Formales Modell einer Domänenspezifische Sprache zur verteilten Programmierung mit Mehrheitenbildung

Im Internet werden zunehmend inhalte kollaborativ erzeugt. Dabei entsteht ein Ergebnis, durch Beiträge einzelner **Akteure**. Eine zentrale Frage ist die Bewertung der einzelnen Beiträge, und damit ihren Anteil am Gesamtergebnis.

Wikipedia folgt einem streng hirarchischem Modell, in welchem Vertrauenspersonen die Ihnalte der Benutzer filtern. Die Verantwortung liegt bei der Organisation. Effizienter sind jedoch selbstregulierende Systheme, bei denen die Benutzer die Inhalte der Anderen bewerten. Beispiele währen die auf *voting* und *reputation* basierende Plattformen Reddit[1] und StackOverflow[2].

Ein solches Prinzip könnte man auf das Verwalten aller digital geteilter Inhalte veralgemeinern.

Nehmen wir z.B. an, es gibt eine Webseite, die sich im Besitz von Akteuren befindet. Alle Akteure wollen **gerecht**, also proportional zu ihrem Besitz, über die Ihnalte der Webseite entscheiden können, sowie ihre Entscheidungsgewalt in bestimten Bereichen an andere vertrauenswürdige Akteure delegieren können. Dieses gilt für Mediale Inhalte, für die Programmierung, Architektur, Werteflüsse wie ein Geteiltes Budget oder eine Einkommensverteilung sowie nicht automatisierbare Prozesse, wie das validiren neuer Beiträge. Das eigendliche Ergebnis wird anhand von einer Mehrheit der Besitzer bestimmt.

Die Piratenbartei hat mit *Liquid Democracy*[3] einen deligierten Abstimmungsprozess digital Abgebildet. Jedoch bedarf es bei ihrem Ansatz einers zentralisierten Servers, welcher als Angrifspunkt die Sicherheit des Prozesses gefährdet.

Auch eignet sich das Konzept auch nur bedingt um damit geteiltes Eigentum wie z.B. eine Webseite zu modellieren, da der Besitz und somit die Stimmengewichtung in solchen nicht unter den mitgliedern Gleichverteilt ist. Auch fehlt es an eienr Rechte und Rollenverteilung.

Das 2009 eingeführte Konzept des Bitcoins[4] hat zumindest den Aspekt der sicherheit gelöst, in dem sie die verteilung von Tokens under Akteuren auf eine dezentrale weise modellieren. Die manipulation der Tokens ist durch eine Identität und ein Kryptografisches systhem **gesichert**.

Sicher bedeutet hierbei, dass einmal getroffene Vereinbarungen auch eingehalten werden.

---

[1] http://reddit.com

[2] http://stackoverflow.com

[3] Friedrich Lindenberg. Konzeption und Erprobung einer Liquid Democracy Plattform anhand von Gruppendiskussionen. TU Ilmenau, 2010.

[4] Satoshi Nakamoto, Bitcoin: A peer-to-peer electronic cash system. http://bitcoin.org/bitcoin.pdf

Das Ethereum Team hat die grundlegende Technologie des Bitcoins generalisiert[5]. Sie haben eine Virtuellen Maschine mit einer turing vollständigen Maschinensprache herrausbringen können. Diese Erlaubt das sichere ausführen von Berechnungen in einem dezentralen Netzwerk, welches nicht nur einen Informationsfluss, sondern auch durch die einbindung der lokalen währung Ether, einen Wertefluss ermöglicht.

Es entstehet eine vielzahl von neuen Anwendungsmöglichkeiten, wie Verbindliche, autonome Verträge zwischen mehreren Parteien oder Dezentrale Autonome Organisationen (DAO) und profitorientierte Cooperationen (DAC).

Ein Beispiel einer solchen DAO ist das "namecoin" konzept, welches als alternative zur ICANN Organisation die TLD ".bit" verwaltet und in naher zukunft die ICANN ablösen könnte.[6] Die Regeln unter denen DACs und DAOs funktionieren, wie das Bewilligen einer neuen TLD, werden auf der Ethereum VM programmiert. Dir Einigung der Akteure auf ein Programmstand geschieht noch durch eine Vertrauensinstanz, z.b. bestimmte Schlüsselpersonen.

Im dieser Arbeit möchte ich ein Modell für eine Meta-Programmiersprache für verteiltes programmieren auf Basis von Ehtereum entwickeln und untersuchen. In dieser werden Einigungsprozesse als Bestandteil des Entwicklungsprozesses angesehen.

Grundlegende Aktionen eines Akteurs ist das vorschlagen von Alternativknoten (klassisches Programmieren), sowie das partizipieren an Wahlen über alternativen.

Das Modell soll mit formaler Logik sowie modelltheoretischen Konzepten beschrieben werden und anschließend auf machbarkeit und wiederspruchsfreiheit Analysiert werden.

Der Prozess des "transitive delegatet voting" aus Liquid Democraty dient als eine Grundlage des Wahlprozesses. Diese wird durch das Modell von Eigentum und Delegationsbedinungen erweitert, welches eine Rechte und Rollenverwaltung ermöglicht. Die Mehrheit der Besitzer bestimmt dabei die für die Programmausführung gewählte Option.

Die Syntax der Programmiersprache ist ein LISP dialekt, mit dem Paradigma, dass Knoten des Abstrakten Syntaxbaumes als Daten sowie als Code interpretiert werden können. Die Daten befinden sich teilweise in einem kryptografisch gesicherten verteilten netzwerk ähnlich der auf BitTorrent aufbauenden IPFS[7] oder der Maidsafe[8] Architektur und Teilweise in dem Ethereum Speicher.

Diese Sprache soll das oben beschriebene Problem der *gerechten* und *sicheren* verwaltung der geteilten Webseite lösen.

[5] Gavin Wood, ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER. http://gavwood.com/paper.pdf

[6] ICANN, Identifier Technology Innovation Panel - Draft Report. https://www.icann.org/en/system/files/files/report-21feb14-en.pdf

[7] Juan Benet, IPFS - Content Addressed, Versioned, P2P File System. http://static.benet.ai/t/ipfs.pdf

[8] David Irvine, MaidSafe Distributed File System. http://maidsafe.net/Whitepapers/pdf/MaidSafeDistributedFileSystem.pdf