HÖHERE TECHNISCHE BUNDESLEHRANSTALT WIEN 16, THALIASTRASSE 125
Höhere Abteilung für Informationstechnologie
Ausbildungsschwerpunkt Netzwerktechnik und Medientechnik

Diplomarbeit

5AHITN – Reife- und Diplomprüfung 2017/18

Gesamtprojekt	**uspeak.io**
Aufgabenstellung des Gesamtprojektes	Die Entwicklung eines dezentralisierten „Blogsystems“, welches Inhalte in einer Blockchain speichert und dadurch Schutz vor Zensur, Bearbeitung oder Entfernung von Inhalten durch Regierungen oder andere Organisationen bietet.

Kandidaten / Kandidatinnen	**Betreuer / Betreuerin**
Dominik Süß	OStR Ing. DI Robert Baumgartner MBA
Martin Stundner	OStR Ing. DI Robert Baumgartner MBA
Marko Cubela	OStR Ing. DI Robert Baumgartner MBA

Erklärung

Die Kandidaten / Kandidatinnen nehmen zur Kenntnis, dass die Diplomarbeit in eigenständiger Weise und außerhalb des Unterrichtes zu bearbeiten und anzufertigen ist, wobei Ergebnisse des Unterrichtes – als solche klar gekennzeichnet – mit einbezogen werden können.
Die Abgabe der vollständigen Diplomarbeit hat bis spätestens

23.03.2017

beim zuständigen Prüfer / der zuständigen Prüferin in ausgedruckter (2 Exemplare) und digitaler Form (CD-ROM, DVD) zu erfolgen.

Kandidaten / Kandidatinnen	Unterschrift
Dominik Süß	
Martin Stundner	
Marko Cubela	

OStR Ing. DI Robert Baumgartner MBA
Betreuer/in

Mag. Thomas Angerer
Abteilungsvorstand

DI Peter Johannes Bachmair
Direktor

Genehmigung

Wien, am _____

LSI Mag.[a] Bernadette Frauscher

Inhaltsverzeichnis

1 Projektidee

1.1 Ausgangssituation

Durch das Sperren, Zensieren und Manipulieren vieler Websites, sowie die aktuelle Position der FCC ist die Netzneutralität immer mehr in Gefahr. Die Meinungsfreiheit ist ein Grundrecht und wir wollen sicherstellen, dass dies nicht unterdrückt werden kann. Die Technik hinter Bitcoin sprach uns sehr an und wir denken, dass sich damit unser Ziel realisieren lässt.

1.2 Beschreibung der Idee

Wir entwickeln ein Portal, welche es ermöglicht Informationen auszutauschen, ohne, dass diese zensiert werden können. Mittels Public-Key Kryptographie ist es möglich, Inhalte zu verschlüsseln oder zu signieren. Alle Daten werden verteilt gespeichert, sodass es keiner Organisation möglich ist, eingetragene Daten zu verändern oder zu löschen. Durch die globale Verteilung der einzelnen Knoten werden konkrete Sperren durch ISPs via IP Blocks verhindert, da immer ein anderer Knoten zur Verfügung steht. Das Portal bietet eine Search-Engine und einen Editor.

2 Projektziele

2.1 MUSS Ziele

2.1.1 Node Software

Eine Software zum Betreiben einer Storage Node ist entwickelt. Die Daten werden auf drei Chains gespeichert: Text, Bilder, Public-Keys. Sie repliziert alle Chains komplett und stellt eine Rest-API zur Verfügung. Durch das Hashen der Blöcke und des Proof-Of-Works Algorithmus lassen sich Daten nicht modifizieren.

2.1.2 Information Website

Eine Homepage für das Produkt ist erstellt. Sie bietet Informationen über das Projekt und das Team.

2.1.3 Verschlüsselung

Das Portal bietet die Möglichkeit, Texte zu verschlüsseln und zu signieren.

2.1.4 Tor Kompatibilität

Zum Schützen der Privatsphäre ist die Software kompatibel mit dem Onion-Router. Es wird eine Bridge für die Node-Replication sowie Anleitungen zum Einrichten als Hidden Service entwickelt.

2.1.5 Web Interface

Ein Webinterface für das Betrachten und Erstellen von Beiträgen ist entwickelt. Es wird auf jeder Node zur Verfügung gestellt und benötigt kein “server-side-rendering”. Die Seite kann heruntergeladen werden und lokal gestartet werden.

2.1.6 Markdown Support

Die Einträge können mit Hilfe von Markdown optisch aufgearbeitet werden. Das Web-Frontend bietet einen WYSIWYG (What You See Is What You Get) Markdown Editor.

2.2 Optionale Ziele (Soll, Kann Ziele)

2.2.1 Keybase Integration

Um sicher zu stellen, dass der Public Key auch wirklich zu einer Person gehört, bieten wir eine Keybase Integration.

2.2.2 Tor Support

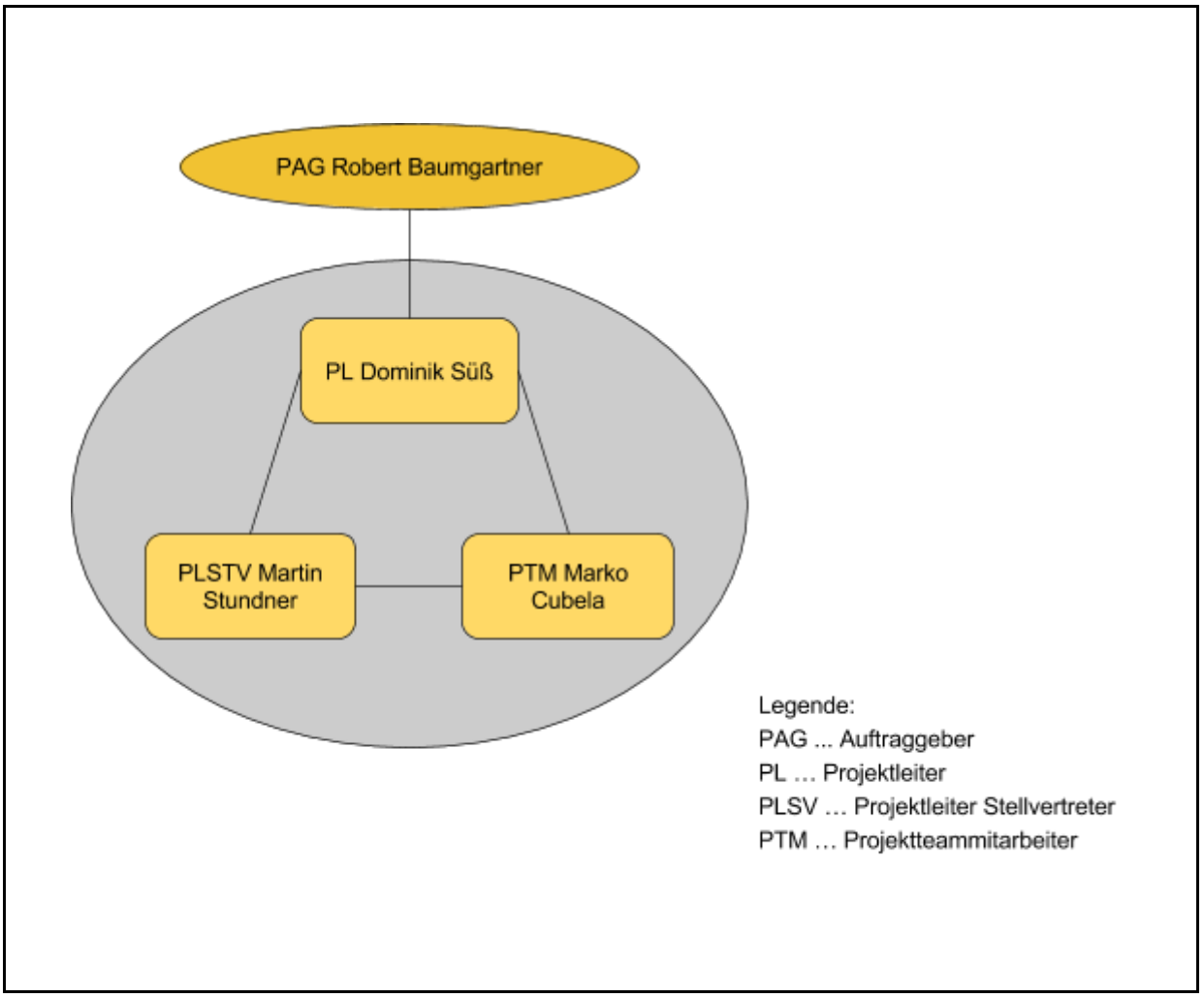
Um komplette Anonymität zu gewährleisten, bieten wir Anleitungen zum Betreiben der Node Software als Tor Hidden-service an.

2.3 NICHT Ziele

2.3.1 Ein eigener Distributed-Data-Storage Algorithmus ist entwickelt.
2.3.2 Mobile Anwendungen sind entwickelt.
2.3.3 Vorhandene Blockchain Implementierungen werden verwendet.

3 Projektorganisation

3.1 Grafische Darstellung (Organigramm)



3.2 Projektteam

Funktion	Name	Kürzel	E-Mail
Betreuer	OStR Ing. DI Robert Baumgartner MBA	baum	robert.baumgartner@htl-ottakring.ac.at
Projektleiter	Dominik Süß	sdo	d.suess99@htl-ottakring.ac.at
Stellvertretender Projektleiter	Martin Stundner	sma	m.stundner99@htl-ottakring.ac.at
Projektmitarbeiter	Marko Cubela	cma	m.cubela97@htl-ottakring.ac.at

3.3 Individuelle Aufgabenstellung

3.3.1 Dominik Süß

- Implementierung der Blockchain
  - Public-Key Chain
  - Image Chain
  - Text Chain
- Entwicklung einer REST-API
- Entwicklung eines automatischen Deployment-Systems
- Entwicklung eines Algorithmus zum Generieren von benutzerfreundlichen Slugs.

3.3.2 Marko Cubela

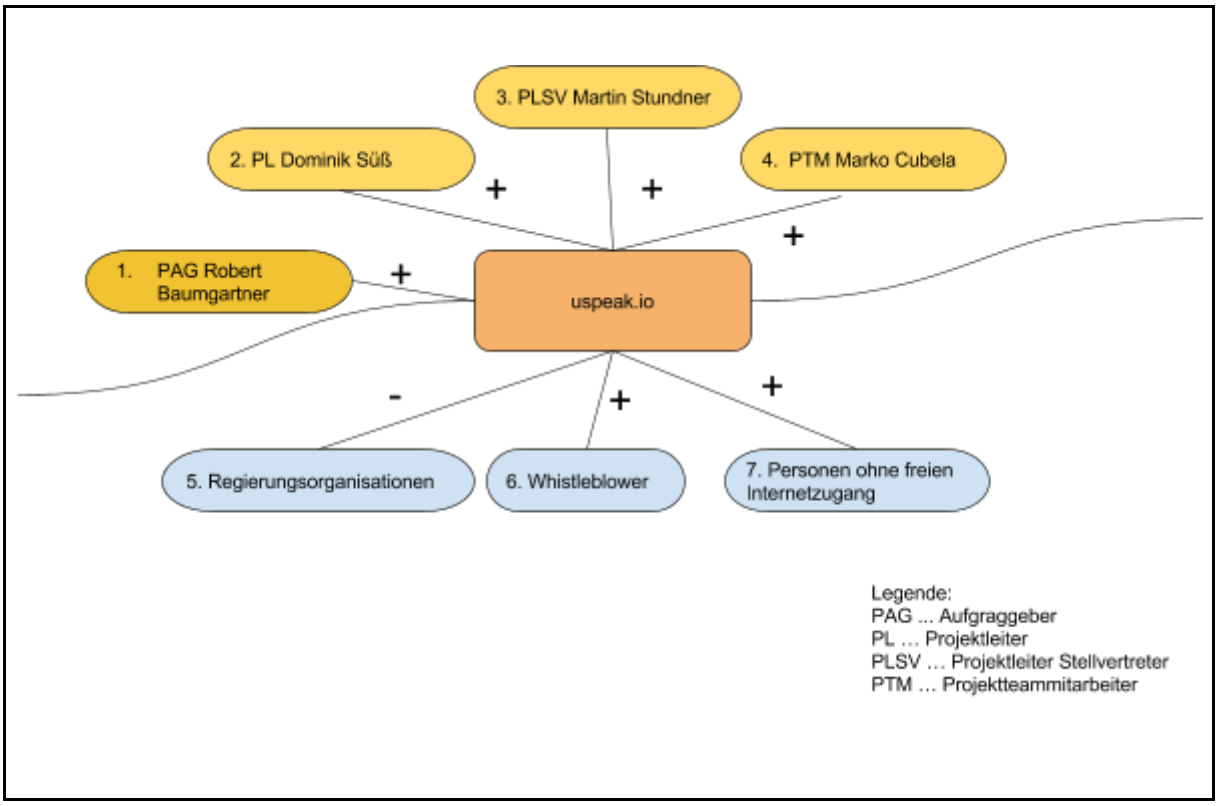
- Entwicklung eines Portals
  - Verschlüsselungsfunktion
  - Signierungsfunktion
  - Search-Engine
  - Markdown Editor
- Exportieren/Importieren eines PGP Keyservers in die Blockchain
- Node Discovery via DNS (manuelle Eingabe möglich)

3.3.3 Martin Stundner

- Entwicklung des Node Replication Algorithmus
  - Lösen von Merge Konflikten
  - Effiziente Replikation der Blockchain auf neue Nodes
  - Sicherer und minimaler Traffic
- Tor-Bridge entwickeln

4 Projektumweltanalyse

4.1 Grafische Darstellung



4.2 Beschreibung der wichtigsten Umwelten

#	Bezeichnung	Beschreibung	Bewertung
1	PAG Robert Baumgartner	Unterstützt das Projektteam mit fachlichen Kenntnissen	+
2	PL Dominik Süß	Arbeitet am Projekt	+
3	PLSV Martin Stundner	Arbeitet am Projekt	+
4	PTM Marko Cubela	Arbeitet am Projekt	+
5	Regierungs-organisationen	Wollen Realisierung des Projekts verhindern	-
6	Whistleblower	Haben eine Plattform um Dokumente zu leaken	+
7	Personen ohne freien Internetzugang	Erhalten Zugang zu sonst zensierten Informationen	+

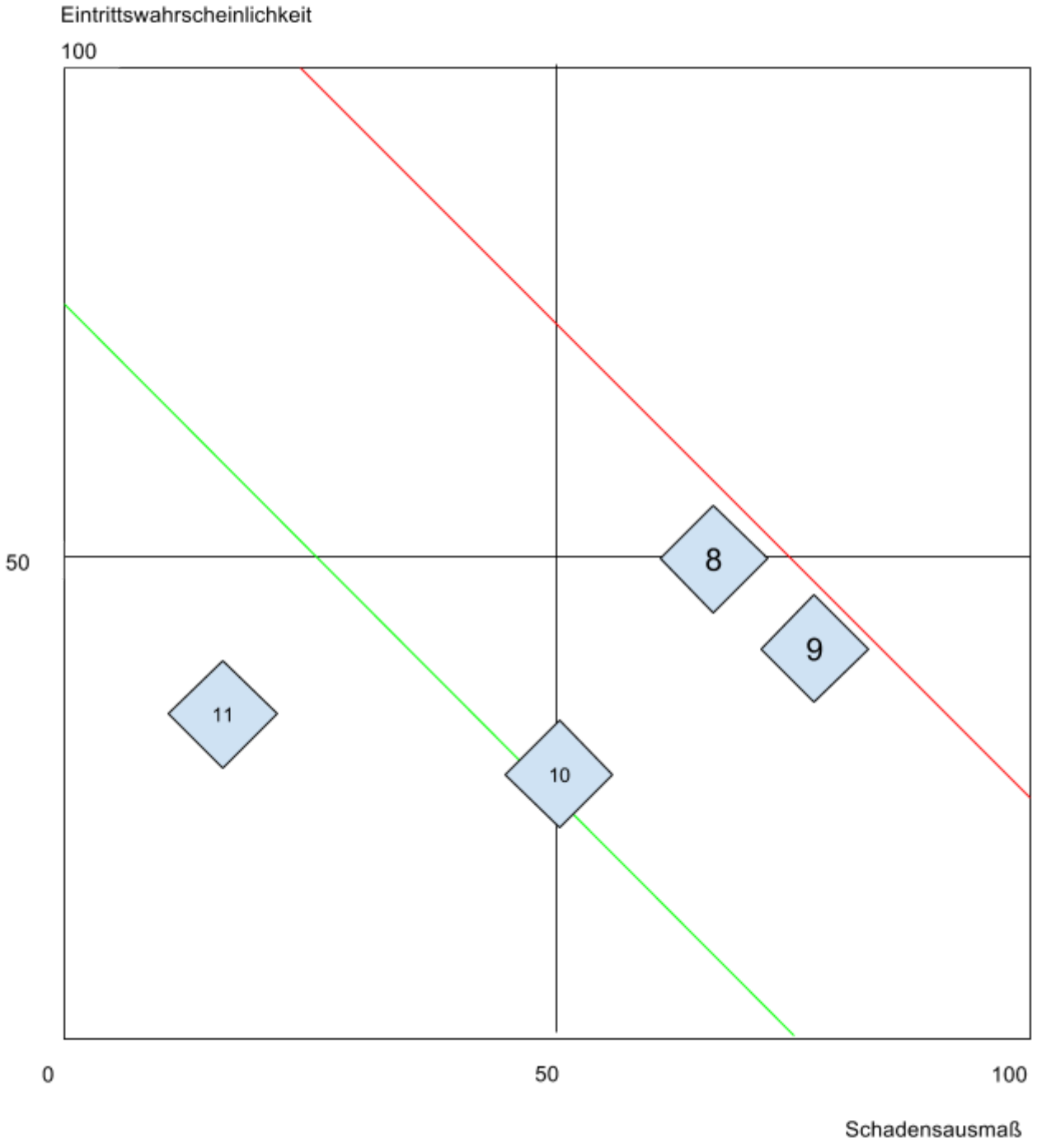
5 Risikoanalyse

5.1 Beschreibung der wichtigsten Risiken

#	Bezeichnung	Beschreibung des Risikos	P	A	RF
8	Technische Schwierigkeiten	Unsere Softwarekomponenten funktionieren nicht miteinander	50	60	3000
9	Tor-Netzwerk	Die Funktionalität des Tor Netzwerks entspricht nicht unseren vorstellungen.	40	70	2800
10	Probleme mit Libraries	Libraries entsprechen nicht den Erwartungen, oder eignen sich nicht für das Projekt	30	50	1500
11	Krankheit von Projektmitgliedern	Projektmitglieder erkranken unerwartet	30	20	600

P...Eintrittswahrscheinlichkeit des Risikos
A...Schadensausmaß bei Eintritt des Risikos
RF...berechneter Risikofaktor

5.2 Risikoportfolio



5.3 Risiko Gegenmaßnahmen

#	Bezeichnung	Gegenmaßnahme
8	Technische Schwierigkeiten	Externe Hilfe besorgen.
9	Tor Netzwerk	Intensives Beschäftigen mit dem Tor Netzwerk und suchen nach alternativen Lösungen
10	Probleme mit Libraries	Wir halten die Augen offen nach alternativen Programmbibliotheken.
11	Krankheit von Projektmitgliedern	Durch kompetentes Projektmanagement können wir die Abwesenheit von einzelnen Teammitgliedern kompensieren.

6 Meilensteinliste

Darstellung der Meilensteine mit geschätzten Terminen

Datum	Meilenstein
15.09.2017	Projekt beauftragt
27.09.2017	Website ist erstellt
29.09.2017	Technische Spezifikation fertiggestellt
10.11.2017	Portal Grundversion ist erstellt
1.12.2017	Minimale Blockchain implementiert
8.12.2017	Distributionsalgorithmus implementiert
15.12.2017	Minimum Viable Product fertiggestellt
2.2.2018	Beta-Test abgeschlossen
28.02.2018	Ziel von 10 Nodes erreicht
23.03.2018	Diplomarbeitsbuch fertiggestellt
24.04.2018	Projekt Abgeschlossen

7 Kostenabschätzung

Abschätzung der Kosten des Projekts

#	Beschreibung der Kostenursache	Kosten
1	Domain	50€
2	Azure/AWS/Google-Compute/etc. Account für Testumgebung	200€
3	Wildcard-SSL	100€
SUMME		350€

7.1 Finanzierung

Es wird versucht Sponsoren zu finden und wir nehmen an diversen Wettbewerben teil.

8 Motivation

8.1 Dominik Süß

Ich habe mich schon immer für all jenes interessiert, was im Hintergrund von verschiedenster Software passiert, wie genau die Daten gespeichert werden und was man daran noch verbessern kann. Andere Gebiete, wie zum Beispiel Kryptographie und verteilte Systeme gehören auch zu meinen Interessen. Diese Diplomarbeit bietet mir eine Gelegenheit, diese Interessen zu kombinieren und noch weiter zu verfolgen und dabei noch etwas gutes zu tun. Rede- und Meinungsfreiheit ist ein bedeutendes Grundrecht und muss geschützt werden.

8.2 Martin Stundner

Im Großen und Ganzen bedeutet mir das Wort “Meinungsfreiheit” eine Menge. Schließlich wünscht sich ja wohl jeder, dass er das Sprechen und Schreiben darf, was er denkt. Und dieses Recht hat auch jeder einzelne Mensch auf dieser Welt. Nun, da es ja offensichtlich ist, dass uns die Medien jeden Tag aufs neue ein verfälschtes Bild der Realität auftischen, wird es Zeit, etwas dagegen zu unternehmen. Das Projektteam dieses Projektes vertritt einstimmig diese Meinung und wird gemeinsam dagegen vorgehen. Noch dazu kommt, dass am Ende dieses Projektes eine Plattform existieren wird, welche es noch nie zuvor gab. Sie ermöglicht es seine eigene Meinung und seine eigenen Aussagen veröffentlichen zu können, ohne, dass diese, weder von der Regierung noch von einem Administrator o.ä., geändert werden kann! Ich bin sehr überzeugt davon, dass dieses Projekt ein Erfolg wird. Ich bin stets an neuer Technologie interessiert und genau aus diesem Grund freue ich mich bereits, die Eigenschaften sowie die exakte funktionsweise der Blockchain kennen- und umsetzen zu lernen.

8.3 Marko Cubela

Ich bin davon überzeugt, dass dieses Projekt dabei helfen wird, Texte/Dokumente/Nachrichten unzensiert, unbearbeitet und ohne, dass sie gelöscht werden können, zu verteilen. Außerdem freue ich mich besonders darauf die Blockchain kennenzulernen und ich mir dabei erhoffe neue Konzepte kennenzulernen, die mir im Unterricht helfen können. Ich arbeite gerne an herausfordernden SEW Aufgaben und ich freue mich auf die Arbeit mit meinen Kollegen.