
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.

Zusammenfassung

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
2	Entwicklungsumgebung	3
2.1	Blockchain	3
2.1.1	Client	3
2.2	Wallet	3
2.3	Smart Contracts	4
2.3.1	Programmiersprache	4
3	Theoretischer Teil	5
3.1	Anwendungsbereich	5
3.2	Aktueller Stand	5
3.3	Recherche	5
3.3.1	Ethereum Blockchain	5
3.3.2	Identitäten	6
3.3.3	Wallets und Smart Wallets	6
3.3.4	Smart Contracts	6
3.3.5	Transaktionen	6
3.3.6	Gas	6
3.3.7	Denial of Service (DOS) Attacken	6
3.4	Lösungsansätze	6
4	Praktischer Teil	7
5	Fazit	8
6	Quellenverzeichnis	9
7	Anhang	10

8 Ehrlichkeitserklärung

13

1 Einleitung

1.1 Problemstellung

Die Aufgabe beinhaltet ein Blockchain Netzwerk [1] für ein Modul zur Verfügung zu stellen, welches von den Studierenden zu test Zwecken genutzt werden kann. Blockchains verfügen über verschiedene Mechanismen, um sich gegen Attacken abzusichern. Eine davon ist eine Gebühr auf jeder Transaktion, der sogenannte Gas Price 3.3.6 [2]. Dadurch können Denial of Service (DoS) Attacken 3.3.7 [3], 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 Attacken.

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 Attacken hat.

1.3 Methodik

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.

Strukturierung des Berichts

Der Bericht ist in einen theoretischen und praktischen Teil gegliedert. Gemachte Literaturstudien, geprüfte Tools und der aktuelle Stand der Ethereum Blockchain 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 und verwendeter Code zu finden.

2 Entwicklungsumgebung

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

2.1 Blockchain

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

Als Blockchain wird Ethereum[4] verwendet. In den nachfolgenden Absätzen werden mögliche Tools besprochen, die für den Aufbau von einer Testumgebung genutzt werden können.

2.1.1 Client

In der Arbeit wird evaluiert ob Geth[5] als Client den Ansprüchen genügt oder ob ein anderer Client (z.B. Parity[6], Aleth[7], etc.) zum Einsatz kommt.

2.1.1.1 Trufflesuite

Trufflesuite[8] wird verwendet, um eine simulierte Blockchain aufzusetzen. Diese kann für die Einarbeitung in die Materie genutzt werden.

2.2 Wallet

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

- uPort[9]
- Metamask[10]
- Atomic Wallet [11]
- Exodus[12]

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[13]

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.

2.3.1 Programmiersprache

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

- Solidity[14]
- Vyper[15]

3 Theoretischer Teil

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 und aktuelle Stand der Ethereum Blockchain behandelt.

3.1 Anwendungsbereich

Hier kommt der Anwendungsbereich unserer Lösung .. also Ausbildungszwecke

3.2 Aktueller Stand

Vielleicht überflüssig? da es noch gar nix dazu gibt an der fhnw?

3.3 Recherche

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 Attacke im Fokus.

3.3.1 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]

3.3.2 Identitäten

3.3.3 Wallets und Smart Wallets

3.3.4 Smart Contracts

3.3.5 Transaktionen

3.3.6 Gas

3.3.7 Denial of Service (DOS) Attacken

3.4 Lösungsansätze

4 Praktischer Teil

5 Fazit

6 Quellenverzeichnis

- [1] „Blockchain - Wikipedia“, 2019. [Online]. Verfügbar unter: <https://en.wikipedia.org/wiki/Blockchain>.
- [2] M. Inc., „What is Gas | MyEtherWallet Knowledge Base“, 2018. [Online]. Verfügbar unter: <https://kb.myetherwallet.com/en/transactions/what-is-gas/>.
- [3] „Denial-of-service attack - Wikipedia“, 2019. [Online]. Verfügbar unter: https://en.wikipedia.org/wiki/Denial-of-service_attack.
- [4] Ethereum, „Home | Ethereum“, 2019. [Online]. Verfügbar unter: <https://www.ethereum.org/>.
- [5] go-ethereum, „Go Ethereum“, 2019. [Online]. Verfügbar unter: <https://geth.ethereum.org/>.
- [6] P. Technologies, „Blockchain Infrastructure for the Decentralised Web | Parity Technologies“, 2019. [Online]. Verfügbar unter: <https://www.parity.io>.
- [7] „<https://github.com/ethereum/aleth>“, 2019. [Online]. Verfügbar unter: <https://github.com/ethereum/aleth>.
- [8] T. B. G. 2019, „Sweet Tools for Smart Contracts“, 2019. [Online]. Verfügbar unter: <https://www.truffle-suite.com/>.
- [9] uPort, „uPort“, 2019. [Online]. Verfügbar unter: <https://www.uport.me/>.
- [10] MetaMask, „MetaMask“, 2019. [Online]. Verfügbar unter: <https://metamask.io/>.
- [11] A. Wallet, „Atomic Cryptocurrency Wallet“, 2019. [Online]. Verfügbar unter: <https://atomicwallet.io/>.
- [12] E. M. Inc., „Crypte Wallet - Send, Receive & Exchange Cryptocurrency | Exodus“, 2019. [Online]. Verfügbar unter: <https://www.exodus.io>.
- [13] MyEtherWallet, „MyEtherWallet | MEW“, 2019. [Online]. Verfügbar unter: <https://www.myetherwallet.com/>.
- [14] Solidity, „Solidity - Solidity 0.5.11 documentation“, 2019. [Online]. Verfügbar unter: <https://solidity.readthedocs.io/en/v0.5.11/>.
- [15] „Vyper-Vyper documentation“, 2019. [Online]. Verfügbar unter: <https://vyper.readthedocs.io/en/v0.1.0-beta.13/#>.

7 Anhang

so bla 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.

The standard chunk of Lorem Ipsum used since the 1500s is reproduced below for those interested. Sections 1.10.32 and 1.10.33 from „de Finibus Bonorum et Malorum“ by Cicero are also reproduced in their exact original form, accompanied by English versions from the 1914 translation by H. Rackham.

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.

The standard chunk of Lorem Ipsum used since the 1500s is reproduced below for those interested. Sections 1.10.32 and 1.10.33 from „de Finibus Bonorum et Malorum“ by Cicero are also reproduced in their exact original form, accompanied by English versions from the 1914 translation by H. Rackham.

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.

The standard chunk of Lorem Ipsum used since the 1500s is reproduced below for those interested. Sections 1.10.32 and 1.10.33 from „de Finibus Bonorum et Malorum“ by Cicero are also reproduced in their exact original form, accompanied by English versions from the 1914 translation by H. Rackham.

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.

The standard chunk of Lorem Ipsum used since the 1500s is reproduced below for those interested. Sections 1.10.32 and 1.10.33 from „de Finibus Bonorum et Malorum“ by Cicero are also reproduced in their exact original form, accompanied by English versions from the 1914 translation by H. Rackham.

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.

The standard chunk of Lorem Ipsum used since the 1500s is reproduced below for those interested. Sections 1.10.32 and 1.10.33 from „de Finibus Bonorum et Malorum“ by Cicero are also reproduced in their exact original form, accompanied by English versions from the 1914 translation by H. Rackham.

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.

The standard chunk of Lorem Ipsum used since the 1500s is reproduced below for those interested.

Sections 1.10.32 and 1.10.33 from „de Finibus Bonorum et Malorum“ by Cicero are also reproduced in their exact original form, accompanied by English versions from the 1914 translation by H. Rackham.

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.

The standard chunk of Lorem Ipsum used since the 1500s is reproduced below for those interested. Sections 1.10.32 and 1.10.33 from „de Finibus Bonorum et Malorum“ by Cicero are also reproduced in their exact original form, accompanied by English versions from the 1914 translation by H. Rackham.

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.

The standard chunk of Lorem Ipsum used since the 1500s is reproduced below for those interested. Sections 1.10.32 and 1.10.33 from „de Finibus Bonorum et Malorum“ by Cicero are also reproduced in their exact original form, accompanied by English versions from the 1914 translation by H. Rackham.

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.

The standard chunk of Lorem Ipsum used since the 1500s is reproduced below for those interested. Sections 1.10.32 and 1.10.33 from „de Finibus Bonorum et Malorum“ by Cicero are also reproduced in their exact original form, accompanied by English versions from the 1914 translation by H. Rackham.

8 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
