Ein dezentrales Transitionssystem zur manipulation von Wörtern einer regulären Sprache

Bachelorarbeit

zur Erlangung des akademischen Grades
Bachelor of Science (B. Sc.)

Humboldt-Universität zu Berlin
Institut für Informatik

eingereicht von:	Denis Erfurt
geboren am:	02.04.1988
in:	Novosibirsk
Gutachter(innen):	Prof. Dr. Klaus Reinhardt
	Prof. Dr. Jens-Peter Redlich

eingereicht am: ..... verteidigt am: .....

Selbständigkeitserklärung

Ich erkläre hiermit, dass ich die vorliegende Arbeit selbständig verfasst und nur unter Verwendung der angegebenen Quellen und Hilfsmittel angefertigt habe. Weiterhin erkläre ich, eine Bachelorarbeit in diesem Studiengebiet erstmalig einzureichen.

Berlin, den 28. Februar 2015 .....

Statement of authorship

I declare that I completed this thesis on my own and that information which has been directly or indirectly taken from other sources has been noted as such. Neither this nor a similar work has been presented to an examination committee.

Berlin, February 28, 2015 .....

Abstract

Im Internet werden zunehmend Inhalte kollaborativ erzeugt. Dabei entsteht ein Inhalt durch Beiträge einzelner Akteure, die räumlich und zeitlich getrennt sein können. Zentral ist dabei die Frage wie der Konsens über einen Inhalt auf eine dezentrale Weise gebildet werden kann. In dieser Arbeit untersuchen wir den Prozess der verteilten Zusammenarbeit für Inhalte die als Wörter einer regulären Sprache beschrieben werden können. Dafür wird ein Modell mit einer Implementation einer Blockchain-Technologie vorgestellt: Ein öffentliches Transitionssysthem mit dezentral validierter Ausführung. Ebenfalls wird eine Grammatik-Erweiterung mit einer Konsens-Funktion für eine beliebige reguläre Grammatik beschrieben. Die Wörter der erweiterten Grammatik beinhalten Informationen über die Besitzallokation der Akteure, alternative Beiträge und deren Bewertung. Die Konsens-Funktion überführt unter Berücksichtigung der Bewertungen ein Wort der erweiterten Grammatik in ein Wort der ursprünglichen Grammatik.

Inhaltsverzeichnis

Kapitel 1

Einleitung

Nehmen wir z.B. an, es gäbe eine Webseite, die sich im Besitz von Akteuren befindet. Alle Akteure wollen gerecht, also proportional zu ihrem Besitz, über die Inhalte der Webseite entscheiden können, sowie ihre Entscheidungsgewalt in bestimmten Bereichen an andere vertrauenswürdige Akteure delegieren können. Dieses gilt für die medialen Inhalte, die Programmierung, die Architektur, die Wertflüsse wie ein geteiltes Budget oder eine Einkommensverteilung, sowie nicht automatisierbare Prozesse, wie das Validieren neuer Beiträge. Das eigentliche Ergebnis wird anhand von einer Mehrheit der Besitzer bestimmt.

Wikipedia folgt einem streng hierarchischem Modell, in welchem Vertrauenspersonen die Inhalte der Benutzer filtern. Die Verantwortung liegt bei der Organisation. Effizienter sind jedoch selbstregulierende Systeme, bei denen die Benutzer die Inhalte der Anderen bewerten. Beispiele wären die auf Voting und Reputation basierenden Plattformen Reddit und StackOverflow. Ein weiteres Beispiel für die Bewertung von Inhalten ist das Konzept Liquid Democracy[Lin10], ein Vorschlag der Piratenpartei für eine moderne politische Konsensbildung. Ein solches Prinzip könnte man auf das Verwalten aller digital geteilter Inhalte verallgemeinern.

Jedoch eignen sich diese Konzepte nur bedingt um damit geteiltes Eigentum wie z.B. eine Webseite zu modellieren, da Abstimmungen auf eine informale Weise vorgenommen werden. Es fehlt einer formalen Syntax, welche die Implikationen einer potentiellen Entscheidung vor der Wahl durch Simulation klarer zeigt, sowie nach der Wahl automatisch ausführt. Außerdem bedarf es bei den Ansätzen eines zentralisierten Servers, welcher als Angriffspunkt die

Glaubwürdigkeit des Prozesses gefährdet, da die Akteure auf die Korrektheit des Servers vertrauen müssen.

Das 2009 eingeführte Konzept des Bitcoins und der Blockchain[Nak08] bietet eine Alternative zur zentralen Server-Architektur. Dieses beschreibt ein Protokoll in einem Netzwerk, welches Inhalte aus einem gebildeten Konsens bereitstellt. Es besitzt eine einfache, nicht turing vollständige Skriptsprache, sowie durch ein asymmetrisches Kryptosystem, Rechte und Rollen. Neue Inhalte werden nach einer Validierung ebenfalls in den Konsens aufgenommen. Die einfachste Interpretation von Bitcoin ist die eines Werteträgers, wobei die Beschränkung der Skriptsprache wenig Spielraum für weitere Interpretationen lässt. Allgemeiner ist das auf dem Bitcoin-Protokoll aufbauende Ethereum[Woo14] , welches eine turing vollständige Skriptsprache besitzt. Es entsteht eine Vielzahl von neuen Anwendungsmöglichkeiten: verbindliche, autonome Verträge zwischen mehreren Parteien, Dezentrale-Autonome-Organisationen (DAO) oder profitorientierte Kooperationen (DAC), die allesamt Werte- und Informationsflüsse ermöglichen. Ein Beispiel einer solchen DAO ist das namecoin[1] Konzept, welches als Alternative zur ICANN[2] Organisation die TLD ".bit"verwaltet und in naher Zukunft die ICANN ablösen könnte.[CN14] Die Regeln unter denen DACs und DAOs funktionieren, wie das Bewilligen einer neuen TLD, werden auf der Ethereum Plattform programmiert. Die Einigung der Akteure auf ein Programmstand geschieht noch durch eine zentrale Vertrauensinstanz, z.b. bestimmten Schlüsselpersonen.

1.1 Leistung und Struktur der Arbeit

Diese Arbeit besteht im wesentlichen aus 3 Teilen: Sie fasst notwendige Theoretische Grundlagen zusammen. Auf diese Aufbauend wird ein Modell für eine selbst-Manipulation-Schicht einer DAO ausgearbeitet und auf DAOs mit regulären Grammatiken angewandt. Schließlich wird das ausgearbeitete Modell Implementiert.

Die weitere Arbeit ist wie folgt aufgebaut: In Kapitel 2 werden Theoretische Konzepte beschrieben auf die diese Arbeit aufbaut. Ebenfalls wird eine ausführliche Definition einer Dezentralen-Autonomen-Organisation gegeben, wie

[1] http://namecoin.info/

[2] Internet Corporation for Assigned Names and Numbers

sie zum Zeitpunkt der Arbeit vorliegt. Darauf aufbauend wird das Problem der selbst-Modifikation erläutert und in Kapitel 3 eine Definition sowie eine Anwendung auf die regulären Sprachen erarbeitet. In Kapitel 4 wird eine Implementation der Anwendung vorgestellt. Schließlich wird in Kapitel 5 eine Zusammenfassung der Ergebnisse, sowie ein Ausblick gegeben.

Kapitel 2

Theoretische Grundlagen

2.1 Reguläre Grammatiken

Eine reguläre Grammatik definiert nach Noam Chomsky ist ein vier Tupel $G = (N, T, S, P)$ bestehend aus

1. N - einer Menge nichtterminaler Symbole
2. T - einer Menge terminaler Symbole, mit $T \cap N = \emptyset$
3. $S \in N$ - einem Startsymbol
4. $P \subseteq N \times \{\epsilon\} \cup T \cup TN$ - einer Menge von Produktionen oder auch Produktionsregeln

Sei weiter $\Sigma := N \cup T$ das Alphabet der Grammatik.

Eine Produktion $(R, r) \in P$ kann auch als $R \to r$ geschrieben werden. Sie sagt aus, dass das Nichtterminal R in einem Schritt überführt werden kann zum Teilwort r:

$$\alpha R \to \alpha r$$

Sind hierfür n Schritte notwendig, schreibt man $R \to^n r$. Um auszudrücken, dass r generell aus R ableitbar ist, kann man sich der reflexiv-transitiven Hülle der Produktionsregeln bedienen: $R \to^* r$.

Die Sprache, die von der regulären Grammatik erzeugt wird, ist die Menge aller Wörter, die vom Startsymbol ableitbar sind:

$$L(G) := \{w | S \rightarrow^* w \wedge w \in T^*\}$$

Existiert eine reguläre Grammatik, die eine Sprache erzeugt, so heißt die Sprache ebenfalls regulär.

Die Klasse der regulären Sprachen heißt REG.

Ein Beispiel für eine reguläre Grammatik mit der dazugehörigen Sprache ist:

$$\begin{aligned}
G_{abc} &= (N, T, S, P) \\
N &= \{S, A, B, C\} \\
T &= \{a, b, c\} \\
P &= \{ \\
&\quad S \rightarrow aA, S \rightarrow bB, S \rightarrow cC, S \rightarrow \varepsilon, \\
&\quad A \rightarrow aA, A \rightarrow bB, A \rightarrow cC, A \rightarrow \varepsilon, \\
&\quad B \rightarrow bB, B \rightarrow cC, B \rightarrow \varepsilon, \\
&\quad C \rightarrow cC, C \rightarrow \varepsilon, \\
&\quad \}
\end{aligned}$$

$$L(G) = \{a^x b^y c^z | x, y, z \in \mathbb{N}\}$$

2.2 Kontextfreie Grammatiken

Kontextfreie Sprachen unterscheiden sich nur in den Produktionsregeln von den regulären. Anders als bei regulären, wird für die rechte Seite einer Produktionsregel keine Einschränkung gemacht: $P \subseteq N \times (N \cup T)^*$

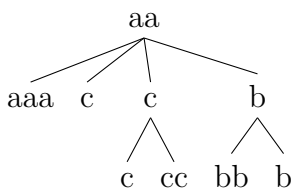
Wortteil

Sei $G = (S, N, T, P)$ eine Grammatik und $w \in L(G)$, dann definieren wir ein Wortteil:

$$w_{i..j} := \begin{cases} (t_k)_{i \leq k \leq j} \text{ mit } t_k \in T & | \ i \leq j \\ \varepsilon & | \ i > j \end{cases}$$

2.3 Trie

Ein Trie oder Prefixbaum ist eine Baum-Datenstruktur, die es erlaubt eine Menge von Worten über einem Alphabet effizient zu Speichern. Dabei werden gemeinsame Präfixe von wörtern in Knoten zusammengefasst. Eine Trie verwandte Datenstruktur, die Patricia-Trie reduziert den Speicherverbrauch indem sie alle Knoten mit nur einem Nachfolger zu einem Knoten zusammenfasst. Alle im Trie und Patricia-Trie gespeicherten Wörter können durch ein Tiefenscan wiederhergestellt werden. [Mor68] Ein Beispiel eines Patricia-Trie für die Menge $\{aaaaa, aac, aacc, aaccc, aabbb, aabb\}$ ist:



2.4 Transitionsystem

Ein initialisiertes Transitionssystem (T) [Gla] gibt einen formalismus vor um ein zustandbasiertes System zu beschreiben. Die Beschreibung zerteilt sich in die des Zustandraumes, beschrieben durch eine Menge M, die der Dynamik, beschrieben durch eine Übergangsfunktion $\tau : M \to M$ und einer Anfangszustandsmenge $I \subset M$.

$$T = (M, I, \tau)$$

Ablauf

Eine Folge $(s_n)_{n\in\mathbb{N}}$ mit $s_n \in M$ ist ein Ablauf von T, wenn gilt:

$$s_0 \in I$$
$$s_{i+1} = \tau(s_i)$$

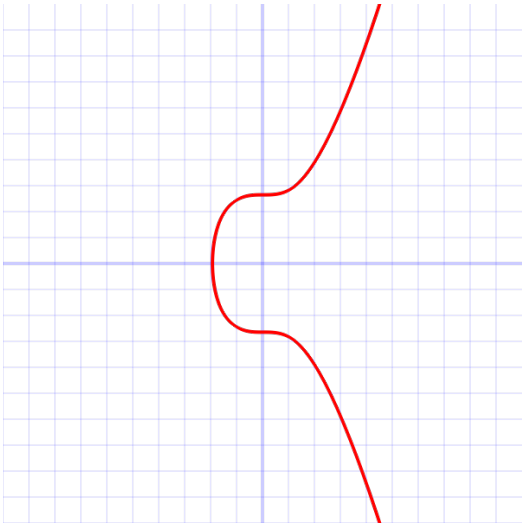


Abbildung 2.1: ECDSA - secp256k1 Kurve https://en.bitcoin.it/wiki/File:Secp256k1.png 25.02.2015

2.5 Kryptografie

asymetrische Verschlüsselung

Bei einem asymmetrischem Verschlüsselungsverfahren generiert der Benutzer ein Schlüsselpaar bestehend aus einem privatem und einem öffentlichem Schlüssel. Der öffentliche Schlüssel wird aus dem Privaten erzeugt und veröffentlicht. Wir werden im Folgenden den öffentlichen Schlüssel ebenfalls Adresse nennen. Die identifiziert einen Akteur.

Für die Signierung und Verifizierung von Nachrichten wird ECDSA mit der secp256k1 Kurve verwendet. ECDSA ist eine DSA Verfahren basierend auf Eliptic Curve Kryptografie. ECDSA bietet viele Vorteile zu alternativen Verfahren wie RSA oder DH.[Pou14]

2.6 Decentralized Autonomous Organization (DAO)

Eine DAO ist ein relativ neues Konzept, welches durch das populärwerden von Technologien wie Bitcoin und Ethereum erstmals aufgetaucht ist. Die

Fachwelt ist sich noch über die genaue Definition und die Abgrenzung zu verwanten Konzepten größtenteils uneinig. Zwar existieren Versuche "Decentralized Applications"(DAs,Dapps) wie BitTorrent oder den "Decentralized Autonomous Corporations"(DACs) von dem der DAOs Abzugrenzen, jedoch gibt es hier keine Garantie auf Persistenz der Terminologie sowie ihrer Definitionen, deshalb werden im Folgenden die Begriffe DA, Dapp, DAC, DAO synonym verwendet.

Intuitiv kann eine DAO als eine Gesellschaft verstanden werden, die ohne menschliche Einwirkung existiert und agiert. Sie kann ebenfalls als eine erweiterung des Open-Source Konzeptes betrachtet werden. Dabei ist nicht nur der Programmcode öffentlich, sondern auch ihre internen Berechnungen sowie wesentliche Teile ihrer Interaktionen. Diese sind durch einen gemeinsamen Konsens von der Erzeugung bis zum aktuellen Zustand determiniert und nachvollziehbar. Dieser Konsens wird auf eine dezentrale Weise gebildet, um zu verhindern, dass eine zentrale Instanz den Konsens manipuliert sowie um Robustheit und Beständigkeit zu sichern.

In ihren Aktionen kann die DAO interne, deterministische Berechnungen anstellen, mit anderen DAOs kommunizieren und so auf Services zugreifen oder nicht selbst ausführbare Aufgaben, wie beispielsweise das Erweitern und Verbessern des Programmcodes, an Menschen delegieren. Ihr Besitz kann durch Anteile determiniert werden, die unter anderen DAOs oder Menschen aufgeteilt sind. Diese berechtigen beteiligte Akteure zu verschiedenen Aktionen innerhalb ihrer Regeln wie z.B. einen Zugriff auf Dividenden oder anderen Ressourcen der DAO, Partizipation bei internen Abstimmungen oder anderen spezifischen Aktionen.

Ethereum, Bitcoin und Namecoin sind allesamt Beispiele für unterschiedliche DAOs. Ethereum ist dabei gleichzeitig eine Plattform für andere DAOs.

Im folgenden möchten wir drei Teilbereiche von DAOs näher beleuchten: Als erstes die Funktionsweise des Blockchain Mechanismus, der eigentlichen Neuerung, die zum Entstehen von DAOs führte. Als nächstes dem Teil, der die Interaktionen der DAO steuert. Als letztes der Selbstmanipulation der DAO, also dem Teil, welcher die Manipulation der Regeln der DAO steuert.

2.6.1 Dezentraler Konsens - Blockchain

Bitcoin hat mit der Einführung der Blockchain eine elegante und universelle Lösung für das Problem der Byzantinischen Generäle vorgeschlagen. Das Problem steht repräsentativ im Bereich der verteilten Systemen für die Schwierigkeit, einen Konsens zwischen Akteuren herzustellen, wenn einige, für Andere unbestimmte Akteure eigennützig sowie manipulativ agieren. Bitcoin hat hier eine statistische Lösung präsentiert: Es führt die Dezentralität des Konsens auf die natürliche Knappheit einer Ressource zurück. Für Bitcoin ist es die Anzahl der Berechnungen, die ein Akteur in einer bestimmten Zeit machen kann. Ein General versucht dabei ein Mathematisches Rätsel zu lösen, welches statistisch gesehen 10 Minuten dauern müsste, wenn alle beteiligten Generäle an dem Problem arbeiten würden. Hat ein General eine Lösung gefunden, teilt er dieses an alle ihm bekannten Generäle mit. Eine solche Lösung wird auch als "Block"bezeichnet. Jeder General arbeitet darauf hin mit dieser Lösung weiter und versucht sie zu erweitern, was wiederum statistisch gesehen 10 Minuten der Kraft aller Generäle kosten müsste. Jeder General arbeitet mit der von ihm zuerst gesehenen längsten Kette von Blöcken. Mit der Anzahl der Erweiterungen konvergiert nun die Beteiligung loyaler Generäle am Konsens zur Majorität, falls diese tatsächlich im Besitz einer Mehrheit der begrenzten Rechenressourcen sind. In einem Block befindet sich neben der vorhergehenden Lösung ebenfalls der aktuelle Konsenses, solange er auf den Vorhergehenden aufbaut und valide ist.

Das Lösen eines Rätsels für das Recht einen neuen Block bestimmen zu können, wird als "Proof of Worköder kurz POW bezeichnet, da ein General eine Arbeitsleistung beweisen muss, um den nächsten Block vorschlagen zu dürfen. Bitcoin und viele andere DAOs benutzen partielle Hash Invertierung als tatsächlichen POW Algorithmus. Dieser baut auf der Eigenschaft einer Hash-Funktion auf, dass es sehr einfach ist, einen Hash einer Nachricht zu berechnen, jedoch sehr schwer aus einem gegebenem Hash eine Nachricht zu rekonstruieren, die diesen Hash erzeugt. Der eigentliche Block besteht dabei aus einer Referenz des vorherigen Blocks (ref) zusammen mit dem neuen Konsens ($kons$) und einer $nonce$, die frei wählbar ist. Zudem existiert durch die vorherigen Blöcke bestimmte Schwierigkeit (ε), so dass die Rechenzeit für den neuen Block bei 10 Minuten bleibt. Akteure, die im Wettbewerb um einen neuen Block stehen (auch "Miner"genannt) müssen nun eine nonce finden,

dass einen Hashwert des Blockes unter der Schwierigkeit liegt:

$$sha256(\ ref \circ kons \circ nonce\ ) < \varepsilon$$

POW ist jedoch umstritten, da das verbrauchen von Rechenressourcen durch Stromkosten, Investitionen in neue Hardware und Infrastruktur einerseits nicht ökonomisch und zum anderen nicht umweltfreundlich ist. Um die Rechenpower des Bitcoin-Netzwerkes in Relation zu setzen hatten die Top 500 Weltbesten Supercomputer der Welt im November 2014 gemeinsam eine Rechenleistung von 309 Pflop/s.[1] Das Bitcoinnetzwerk besitzt derzeit (18.02.2015) eine Rechenleistung von 4172436 Pflop/s.[2].

Neben POW gibt es jedoch auch andere Mechanismen für das Recht einen Block erstellen zu dürfen. Hier gilt "Proof of Stake"(POS) und seine Erweiterung "Deligated Proof of Stake"(DPOS) als wesentlicher Konkurrent. Bei POS beweist ein Akteur, dass ihm ein bestimmter Anteil an der Blockchain zugehörigen DAO gehört. Bei DPOS kann ein Anteilseigner zusätzlich sein Anteil an einen Miner delegieren und muss nicht selbst an der Erstellung eines Blocks teilnehmen. Jedoch sind hier theoretische Attacken möglich (siehe dazu [Eth] [Vas15]), weshalb diese POW noch nicht abgelöst haben. Bitshares [3] - ein Bitcoin Fork mit einem DPOS oder Peercoin[4] ebenfalls ein Fork mit reinem POS sind jedoch real wirtschaftliche Beispiele für DAOs mit einem Alternativen Konsensmechanismus die zumindest zeigen, dass diese Mechanismen es schaffen ebenfalls in der Praxis zu bestehen.

Das erstellen von Blocks durch Miner ist bei den Blockchain-Mechanismen der hier vorgestellten DAOs ökonomisch motiviert. Jede DAO schüttet eine Belohnung an den Miner aus, der einen neuen Block findet. Die Belohnung ist ein interner Token(auch Coin genannt) der aufgrund seiner Knappheit einen Marktwert besitzt. Er kann jedoch auch als Besitzanteil der DAO interpretiert werden oder dient anderen zwecken. Bei Ethereum z.B. benötigen Akteure diesen Token um in der DAO agieren zu können. Im Bitcoins Blockchain Mechanismus werden derzeit (18.02.2015) 25 Bitcoins pro Block ausgeschüttet, was zum derzeitigen Marktpreis (240$/Btc) einem Wert von 6000$/Block entspricht. Zum Zeitpunt des ersten Blocks existieren noch keine

[1] http://www.top500.org/lists/2014/11/ 18.02.2015
[2] http://bitcoinwatch.com/ 18.02.2015
[3] https://bitshares.org/blog/delegated-proof-of-stake/ 18.02.2015
[4] http://peercoin.net/ 18.02.2015

Coin-Bestände, diese werden von dem ersten Block an an konkurierende Miner für die Blockerstellung ausgeschüttet. Die Größe der Belohnung wird mit der Zeit kleiner, bis irgendwann eine Menge von 21 Millionen Coins erreicht ist. Eine andere Motivation der Miner ist eine Transaktionsgebühr, die ein Akteur seiner Transaktion anhängt. Diese Gebühr bekommt ein Miner, wenn er diese in seinem Block berücksichtigt.

2.6.2 Interaktion

Die Art der Interaktion mit einer DAO hängt von ihrer Programmierung ab. Handelt es sich um eine Blockchain basierte DAO so ist das bereits beschriebene Erstellen von Blöcken eine Iteraktion sowie das Überweisen von eigenen Coins an einen anderen Akteur. Bitcoin bietet zudem eine einfache Skriptsprache mit der die Akteure kleine Skripte erstellen können wie "Multisignature"bei dem ein Coinbestand erst freigegeben wird, wenn die Mehrheit der angegebenen Adressen ihn freigeben. Diese Skriptsprache ist jedoch nicht Turing-Vollständig. Die Ethereum DAO hingegen besitzt eine Turing-Vollständige Skriptsprache und wird aufgrund dessen als eine DAO Plattform referenziert. Das ermöglicht das einfache Erstellen von Nicht Blockchain basierter DAOs, da der Bereich der Dezentralisierung von der Ethereum Plattform abgenommen wird. Aktionen in Ethereum währen unter anderem das hinzufügen eines neuen Programms oder die Übermittlung der Interaktionen an interne DAOs. In Ethereum können sich Akteure einerseits außerhalb der Ethereum DAO befinden, andererseits sind alle DAOs innerhalb von Ethereum ebenfalls Akteure.

Die Interaktion eines Akteurs mit einer Blockchain basierten DAO besitzt folgende Struktur:

Der Akteur:

1. läd sich den für ihn relevanten Teil des Konsens herunter
2. manipuliert diesen, jedoch muss die Manipulation den Regeln der DAO folgen, da sie sonst von den Minern abgelehnt wird
3. signiert die Manipulation
4. sendet seine Transaktion an ihn bekannte Miner, damit diese zu einen Block hinzugefügt wird.

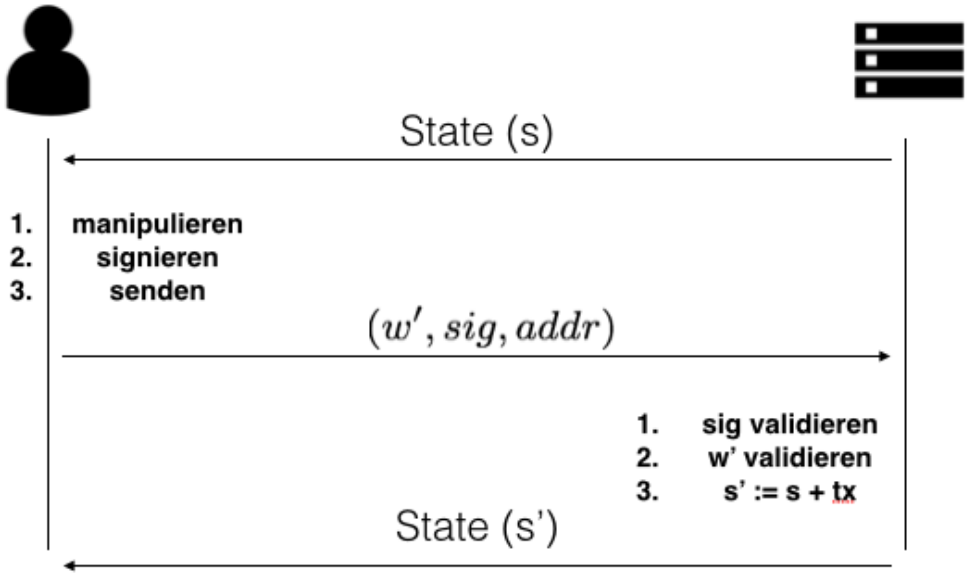


Abbildung 2.2: Interaktion eines Akteurs mit einer dao.

Der Miner:

1. bekommt von unterschiedlichen Quellen Transaktionen
2. die Signatur jeder Transaktion wird validiert: ist der angegebene Akteur auch ihr Erzeuger?
3. die Manipulation des derzeitigen Zustandes wird validiert: ist die Manipulation des aktuellen Zustandes nach den aktuellen Regeln valide?
4. falls die Signatur und Manipulation valide ist, wird der derzeitige zustand aktualisiert und die Transaktion wird der Menge valider, bekannter Transaktionen hinzugefügt, die vom Miner in den nächsten Block hinzugefügt werden sollen.
5. Der Miner versucht nun nach dem "Proof of *"Mechanismus eine Berechtigung vom Netzwerk zu erhalten um seinen privaten Konsens zum allgemeinen Konsens der DAO zu machen.

Wie bereits erwähnt benötigt ein Akteur für das Agieren in der Ethereum DAO ein Bestand an der Interner Währung. Wie viel, hängt von der Komplexität

der ausgelösten Transaktion ab: Für jeden Berechnungsschritt wird ein kleiner Betrag erhoben. Ist nicht genügend Wert verfügbar, terminiert die Transaktion und wird vom Netzwerk abgelehnt. So wird auch das Halteproblem umgangen.

> [...] halting problem: there is no way to tell, in the general case, whether or not a given program will ever halt. [...] our solution works by requiring a transaction to set a maximum number of computational steps that it is allowed to take, and if execution takes longer computation is reverted but fees are still paid.
>
> (Ethereum Whitepaper p. 28 [But14])

Eine Ethereum interne DAO besteht aus einem assoziativem Speicher der den Programmcode sowie Daten beinhaltet. Sie besitzt eine Adresse und hat einen Bestand an interner Währung: Ether.

Ein Beispiel für eine interne DAO ist eine dezentrale Währung, wie sie derzeit vom Bitcoin repräsentiert wird (Quelle [But14]):

```
1  from = msg.sender
2  to = msg.data[0]
3  value = msg.data[1]
4
5  if self.storage[from] >= value:
6  self.storage[from] = self.storage[from] - value
7  self.storage[to] = self.storage[to] + value
```

Ein weiteres Beispiel ist ein dezentrales DNS System wie ihn die Namecoin DAO implementiert:

```
1  if !contract.storage[msg.data[0]]:
2      contract.storage[msg.data[0]] = msg.data[1]
3      return(1)
4  else:
5      return(0)
```

Diese beiden Beispiele illustrieren wie vergleichsweise einfach es ist eine DAO auf einer bestehenden Plattform, wie der von Ethereum, zu erstellen, anstadt der bisherigen Blockchain-Basierten Ansätzen.

Kapitel 3

selbst-Modifikation-Schicht einer DAO

Durch eine Plattform wie Ethereum wird nun das Erstellen von DAOs um ein vielfaches leichter gemacht, jedoch gibt es noch keine einheitliche Lösungsansätze um die DAOs oder generell dezentrale Inhalte ebenfalls auf eine dezentrale Weise zu erstellen oder diese zu modifizieren. Es Fehlt einer Entkopplung der DAO von den Regeln, wie diese von den Inhabern gerecht, also proportional zu ihrem Besitz, Manipuliert werden können.

Derzeit werden DAOs, entweder von einer einzelnen Schlüsselperson, einer Organisation (wie bei Bitcoin die "Bitcoin-Foundation"[1]) oder einem Unternehmen (wie bei Ethereum Ëthereum Switzerland GmbH"[2]) entwickelt und manipuliert. Trotz der dezentralen Natur der DAOs ist die Kontrolle über diese noch Zentralisiert.

Der Besitz von Bitcoin und Ethereum lässt sich nicht determinieren. Falls man die interen Tokens aus der Blockchain Schicht ebenfalls als Besitzanteil an den DAOs interpretiert, so können die Besitzer nicht über die Manipulationen der Regeln der DAO mitentscheiden.

Das Problem ist in der Community jedoch bekannt. Im Juni 2014 hat Oliver Janssens, einer der Early-Adopter von Bitcoin ein Preisgeld von 100 000 USD in BTC an denjenigen ausgeschrieben, der ein Konzept vorschlägt, wie die Bitcoin Foundation auf dezentrale weise abgelöst werden kann.

[1] https://bitcoinfoundation.org/ 25.02.2015
[2] https://www.ethereum.org/ 25.02.2015

> The Bitcoin foundation [...] is internally recreating the same archaic political system that fails to work for society. Bitcoin is the currency of the internet generation. It puts the power back into the hands of the people. You cannot expect its main representative organisation to be exactly the opposite: A non-transparent, political and secretive elite.
>
> (Reddit - Oliver Jansens http://redd.it/25sf4f 19.02.2015)

Der Gewinner war die Bitcoin-Basierte dezentrale Crowdfunding Plattform Lighthouse[3]. Diese erfüllt nicht wirklich die Ansprüche an eine solche selbst-Modifikationsschicht. Der Mechanismus einer solchen Schicht muss einerseits eine große Anzahl an Stimmberechtigten Kandidaten (derzeit wurden rund 200k Bitcoin Adressen verwendet) berücksichtigen sowie eine ähnlich große Menge an Vorschlägen. Er sollte schnell und agil auf aufkommende Probleme reagieren können, jedoch niedrige Einstiegsbarrieren für Benutzer besitzen. Die Besitzverteilung sollte genau determiniert sein und die Manipulation der DAO gerecht - also proportional zu dem Besitz.

Im folgenden möchte ich meinen Vorschlag einer solchen Schicht vorstellen. Hierfür werden wir als erstes die theoretischen Komponenten betrachten, dann ihre Anwendung auf die regulären Grammatiken und schließlich ihre Implementation.

Theoretisch kann eine solcher Mechanismus durch ein **initialisiertes Transitionssysthem** $T = (M, I, \tau)$ nach [Gla] modelliert werden. Hierzu muss eine passende Zustandsmenge definiert werden, einen Initialzustand sowie die Übergangsfunktion, die valide Manipulationen (Transitionen) der DAO beschreibt.

Durch die Dezentralisierung-Schicht wird sichergestellt, dass Transitionen **immer** von einem Akteur a ausgelöst werden und das dieser Akteur ebenfalls ihr Urheber ist. Damit besitzen eine Transition die Form (a, O'). O' beinhaltet dabei die Manipulationen des Akteurs.

[3] https://www.vinumeris.com/lighthouse

3.1 Definition

In der selbst-Modifikation-Schicht können wir davon ausgehen, dass für die Dezentralität der DAO bereits gesorgt ist. Es handelt sich entweder selbst um eine Blockchain-Basierte DAO oder eine, die eine Plattform wie Ethereum benutzt. Insofern gilt die DEzentralität im folgenden als gegeben.

Eine DAO in einer Grammatik G ist ein Tupel $O_G = (A, K, <, share, vote)$ bestehend aus:

1. eine endliche Menge von Akteuren A
2. eine eindeutige **Besitzverteilung** von Akteuren zur DAO

$$share : A \to \mathbb{N}$$

3. eine endliche Menge von validen **Kandidaten** mit mindestes einem Element

$$K_G \subseteq L(G) \wedge |K_G| \geq 1$$

4. eine strickte Totalordnung der Kandidaten

$$<\subset K \times K$$

5. eine Bewertung der Kandidaten durch die Akteure.

$$vote : A \times K \to [0, 1]$$

Sei $\mathbf{DAO_G} = \{O_G \mid O_G$ ist DAO in der einer Grammatik $G\}$ die Menge aller DAOs in der Grammatik G.

Zudem existiert eine Konsensfunktion die eine DAO in ein valides Wort überführt.

$$consens : DAO_G \to L(G)$$

3.2 Diskussion der Eigenschaften

3.2.1 Kandidaten

Der Hier verfolgte Ansatz ist nur DAOs in regulären Grammatiken zu Betrachten. Diese Eigenschaft schränkt die Menge der möglichen Kandidaten ein. Zu der Kandidatenmenge existiert eine strickte Ordnungsrelation, die die Reihenfolge angibt, in der die Kandidaten hinzugefügt wurde.

3.2.2 Besitzverteilung

Die Besitzverteilung wird ähnlich dem Aktienmarkt Modelliert. Dabei hat eine DAO ein bestimmte Anzahl an Teilen (geschrieben $|O_G| \in \mathbb{N}$), die unter den Akteuren aufgeteilt sind.

Die Funktion $share : A \to \mathbb{N}$ gibt den Anteil von O_G an, der im Besitz von einem Akteur ist.

$$|O_G| := \sum_{a \in A} share(a)$$

Der Besitz einer DAO O_G wird durch das Recht definiert, dieses Kontrollieren zu können[Wal04]. Ist der Besitz unter mehreren Akteuren aufgeteilt, so gibt der Anteil am Objekt an, zu welcher Gewichtung jeder einzelne Akteur über die DAO mitbestimmen kann.

Eine Konsensfunktion entscheidet schließlich über die Ausführung der Kontrolle.

Für die Bestimmung der Besitzverteilung können einerseits die Tokens benutzt werden, die in der Dezentralisierung-Schicht verwendet werden. Andererseits können auch neue eingeführt werden. Für den Blockchain basierten Ansatz der Dezentralisierung muss bei getrennten Besitz-Tokens jedoch sicher gestellt werden, dass die Tokens der Blockchain-Schicht einen Wert für die Miner und damit eine motivierende Funktion am Mining-Prozess teilzunehmen besitzen.

3.2.3 Konsens

$$consens : DAO_G \to L(G)$$

Die Konsensfunktion überführt jede DAO in ein Wort der $L(G)$ Sprache. Dabei sucht die Funktion nach dem Kandidaten aus der Kandidatenmenge mit der maximalsten Bewertung. Die Bewertung eines Kandidaten ergibt sich dabei durch die Summe der gewichteten Bewertungen der Akteure. Falls mehrere Kandidaten die maximale Bewertung besitzen, wird der älteste Kandidat genommen.

$$value(k) := \sum_{a \in A} share(a) \cdot vote(a, k)$$

$$consens(O_G) := min_<(\{k|\ value(k) = \max_{k' \in K_G}(value(k'))\})$$

3.2.4 Beispiel einer DAO

Im folgenden ein Beispiel einer DAO $O^1_{G_{abc}} := (A, K, <, share, vote)$ für die Grammatik G_{abc} definiert wie in 2.1.

$$A = HASH \tag{3.1}$$

$$h_1 = 1HTN35UxBFTbcN8g2KfXC6TW2ipbytsysh \tag{3.2}$$

$$h_2 = 16iF9qZWG1tKhnjnX5KKCYdYdLv4A1FQ4b \tag{3.3}$$

$$h_3 = 1P3wGbbgDgLxivHw5BGGbLCHugsHBnjnjP \tag{3.4}$$

$$share : hash \mapsto \begin{cases} 10 & |hash = h_1 \\ 7 & |hash = h_2 \\ 6 & |hash = h_3 \\ 0 & |otherwise \end{cases} \tag{3.5}$$

$$K = \{aaaaa, aac, aacc, aaccc\} \tag{3.6}$$

$$aaaaa < aac < aacc < aaccc \tag{3.7}$$

$$vote : hash, k \mapsto \begin{cases} 1.0 & |hash = h_1, k = aaaaa \\ 0.9 & |hash = h_2, k = aacc \\ 0.9 & |hash = h_3, k = aacc \\ 0.9 & |hash = h_2, k = aaccc \\ 0.9 & |hash = h_3, k = aaccc \\ 0 & |otherwise \end{cases} \tag{3.8}$$

$$consens(O^1_{G_{abc}}) = aacc$$

3.2.5 Qualitätskriterien

Für die Implementation ist auf folgende Qualitätskriterien zu achten:

RESMIN:
Es sind möglichst wenig Ressourcen (Speicher und Rechenleistung) vom Ethereum-Netzwerk notwendig, um Transaktionen zu validieren.

INTMIN:
Eine Akteur soll möglichst wenig Interaktionen benötigen, um auf eine gewünschte, von ihm erreichbare Manipulation zu kommen.

3.3 Grammatikerweiterung

Als Zustandsmenge für das Transitionssystem können wir nun die Menge aller möglichen DAOs nehmen. Allerdings muss man die Menge für die Implementation codieren sowie die Validitätsbedingungen auf der codierten Menge definieren. Eine passende Codierung die wir näher betrachten wollen ist eine DAO zu einem Wort einer Sprache zu machen. Diese Sprache nennen wir **Metasprache** der ursprünglichen Sprache ($L(G)$). Eine Bedingung muss jedoch sein, dass das Wort ohne Verlust von Informationen wieder zurück zur selben DAO decodiert werden kann. Damit können wir Transitionsbedingungen als Manipulationen des codierten Wortes definieren.

Da die Wörter der codierten DAOs ebenfalls valide und invalide Teile der Wörter der ursprünglichen Sprache ($L(G)$) erkennen müssen und somit die Metasprache konstruierende Grammatik, ebenfalls die ursprüngliche Grammatik beinhalten muss, wird eine Funktion S angegeben, die die ursprüngliche Grammatik G so erweitert, dass diese zur gesuchten Metasprache wird $L(S(G))$.

Formaler gesagt muss eine Funktion $S : REG \to CFG$ gefunden werden, zusammen mit den Funktionen $\phi : DAO_G \to L(S(G))$ und $\phi^{-1} : L(S(G)) \to DAO_G$ für die die Eigenschaft $\phi \circ \phi^{-1} = id_{DAO_G}$ gilt.

Da die Funktion S, ϕ sowie ϕ^{-1} viele Komponenten haben, werden sie inkrementell eingeführt: Zuerst wird S_1, ϕ_1, ϕ_1^{-1} definiert, diese codieren und decodieren die Kandidatenmenge einer DAO in ein Wort. Anschließend wird die Besitzverteilung sowie die Kandidatenbewertung ebenfalls eingearbeitet, sodass wir die gesuchten Funktionen erhalten.

3.3.1 Codierung der Kandidatenmenge

Die reguläre Grammatik wird so zu einer kontextfreien Grammatik erweitert, dass alle Wörter aus der Kandidatenmenge in einem Wort der erweiterten Grammatik codiert werden können.

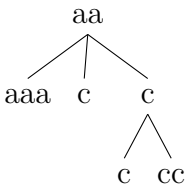
Dazu muss es eine Grammatik-Erweiterung $S_1 : REG \rightarrow CFG$ gefunden werden. Um zu zeigen, dass es sich bei S_1 um die gesuchte Erweiterung handelt, muss die Existenz der Funktionen $\phi_1 : P(L(G)) \rightarrow L(S(G))$ und $\phi_1^{-1} : L(S(G)) \rightarrow P(L(G))$ gezeigt werden, für die die Bedingungen $\phi_1 \circ \phi_1^{-1} = id_{P(L(G))}$ erfüllt ist.

Dieses kann mit Hilfe eine Trie-Datenstruktur realisiert werden, die redundant auftauchende Präfixe der Kandidaten zusammengefasst. Die preorder-Serialisierung der Tries ist eben ein Wort der Metasprache, die durch die Grammatikerweiterung S_1 konstruiert wird:

Sei $T(K_G)$ die Trie Datenstruktur, die die Menge K_G codiert. Wir wissen, dass es eine Funktion $c : K_G \mapsto T(K_G)$ sowie $c^{-1} : T(K_G) \mapsto K_G$ existiert, für die $c \circ c^{-1} = id_{P(L(G))}$ gilt [Mor68]. Zu finden ist demnach ein Isomorphismus $s : T(K_G) \mapsto w \in L(S_1(G))$ sowie $s^{-1} : w \in L(S_1(G)) \mapsto T(K_G)$ die ein Trie serialisieren und deserialisieren. Da ein Trie ein Baum ist wird für die Serialisierung einfach die preorder Notation verwendet, die bekannterweise Isomorph ist. Damit haben wir die Funktionen $\phi_1 := c \circ s$ sowie $\phi_1^{-1} := c^{-1} \circ s^{-1}$ gefunden.

Dieses möchten wir anhand eines Beispiels für die Sprache $L(G) = \{a^x b^y c^z \mid x, y, z \in \mathbb{N}\}$ und die Kandidatenmenge $\{aaaaa, aac, aacc, aaccc\}$ illustrieren.

Sei $T(K_G)$ die Trie Datenstruktur, die die Kandidatenmenge K_G codiert:



Mit der dazugehörigen preorder-Serialisierung die $[,]$ als Klammerzeichen sowie & als Trennzeichen verwendet:

$$aa[aaa\&c\&c[c\&cc]]$$

Für die grammatik-erweiternde Funktion S_1 wird an jedem Ableitungsschritt in der Grammatik G eine Mehrdeutigkeit zugelassen. Dafür werden die Produktionsregeln folgendermaßen erweitert:

$$P_{Options} := \{R \to [O_R], O_R \to r\&O_R, O_R \to r \mid R \to r \in P \wedge r \in \Sigma^*\}$$

Diese Mehrdeutigkeit ($[O_R]$) nennen wir **Optionsmenge** sowie die darin enthaltenen Elemente (r) **Option**.

Eine solche Grammatikerweiterung erzeugt eben die Serialisierung einer Trie welche eine Menge valider Worte codiert:

$$aa[aaa\&c\&c[c\&cc]] \in L(S_1(G))$$

3.3.1.1 Grammatik-Erweiterung S1

Sei $G = (N, T, S, P)$ eine reguläre Grammatik.

$$\begin{aligned} S_1(G) &:= (N', T', S, P') \\ N' &:= N \cup \{O_R \mid (R \to r) \in P \wedge O_R \notin \Sigma\} \\ T' &:= T \cup \{[,],\& \mid [,],\& \notin \Sigma\} \\ P_{Options} &:= \{R \to [O_R], O_R \to r\&O_R, O_R \to r \mid R \to r \in P \wedge r \in \Sigma^*\} \\ P' &:= P \cup P_{Options} \end{aligned}$$

TODO: ist hier ein formaler Beweis notwendig?

3.3.2 Codierung der Besitzverteilung

Die Akteure lassen sich durch ein 20-Byte String genau identifizieren. Sei $HASH$ die Menge aller 20-Byte Strings. Im Folgenden werden die Hash-Strings in der Base58[4] Notation angegeben. Die Besitzverteilung ist eine Auflistung aller beteiligter Akteure sowie deren Anteile an der DAO. Sei $hash \in HASH$ sowie $number \in \mathbb{N}$.

$$P_{Acteurs} := \{A \to [hash\ number]A, A \to \varepsilon\}$$

Eine Beispiel-Verteilung ist:

$$\begin{aligned} h_1 &= 1HTN35UxBFTbcN8g2KfXC6TW2ipbytsysh && (3.9)\\ h_2 &= 16iF9qZWG1tKhnjnX5KKCYdYdLv4A1FQ4b && (3.10)\\ h_3 &= 1P3wGbbgDgLxivHw5BGGbLCHugsHBnjnjP && (3.11)\\ a &= [h_1\ 10][h_2\ 7][h_3\ 5] && (3.12)\\ A &\to^* a && (3.13) \end{aligned}$$

In diesem Beispiel gehören Akteur h_1 - 10 Anteile, h_2 - 7 Anteile und h_3 - 5 Anteile. Somit ist die DAO - Größe 22 Anteile.

3.3.3 Codierung der Kandidatenbewertung

Um jede DAO ohne Verlust von Information codieren zu können, muss jede mögliche Bewertungsverteilung von Akteuren und Kandidaten im Metawort enthalten sein können. Dieses kann erreicht werden, wenn die Bewertung der Kandidaten (V) an Optionen gebunden sind ($O_R \to r\&\ [V]O_R$). Da es für jeden Kandidaten aus der Kandidatenmenge genau eine Option gibt, die nur diesem Kandidaten zugeordnet ist (ein Blatt eines Tries), lässt sich jede Bewertungsverteilung des Kandidaten codieren, wenn sie dieser Option zugeordnet sind. Zusätzlich möchten wir Bewertungen einer Option zulassen, die mehreren Kandidaten zugeordnet sind. Dies sind solche, die wiederum eine Optionsmenge beinhalten. Wenn ein Akteur eine Option in einer Optionsmenge bewertet, so gibt er seine Stimme der Option im Kontext zu

[4] https://en.bitcoin.it/wiki/Base58Check_encoding 26.02.2015

dem bisherigen Präfix des Wortes. Die Bewertung dieser Option wird als ein Attribut in der Ableitung Synthetisiert[Knu68] und damit jeweils von einer Bewertung einer tieferen Ebene ersetzt.

Sei $FLOAT = [0, 1]$ die Menge der maschinell darstellbaren Fließkommazahlen zwischen 0 und 1: $float \in FLOAT$

$$P_{Voting} := \{V \to [hash\ float]V, V \to \varepsilon\}$$

Ein Beispiel ist:

$$\begin{aligned} h_1 &= 1HTN35UxBFTbcN8g2KfXC6TW2ipbytsysh && (3.14)\\ v &= [h_1\ 1.0] && (3.15)\\ V &\to^* v && (3.16)\\ O_R &\to^* r\&[v] && (3.17) \end{aligned}$$

3.3.4 Codierung der Delegationen

Für die Minimierung der Interaktion(INTMIN) wird transitives Abstimmen zugelassen. Akteure können nicht nur für die Option selbst abstimmen, sondern auch ihre Stimme für Optionsmengen an andere Akteure delegieren. Diese können im Kontext der delegierten Option für den Akteur mitbestimmen.

Ein solcher Akteur kann wiederum entweder eine Person, ein Zusammenschluss von Personen wie eine Interessengemeinschaft in Form einer DAO oder eine DAO ohne Fremdeinwirkung sein, die bestimmte Werte zu optimieren versucht.

Delegationen werden für Optionsmengen vererbt. Durch die lineare Struktur der Worte ergibt sich eine strickte Totalordnung der Delegationen, womit bei konkurierenden Delegationen immer die Delegation niedrigerer Ordnung genommen wird. Eine Stimme des Akteurs selbst, wird einer Stimme eines Deleganten vorgezogen.

$$P_{Delegations} := \{D \to [hash\ hash]D, D \to [hash\ hash]\}$$

Eine Beispiel-Verteilung ist:

$$h_2 = 16iF9qZWG1tKhnjnX5KKCYdYdLv4A1FQ4b \quad (3.18)$$
$$h_3 = 1P3wGbbgDgLxivHw5BGGbLCHugsHBnjnjP \quad (3.19)$$
$$d = [h_2\ h_3] \quad (3.20)$$
$$D \rightarrow^* d \quad (3.21)$$

3.3.5 Vollständige Grammatik-Erweiterung S

$$S(G) := (N', T', S', P') \quad (3.22)$$
$$N' := N \cup \{O_R | (R \rightarrow r) \in P \wedge O_R \notin N\} \cup \{D, A, S'\} \quad (3.23)$$
$$T' := T \cup \{[,], \&, |\ [,], \& \notin \Sigma\} \cup HASH \cup NUMBER \cup FLOAT \quad (3.24)$$
$$P_{Acteurs} := \{A \rightarrow [hash\ number]A, A \rightarrow \varepsilon \quad (3.25)$$
$$| hash \in HASH, number \in NUMBER\} \quad (3.26)$$
$$P_{Options} := \{R \rightarrow [O_R][D], O_R \rightarrow r\&\ [V]O_R, O_R \rightarrow \varepsilon \mid R \rightarrow r \in P \wedge r \in \Sigma^*\} \quad (3.27)$$
$$P_{Start} := \{S' \rightarrow [A][O_S][D]\} \quad (3.28)$$
$$P_{Delegations} := \{D \rightarrow [hash\ hash]D, D \rightarrow [hash\ hash] | hash \in HASH\} \quad (3.29)$$
$$P_{Voting} := \{V \rightarrow [hash\ float]V, V \rightarrow \varepsilon | hash \in HASH, float \in FLOAT\} \quad (3.30)$$
$$P' := P \cup P_{Options} \cup P_{Start} \cup P_{Delegations} \cup P_{Voting} \cup P_{Acteurs} \quad (3.31)$$

3.3.6 Beispielwort

Das zugehörige Metawort zur DAO $O^1_{G_{abc}}$ definiert wie in 3.2.4 $\phi(O^1_{G_{abc}}) = w \in L(S(G))$ ist:

$$consens(w) = aacc$$

```
1   [
2     [h_1  10]
3     [h_2  7]
4     [h_3  5]
5   ]  [
6     aa[
7       aaa&[h_1  1.0]
8       c&[]
9       c[
10        c&[]
11        cc&[]
12      ][]&[h_3  0.9]
13    ][h_2  h_3]&[]
14  ][]
```

Abbildung 3.1: Metawort $w \in L(S(G))$

3.3.7 Konsens

Nach dem die Kandidaten, die Akteure sowie ihre Anteile und die Bewertung der Kandidaten durch die Akteure in der Metasprache enthalten sind, erlaubt dies den Konsens der DAO als Interpretation des Wortes der $L(S(G))$ Sprache zu definieren.

$$consens : L(S(G)) \to L(G)$$

Die Idee hier ist, dass die transitive Hülle der Delegationen als Attribut während der Ableitung vererbt(inherited) wird. Die Stimmenge wird hingegen als Attribut synthetisiert.[Knu68] Delegationen zusammen mit den Stimmen quantifizieren jede Option aus einer Optionsmenge und wählen eine Konsens-Option mit den Maximalsten Stimmen niedrigster Ordnung.

3.4 Transitionssystem

Zur Wiederholung besteht ein Transitionssystem $T = (M, I, \tau)$ aus einer Zustandsmenge M, einem Initialzustand I und einer Übergangsfunktion τ. Nach dem wir nun die Zustandsmenge als Metasprache $M = L(S(G))$ sowie

die Codierung und Decodierung einer DAO in ein Wort der Metasprache gefunden haben, widmen wir uns der Übergangsfunktion τ.

Als Initialzustand wird ein beliebiges Wort aus der Metasprache verwendet, welches weder Stimmen, noch Delegationen beinhaltet.

$$I = \{s_0 \in L(S(G))\}$$

Wir werden uns auf die Manipulation der Kandidatenmenge sowie der Kandidatenbewertung beschränken. Weitere Manipulationen werden in Aussicht gestellt. Valide Manipulationen der Kandidatenmenge soll das Erstellen und das Erweitern von Optionsmengen sein. Für die Kandidatenbewertung sollen das Hinzufügen und Entfernen der eigenen Stimmen sowie der eigenen Delegationen für Optionsmengen valide sein.

Falls die Besitzverteilung von der Blockchain-Schickt übernommen wird, greift die Dynamik dieser Schickt ebenfalls auf den derzeitigen Zustand des Metawortes. Wir möchten uns jedoch auf solche DAOs beschränken, bei denen die Besitzverteilung ausschließlich in der Selbstmanipulation-Schicht manipuliert wird. Hier möchten wir das Überweisen eines Akteurs von eigenen Anteilen an einen anderen Akteur zulassen.

3.4.1 Aktualisierung

Durch die Blockchain-Schicht ist jede Interaktion mit einer DAO eindeutig und nachweislich einem Akteur zugeordnet. Demnach ist jede Aktualisierung des derzeitigen Zustandes $w := s_i$ ein Tupel $\delta = (a, w')$ mit $hash = a \in A = HASH,\ w' \in L(S(G))$.

Sei $\Delta \subseteq A \times L(S(G))$ die Menge aller vom Miner gesehenen Aktualisierungen, die noch nicht auf Validität überprüft wurden und somit nicht Teil seines privaten Konsenses sind.

Akteure können jederzeit die Aktualisierungsmenge erweitern in dem sie eine Aktualisierung an einen Miner schicken:

$$\Delta' := \Delta \cup \{(a, w')\}$$

3.4.2 Transformation

Sei $\Delta \neq \emptyset$

$$\tau(w) = \begin{cases} w' & \exists(a, w') \in \Delta \wedge \beta(a, w, w') = true \\ w & andernfalls \end{cases}$$

Nach jeder Transformation wird die Aktualisierungsmenge ebenfalls aktualisiert, in dem die für die Transformation verwendete Aktualisierung entfernt wird. Wurde keine Aktualisierung verwendet, so sind alle Aktualisierungen invalide:

$$\Delta' = \begin{cases} \Delta \setminus \{(a, w')\} & (a, w') \text{ wurde in der Transformation verwendet} \\ \{\} & andernfalls \end{cases}$$

3.4.3 Validierung der Aktualisierung

Um die Validität einer Transformation zu testen, wird das derzeitige Wort w zusammen mit dem auslösenden Akteur a sowie seinem manipuliertem Wort w' betrachtet. Die Transformation ist valide, falls eines der folgenden Fälle zutrifft.

3.4.4 Manipulation der Kandidaten

Eine Optionsmenge kann an jeder Position im Wort erzeugt oder erweitert werden, solange das neu vorgeschlagene Wort, ein Wort der Metasprache ist, sowie die Bewertungen der Kandidaten nicht verändert werden.

$$\begin{aligned} (A, K', share', vote') &= \phi^{-1}(w') \\ \wedge (A, K, share, vote) &= \phi^{-1}(w) \\ \Rightarrow vote &= vote' \qquad (3.32) \\ w' &\in L(S(G)) \qquad (3.33) \end{aligned}$$

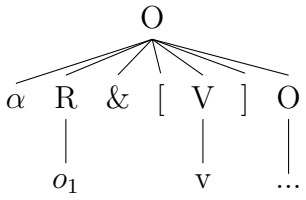
Die neu hinzukommenden Optionen dürfen keine Delegationen oder Stimmen enthalten, sowie noch nicht in der bisherigen Optionsmenge enthalten sein.

3.4.4.1 Erzeugen einer Optionsmenge

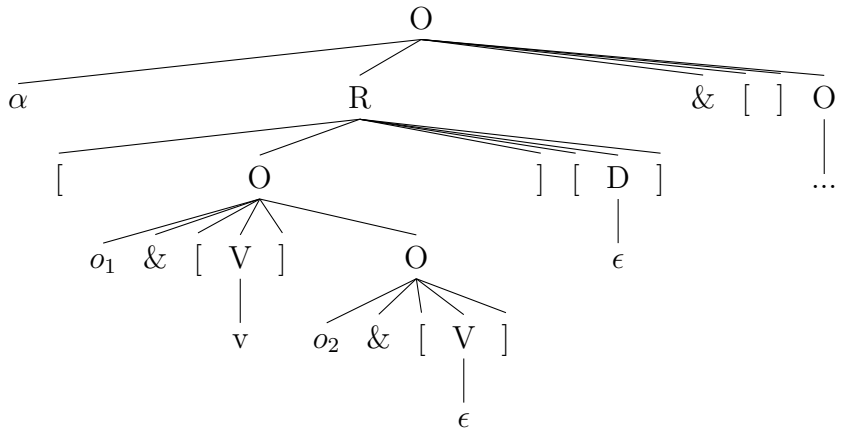
Sei $S(G) = (T', N', S', P')$ eine erweiterte Grammatik. Sei weiter $O, S' \in N'$ sowie $v, o_1, o_2 \in T'^*$, $o_1 \neq 0_2$ und $0 \leq i \leq j \leq n$ mit $i, j, k, n \in \mathbb{N}$

$$
\begin{aligned}
w &= w_{0..i-1}\ w_{i..j}\ w_{j+1..n} && (3.34)\\
w_{i..j} &= \alpha o_1 \& [v] && (3.35)\\
O &\rightarrow^* \alpha R \& [v] && (3.36)\\
R &\rightarrow^* o_1 && (3.37)\\
S' &\rightarrow^* w_{0..(i-1)}\ O\ w_{(j+1)..n} && (3.38)\\
R &\rightarrow^* o_2 && (3.39)\\
w' &= w_{0..i-1}\ \alpha[o_1 \& [v] o_2 \& [][]][]\ w_{j+1..n} && (3.40)
\end{aligned}
$$

Für w hat O folgende Struktur:



Für w' besitzt O folgende Struktur:



Dabei muss o_2 frei von Delegationen und Stimmen sein.

TODO: ist hier ein Beweis das die Kritärien nicht verletzt werden notwendig?

3.4.4.2 Erweitern einer Optionsmenge

Sei $o, d, r \in T'^*$ sowie $R, O_R \in N'$

$$
\begin{aligned}
w &= w_{0..i-1}\ w_{i..j}\ w_{j+1..n} && (3.41)\\
w_{i..j} &= \alpha[o][d] && (3.42)\\
R &\rightarrow^* w_{i..j} && (3.43)\\
O_R &\rightarrow_P^* o && (3.44)\\
O_R &\rightarrow^* r && (3.45)\\
w' &= w_{0..(i-1)}\ \alpha[or\&[]][d]\ w_{(j+1)..n} && (3.46)
\end{aligned}
$$

r muss dabei Delegations- und Stimmfrei sein sowie neu:

$$
\begin{aligned}
(A, K', share', vote') = \phi^{-1}(w_{0..i-1}\ \alpha[r\&[]][d]\ w_{j+1..n}) && (3.47)\\
\wedge(A, K, share, vote) = \phi^{-1}(w) && (3.48)\\
\Rightarrow K' \cap K = \emptyset && (3.49)
\end{aligned}
$$

3.4.5 Manipulation der Kandidatenbewertung

Sei für alle Manipulationen $a \in HASH$ der auslösende Akteur.

3.4.5.1 Hinzufügen einer Stimme

Sei $b_1, b_2, v, r \in T'^*$

$$
\begin{aligned}
w &= w_{0..i-1}\ w_{i..j}\ w_{j+1..n} && (3.50)\\
v &\neq b_1 a b_2 && (3.51)\\
w_{i..j} &= r\&[v] && (3.52)\\
w' &= w_{0..i-1}\ r\&[v[a\ n]]\ w_{j+1..n} && (3.53)
\end{aligned}
$$

3.4.5.2 Löschen einer Stimme

Sei $v_1, v_2 \in T'^*$ sowie $n \in \mathbb{N}$

$$
\begin{aligned}
w &= w_{0..i-1}\ w_{i..j}\ w_{j+1..n} && (3.54)\\
w_{i..j} &= r\&[v_1[a\ n]v_2] && (3.55)\\
w' &= w_{0..(i-1)}r\&[v_1\ v_2]w_{(j+1)..n} && (3.56)
\end{aligned}
$$

3.4.5.3 Hinzufügen einer Delegation

Da die Reihenfolge der Delegationen wichtig ist, für die Auflösung konkurrierender Delegationen, daher ist das Hinzufügen einer Delegation an jeder Stelle in einer Delegationsmenge möglich.

Sei $o, d_i \in T'^*$ sowie $h' \in HASH$ und $h \neq a$

$$
\begin{aligned}
w &= w_{0..i-1}\ w_{i..j}\ w_{j+1..n} && (3.57)\\
u, v &\in \{w | w = ([h_1\ h_2])^* \text{ mit } h_1, h_2 \in HASH\} && (3.58)\\
w_{i..j} &= [o][uv] && (3.59)\\
w' &= w_{0..(i-1)}\ [o][u[a\ h']v]\ w_{(j+1)..n} && (3.60)
\end{aligned}
$$

Löschen einer Delegation

Sei $o, d_i \in T'^*$ sowie $h' \in HASH$

$$
\begin{aligned}
w &= w_{0..i-1}\ w_{i..j}\ w_{j+1..n} && (3.61)\\
u, v &\in \{w | w = ([h_1\ h_2])^* \text{ mit } h_1, h_2 \in HASH\} && (3.62)\\
w_{i..j} &= [o][u[a\ h']v] && (3.63)\\
w' &= w_{0..(i-1)}\ [o][uv]\ w_{(j+1)..n} && (3.64)
\end{aligned}
$$

3.4.6 Überweisung von Anteilen

Ein Akteur kann seine Anteile an einen Anderen überweisen. Dabei müssen die Fälle unterschieden werden, ob der Empfänger bereits Anteile hält, bei dem Fall wird die Überweisungssumme seinen Beständen addiert, oder ob es sich um einen neuen Akteur handelt. Dieser wird mit der Überweisungssumme neu hinzugefügt.

Sei $h' \in HASH$ mit $h' \neq a$ sowie $l, m, n \in \mathbb{N}$

TODO: hier ist zum ersten mal nicht die Symbolkonkatination gemeint sondern die Interpretation der werte(+,-), muss das als Interpretation geschrieben werden?

$$w = w_{0..i-1}\ w_{i..j}\ w_{j+1..n} \tag{3.65}$$

$$b_1, b_2, b_3, b_4, b_5, b_6 \in \{w | w = ([h\ n])^* \text{ mit } h \in HASH \text{ und } n \in \mathbb{N}\} \tag{3.66}$$

$$w_{i..j} = [b_1 b_2 b_3 [a\ n] b_4 b_5 b_6] \tag{3.67}$$

$$m' = (m + l) \tag{3.68}$$

$$n' = (n - l) \tag{3.69}$$

$$n - l \geq 0 \tag{3.70}$$

$$\text{Fall 1:} \quad b_2 = [h' m] \tag{3.71}$$

$$w' = w_{0..(i-1)}\ [b_1 [h' m'] b_3 [a\ n'] b_4 b_5 b_6]\ w_{(j+1)..n} \tag{3.72}$$

$$\text{Fall 2:} \quad b_5 = [h' m] \tag{3.73}$$

$$w' = w_{0..(i-1)}\ [b_1 b_2 b_3 [a\ n'] b_4 [h' m'] b_6]\ w_{(j+1)..n} \tag{3.74}$$

$$\text{Fall 3:} \tag{3.75}$$

$$w' = w_{0..(i-1)}\ [b_1 b_2 b_3 [a\ n'] b_4 b_5 b_6 [h' l]]\ w_{(j+1)..n} \tag{3.76}$$

Kapitel 4

Implementation

Implementiert wurde im Rahmen dieser Arbeit eine zentralisierte Version einer selbst-Modifikation-Schicht einer DAO, welche eine regulären Grammatik besitzt. Die Dezentralität wurde erst einmal ignoriert, da die Funktionsweise der Selbst-Modifikation im Vordergrund steht. Jedoch sind alle Grundlagen dafür gelegt die hier erarbeitete Lösung auf Ethereum oder eine andere Turing-Vollständige DAO Platform zu portieren und damit zu dezentralisieren.

4.1 Architektur

Ziel der Implementation ist einerseits eine lauffähige Implementierung des Konzeptes. Andererseits einem Benutzer zu ermöglichen mit Anwendungsbeispielen zu experimentieren: reguläre Grammatiken anzulegen sowie diese mit der Angabe der Besitzverteilung und eines Initialwortes zu einer DAO zu machen. Implementiert ist die Interaktion mit der DAO Selbst-Modifikation-Schicht wie in 2.6.2 beschrieben. Ein Akteur kann dabei entweder eine vorhandene DAO manipulieren oder eine neue erstellen. Technisch wurde hier eine Klassische Client-Server Architektur benutzt4.1. Dafür wurde das MeteorJS[1] Web Framework verwendet welches auf NodeJS[2] basiert - einem serverseitigen JavaScript Compiler. Für die Datenspeicherung wird MongoDB[3] verwendet -

[1] http://meteor.com 25.02.2015
[2] http://nodejs.org/ 25.02.2015
[3] http://www.mongodb.org/ 25.02.2015

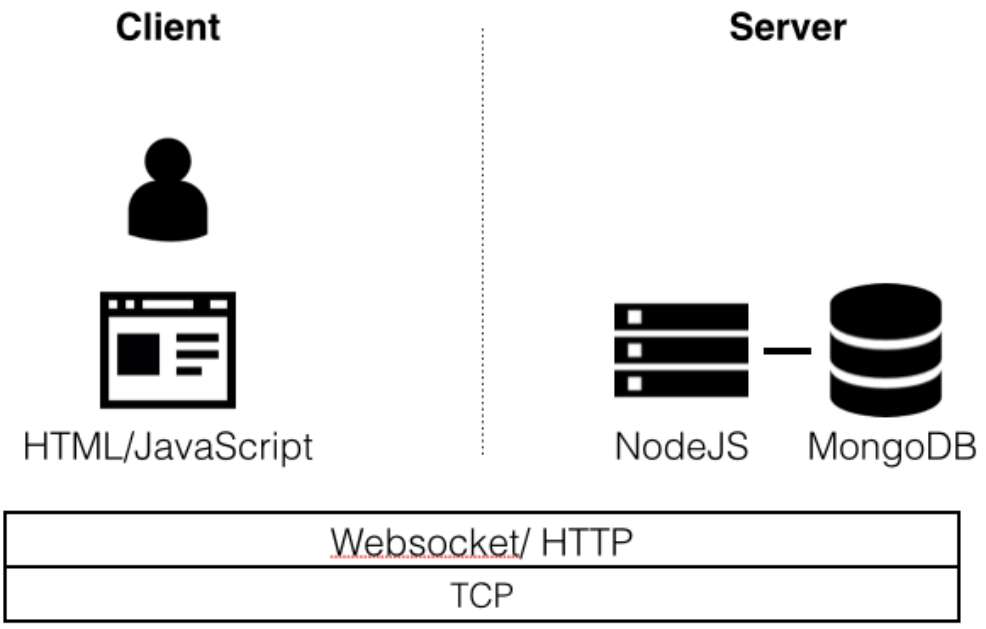


Abbildung 4.1: Benutzte Technologie

eine NoSQL Datenbank. Der Client kommuniziert über HTTP und WebSocket mit dem Server.

Das Datenmodell ist in 2 Bereiche unterteilt: Einerseits die DAOs und andererseits die Grammatiken.

Ein Akteur hat nun die Möglichkeiten

1. vorhandene Grammatiken aufzulisten
2. eine vorhandene Grammatik zu inspizieren
3. eine neue Grammatiken hinzuzufügen
4. DAOs aufzulisten
5. den Aufbaue und die Historie einer DAO einzusehen
6. eine DAO zu manipulieren
7. eine neue DAO zu erstellen

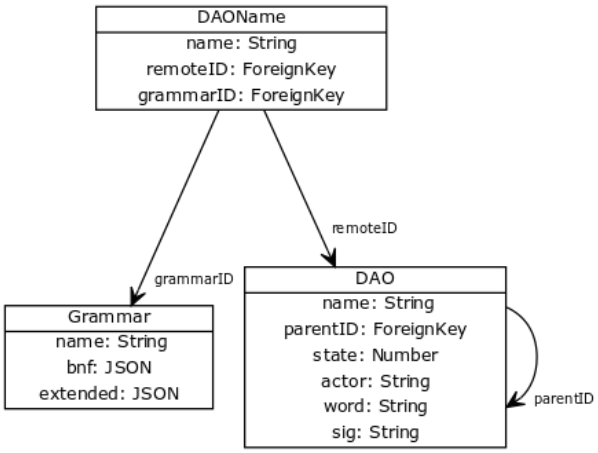


Abbildung 4.2: Datenmodell

Für die Signierung wird die Bibliothek BitcoinJS-lib[4] verwendet. Sie stellt die notwendigen ECDSA sowie SHA Funktionen zu Verfügung. Für dem Umgang mit Grammatiken und Worten wird JISON[5] eine JavaScript Portierung des Bison/Flex LALR(1) Parser-Generators verwendet.

BitcoinJS-lib stellt notwendige kryptografische Funktionen bereit: das Erstellen von einem Private-Key auf Basis eines Strings, das erstellen eines Public-Key und einer Adresse auf Basis des Private-Keys, das Signieren von Nachrichten mit einem Private-Key sowie das Verifizieren von Nachrichten mit ihrer Signatur und einer Adresse. Dieses deckt alle Funktionen ab, die für die sichere Kommunikation von einem Akteur und der DAO notwendig sind.

4.1.1 Metasprache

Für das erzeugen von Parsern wird der Parser-Generator JISON so erweitert, dass dieser bei Eingabe einer regulären Grammatik G einen Parser für die zur Grammatik zugehörigen Metasprache erzeugt. Dieser Parser interpretiert eine Wort der $L(S(G))$ Sprache als ein Parse Baum Objekt (PTO). Eine Grammatik wird als Bison Grammatik (Figure 4.4) in der EBNF Schreibweise angegeben.

Das Parse Baum Objekt besitzt folgende Funktionen:

[4]https://github.com/bitcoinjs/bitcoinjs-lib 26.02.2015
[5]http://zaach.github.io/jison 26.02.2015

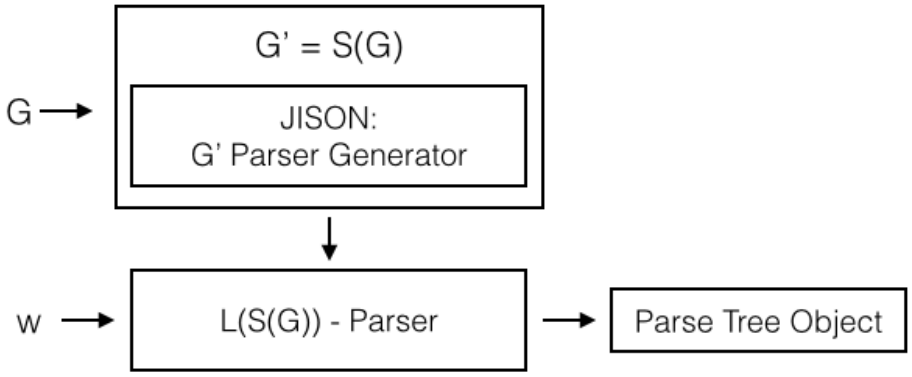


Abbildung 4.3: Grammatikerweiterung und Parser Generator

toString wandelt das Parse Baum Objekt wieder um in ein Wort der Metasprache, das dieses Parse Baum Objekt konstruiert.

getConsensString wählt den Konsens-Kandidaten aus: wendet die Konsensfunktion an und liefert ein Wort der $L(G)$ Sprache zurück.

validate erhält ein weiteres (PTO), die eine Manipulation des derzeitigen PTOs beinhaltet, sowie eine Akteur-Adresse und überprüft ob die Manipulation des derzeitigen PTOs vom Akteur valide ist.

add erhält ein Wort w der $L(G)$ Sprache und fügt es dem Derzeitigen PTO hinzu. Diese Operation fügt der DAO einen neuen Kandidaten hinzu.

getCandidates liefert K_G der DAO zurück: ein Array aller Kandidaten mit ihren Bewertungen. Dadurch lässt sich leicht die Funktion *vote* rekonstruieren.

```
1  %lex
2  %%
3  \s                              /* IGNORE */
4  (a)                             return 'a'
5  (b)                             return 'b'
6  (c)                             return 'c'
7  .                               return 'INVALID'
8  /lex
9
10 %start A
11 %%
12
13
14 A: 'a' A | 'a'
15   | 'b' B | 'b'
16   | 'c' C | 'c'
17   | ;
18
19 B: 'b' B | 'b'
20   | 'c' C | 'c';
21
22 C: 'c' C | 'c';
23 %%
```

Abbildung 4.4: Bison Grammatik für die Sprache $L(G) = \{a^x b^y c^z | x, y, z \in \mathbb{N}\}$

Aufgaben

Kapitel 5

Zusammenfassung und Ausblick

5.1 Anwendung auf kontextfreie Grammatiken

Eine interessante Anwendung des hier vorgestellten Ansatzes einer selbst-Modifikation-Schicht ist die Anwendung auf die kontextfreien Sprachen. Damit können alle Programmiersprachen zumindest Syntaktisch abgebildet werden. Dieses ist jedoch nicht Trivial. Das Problem hierbei ist die Kodierung der Kandidatenmenge. Auf Grund der Limitierung der Ableitungsregeln kann ein Ableitungsbaum einer regulären Grammatik keine Knoten haben, die mehrere Kinder mit Nichtterminalen Besitzen(Äste). Somit ist der Ableitungsbaum eine lineare Struktur. Dieses ermöglicht die Konstruktion eines Präfixbaumes bei dem Äste als Optionen angesehen werden. Zwar lässt sich die Zusammenfassung der Kandidaten bei kontextfreien Grammatiken mit der selben Methode anhand des Ableitungsbaumes konstruieren, jedoch multiplizieren sich die Optionen in unterschiedlichen Kindern eines Knotens. Dadurch gilt die in 3.3.1 geforderte Bedingung $\phi_1 \circ \phi_1^{-1} = id_{P(L(G))}$ nicht, da Optionen hinzu kommen. Ebenfalls lässt sich nicht jede Kandidatenbewertung durch das Anhängen an Optionsknoten codieren.

Betrachten wir einmal das Beispiel der Sprache $L(G) = [ab][abc]$ mit der konstruierenden Grammatik:

$$
\begin{aligned}
G &= (T, N, P, S) && (5.1)\\
T &= \{a, b\} && (5.2)\\
N &= \{S, B\} && (5.3)\\
P &= \{S \to BB, B \to a, B \to b\} && (5.4)
\end{aligned}
$$

Die Kandidatenmenge $K_1 = ab, ac, ba$ Sowie das anhand des Ableitungbaumes valide Metawort:

$$[A][a\&[v_1]b\&[v_2]][][a\&[v_3]b\&[v_4]c\&[v_5]][]][]$$

Die sich aus dem Metawort bildenden Kandidaten sind: $K_2 = \{aa, bb, ab, ba, ac, bc\}$

Weiter gibt es kein Mechanismus der jedes mögliche Kandidatenbewertung in der Sprache darstellen kann: Es stehen in diesem Beispiel 5 Bewertungsvariablen für 6 Kandidaten zur Verfügung.

5.2 Dezentralisierung

Wie bereits erwähnt ist die Dezentralisierung der selbst-Manipulation-Schicht der DAO z.B. durch eine Portierung auf die Ethereum Plattform der nächste notwendige Schritt.

5.3 Anonymisierung

Durch die Pseudonüme Natur der Anteilseigener lassen sich Rückschlüsse darüber ziehen, welcher Akteur für welche Option abgestimmt hat. Dadurch lässt sich der Konsens manipulieren in dem auf strategisch wichtige Akteure Druck ausgeübt wird um ihre Stimme zu ändern. Auch wird das Abstimmverhalten der Anteilseigener beeinflusst, da diese fürchten könnten ihre Pseudonümen Status verlieren zu können. Die Anonyme Wahl ist ebenfalls ein Kriterium für demokratische Wahlen in vielen Organisationen, sodass eine Anonymisierung

der Abstimmung eine weitere erstrebenswerte Erweiterung ist. Diese Anonymisierung könnte durch Homomorphe Verschlüsselung[Gen09] oder durch andere kryptografische Mittel realisiert werden. Siehe dazu [FDL07].

5.4 Manipulation der Besitzverteilung

Derzeit ist die Größe einer DAO fest, sodass die einzige Möglichkeit an Anteile zu gelangen, diese von Anderen überwiesen zu bekommen ist. Eine mögliche Erweiterung währe die der Erschaffung neuer Anteile. Diese können entweder von der DAO verkauft oder anhand festgelegter Regeln herausgegeben werden. Ein Beispiel Regelsatz währe das binden an Optionsmengen. Derjenige Akteur erhält die neuen Anteile, dessen vorgeschlagene Option für eine bestimmte Dauer den Platz der Konsens-Option einnimmt.

Literaturverzeichnis

[But14] V Butterin. A next-generation smart contract and decentralized application platform. (January):1–36, 2014.

[CN14] The Internet Corporation and Assigned Names. Identifier Technology Innovation Panel - Draft Report. 2014.

[Eth] https://blog.ethereum.org/2014/07/05/stake/ - Proof of Stake 18.02.2015.

[FDL07] Laure Fouard, Mathilde Duclos, and Pascal Lafourcade. Survey on electronic voting schemes. *supported by the ANR ...*, 2007.

[Gen09] Craig Gentry. a Fully Homomorphic Encryption Scheme. *PhD Thesis*, (September):1–209, 2009.

[Gla] Andreas Glausch. Abstract-State Machines Eine Sammlung didaktischer Beispiele. pages 1–19.

[Knu68] Donald E. Knuth. Semantics of context-free languages. *Mathematical Systems Theory*, 2(2):127–145, June 1968.

[Lin10] Lindenberg. Konzeption und Erprobung einer Liquid Democracy Plattform anhand von Gruppendiskussionen. 2010.

[Mor68] Donald R. Morrison. PATRICIA—Practical Algorithm To Retrieve Information Coded in Alphanumeric. *Journal of the ACM*, 15:514–534, 1968.

[Nak08] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Consulted*, pages 1–9, 2008.

[Ott] Friedrich Otto. Formale Sprachen und Automaten.

[Pou14] Nicolas Pouillard. Master ' s thesis Private , trustless and decentralized message consensus and voting schemes. 2014.

[Vas15] Khushita Vasant. A Treatise on Altcoins. Technical report, 2015.

[Wal04] Jeremy Waldron. Property and Ownership. September 2004.

[Woo14] Gavin Wood. ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER. 2014.