert. Gemachte Literaturstudien, geprüfte Tools, der aktuelle Stand der Ethereum Blockchain, sowie die konzipierten Lösungsansätze und deren Evaluation werden im theoretischen Teil behandelt. Im praktischen Teil wird beschrieben, wie das gewonnene Wissen umgesetzt wird. Es wird auf die implementierte Lösung und deren Vor- und Nachteile eingegangen. Geprüfte Alternativen und deren Argumente sind ebenfalls enthalten. Das Fazit bildet den Abschluss des eigentlichen Berichts. Im Anhang ist eine Beschreibung der Entwicklungsumgebung, die Installationsanleitung und verwendeter Code zu finden.

2 Theoretische Grundlagen

Dieses Kapitel befasst sich nebst dem Kontext der Arbeit, mit den gemachten Literaturrecherchen, welche für die Erarbeitung der Lösungsansätze nötig sind. Weiter wird der Anwendungsbereich der Lösung behandelt.

2.1 Anwendungsbereich

Die FHNW möchte zu Ausbildungszwecken eine eigene Ethereum Blockchain betreiben. Die Blockchain soll die selbe Funktionalität wie die öffentliche Ethereum Blockchain vorweisen. Sie soll den Studenten die Möglichkeit bieten, in einer sicheren Umgebung Erfahrungen zu sammeln und Wissen zu gewinnen. Obwohl eine öffentliche Blockchain für jedermann frei zugänglich ist, sind fast alle Aktionen mit Kosten verbunden. Die Kosten sind ein fixer Bestandteil einer Blockchain. So fallen zum Beispiel bei jeder Transaktionen Gebühren an. Diese ermöglichen nicht nur deren Verarbeitung, sondern garantieren auch Schutz vor Attacken.

Im Gegensatz zu einer öffentlichen Blockchain, sind Transaktionsgebühren in einer Lernumgebung nicht praktikabel. Die Studenten sollen gratis mit der Blockchain agieren können, ohne dass der Betrieb oder die Sicherheit der Blockchain kompromittiert werden.

Die FHNW bietet die kostenlose Verarbeitung von Transaktionen zu Verfügung. Damit sichert sie den Betrieb der Blockchain. Die Implementation von gratis Transaktionen und einem Schutzmechanismus wird in diesem Bericht behandelt.

2.2 Ethereum Client

Für die Betreuung von einem Ethereum Node ist ein Client nötig. Dieser muss das Ethereum Protokoll[5] implementieren. Das Protokoll definiert die minimal Anforderungen an den Clienten. Das erlaubt, dass der Client in verschiedenen Sprachen, von verschiedenen Teams, realisiert werden kann. Nebst der verwendeten Programmiersprache, unterscheiden sich die Clienten bei implementierten Zusatzfunktionen, die im Protokoll nicht spezifiziert sind. Die populärsten Clients sind Go Ethereum (GETH)[6], Parity[7], Aleth[8] und Trinity[9]. Die Clients wurden auf die Zusatzfunktionalität untersucht, für eine definierte Gruppe von Accounts gratis Transaktionen zu ermöglichen.

2.2.1 Parity

Geschrieben in Rust[10], ist es der zweit populärste Client nach Geth[6]. Verfügbar ist Parity für Windows, macOS und Linux. Die Entwicklung ist noch nicht abgeschlossen und es wird regelmässig eine neue Version vorgestellt. Konfiguriert wird das Programm mittels Konfigurationsdateien. Interaktion zur Laufzeit ist über die Kommandozeile möglich.

2.2.1.1 Whitelist

Parity verfügt über eine Whitelist Funktionalität. Die Liste ist als Smart Contract geschrieben. Im Genesisblock[11] wird der Bytecode des Smart Contracts an der gewünschten Adresse hinterlegt. In der Liste können Accounts hinterlegt werden. Diese geniessen das Privileg, gratis Transaktionen tätigen zu dürfen. Dabei wird nur geprüft, ob der Sender einer Transaktion mit einem Gas Price von Null, sich in der Whitelist befindet. Ist er das, wird die Transaktion vom Node akzeptiert. Befindet sich der Account nicht in der Whitelist, wird die Transaktion vom Node abgelehnt. Das heisst, dass die eine abgelehnte Transaktion verworfen wird, bevor sie auf das Netzwerk der Blockchain gelangt. Die Whitelist wird initial von der FHNW mit Accounts befüllt. Die FHNW verfügt über einen Account, der berechtigt ist die Liste notfalls anzupassen. Idealerweise benutzt die FHNW diesen Account ausschliesslich zur Befüllung der Liste. Ein weiterer Account, der die Liste anpassen kann, wird vom entwickelten Schutzmechanismus kontrolliert. So kann bei einer Bedrohung, der bösertige Account von der Liste entfernt werden.

2.2.2 Geprüfte Alternativen

Die Clients Geth, Aleth und Trinity sind ebenfalls evaluiert worden. Bei diesen Clients ist keine Möglichkeit gefunden worden, bestimmte Accounts für gratis Transaktionen zu privilegieren. Daher sind sie zu diesem Zeitpunkt nicht für die FHNW geeignet.

2.3 Komponenten

//TODO Spellcheck

Die folgenden Abschnitte behandeln die gemachten Literaturrecherchen. Für jedes Thema sind die gewonnen Erkenntnisse aufgeführt. Dabei ist nebst einem grundsätzlichen Verständnis für die Materie immer der Schutz vor einer Denial of Service (DoS) Attacke im Fokus.

2.3.1 Ethereum Blockchain

Eine Blockchain ist eine kontinuierlich erweiterbare Liste von Datensätzen, „Blöcke“ genannt, die mittels kryptographischer Verfahren miteinander verkettet sind. Jeder Block enthält dabei typischerweise einen kryptographisch sicheren Hash (Streuwert) des vorhergehenden Blocks, einen Zeitstempel und Transaktionsdaten.[1]

Blockchains sind auf einem peer-to-peer (P2P) Netzwerk[12] aufgebaut. Ein Computer der Teil von diesem Netzwerk ist, wird Node genannt. Jeder Node hat eine identische Kopie der Historie aller Transaktionen. Es gibt keinen zentralen Server der angegriffen werden kann. Das erhöht die Sicherheit der Blockchain. Es muss davon ausgegangen werden, dass es Nodes gibt, die versuchen die Daten der Blockchain zu verfälschen. Dem wird mit der Verwendung von diversen Consensus Algorithmen[13] entgegengewirkt. Die Consensus Algorithmen stellen sicher, dass die Transaktionen auf der Blockchain valide und authentisch sind.

Im Gegensatz zur Bitcoin[14] kann bei Ethereum[15] auch Code in der Chain gespeichert werden, sogenannte Smart Contracts, siehe 2.3.2. Ethereum verfügt über eine eigene Kryptowährung, den Ether (ETH).

2.3.2 Smart Contracts

Der Begriff Smart Contract, wurde von Nick Szabo[16] in den frühen 1990 Jahren zum erten Mal verwendet. Es handelt sich um ein Stück Code, das auf der Blockchain liegt. Es können Vertragsbedingungen als Code geschrieben werden. Sobald die Bedingungen erfüllt sind, führt sich der Smart Contract selbst aus. Der Code kann von allen Teilnehmern der Blockchain inspiziert werden. Da er dezentral auf der Blockchain gespeichert ist, kann er auch nicht nachträglich manipuliert werden. Das schafft Sicherheit für die beteiligten Parteien.

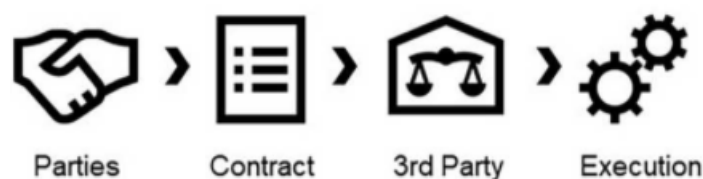


Abbildung 2.1: Ein traditioneller Vertrag[17]

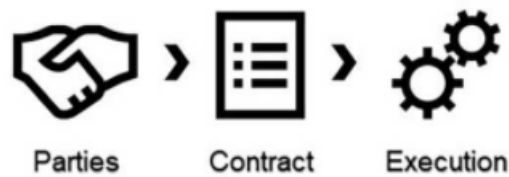


Abbildung 2.2: Ein Smart Contract[17]

Der grosse Vorteil von Smart Contracts ist, dass keine third parties benötigt werden, das ist auf den Bildern 2.1 und 2.2 dargestellt. Der Code kontrolliert die Transaktionen, welche Nachverfolgbar und irreversibel sind. Bei einem traditionellen Vertrag werden diese durch third parties kontrolliert und meistens auch ausgeführt.

Sobald ein Smart Contract auf Ethereum deployed ist, verfügt er über eine Adresse, siehe Abschnitt 2.3.5.1. Mit dieser, kann auf die Funktionen des Smart Contracts zugegriffen werden.

2.3.2.1 Decentralized application (DApp)

Eine DApp ist eine Applikation (App), deren backend Code dezentral auf einem peer-to-peer Netzwerk läuft, zum Beispiel die Ethereum Blockchain. Der frontend Code kann in einer beliebigen Sprache geschrieben werden, sofern Aufrufe an das Backend möglich sind. DApp's für die Ethereum Blockchain werden mit Smart Contracts realisiert. Das prominenteste Beispiel einer DApp ist CryptoKitties[18]. Die Benutzer können mit digitale Katzen handeln und züchten.

2.3.3 Transaktionen

Um mit der Blockchain zu interagieren, werden Transaktionen benötigt. Sie erlauben es Daten in der Blockchain zu erstellen oder anzupassen. Eine Transaktion verfügt über folgende Felder:

From Der Sender der Transaktion. Wird mit einer 20 Byte langen Adresse, siehe Abschnitt 2.3.5.1, dargestellt.

To Der Empfänger der Transaktion. Wird ebenfalls mit einer 20 Byte langen Adresse dargestellt. Falls es sich um ein Deployment von einem Smart Contract handelt, wird dieses Feld leer gelassen.

Value Mit diesem Feld wird angegeben, wieviel Wei[19] übertragen werden soll. Der Betrag wird von „From“ nach „To“ übertragen.

Data/Input Dieses Feld wird hauptsächlich für die Interaktion mit Smart Contracts, siehe Abschnitt 2.3.2, verwendet. Wenn ein Smart Contract deployed werden soll, wird in diesem Feld der dessen

Bytecode[20] übertragen. Bei Funktionsaufrufen auf einen Smart Contract wird die Funktionssignatur und die codierten Parameter mitgegeben. Bei reinen Kontoübertragungen wird das Feld leer gelassen.

Gas Price Gibt an, welcher Preis pro Einheit Gas man gewillt ist zu zahlen. Mehr dazu im Abschnitt 2.3.4

Gas Limit Definiert die maximale Anzahl Gas Einheiten, die für diese Transaktion verwendet werden können, siehe Abschnitt 2.3.4 [21]

Damit eine Transaktion in die Blockchain aufgenommen werden kann, muss sie signiert[22] sein. Dies kann beim Benutzer offline gemacht werden. Die signierte Transaktion wird dann an die Blockchain übermittelt.

Die Übermittlung der Transaktionen wird mittels Remote procedure call(RPC)[23] gemacht.

2.3.4 Gas

Mit Gas[3] ist in der Ethereum Blockchain eine spezielle Währung gemeint. Mit ihr werden Transaktionskosten gezahlt. Jede Aktion in der Blockchain kostet eine bestimmte Menge an Gas (Gas Cost). Somit ist die benötigte Menge an Gas proportional zur benötigten Rechenleistung. So wird sichergestellt, dass die anfallenden Kosten einer Interaktion gerecht verrechnet werden. Die anfallenden Gas Kosten werden in Ether gezahlt. Für die Berechnung der Transaktionskosten wird der Preis pro Einheit Gas (Gas Price) verwendet. Dieser kann vom Sender selbst bestimmt werden. Ein zu tief gewählter Gas Price hat zur Folge, dass die Transaktion nicht in die Blockchain aufgenommen wird, da es sich für einen Miner, siehe Abschnitt ??, nicht lohnt, diese zu verarbeiten. Ein hoher Gas Price stellt zwar sicher, dass die Transaktion schnell verarbeitet wird, kann aber hohe Gebühren generieren.

$$TX = gasCost * gasPrice$$

Die Transaktionskosten werden nicht direkt in Ether berechnet, da dieser starken Kursschwankungen unterworfen sein kann. Die Kosten für Rechenleistung, also Elektrizität, sind hingegen stabiler Natur. Daher sind Gas und Ether separiert.

Ein weiterer Parameter ist Gas Limit. Mit diesem Parameter wird bestimmt, was die maximale Gas Cost ist, die man für eine Transaktion bereitstellen möchte. Es wird aber nur so viel verrechnet, wie auch wirklich benötigt wird, der Rest wird einem wieder gutgeschrieben. Falls die Transaktionskosten höher als das gesetzte Gas Limit ausfallen, wird die Ausführung der Transaktion abgebrochen. Alle gemachten Änderungen auf der Chain werden rückgängig gemacht. Die Transaktion wird als „fehlgeschlagene Transaktion“ in die Blockchain aufgenommen. Das Gas wird nicht zurückerstattet, da die Miner bereits Rechenleistung erbracht haben.

2.3.5 Account

Um mit Ethereum interagieren zu können, wird ein Account benötigt. Es gibt zwei Arten von Accounts, solche von Benutzern und jene von Smart Contracts. Ein Account ermöglicht es einem Benutzer oder Smart Contract, Transaktionen zu empfangen und zu senden.

2.3.5.1 Benutzer Account

Der Account eines Benutzers besteht aus Adresse, öffentlichen und geheimen Schlüssel. Diese Art von Accounts haben keine Assoziation mit Code. Sie werden von Benutzer verwendet um mit der Blockchain zu interagieren.

Geheimer Schlüssel Der geheime Schlüssel ist ein 256 Bit lange zufällig generierte Zahl. Er definiert einen Account und wird verwendet um Transaktionen zu signieren. Daher ist es von grösster Wichtigkeit, dass ein geheimer Schlüssel sicher gelagert wird. Wenn er verloren geht, gibt es keine Möglichkeit mehr auf diesen Account zuzugreifen.

Öffentlicher Schlüssel Der öffentliche Schlüssel wird aus dem geheimen Schlüssel abgeleitet. Für die Generierung wird Keccak[24] verwendet, ein „Elliptical Curve Digital Signature Algorithm“[25]. Der öffentliche Schlüssel wird verwendet um die Signatur einer Transaktion zu verifizieren.

Adresse Die Adresse wird aus dem öffentlichen Schlüssel abgeleitet. Es wird SHA3[26] verwendet um einen 32 Byte langen String zu bilden. Von diesem bilden die letzten 20 Bytes, also 40 Zeichen, die Adresse von einem Account. Die Adresse wird bei Transaktionen oder Interaktionen mit einem Smart Contract verwendet.

2.3.5.2 Contract Accounts

Contract Accounts sind durch ihren Code definiert. Sie können keine Transaktionen initiieren, sondern reagieren nur auf zuvor eingegangene. Das wird auf der Abbildung 2.3 dargestellt. Ein Benutzer Accounts wird als „Externally owned account“ bezeichnet.

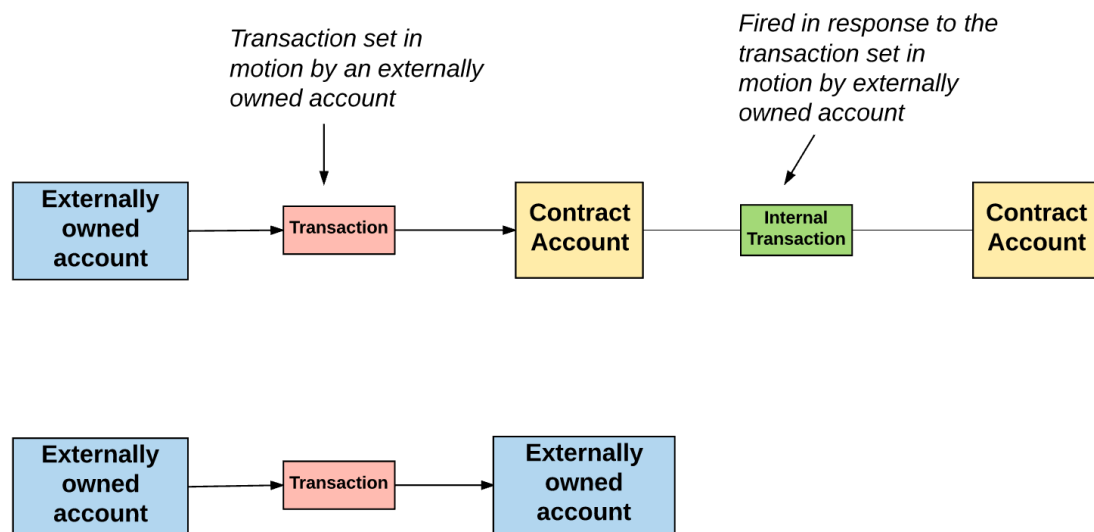


Abbildung 2.3: TX zwischen Accounts

Im Gegensatz zu einem Benutzer Account hat ein Contract Account keine Verwendung für einen geheimen oder öffentlichen Schlüssel. Es wird nur eine Adresse benötigt. Analog zu einem Benutzer Account, wird diese benötigt, um Transaktionen an diesen Smart Contract zu senden. Sobald ein Smart Contract deployed wird, wird eine Adresse generiert. Verwendet wird die Adresse und Anzahl getätigte Transaktionen (nonce[27]) des Benutzer Accounts, der das Deployment vornimmt.[28]

2.3.6 Blockchain Wallet

Eine Blockchain Wallet, kurz Wallet, ist ein digitales Portmonaie. Der Benutzer hinterlegt in der Wallet seinen geheimen Schlüssel, siehe 2.3.5.1. Dadurch erhält er eine grafische Oberfläche für die Verwaltung seines Accounts. Nebst dem aktuellen Kontostand, wird meistens noch die Transaktionshistorie angezeigt. In der Wallet können mehrere Accounts verwaltet werden. So muss sich der Benutzer nicht selbst um die sichere Aufbewahrung der geheimen Schlüssel kümmern. Bei den meisten Wallets ist es möglich verschiedene Währungen zu verwalten. Es existieren zwei unterschiedliche Arten von Wallets, Hot und Cold Wallets:

Hot Wallet Ein Stück Software, welches die geheimen Schlüssel verwaltet.

Es existieren drei unterschiedliche Typen, Desktop, Web und Mobile Wallets. [29], [30], [31]

Cold Wallet Der geheime Schlüssel wird in einem Stück Hardware gespeichert. Dadurch können die geheimen Schlüssel offline gelagert werden. Das erhöht die Sicherheit der Wallet, da Angriffe aus dem Internet ausgeschlossen werden können. [29], [30], [31]

2.3.6.1 Smart Wallet

Smart Wallets basieren auf Smart Contracts. Der Benutzer ist der Besitzer der Smart Contracts und somit der Wallet. Die Verwendung von Smart Contract bei der Implementierung der Wallet ermöglicht mehr Benutzerfreundlichkeit ohne die Sicherheit zu kompromittieren. [32], [33], [34] //TODO ..

2.3.7 Denial of Service (DoS) Attacken

Bei einer DoS Attacke versucht der Angreifer einen Service mit Anfragen zu überlasten. Die Überlastung schränkt die Verfügbarkeit stark ein oder macht den Service sogar gänzlich unverfügbar für legitime Anfragen.

Zurzeit sind Blockchains noch relativ langsam bei der Verarbeitung von Transaktionen. Ethereum kann ungefähr 15 Transaktionen pro Sekunde abarbeiten.[35] Dadurch ist ein möglicher Angriffsvektor, die Blockchain mit Transaktionen zu fluten. Das würde dazu führen, dass Benutzer sehr lange auf die Ausführung ihrer Transaktionen warten müssen. Blockchains schützen sich vor diesem Angriff mit einer Transaktionsgebühr. Diese werden durch Angebot und Nachfrage bestimmt. Das heisst, wenn es viele Transaktionen gibt, steigt der Bedarf an deren Verarbeitung und es kann davon ausgegangen werden, dass auch die Transaktionsgebühren steigen. Das bedeutet, dass bei einer DoS Attacke die Transaktionsgebühren tendenziell steigen. Um sicherzustellen, dass seine Transaktionen weiterhin zuverlässig in die Blockchain aufgenommen werden, muss der Angreifer seinen Gas Price kontinuierlich erhöhen. Ein DoS Angriff auf eine Blockchain wird dadurch zu einem sehr kostspieligen Unterfangen. Die hohen Kosten schrecken die meisten Angreifer ab und sind somit ein sehr effizienter Schutzmechanismus.[36]

2.3.7.1 DoS Attacke identifizieren

Auf der Blockchain der FHNW existiert eine privilegierte Benutzergruppe. Diese dürfen gratis Transaktionen ausführen. Diese Gruppe von Benutzer ist eine potentielle Bedrohung. Ohne Transaktionskosten hat die Blockchain keinen Schutzmechanismus gegen eine DoS Attacke. Aus diesem Grund muss das Verhalten der privilegierten Accounts überwacht werden. Falls einer dieser Accounts eine DoS Attacke einleitet, muss das frühst möglich erkannt und unterbunden werden können.

//TODO Möglich Vorgehensweisen nebst TX limite pro ACC

Transaktionslimite pro Account Jeder Account darf nur eine gewisse Anzahl von gratis Transaktionen pro Zeiteinheit tätigen. Beim Überschreiten des Limits, wird er von der Whitelist gelöscht und muss die Transaktionsgebühr zahlen. Der Account kann nach einer bestimmten Zeit automatisch wieder in die Whitelist eingefügt werden.

2.4 Lösungsansätze

//TODO Spellcheck über ganze Seite

//TODO Erläuterungen zu Flow Charts

In diesem Kapitel werden die erarbeiteten Lösungsansätze vorgestellt. Die Stärken und Schwächen von jedem Lösungsansatz (LA) werden analysiert und dokumentiert. Mit der vorgenommenen Analyse wird ein Favorit bestimmt. Dieser wird weiterverfolgt und implementiert.

2.4.1 Lösungsansatz 1: Smart Wallet

Es wird selbst eine Smart Wallet entwickelt. Diese benötigt die volle Funktionalität einer herkömmlichen Wallet. Zusätzlich ist ein Schutzmechanismus gegen DoS Attacken implementiert. Wie in Abbildung ?? ersichtlich, wird für jeden Benutzer eine Smart Wallet deployed. Dies wird von der FHNW übernommen. So fallen für die Benutzer keine Transaktionsgebühren an. Wie unter 2.2.1.1 beschrieben, wird für die Betreuung der Blockchain der Client Parity mit einer Withelist verwendet.

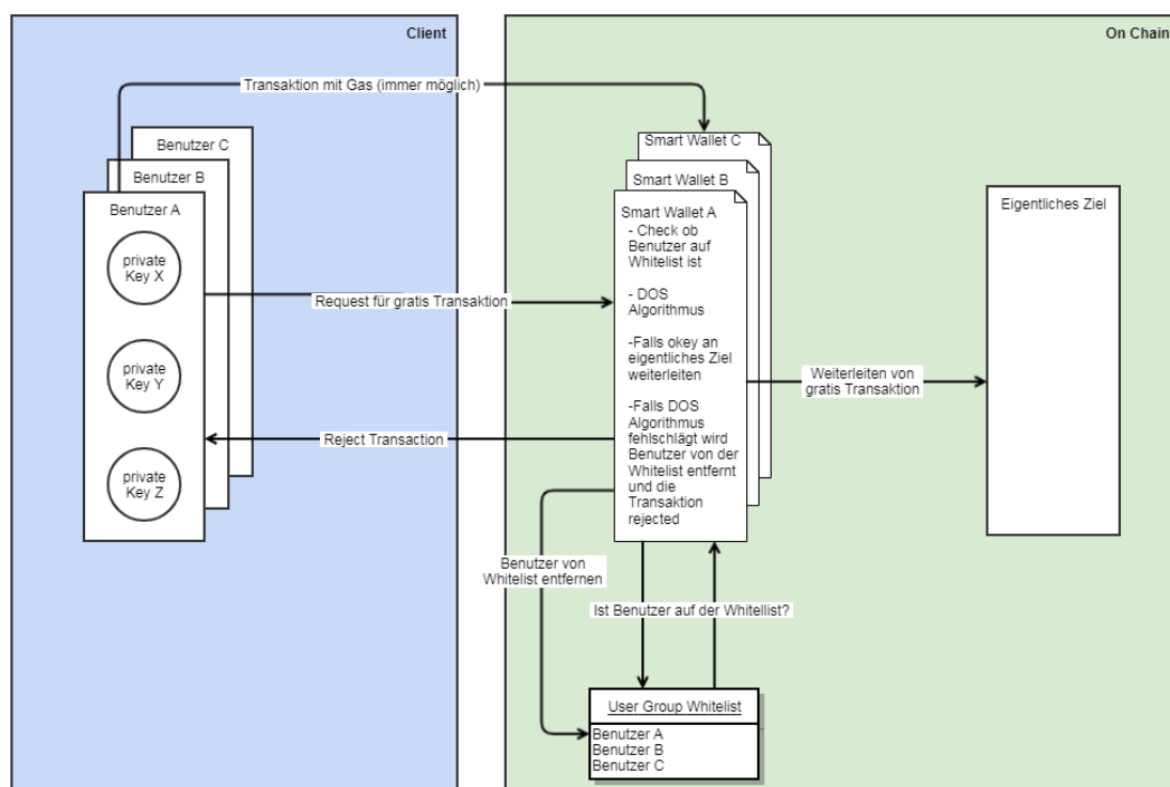


Abbildung 2.4: Lösungsansatz1

Es muss sichergestellt werden, dass ein Benutzer auf seine Smart Wallet zugreifen kann, unabhängig davon ob er gratis Transaktionen tätigen darf oder nicht. Dies ist in der Abbildung 2.4 dargestellt.

Wie in 2.2.1.1 beschrieben, prüft Parity bei einer gratis Transaktion nur, ob sich der Account in der Whitelist befindet. Das bedeutet, dass mit einem whitelisted Account auch gratis Transaktionen getätigt werden können, die nicht an die Smart Wallet gerichtet sind. Somit kann der Benutzer den DoS Schutzmechanismus umgehen. Deswegen muss ein Weg gefunden werden, der den Benutzer zwingt Transaktionen über die Smart Wallet abzuwickeln. Eine Möglichkeit ist Parity selbst zu erweitern. Anstelle einer Liste mit Accounts, muss eine Liste von Verbindungen geführt werden. So kann definiert werden, dass nur eine Transaktion auf die Smart Wallet gratis ist.

2.4.1.1 Pro

Dieser Ansatz besticht durch die Tatsache, dass alles auf der Blockchain läuft. Somit werden grundlegende Prinzipien, wie Dezentralität und Integrität, einer Blockchain bewahrt.

2.4.1.2 Contra

Die Machbarkeit des Ansatzes ist unklar. Um diesen Ansatz umzusetzen, muss der Blockchain Client, Parity, erweitert werden. Es ist unklar, wie weitreichend die Anpassungen an Parity sind. Zusätzlich wird eine zusätzliche Programmiersprache, Rust[10], benötigt. Ein weiterer Nachteil ist, dass bei einer Änderung am DoS Schutzalgorithmus eine neue Smart Wallet für jeden Account deployed werden muss. Das bedingt, dass die Whitelist ebenfalls mit den neuen Accounts aktualisiert wird.

2.4.1.3 Prozessworkflow

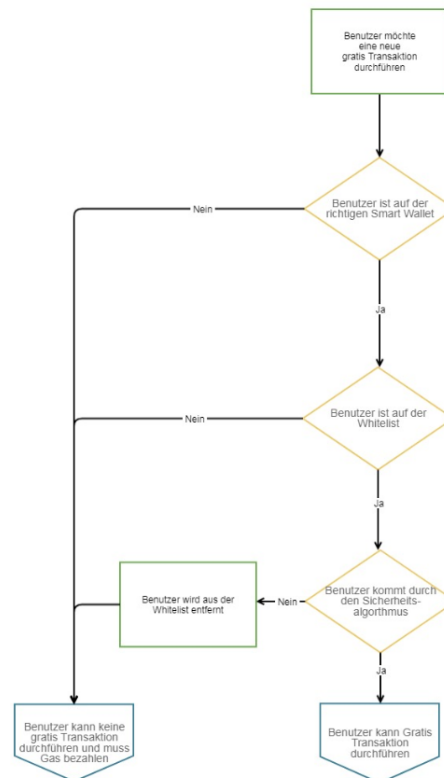


Abbildung 2.5: Flowchart Lösungsansatz 1

In der Abbildung 2.5 ist der Prozessablauf für eine gratis Transaktion dargestellt.

//TODO weitere Erläuterung?

2.4.2 Lösungsansatz 2: Smart Wallet mit externen Programm nach Whitelist-Check

Bei diesem Ansatz wird auf die Entwicklung einer Smart Wallet verzichtet. Stattdessen wird der Schutzmechanismus gegen DoS Attacken mit einem externen Programm implementiert, dargestellt in Abbildung 2.6.

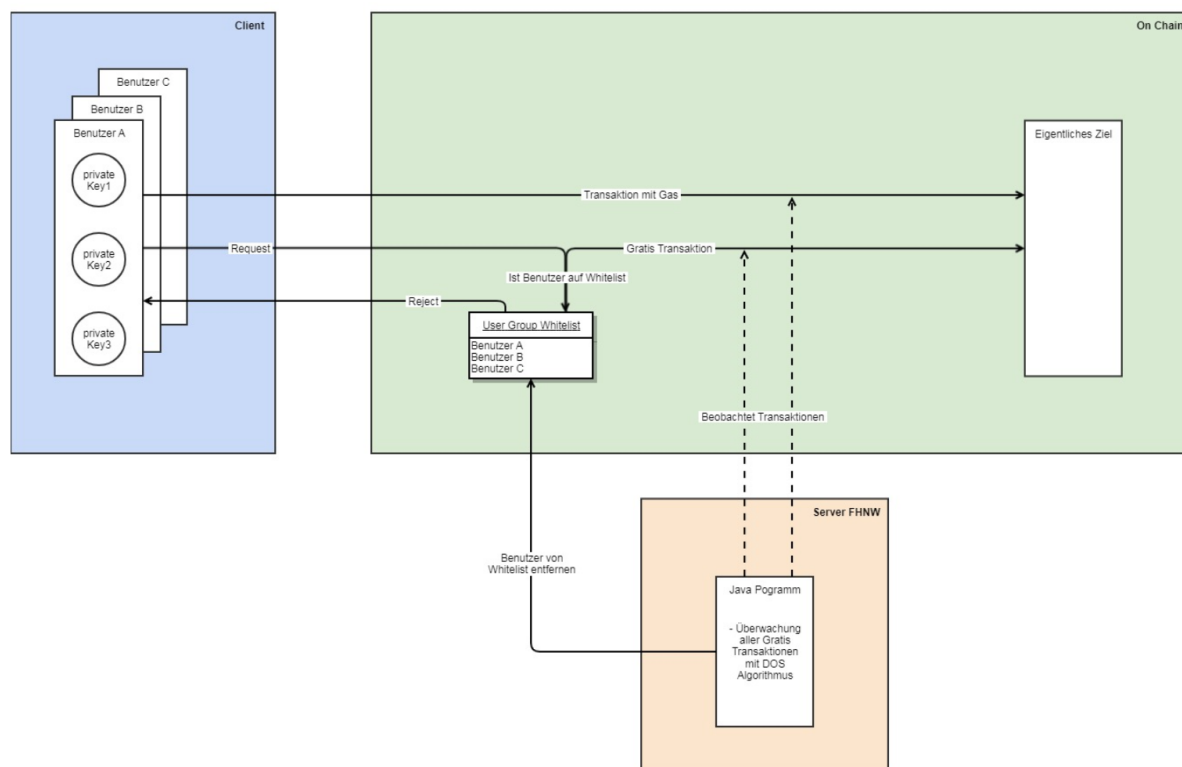


Abbildung 2.6: Lösungsansatz 2

Es wird auch für diesen Ansatz die Whitelist von Parity verwendet, siehe 2.2.1.1. Im externen Programm werden alle gratis Transaktionen analysiert, die das Blockchain Netzwerk erreichen. Das Programm verfügt über einen eigenen Benutzer Account, siehe 2.3.5. Dieser ist berechtigt, die Whitelist zu manipulieren. Dadurch kann bei einer identifizierten Attacke, der angreifende Account automatisch von der Whitelist gelöscht werden.

Transaktionen für die ein Transaktionsgebühren gezahlt werden sind immer möglich. Diese werden vom externen Programm auch nicht überwacht. Die anfallenden Gebühren sind Schutz genug.

2.4.2.1 Pro

Dieser Ansatz ist sicher umsetzbar in der zur Verfügung stehenden Zeit. Falls eine Anpassung des DoS Schutzalgorithmus nötig ist, muss nur das externe Programm neu deployed werden. Eine aktualisierung der Whitelist ist nicht nötig.

2.4.2.2 Contra

Es wird das Hauptprinzip, Dezentralität, einer Blockchain verletzt. Das externe Programm ist eine zentrale Autorität, die von der FHNW kontrolliert wird. Durch das externen Programm kommt eine weitere Komponente dazu. Diese muss ebenfalls administriert werden.

2.4.2.3 Prozessworkflow

//TODO Flowchart falsch.. gibt keine Smart wallet, Transaktion kommt immer durch Java wenn auf white list, da java nur passiv mithört

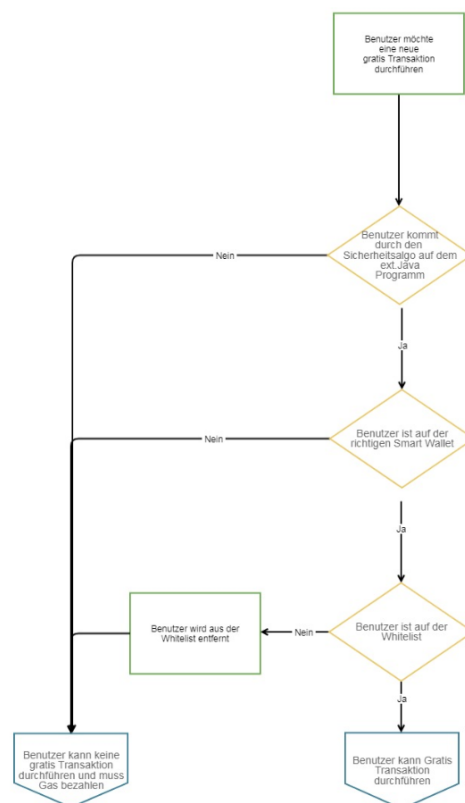


Abbildung 2.7: Flowchart Lösungsansatz 2

Auf dem Flowchart 2.7 dargestellt ist, kann ein Benutzer mit einem whitelisted Account direkt gratis Transaktionen ausführen.

2.4.3 Lösungsansatz 3: Smart Wallet mit externen Programm vor Whitelist-Check

Wie in Abbildung 2.8 illustriert, ist der Blockchain ein externes Programm vorgelagert. Das Programm verwaltet eine eigene Whitelist mit Accounts. Diese sind für gratis Transaktionen berechtigt. Weiter beinhaltet es den DoS Schutzalgorithmus. Dieser prüft ob der Account auf der Whitelist ist und ob die Transaktion die Schutzrichtlinien verletzt. Falls ein Account die Sicherheitsrichtlinien verletzt, wird dieser vom Algorithmus aus der eigenen Whitelist gelöscht.

Sofern keine Richtlinien verletzt werden, wird die Transaktion ins Data-Feld, siehe 2.3.3, einer neuen Transaktion gepackt. Das ist nötig, um die Transaktionsinformationen (wie z.B. Sender Identität) zu präservieren. Die neue erstellte Transaktion wird vom Programm an die Smart Wallet gesendet.

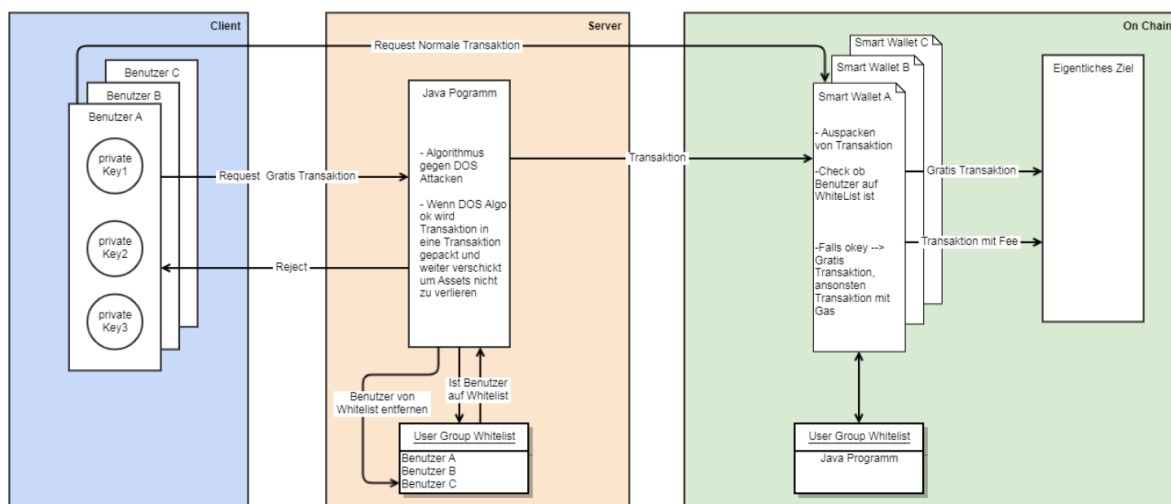


Abbildung 2.8: Lösungsansatz 3

Weiter wird eine Smart Wallet entwickelt. Diese ist nötig, um die verschachtelten Transaktionen des Programms zu verarbeiten. Aus dem Data-Feld wird die eigentliche Transaktion extrahiert und abgesetzt.

Jeder Benutzer besitzt eine eigene Smart Wallet um die Sender Identität für jeden Benutzer einmalig zu halten. Auf der im Abschnitt 2.2.1.1 beschriebenen Whitelist ist nur der Account des externen Programms aufgelistet. So ist sichergestellt, dass nur Transaktionen die vom Programm weitergeleitet werden, kostenfrei durchgeführt werden können. Der Benutzer kann immer mit kostenpflichtigen Transaktionen auf die Smart Wallet zugreifen. Dies ist insbesondere wichtig, falls das Programm nicht aufrufbar ist, wenn z.B. der Server ausfällt.

2.4.3.1 Pro

Dieser Ansatz ist in der gegebenen Zeit umsetzbar. Falls eine Anpassung des DoS Schutzalgorithmus nötig ist, muss nur das externe Programm neu deployed werden. Eine aktualisierung der Whitelist ist nicht nötig.

2.4.3.2 Contra

Es wird das Hauptprinzip, Dezentralität, einer Blockchain verletzt. Das externe Programm ist eine zentrale Autorität, die von der FHNW kontrolliert wird. Durch das externen Programm kommt eine weitere Komponente dazu. Diese muss ebenfalls administriert werden. Dieser Ansatz bietet keine Vorteile im Vergleich zum LA 2, ist aber mit der Verschachtelung von Transaktionen komplexer.

2.4.3.3 Prozessworkflow

//Todo flowchart falsch, zuerst Java dann richtige smart wallet

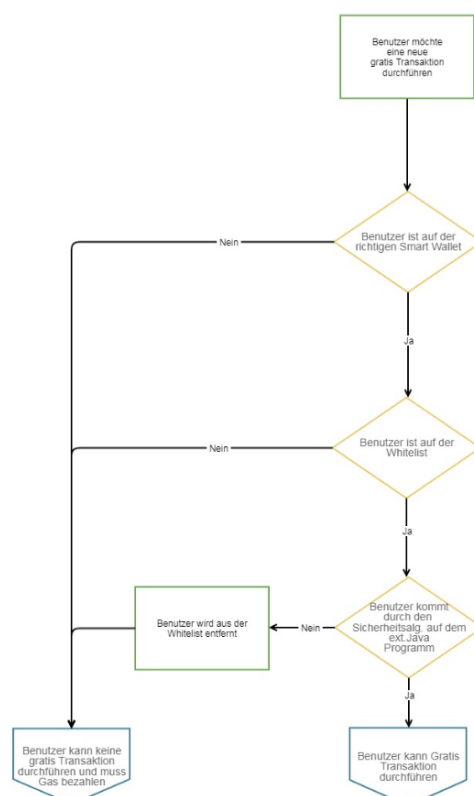


Abbildung 2.9: Flowchart Lösungsansatz 3

Die Abbildung 2.9 zeigt, dass alle gratis Transaktionen in erster Instanz von einem Programm geprüft werden. Falls keine Richtlinien verletzt werden, wird die Transaktion im Data-Feld einer neu generierten Transaktion an die Smart Wallet übermittelt.

2.4.4 Lösungsansatz 4: Super Smart Wallet

Es wird eine zentrale Smart Wallet entwickelt. Im Gegensatz zu LA 1, 2.4.1, wird nicht für jeden Benutzer eine Smart Wallet deployed, sondern nur eine einzige. Diese kann von allen Benutzern der Blockchain genutzt werden. Bei diesem Ansatz wird mit der in Absatz 2.2.1.1 beschriebenen Whitelist gearbeitet.

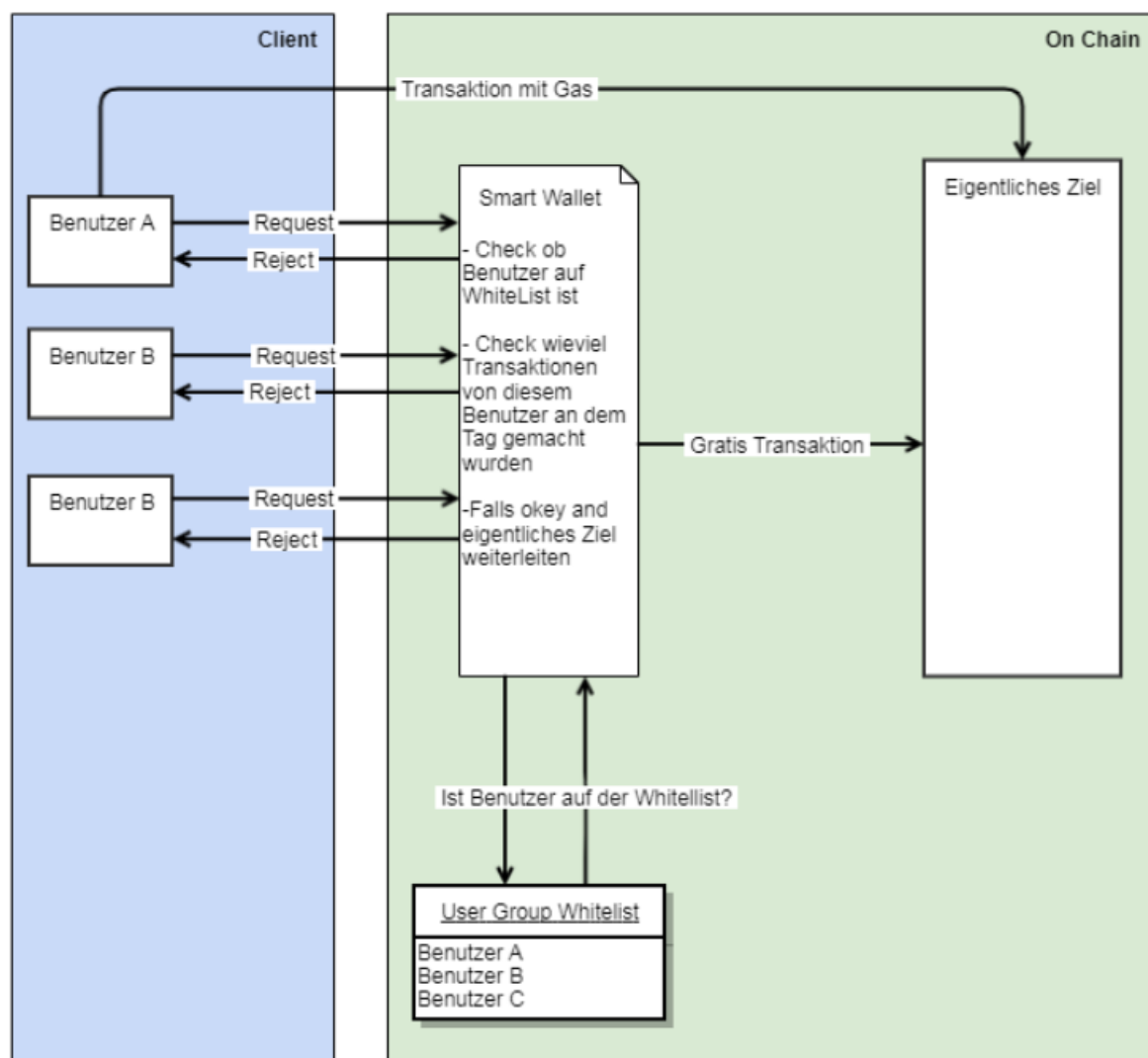


Abbildung 2.10: Lösungsansatz 4

Die Smart Wallet verwaltet die Whitelist und den Schutzmechanismus gegen DoS Attacken. Das ist auf Abbildung 2.10 ersichtlich. Wird eine DoS Attacke identifiziert, wird der entsprechende Account aus der Whitelist gelöscht.

2.4.4.1 Pro

Es existiert nur eine einzige Smart Wallet. Das Deployment ist somit weniger aufwändig. Falls eine Änderung am Code gemacht nötig ist, muss nur eine Smart Wallet neu deployed werden.

2.4.4.2 Contra

Bei diesem Ansatz ist die Machbarkeit unklar. Parity muss umgeschrieben werden, da nicht die Senderidentität der Smart Wallet genutzt werden muss, sondern die des Benutzeraccounts. Ebenfalls muss die Whitelist-Funktionalität von Parity angepasst werden, analog zu LA 1.

2.5 Evaluation der Lösungsansätze

Die erarbeiteten Lösungsansätze werden gegeneinander verglichen. Um zu bestimmen, welcher Ansatz weiter verfolgt wird, wurden folgende Kriterien definiert:

Machbarkeit (MK) Bewertet die Machbarkeit des Ansatzes. Das berücksichtigt den gegebenen Zeitrahmen und die Komplexität des Ansatzes.

Da dieses Projekt im gegebenen Zeitrahmen abgeschlossen werden muss, ist es das wichtigste Kriterium. Daher wird es auch mit der höchsten Gewichtung versehen.

Gewichtung 3

Blockchainprinzipien (BCP) Gibt an ob die Prinzipien einer Blockchain berücksichtigt werden. Wie Dezentralität, Trust und Security

Die Einhaltung der Prinzipien ist wichtig, aber für die FHNW nicht zwingend. Daher eine mittlere Gewichtung.

Gewichtung 2

Betrieb (BT) Bewertet den administrativen Aufwand im Betrieb und die Möglichkeit zur Automatisierung. Das umfasst Deployment Smart Contracts, Anpassungen der Whitelist und Betreuung von zusätzlichen Servern.

Wird mit einer mittleren Gewichtung versehen. Ein zu hoher administrativer Aufwand ist nicht praktikabel.

Gewichtung 2

Jeder LA wird auf diese drei Kriterien untersucht. Pro Kriterium können zwischen 3 und 1 Punkt erreicht werden, wobei 3 das Maximum ist. Die erreichten Punkte werden mit der entsprechenden Gewichtung multipliziert. Für die Evaluation, werden alle Punkte zusammengezählt. Der Ansatz mit den meisten Punkten wird weiterverfolgt.

Tabelle 2.1: Evaluation Lösungsansätze

	MK	BCP	BT	Total
Gewichtung	3	2	2	
LA 1	1	3	2	13
LA 2	3	2	2	17
LA 3	2	1	3	12
LA 4	1	2	2	11

2.5.1 Lösungsansatz 1: Smart Wallet

Wir haben diesen Ansatz als sehr komplex eingestuft. Für die Anpassung von Parity muss eine zusätzliche Programmiersprache verwendet werden. Es ist nicht klar, wie weitreichend die nötigen Anpassungen sind. Zusätzlich muss eine Smart Wallet entwickelt werden.

Dieser Ansatz ist komplett dezentral und in die Blockchain integriert. Daher maximale Punktzahl bei Blockchain Prinzipien.

Falls ein Anpassung am DoS Algorithmus nötig ist, muss jede Smart Wallet neu deployed werden. Das bedingt, dass die Whitelist ebenfalls aktualisiert wird. Die Adressen aller bestehenden Smart Wallets müssen ersetzt werden. Alle Studierenden müssen informiert werden, dass sie für ihre Smart Wallet eine neue Adresse verwenden müssen. Die Automatisierung dieser Prozesse wird als komplex aber machbar eingeschätzt. Daher sind bei Betrieb 2 Punkte gesetzt.

2.5.2 Lösungsansatz 2: Smart Wallet mit externen Programm nach Whitelist-Check

Die Entwicklung eines externen Programmes, welches getätigte Transaktionen der Blockchain prüft, ist in der gegebenen Zeit sicher realisierbar. Daher erhält der LA für Machbarkeit die volle Punktzahl.

Mit der Verwendung von einem externen Programm, wird eine zentrale Autorität verwendet. Diese ist nicht dezentral und wird von der FHNW administriert. Da das Programm die Transaktionshistorie der

Blockchain überwacht und nur bei einer DoS Attacke aktiv ist, wird 2 Punkte für Blockchainprinzipien gegeben.

Falls eine Anpassung am DoS Algorithmus nötig ist, muss das externe Programm neu deployed werden. Es benötigt keine Anpassungen an der Blockchain selbst. Für die Verwaltung der Whitelist, braucht das Programm eine Funktion, um Accounts zur Whitelist hinzuzufügen. Diese Funktion kann einfach erweitert werden, um eine Liste von Accounts zur Whitelist hinzuzufügen. Dadurch ist das hinzufügen von neuen Accounts für eine Klasse einfach automatisierbar. Für die Betreuung des externen Programms wird ein zusätzlicher Server benötigt. Das bedeutet einen Mehraufwand für die FHNW. Da der LA einfach zu Automatisieren ist, sind für Betrieb 2 Punkte gesetzt worden.

2.5.3 Lösungsansatz 3: Smart Wallet mit externem Programm vor Whitelist-Check

Bei diesem LA muss eine Smart Wallet und ein externes Programm entwickelt werden. Transaktionen werden im externen Programm verpackt und müssen von der Smart Wallet wieder entpackt werden. Somit liegt die Machbarkeit zwischen dem von LA 1 und LA 2. Daher werden 2 Punkte für Machbarkeit vergeben.

Mit der Verwendung von einem externen Programm, wird eine zentrale Autorität verwendet. Diese ist nicht dezentral und wird von der FHNW administriert. Im Gegensatz zu LA 2, hat dieses Programm eine sehr viel zentralere Rolle. Das Programm interagiert nicht nur bei einer DoS Attacke mit der Blockchain, sondern ständig. Jede Transaktion wird an das Programm übermittelt und dort verarbeitet. Da die zentrale Autorität im Vergleich zu LA 2 viel aktiver ist, ist für Blockchainprinzipien 1 Punkt vergeben worden.

Für die Betreuung des externen Programms ist ein zusätzlicher Server nötig. Änderungen an der Smart Wallet bedingen ein erneutes Deployment. In der Whitelist der Blockchain ist nur der Account des externen Programmes hinterlegt. Das Programm führt eine eigenen List von Accounts, die für gratis Transaktionen berechtigt sind. Das externe Programm hat eine sehr zentrale Rolle, da es die Whitelist und den DoS Schutzalgorithmus enthält. Die Automatisierung wird daher als einfach eingestuft, da das externe Programm mit Java geschrieben wird und somit sehr viel zugänglicher ist. Daher sind bei Betrieb 3 Punkte vergeben worden.

2.5.4 Lösungsansatz 4: Super Smart Wallet

//TODO or not TODO ? XD

2.5.5 Resultat Evaluation

Durch die hohe Gewichtung von Machbarkeit, erzielt LA 2 die meisten Punkte. Im weiteren Verlauf des Projektes wird daher LA 2 umgesetzt. //TODO ausfleischen?

3 Praktischer Teil

Dieses Kapitel beschreibt, wie die gewonnen theoretischen Grundlagen umgesetzt sind. Die realisierte Lösung wird kritisch hinterfragt und anderen Lösungsansätzen gegenübergestellt.

3.1 Parity

In diesem Abschnitt ist beschrieben, wie die Blockchain konfiguriert ist. Als Client wird die stable Version[37] von Parity verwendet.

3.1.1 Konfiguration der Blockchain

Parity wird mit der Konsole gestartet. Der Benutzer hat hier die Möglichkeit, gewisse Parameter an Parity zu übergeben. Eine einfache Konfiguration ist somit möglich. Für kompliziertere Konfigurationen, wird die Verwendung von einer Konfigurationsdatei empfohlen.

3.1.1.1 Config.toml

Für die Konfiguration der Blockchain wird eine Konfigurationsdatei verwendet. Diese hat das Dateiformat .toml[38].

```
1 [parity]
2 chain = "/home/parity/.local/share/io.parity.ethereum/genesis/
   instant_seal.json"
3 base_path = "/home/parity/"
4
5 [rpc]
6 cors = ["all"]
7 apis = ["net", "private", "parity", "personal", "web3", "eth"]
8
9 [mining]
10 min_gas_price = 10000000000
11 refuse_service_transactions = false
12 tx_queue_no_unfamiliar_locals = true
13 reseal_on_txs = "all"
```

```
14 reseal_min_period = 0
15 reseal_max_period = 6000
16
17 [misc]
18 unsafe_expose = true
```

Der oben aufgeführte Codeblock ist in Sektionen gegliedert. Diese sind durch einen Namen in eckigen Klammern definiert. Innerhalb einer Sektion existieren bestimmte Schlüssel mit einem Wert. Jede Sektion ist in den folgenden Abschnitten erklärt.

Parity In dieser Sektion sind die grundlegenden Eigenschaften der Blockchain definiert. Dazu gehören Genesisblock und der Speicherort.

Zeile 2 Hier wird der zu verwendende Genesisblock definiert. Es wird der Pfad zu der entsprechenden JSON Datei[39] angegeben.

Zeile 3 Mit „base_path“ wird angegeben, wo die Blockchain abgespeichert werden soll. Hier wird das gewünschte Verzeichnis angegeben.

RPC Hier wird definiert, wie und von der Blockchain erreichbar ist.

Zeile 6 „cors“ steht für Cross-Origin Requests. Dieser Parameter wird benötigt, um die Interaktion von Remix[40] oder Metamask[41] mit der Blockchain zu ermöglichen.

Zeile 7 Hier sind die API's definiert, welche über HTTP zur Verfügung gestellt werden.

Mining Diese Sektion regelt das Verhalten beim Mining von Blocks.

Zeile 10 Der minimale Gas-Preis der gezahlt werden muss, damit eine Transaktion in einen Block aufgenommen wird. Der Preis ist in WEI angegeben. Um sicherstellen, dass nur die definierte Benutzergruppe gratis Transaktionen tätigen kann, muss dieser Wert grösser als Null sein.

Zeile 11 Service Transaktionen haben einen Gas-Preis von Null. Wird hier „true“ gesetzt, können keine gratis Transaktionen getätigt werden, unabhängig davon, ob eine Whitelist vorhanden ist oder nicht.

Zeile 12 Dieser Parameter wird benötigt, dass Transaktionen die mittels RPC an Parity übermittelt werden, nicht als lokal betrachtet werden. Das ist sehr wichtig, da lokale Transaktionen standardmässig auch über einen Gas-Preis von Null verfügen dürfen. So wird sichergestellt, dass nur die definierte Benutzergruppe gratis Transaktionen tätigen darf.

Zeile 13 Durch die Einstellung „tx_queue_no_unfamiliar_locals = true“ werden alle eingehenden Transaktionen behandelt, als ob fremd, also nicht lokal, behandelt. Standardmässig, werden aber nur lokale Transaktionen verarbeitet. Daher muss hier explizit definiert werden, dass alle Transaktionen verarbeitet werden.

[illegible]

[illegible]

3.1.1.3 Docker

3.1.2 Whitelist

3.1.2.1 SimpleRegistry

3.1.2.2 SimpleCertifier

3.2 Schutz vor DoS Attacken

4 Fazit

4.0.0.1 Dokumentation

Parity wird stetig weiterentwickelt. Die letzte Minorversion[42] ist im April 2019 veröffentlicht worden. Obwohl es sich um eine Minorversion handelt, hat es Änderungen in der Code-Syntax. Daher verhält sich das Update eher wie eine neue Majorversion[42]. Das hat zur Folge, dass praktisch alle gefundenen Tutorials nicht mehr gültig sind. # Quellenverzeichnis

[1] „Blockchain - Wikipedia“, 2019. [Online]. Verfügbar unter: <https://en.wikipedia.org/wiki/Blockchain>.

[2] „University of Applied Sciences and Arts Northwestern Switzerland“, 2019. [Online]. Verfügbar unter: <https://www.fhnw.ch/>.

[3] M. Inc., „What is Gas | MyEtherWallet Knowledge Base“, 2018. [Online]. Verfügbar unter: <https://kb.myetherwallet.com/en/transactions/what-is-gas/>.

[4] „Denial-of-service attack - Wikipedia“, 2019. [Online]. Verfügbar unter: https://en.wikipedia.org/wiki/Denial-of-service_attack.

[5] „ethereum/yellowpaper: The Yellow Paper: Ethereum’s formal specification“, 2019. [Online]. Verfügbar unter: <https://github.com/ethereum/yellowpaper>.

[6] go-ethereum, „Go Ethereum“, 2019. [Online]. Verfügbar unter: <https://geth.ethereum.org/>.

[7] P. Technologies, „Blockchain Infrastructure for the Decentralised Web | Parity Technologies“, 2019. [Online]. Verfügbar unter: <https://www.parity.io>.

[8] „<https://github.com/ethereum/aleth>“, 2019. [Online]. Verfügbar unter: <https://github.com/ethereum/aleth>.

[9] „ethereum/trinity: The Trinity client for the Ethereum network“, 2019. [Online]. Verfügbar unter: <https://github.com/ethereum/trinity>.

[10] „Rust Programming Language“, 2019. [Online]. Verfügbar unter: <https://www.rust-lang.org/>.

[11] „Genesis block - Bitcoin Wiki“, 2019. [Online]. Verfügbar unter: https://en.bitcoin.it/wiki/Genesis_block.

- [12] „Peer-to-peer - Wikipedia“, 2019. [Online]. Verfügbar unter: <https://en.wikipedia.org/wiki/Peer-to-peer>.
- [13] „What Is a Blockchain Consensus Algorithmen | Binance Academy“, 2019. [Online]. Verfügbar unter: <https://www.binance.vision/blockchain/what-is-a-blockchain-consensus-algorithm>.
- [14] „Bitcoin - Wikipedia“, 2019. [Online]. Verfügbar unter: <https://en.wikipedia.org/wiki/Bitcoin>.
- [15] Ethereum, „Home | Ethereum“, 2019. [Online]. Verfügbar unter: <https://www.ethereum.org/>.
- [16] „Nick Szabo - Wikipedia“, 2019. [Online]. Verfügbar unter: https://en.wikipedia.org/wiki/Nick_Szabo.
- [17] „Smart Contracts for Alpiq | ETH Zürich“, 2019. [Online]. Verfügbar unter: <https://ethz.ch/en/industry-and-society/industry-relations/industry-news/2019/04/smart-contract-for-alpiq.html>.
- [18] „CryptoKitties | Collect and breed digital cats!“, 2019. [Online]. Verfügbar unter: <https://www.cryptokitties.co/>.
- [19] „Wei“, 2019. [Online]. Verfügbar unter: <https://www.investopedia.com/terms/w/wei.asp>.
- [20] S. Fontaine, „Understanding Bytecode on Ethereum - Authereum - Medium“, 2019. [Online]. Verfügbar unter: <https://medium.com/authereum/bytecode-and-init-code-and-runtime-code-oh-my-7bcd89065904>.
- [21] K. Tam, „Transactions in Ethereum - KC Tam - Medium“, 2019. [Online]. Verfügbar unter: <https://medium.com/@kctheservant/transactions-in-ethereum-e85a73068f74>.
- [22] Y. Riady, „Signing and Verifying Ethereum Signatures - Yos Riady“, 2019. [Online]. Verfügbar unter: <https://yos.io/2018/11/16/ethereum-signatures/>.
- [23] „Remote procedure call - Wikipedia“, 2020. [Online]. Verfügbar unter: https://en.wikipedia.org/wiki/Remote_procedure_call.
- [24] „<https://keccak.team/>“, 2019. [Online]. Verfügbar unter: [Keccak%20Team](https://keccak.team/).
- [25] „Elliptic Curve Digital Signature Algorithm - Wikipedia“, 2019. [Online]. Verfügbar unter: https://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm.
- [26] „SHA-3 - Wikipedia“, 2019. [Online]. Verfügbar unter: <https://en.wikipedia.org/wiki/SHA-3>.
- [27] „Ethereum Series - Understanding Nonce - The Startup - Medium“, 2019. [Online]. Verfügbar unter: <https://medium.com/swlh/ethereum-series-understanding-nonce-3858194b39bf>.
- [28] N. Jabes, „Nu Jabe’s answer to What is an Ethereum contract address? - Quora“, 2019. [Online]. Verfügbar unter: <https://www.quora.com/What-is-an-Ethereum-contract-address/answer/Nu-Jabes>.

- [29] „Crypto Wallet Types Explained | Binance Academy“, 2019. [Online]. Verfügbar unter: <https://www.binance.vision/blockchain/crypto-wallet-types-explained>.
- [30] M. Wachal, „What is a blockchain wallet? - SoftwareMill Tech Blog“, 2019. [Online]. Verfügbar unter: <https://blog.softwaremill.com/what-is-a-blockchain-wallet-bbb30fbf97f8>.
- [31] StellaBelle, „Cold Wallet Vs. Hot Wallet: What’s The Difference?“, 2019. [Online]. Verfügbar unter: <https://medium.com/@stellabelle/cold-wallet-vs-hot-wallet-whats-the-difference-a00d872aa6b1>.
- [32] M. Wright, „So many mobile wallets, so little differentiation - Argent - Medium“, 2019. [Online]. Verfügbar unter: <https://medium.com/argenthq/recap-on-why-smart-contract-wallets-are-the-future-7d6725a38532>.
- [33] E. Conner, „smart Wallets are Here - Gnosis“, 2019. [Online]. Verfügbar unter: <https://blog.gnosis.pm/smart-wallets-are-here-121d44519cae>.
- [34] D. Labs, „Why Dapper is a smart contract wallet - Dapper Labs - Medium“, 2019. [Online]. Verfügbar unter: <https://medium.com/dapperlabs/why-dapper-is-a-smart-contract-wallet-ef44cc51cfa5>.
- [35] „Crypto Bites: Chat with Ethereum founder Vitalik Buterin“, 2019. [Online]. Verfügbar unter: https://www.youtube.com/watch?v=u-i_mTWL-FI&feature=emb_logo.
- [36] R. Greene und M. N. Johnstone, „An investigation into a denial of service attack on an ethereum network“, 2018. [Online]. Verfügbar unter: <https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1219&context=ism>.
- [37] P. Technologies, „Releases - paritytech/parity-ethereum“, 2020. [Online]. Verfügbar unter: <https://github.com/paritytech/parity-ethereum/releases>.
- [38] „TOML - Wikipedia“, 2020. [Online]. Verfügbar unter: <https://en.wikipedia.org/wiki/TOML>.
- [39] „JSON - Wikipedia“, 2020. [Online]. Verfügbar unter: <https://en.wikipedia.org/wiki/JSON>.
- [40] „Remix - Ethereum IDE“, 2020. [Online]. Verfügbar unter: <https://remix.ethereum.org/>.
- [41] MetaMask, „MetaMask“, 2019. [Online]. Verfügbar unter: <https://metamask.io/>.
- [42] „Software versioning“, 2020. [Online]. Verfügbar unter: https://en.wikipedia.org/wiki/Software_versioning.
- [43] T. B. G. 2019, „Sweet Tools for Smart Contracts“, 2019. [Online]. Verfügbar unter: <https://www.truffle-suite.com/>.
- [44] uPort, „uPort“, 2019. [Online]. Verfügbar unter: <https://www.uport.me/>.
- [45] A. Wallet, „Atomic Cryptocurrency Wallet“, 2019. [Online]. Verfügbar unter: <https://atomicwallet.io/>.

[46] E. M. Inc., „Crypte Wallet - Send, Receive & Exchange Cryptocurrency | Exodus“, 2019. [Online]. Verfügbar unter: <https://www.exodus.io>.

[47] MyEtherWallet, „MyEtherWallet | MEW“, 2019. [Online]. Verfügbar unter: <https://www.myetherwallet.com/>.

[48] Solidity, „Solidity - Solidity 0.5.11 documentation“, 2019. [Online]. Verfügbar unter: <https://solidity.readthedocs.io/en/v0.5.11/>.

[49] „Vyper–Vyper documentation“, 2019. [Online]. Verfügbar unter: <https://vyper.readthedocs.io/en/v0.1.0-beta.13/#>.

5 Anhang

5.1 Glossar

Begriff	Bedeutung
---------	-----------

5.2 Entwicklungsumgebung

In diesem Abschnitt wird die geplante Testumgebung und deren Verwendung beschrieben.

5.2.1 Blockchain

Es wird eine Test-Blockchain aufgesetzt. Diese wird benötigt, um geschriebenen Code zu testen und analysieren.

Als Blockchain wird Ethereum[15] verwendet. In den nachfolgenden Absätzen werden mögliche Tools besprochen, die für den Aufbau von einer Testumgebung genutzt werden können.

5.2.1.1 Client

In der Arbeit wird evaluiert ob Geth[6] als Client den Ansprüchen genügt oder ob ein anderer Client (z.B. Parity[7], Aleth[8], etc.) zum Einsatz kommt.

Trufflesuite Trufflesuite[43] wird verwendet, um eine simulierte Blockchain aufzusetzen. Diese kann für die Einarbeitung in die Materie genutzt werden.

5.2.2 Wallet

Wallets werden für die Verwaltung von Benutzerkonten und deren Transaktionen benötigt. Zu den möglichen Wallets gehören z.B.:

- uPort[44]
- Metamask[41]
- Atomic Wallet [45]
- Exodus[46]

Es wird davon ausgegangen, dass keine Wallet alle Bedürfnisse abdecken kann, daher wird die gewählte Wallet im Zuge dieses Projekts erweitert. Für Ethereum existiert ein offizieller Service um eine eigene Wallet zu erstellen: MyEtherWallet[47]

5.2.3 Smart Contracts

Smart Contracts werden benötigt, um zu bestimmen, wer auf einer Blockchain gratis Transaktionen ausführen kann. Sobald eigene Smart Contracts entwickelt werden, kann die Testumgebung genutzt werden, um diese zu testen.

5.2.3.1 Programmiersprache

Für die Entwicklung von Smart Contracts werden folgende zwei Sprachen evaluiert:

- Solidity[48]
- Vyper[49]

6 Ehrlichkeitserklärung

Die eingereichte Arbeit ist das Resultat unserer persönlichen, selbstständigen Beschäftigung mit dem Thema. Alle wörtlichen und sinngemässen Übernahmen aus anderen Werken sind als solche gekennzeichnet

Datum _____

Ort _____

Faustina Bruno _____

Serge Jurij Maïkoff _____