IP6: Blockchain Transactionmanager

Projektvereinbarung

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

Inhaltsverzeichnis

1 Aufgabenstellung

Blockchains verfügen über verschiedene Mechanismen um sich gegen Attacken abzusichern. Eine davon ist eine Gebühr auf jeder Transaktion, der sogenannte Gas Price[1]. Dadurch können Denial of Service (DoS)[2] Attacken, bei denen das Netzwerk mit unzähligen Transaktionen geflutet wird, effizient bekämpft werden. Der Angreifer kann die Attacke nicht aufrechterhalten, 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.

Die Projektaufgabe besteht darin, eine Lösung zu finden, bei der die Sicherheit der Blockchain auch ohne eine Transaktionsgebühr gewährleistet werden kann.

Das Ziel der Arbeit ist es zuerst eine konzeptionelle Erarbeitung eines Testnetzwerkes welches:

- nicht permanent ist (Reboot möglich)
- kostenlose Transaktionen ermöglicht
- Sicherheit gewährleistet

In einem zweiten Schritt die Umsetzung/Realisierung dieses Netzwerkes.

Um diese Ziele zu erriechen sind folgende Fragestellungen von Bedeutung:

- wie kann die Gebühr für Transaktionen auf null gesetzt und die Sicherheit der Blockchain trotzdem gewährleistet werden
- Unterstützt uPort[3] unsere gewünschten Anfroderungen einer SmartWallet oder müssen wir selber eine SmartWallet programmieren
- Wie kann man Attacken vermeiden (zB algorithmisch: nur eine beschränkte Anzahl Transaktionen pro Monat pro Benutzer möglich)

2 Planung

In diesem Kapitel wird beschrieben, wie das Projekt geplant wird. Dazu gehören Meilensteine und die Benennung der wichtigsten Teilaufgaben.

2.1 Meilensteine

2.2 Termine

In der untenstehenden Tabelle 2.1 sind die bereits bekannten Meilensteine aufgeführt. Diese Liste ist noch nicht abschliessend und kann in Absprache mit den Betreuern noch angepasst werden.

2.3 Aufgaben

Tabelle 2.1: Grober Zeitplan

Datum	Event
24.09.2019	Kickoff
08.10.2019	Entwurf Projektvereinbarung
08.10.2019	Testumgebung
15.10.2019	Projektvereinbarung abgeschlossen
15.10.2019	Aufbau Bericht/Inhaltsverzeichnis
22.10.2019	Analyse Phase
05.11.2019	Gratis Transaktionen in der Blockchain
05.11.2019	Wallets analysieren
12.11.2019	Definieren der Themen für Zwischenpräsentation

Datum	Event
19.11.2019	Erster Bericht Entwurf für Feedback
28.11.2019	Zwischenpräsentation
03.12.2019	Feedback des Berichtes einbauen
10.12.2019	Analyse Smart Contracts
14.01.2020	Erweiterung der Wallet
11.02.2020	Steuerung für gratis Transaktionen über Gruppen
18.02.2020	zweite Bericht Version
25.02.2020	Analyse von Algorithmen für automatische Gruppenverwaltung
03.03.2020	Implementierung Algorithmen in Smart Contracts
20.03.2020	Testen und Überarbeiten von Netzwerk
20.03.2020	Abgabe Bachelorthesis
13. - 24.04.2020	Verteidigung

In der Grafik 2.1 wird die Tabelle 2.1 dargestellt.

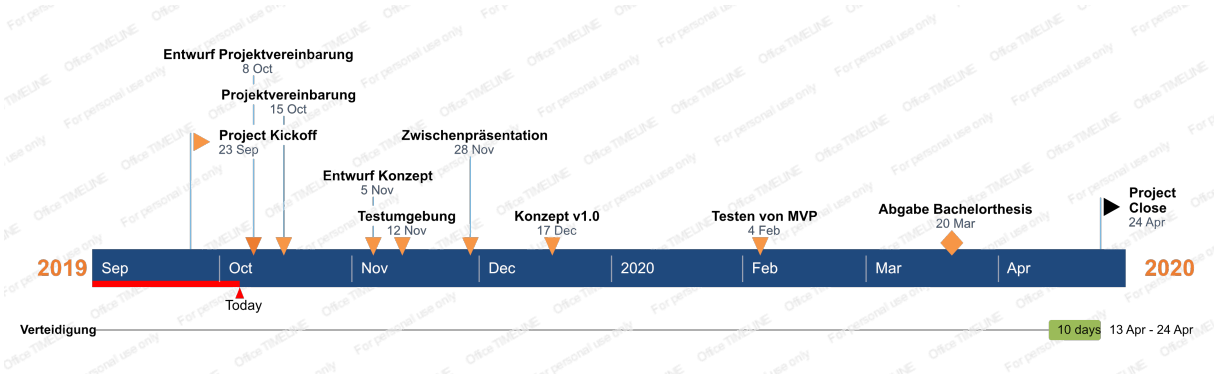

Abbildung 2.1: Zeitstrahl

3 Risiken

In der Tabelle 3.1 sind die wichtigsten Risken aufgelistet. In der Spalte Auftreten wird die gschätzte Wahrscheinlichkeit eines Eintreffen des Risikos beschrieben. Die Spalte Auswirkung beschreibt die Schwere beim Eintreffen des Risikos. Bei beiden Spalten ist der Wert 1 das Minimum und der Wert 3 das Maximum. Der Wert in der Spalte Kategorie wird aus der Multiplikation von Auftreten und Auswirkung gebildet. Ein Risiko kann also von 1 bis 9 gewertet werden. Je höher die Kategorie, umso gefährlicher ist ein Risiko.

Tabelle 3.1: Risiken

Risiko	Auftreten	Auswirkung	Kategorie	Gegenmassnahme
Teammitglied bricht Projekt ab	1	3	3	Gute Kommunikation unter den Teammitgliedern. Protokollieren, wer was erledigt hat. Planung in Zusammenarbeit mit den Betreuern überarbeiten
Unterschätzen des Projektumfanges	2	2	4	Sorgfältige Planung und regelmässig Rücksprache mit den Betreuern
Ausfall von einem Teammitglied (mehr als 2 Wochen)	2	2	4	Sofortiges Informieren von Betreuern. Planung überarbeiten und Ausfall berücksichtigen

4 Entwicklungsumgebung

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

4.1 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.

4.1.1 Client

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

4.1.1.1 Trufflesuite

Trufflesuite[6] wird verwendet, um eine simulierte Blockchain aufzusetzen. Diese kann für die Einarbeitung in die Materie genutzt werden.

4.2 Wallet

Es werden verschiedene Wallets auf ihre Funktionalität untersucht. Es wird davon ausgegangen, dass keine Wallet alle Bedürfnisse abdecken kann, daher wird die gewählte Wallet im Zuge dieses Projekts erweitert. Zu den möglichen Wallets gehören z.B.: - uPort[3] - Nano X **???** - Nano S **???** - Trezor **???** - Atomic Wallet **???**

4.3 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.

4.3.1 Programmiersprache

Für die Entwicklung von Smart Contracts werden folgende Sprachen evaluiert: - Solidity[7] - Vyper**???** - LLL**???** - Bamboo**???** - eWASM**???**

5 Quellenverzeichnis

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

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

[3] uPort, „uPort“, 2019. [Online]. Verfügbar unter: https://www.uport.me/.

[4] Ethereum, „Home | Ethereum“, 2019. [Online]. Verfügbar unter: https://www.ethereum.org/.

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

[6] T. B. G. 2019, „Sweet Tools for Smart Contracts“, 2019. [Online]. Verfügbar unter: https://www.trufflesuite.com/.

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