Geheimes und öffentlich voll nachprüfbares, sicheres* E-Voting ist möglich!

Vorschlag für eine liquid-demokratische Ständige Mitgliederversammlung (SMV) und Erinnerung an wenig bekannte Liquid-Democracy-Aspekte

von Christian Jacken (www.LiquidDemocracy.de, @OriginalLiquidD), basierend auf der für die SMVcon der Piratenpartei Deutschland (9.-10.03.2013) erstellten Version, welche wiederum auf auf dem von John Washington Donoso (Pseudonym Sayke) und mir 2004 auf dem European Social Forum vorgestellten Liquid-Democracy-Konzept und -Implementationsvorschlag basiert. *Sicher bedeutet, daß nach dem Stand der Technik keine ausnützbaren technischen Schwachstellen existieren.

OpenPGP-„Schlüsselverteilungspartys" bei physischer Anwesenheit der Teilnahmeberechtigten und „Abstimmungsempfehlungen" statt Delegationen lösen wesentliche Teile des „Transparenz/Wahlgeheimnis-Konfliktes"

(Ich bitte um Verständnis, daß ich aus Gründen der Lesbarkeit/Verständlichkeit im folgenden nur zum Teil gendergerecht schreibe)

Zu der Zeit, als ich meine Vision von einem freiem elektronischen Wettbewerb der Ideen in einer frei fließenden, nicht durch unnötige Einschränkungen gehemmten Demokratie und Gesellschaft im Januar 2003 auf dem Weltsozialforum in Porto Alegre vorgestellt habe (ich wohnte damals in Brasilien und wußte noch nicht, daß Sayke sehr ähnliche Ideen hatte und wir 2004 zusammenarbeiten würden), engagierte ich mich auch dafür, daß alle brasilianischen Wahlcomputer mit einem *paper audit trail* ausgestattet werden sollten. Vor Abschluß einer jeden Stimmabgabe würde dabei der Wahlcomputer einen auf das wesentliche beschränkten ausgefüllten Stimmzettel ausdrucken, den die Wähler unter Plexiglas kontrollieren könnten, bevor er in eine Urne wandert, die am Ende des Tages manuell ausgezählt würde, um einen Vergleich mit dem vom Wahlcomputer ermittelten Ergebnis zu ermöglichen. Leider beschloß die oberste brasilianische Wahlbehörde stattdessen, die wenigen so ausgestatten Wahlcomputer zur Kostenersparnis abzuschaffen, da die Tests schließlich gezeigt hätten, daß die Wahlcomputer korrekt funktionieren würden. Nicht ohne Grund war für mich schon damals die Vorstellung von nicht öffentlich nachprüfbarem E-Voting in Verbindung mit manupulierbaren Online-Diskussionen ein Albtraum (mit Nachprüfbarkeit meine ich harte Nachprüfbarkeit mit mathematischen Verfahren und nicht bloß Anscheins-„Beweise").

Während nicht alle Probleme des Zielkonfliktes zwischen geheimen Abstimmungen/Datenschutz und maximaler Transparenz/Sicherheit lösbar sind, gibt es m. E. einen Kompromiss, der nur zu geringen Einbußen an Liquid-Democracy-Features führt und dennoch eine mindestens gleichwertige Sicherheit im Vergleich zu herkömmlichen Abstimmungen bietet. Selbst bei letzteren wird allerdings auch in Deutschland mutmaßlich weitaus häufiger betrogen als allgemein angenommen, weswegen ich den Einsatz von Wahlcomputern mit *paper audit trail* begrüßen würde, solange Wähler auf Wunsch auch weiterhin nach dem alten Verfahren abstimmen könnten.

Auch bei dem in diesem Paper „LD-SMV" genannten System dürfte natürlich niemand zur Teilnahme gezwungen werden, ist doch die Entscheidung, einem solchen sicherheitsbedingt notwendigerweise komplexen Verfahren zu vertrauen, eine recht persönliche. Andererseits wäre der Aufwand unverhältnismäßig groß, wenn man versuchen würde, im elektronischen Zeitalter greifbar gewordenene Partizipationsmöglichkeiten über herkömmliche Wahlverfahren zu ermöglichen. Damit aber die LD-SMV-Ablehner dennoch fair beteiligt und eingebunden bleiben, könnten diese z. B. über eine herkömmliche Abstimmung Delegierte in die LD-SMV entsenden, sofern dies rechtlich in Deutschland zulässig ist. Dies ist jedoch fragwürdig, da dadurch später manche Teilnehmer doppelt (als normale LD-SMV-Teilnehmer und als Delegierte) abstimmen könnten. Um dieses und das im nächsten Absatz erwähnte Problem zu umgehen, schlage ich generell statt der Wahl von Delegierten bzw. der Delegation von Stimmen den Einsatz von Abstimmungsempfehlungen vor wie ursprünglich von Sayke's Liquid-Democracy-Konzeption vorgesehen. Abstimmungsempfehlungen kann jeder Teilnehmer unter seinem Klarnamen oder Pseudonym unter Wahrung einer bestimmten Form

veröffentlichen (bei den LD-SMV-Ablehnern würde eine Stimme für einen bestimmten Abstimmungsempfehlungsveröffentlicher bedeuten, daß diese Stimme bei allen künftigen Abstimmungen innerhalb eines bestimmten Zeitraums automatisch gemäß der jeweiligen Abstimmungsempfehlungen des gewählten Abstimmungsempfehlungsveröffentlichers gezählt wird). Eine der Form entsprechende Abstimmungsempfehlung ist dabei wie eine wählbare Option auf dem Stimmzettel. Diese kann auch darin bestehen, der Abstimmungsempfehlung einer anderen Person zu folgen usw. (das Äquivalent zu Delegationen ab dem 2. Grad) oder gerade um dies zu vermeiden lieber einer anderen Person zu folgen, die nicht empfiehlt, einer anderen Person zu folgen (vgl. auch das Prinzip der übertragbaren Einzelstimmgebung (STV), für dessen Einführung bei Bundestagswahlen die Macher von wahlreform.de übrigens bereits vor dem Bundesverfassungsgericht mit sehr guten Argumenten gegen die jetzige Ausgestaltung der 5%-Hürde klagten; leider zeigte dieses (noch) nicht die gleiche Sensibilität für politische Minderheiten wie sein brasilianische Äquivalent STJ, welches 2006 der Einführung einer Sperrklausel trotz lobbyistischer Bemühungen der großen Parteien die rote Karte zeigte).

Mittels Abstimmungsempfehlungen läßt sich auch der Konflikt umgehen, der dadurch entsteht, daß auf Grund der unterschiedlichen Stimmengewichte ab der 1. Delegationsebene das Wahlgeheimnis oft nicht mehr gewährleistet werden kann, wenn das Auszählen der Stimmen (einschließlich der Delegationen) weiterhin von außen kontrollierbar sein soll (Beispiel: Teilnehmer Y erhält 17 Delegationen. Im *audit trail* kann nachvollzogen werden, daß jemand mit 18 Stimmen (eigene Stimme + 17 Delegationsstimmen) für x gestimmt hat => es ist naheliegend, anzunehmen, daß es Y war.) §15(2) des Parteiengesetzes sieht aber auf Antrag jederzeit geheime Abstimmungen vor. Über Abstimmungsempfehlungen bleibt das Wahlgeheimnis eines jeden Einzelnen (auch der Abstimmungsempfehlenden) gewahrt, da diese ja auch die Möglichkeit haben, entgegen ihrer Empfehlungen abzustimmen, was jedoch im Gegensatz zu einem Delegiertensystem keine Auswirkungen auf die eigene Abstimmungsempfehlung hat. Ferner kann jeder zwar sehen, daß bestimmte Wähler bestimmten Abstimmungsempfehlungen folgen; dank Public-Key-Kryptographie (s. weiter unten) kann aber niemand wissen, welche Wähler dahinterstecken.

Nach diesen einleitenden Überlegungen nun konkreteres zur Sicherheitsarchitektur meines Vorschlages für eine liquid-demokratisch SMV, wobei ich mich auf die wichtigsten Aspekte beschränken möchte (nicht technisch Versierte mögen bitte die zu technischen Stellen überfliegen). Zuvor möchte ich aber noch erwähnen, daß Sicherheit stets ihren Preis hat, dieser aber weitaus geringer ist als der Schaden, der allein schon durch langfristig negative Berichterstattung über die Nutzung eines unsicheres Systems entstehen würde, bis es vermutlich am Ende wie die früher in Deutschland eingesetzten Wahlcomputer sowieso eingemottet wird.

1. Zunächst benötigen wir einen Hauptserver (betrieben von der Bundes-IT unter Aufsicht eines gewählten Sicherheitsgremiums), beliebig viele unabhängig betriebene Kontrollserver (z. B. einer zukünftigen „AG LD-Audit“, „Parteilose Wahlprüfer e.V.“ etc.) und/oder das Usenet als öffentlichen Speicherort, bei dem einmal heraufgeladene Daten nur schwer gelöscht werden können.

2. Auf „Schlüsselverteilungspartys“, an denen nur LD-SMV-Teilnahmeberechtigte bzw. klar als solche gekennzeichnete Beobachter teilnehmen dürfen, werden mit Hilfe eines öffentlich geprüften und bereitgestellten Skriptes für die freie Software GnuPG auf den Notebooks der Teilnahmeberechtigten große Mengen an öffentlichen OpenPGP-Schlüsseln samt geheimen Passphrasen erstellt. (Eine Variante wäre, diese Schlüssel auf dem unter 2.3.5. erwähnten Computer zu erstellen und anschließend zu verlosen, was jedoch sicherheitstechnisch eine Schwachstelle darstellen würde.)
   2.1. Mit einem OpenPGP-Schlüssel kann nur derjenige, der auch im Besitz der passenden Passphrase ist, eine Datei (hier „elektronische Stimmzettel“, Abstimmungsempfehlungen oder Diskussionsbeiträge) digital signieren; es kann jedoch jeder, der auf einen öffentlichen Schlüssel und eine damit signierten Datei (oder einer Kopie von beiden) Zugriff hat, mit GnuPG mit an absoluter Sicherheit grenzender Wahrscheinlichkeit mathematisch feststellen lassen, ob diese wirklich mit diesem Schlüssel signiert und danach nicht verändert wurde.
   2.2. Für Nachkömmlinge bzw. Teilnahmeberechtigte, die nicht zu einer Schlüsselverteilungsparty erscheinen konnten, gibt es weitere Termine, die aber u.a. zum Schutz des Wahlgeheimnisses eine möglichst hohe Zahl an Teilnehmern aufweisen sollen.
   2.3. Am Ende haben alle LD-SMV-Teilnahmeberechtigte
      2.3.1. einen Schlüssel samt Passphrase, der zur Signierung von Diskussionsbeiträgen und Abstimmungsempfehlungen unter dem Klarnamen und Mitgliedsnummer verwendet werden kann (bis auf Widerruf gültig);

2.3.2. einen Schlüssel samt Passphrase, der zur Signierung von Diskussionsbeiträgen und Abstimmungsempfehlungen unter einem beim ersten Einsatz frei wählbaren eindeutigen Pseudonym verwendet werden kann (bis zur nächsten allgemeinen Schlüsselverteilungsparty gültig);

2.3.3. eine große Zahl von Schlüsseln samt Passphrases, die zur Signierung einzelner anonymer Diskussionsbeiträge verwendet werden können (jeweils nur für einen Diskussionsbeitrag gültig);

2.3.4. eine große Zahl von Schlüsseln samt Passphrases, die zur Signierung einzelner Stimmzettel verwendet werden können (jeweils nur für eine Abstimmung gültig);

2.3.5. eine große Zahl an Keyrings mit den Schlüsseln aller Teilnehmer des Typs 2.3.1, 2.3.2, 2.3.3 (je fortlaufend nummerierte Diskussion ein Ring) und 2.3.4 (je fortlaufend nummerierte Abstimmung ein Ring). Diese Keyrings werden auf der Schlüsselverteilungsparty im Beisein mehrerer technisch versierter Zeugen auf einem Computer mit vertrauenswürdiger Hard- und Software zusammengestellt (z. B. Debian-Live-CD, keine Festplatte, keine externe Konnektivität). Immer wenn ein Teilnehmer seine Schlüssel den Keyrings hinzugefügt hat, wird dies auf einem schriftlichen Protokoll festgehalten, damit dieser Teilnehmer im Gültigkeitszeitraum der Schlüssel an keinen weiteren Schlüsselverteilungspartys teilnehmen kann. Es wird aber mit Ausnahme von Schlüssel 2.3.1 ausdrücklich nicht vermerkt, welche Schlüssel wem gehören.

2.3.6. Alternativ könnte auch die Möglichkeit bestehen, Schlüssel auch ohne physische Anwesenheit über eine LD-SMV-Akkreditierungsstelle in die Keyrings mit den teilnahmeberechtigten Schlüsseln aufnehmen zu lassen. Dies hätte den Vorteil, daß sich bei Verlust von Schlüsseln bzw. Kompromittierung von Passphrasen die Schlüssel austauschen lassen (ansonsten kann man, wenn man ein Backup hat, sie lediglich sperren), aber auch den Nachteil, daß das Wahlgeheimnis kompromittiert werden könnte, falls jemand seinen Zugriff auf die nichtöffentlichen Daten der LD-SMV-Akkreditierungsstelle mißbraucht, und diese Daten mit den öffentlichen *audit-trail*-Daten des LD-SMV-Systems abgleicht (dies wäre das elektronische Analogon zum Bruch des Briefwahlgeheimnisses durch Öffnen des inneren Umschlages vor der Auszählung, wenn doch zunächst nur die Abstimmungsberechtigung geprüft werden soll und der innere Umschlag ungeöffnet in die Briefwahlurne gelegt werden soll). Zudem könnte die Akkreditierungsstelle versehentlich oder mißbräuchlich Unberechtigte akkreditieren, was allerdings auch bei herkömmlichen (Briefwahl-)Abstimmungen in Kauf genommen wird.

2.4. Keyrings, Diskussionsbeiträge, Abstimmungsempfehlungen und elektronische Stimmzettel werden von den Teilnehmern mit dem passenden Schlüssel signiert und z. B. unter Verwendung eines Anonymizers wie JAP/TOR an den Hauptserver, die Kontrollserver und/oder das Usenet geschickt. Der Hauptserver und die Kontrollserver signieren diese sofort (entspricht einer Empfangsbestätigung) und stellen diese umgehend (Keyrings, Diskussionsbeiträge und Abstimmungsempfehlungen) oder zeitverzögert (Stimmzettel) in themen-/abstimmungsbezogenen Containern/Verzeichnissen online.

2.5. Da die Keyrings mit allen signierberechtigten Schlüsseln (aus allen Schlüsselverteilungspartys und LD-SMV-Akkreditierungen) sowie alle Container („elektronische Wahlurnen“) mit signierten Diskussionsbeiträgen, Abstimmungsempfehlungen und elektronischen Stimmzetteln auf dem Hauptserver, den Kontrollservern und/oder im Usenet abrufbar sind, kann jeder nachprüfen, daß diese nur von zugelassenen Teilnehmern kommen, nicht verändert/manipuliert und korrekt ausgewertet wurden. Auch kann jeder Teilnehmer überprüfen, ob sich sein Diskussionsbeitrag, Abstimmungsempfehlung bzw. Stimmzettel im richtigen Container wiederfindet. Jeder Interessierte kann z. B. auch ein freies Softwaretool verwenden, das alle möglichen (oder die sinnvollsten) Kontrollen automatisiert ausführt, mit denen anderer vergleicht bzw. beim Upload von Daten (s. 2.4.) hilft. (Das Ganze hört sich jetzt für die meisten wahrscheinlich schrecklich kompliziert an; mit einem guten Benutzeroberfläche würden dies aber auch normale Computeranwender problemlos schaffen.)

2.6. Auf Wunsch kann nach Ablauf eines Schlüssels vom Typ 2.3.1 oder 2.3.2 der alte mit dem neuen Schlüssel verknüpft werden und so die Bewertungen der eigenen Aktivitäten durch die anderen Teilnehmer von vorherigen Zeiträumen („User-Karma“) übernommen werden.

2.7. Als Wahlverfahren soll möglichst die gewichtete Zustimmungswahl (*weighted approval voting)* verwendet werden, die der Schulze-Methode ähnelt, aber einen Verlust der Information vermeidet, wie stark die Wähler jeweils eine Alternative der anderen vorziehen. Wie bereits auf Seite 1 beschrieben kann der Wähler auf dem Stimmzettel aber auch vermerken, daß er der Abstimmungsempfehlung einer bestimmten Person folgen will usw. (hier sind natürlich Regeln für den Fall exzessiver Machtakkumulation bzw. der Entstehung

von Zirkelbezügen wichtig, wobei ich ersteres gar nicht so kritisch sehe, sofern die Teilnehmer die Möglichkeit haben, innerhalb einer bestimmten Frist ein Abstimmungsergebnis zu widerrufen).

Weitere, weniger technische Überlegungen

- Bei den auf „Schlüsselverteilungspartys“ erstellten Schlüsseln gibt es das Problem, daß diese vor ihrem einprogrammierten Verwendbarkeitsdatum nicht extern (also z. B. von der Mitgliederverwaltung bei Austritt des Mitglieds) deaktiviert werden können, wenn das Ex-Mitglied sich weigert, diese bei Austritt oder Verlust der Stimmberechtigung freiwillig zu sperren bzw. dies nachzuweisen, was zu größeren rechtlichen Problemen führen würde. Die Methode unter 2.3.6. ist nach meiner Auffassung aber so wie das Briefwahlverfahren gesetzeskonform.

- Leider läßt sich m. E. bei öffentlich nachprüfbarem E-Voting nicht verhindern, daß ein Teilnehmer freiwillig (oder unter Zwang) einem Dritten einen eigenen Schlüssel samt Passphrase verrät, wodurch dieser Dritte überprüfen kann, wie der Teilnehmer abgestimmt hat. Wenn man diese Möglichkeit ausschließen wollte, würde man auch dem Teilnehmer die Möglichkeit nehmen, zu überprüfen, ob seine Stimme ordnungsgemäß vom Hauptserver erhalten und gezählt wurde. Verrät der Teilnehmer jedoch niemandem den eigenen Schlüssel, bleibt das Wahlgeheimnis wie bei Papierstimmzetteln gewahrt. Eine herkömmliche Abstimmung hat allerdings den Vorteil, daß im Nachhinein (sofern man bei der Stimmabgabe nicht beobachtet oder gefilmt wurde) niemand mehr beweisen kann, wie man abgestimmt hat. Sollte jedoch jemand oder eine Gruppierung versuchen, diese soziale (nicht technische!) E-Voting-Schwachstelle in größerem Umfang auszunutzen (z. B. durch Stimmenkauf oder Gewaltandrohung), würde dies aber mit hoher Wahrscheinlichkeit auffliegen.

- Um Diskussionsbeiträge qualitativ zu filtern, würde es sich anbieten, diese zunächst einer bestimmten Zahl von nach einem fairen, kontrollierbaren Algorithmus ausgewählten Teilnehmern vorzulegen, die dann über die Qualität dieser Beiträge geheim abstimmen könnten (dafür wären zusätzliche Schlüssel notwendig). Je nachdem, wie gut ein Beitrag bewertet wurde, würde dieser im nächsten Schritt vielen, wenigen oder gar keinen weiteren Teilnehmern empfohlen usw. (alle Beiträge können natürlich auf Wunsch für immer von jedem aufgerufen werden; es geht mir hier aber um ein öffentlich nachprüfbar faires Filtersystem, damit die Teilnehmer, die überwiegend nicht so viel Zeit haben, nicht standardmäßig an Beiträgen ersticken). Während manche Beiträge in diesem System dermaßen in der Gunst der Teilnehmer steigen können, daß sie am Ende allen Teilnehmern empfohlen werden, haben andererseits mit diesem System auch Minderheitenpositionen die Chance, längerfristig „am Leben zu bleiben“ und dadurch positive Denkanstöße zu liefern.

- Die genauen LD-Regeln für Anträge, Diskussionsbeiträge etc. (wobei ich gerade an Conway's „Game of Life“ denken muß) sind natürlich eine Debatte für sich. Für mich ist Liquid Democracy auch der Versuch, die Kräfte eines freien und fairen „evolutionären“ Wettbewerbs stärker im Politisch-Kulturellen Früchte tragen zu lassen. Statt Gene und Verhaltensstrategien sind es hier Meme, die ums Überleben bzw. um ihren Platz im kulturellen Ökosystem kämpfen. Doch die wenigsten Politiker sind sich z. B. bewußt, daß Homo sapiens heute überhaupt nicht existieren würde, wenn die Evolution beispielsweise eine 5%-Hürde für neue Spezien vorgesehen hätte. Laßt uns daher bitte in Liquid-Democracy-Implementierungen die Hürden so gering wie möglich halten, und die Regeln so flexibel wie möglich!

- In einer echten Liquid Democracy gäbe es übrigens keine Parteien mehr, sondern nur noch Bündnisse zur Erreichung bestimmter Ziele. Parteien sind für mich eigentlich wie Supermärkte, in denen man nur Warenkörbe kaufen könnte. Solche wären wahrscheinlich bei den Verbrauchern nicht sehr beliebt ;) Als ich ferner darüber nachdachte, was passieren könnte, wenn sich Liquid Democracy durchsetzt (auch z. B. in Vereinen, Genossenschaften, Aktiengesellschaften etc.), schwebte mir eine „Liquid Society“ vor, in der alle wesentlichen kollektiven Diskussionen und Entscheidungen unter diskursethischen Grundsätzen (vgl. Karl-Otto Apel, Wolfgang Kuhlmann, Vittorio Hösle) per LD getroffen werden und sich jeder mit anderen zusammenschließen kann, um selbstverwaltete Mikronationen zu gründen. Ich betrachte es als ein menschliches Grundrecht, sich aussuchen zu können, in welcher Gesellschaft (Mikronation) man leben will (sofern diese einverstanden ist) bzw. eine neue Mikronation zu gründen. Auf diese Weise könnte man auch

vermeiden, daß unglaublich viel Zeit und Energie vergeudet wird, wenn immer sich zu viele Köche darüber streiten, welches Einheitsgericht gekocht werden soll (mit dem am Ende viele Bürger so oder so nicht zufrieden sein werden). Die Aufgabe eines Staates bestünde in einer vollständigen Liquid Society überwiegend darin, Menschengrundrechte, LD und das friedliche Neben- und Miteinander der Mikronationen zu sichern. Während beispielsweise das das Seasteading Institute Mikronationen auf schwimmenden Plattformen ermöglichen will, würde ich so etwas gerne irgendwo auf dem Festland ausprobieren. Welcher Staat möchte dafür ein wenig Raum und Freiheit zur Verfügung stellen? ;)

- Dies war nur ein Umriß, der aber zeigt, daß nur einen Teil der Komplexität und Philosophie des ursprünglichen Liquid-Democracy-Konzeptes allgemein bekannt ist. John und ich werden in Kürze mehr u.a. auf liquiddemocracy.de publizieren und auch erklären, warum wir das nach 2004 nicht mehr öffentlich getan haben. Übrigens: Nachdem der ursprüngliche englische Wikipedia-Artikel trotz Diskussionen 2004 wegen Irrelevanz gelöscht wurde (Lanier's Essay „Digital Maoism“ läßt grüßen ;)), wird en.wikipedia.org/wiki/Liquid_Democracy heute auf en.wikipedia.org/wiki/Proxy_voting#Delegated_voting umgeleitet. Mag jemand helfen, dies zu ändern?

Ich würde mich freuen, wenn Ihr mir unter @OriginalLiquidD und fb.com/OriginalLiquidDemocracy folgen würdet!

 Dieses Paper basiert auf auf dem von John Washington Donoso (Pseudonym Sayke) und mir 2004 auf dem European Social Forum vorgestellten Liquid-Democracy-Konzept und -Implementationsvorschlag. John und ich haben sehr änliche Konzepte von 2000-2003 unabhängig voneinander entwickelt und uns dann 2004 für ein Startup in Berlin zusamengetan, welches leider zum damaligen Zeitpunkt nicht erfolgreich war. Aus diesem Grund haben wir auch die gemeinsame Marken- und Patentanmeldung für Liquid Democracy nicht weiterverfolgt. An dieser Stelle möchte ich auch Rasmus Tenbergen erwähnen, der 2003 auf dem Weltsozialforum bereits mit einem funktionierenden Webinterface für sein World Parliament Experiment (world-parliament.org) beeindruckte, welches Delegated Voting ermöglichte. Nicht ohne Grund habe ich jedoch Sayke 2004 beigepflichtet, daß (transitive) Abstimmungsempfehlungen in manchen Fällen besser als (transitive) Stimmendelegationen sind und man deshalb besser auf Abstimmungsempfehlungen setzen sollte. Unabhängig davon wollten wir bei einer Liquid-Democracy-Implementation auch gleich einen Markt für Abstimmungsempfehlungen bzw. Delegierte und Experten einbauen (mittels Mikropayments), damit diese unabhängig von Geldern vom Staat oder der Wirtschaft sein können und damit der Übergang vom Hobbypolitiker zum Berufspolitiker barrierefreier verläuft.