WunderPass-White-Paper

G. Fricke, S.Tschurilin

November 8, 2021, Berlin

Contents

1 Abstract

TODO: Abstract

2 Einleitung

2.1 Identität

Zunächst einmal eine gänzlich kontextfreie Sicht auf den Begriff "Identität" quasi "ganz von Null". Es folgt die Wikipedia-Definition:

Definition 1: Identität

Identität ist die Gesamtheit der Eigentümlichkeiten (**"Gesamtheit persönlicher Eigenheiten"**), die eine Entität, einen Gegenstand oder ein Objekt kennzeichnen und als **Individuum** von anderen unterscheiden. In ähnlichem Sinn wird der Begriff auch zur **Charakterisierung von Personen** verwendet. [...] So folgt die rechtliche Identitätsfeststellung den für **Inklusion** und **Exklusion** relevanten Markern moderner bürgerlicher Gesellschaften.

Die nahezu philosophische Auseinandersetzung mit dem allgemeinen Verständnis der Identität wollen wir an dieser Stelle nicht weiter vertiefen und verweisen stattdessen u. a. folgende Quellen:

Quellen 1

- Confluence
- Diplomarbeit - Christian Philip Kunze

TODO: Oben zitierter Confluence-Artikel ist natürlich nicht öffentlich. Ggf. sollte man relevante Dinge daraus hier einarbeiten und den Link entfernen. Insbesondere der im Confluence thematisierte Begriff der **Identitäts-Feststellung** könnte für unsere Zwecke von Relevanz sein.

Die Deutung des Begriffs der **Identität** ist also ungemein stark abhängig von der Perspektive, aus der die Deutung erfolgt. Die Schaffung eines übergeordneten Identitäts-Verständnis - insbesondere unter Einbeziehung der **"Identitäts-Digitalisierung** - ist eine riesengroße Herausforderung. Aber gleichzeitig eine eben so große Chance. Da die eben angesprochene Digitalisierung aktuell nach wie vor größtenteils in staatlicher Hand liegt, im Folgenden noch eine weitere wesentliche (Perspektive-abhängige und etwas überspitzt formulierte) Identitäts-Definition:

Definition 2: gesellschaftliches/staatliches Verständnis der Identität

Ich bin genau der, von dem mein Ausweis behauptet, ich sei es.

2.2 Verständnis der digitalen Identität

Der Begriff der Identität ist unheimlich vielschichtig und komplex. Er kann aber auch - bei Weglassen philosophischer und subtiler Sichtweisen - intuitiv gänzlich trivial aufgefasst werden. Zumindest in der realen (analogen) Welt:

Ich bin ich! Ich trete stets mit derselben Identität auf - ob im Freundeskreis, bei der Arbeit oder beim Elternabend. Die Rollen und die relevanten Identitätsmerkmale mögen sich bei unterschiedlichen Anlässen unterscheiden, aber es bleibt dieselbe Person. Wenn man sich Geld von einem Kollegen auf Arbeit leiht, kann man es ihm auch dann zurückgeben, wenn man sich zufällig im Restaurant trifft. Weil kein Zweifel an den Identitäten der beiden Betroffenen besteht. **Dies ist in der digitalen Welt ganz anders.**

Die Definition von digitaler Identität erscheint auf den ersten Blick nahezu trivial:

Definition 3: Digitale Identität

Die digitale Identität ist nichts anderes als ein eindeutiger (technischer) Identifier/Username/Kundennummer - ein Primary Key in einer Datenbanktabelle, wo

das vermeintliche Individuum zu einer "Entität" wird.

Angereichert wird der zum technischen Identifier gehörende Entitäts-Datensatz mit zusätzlichen Properties ganz im Sinne der obigen allgemeinen Identitäts-Definition 1.

Mit ein wenig technischem Verständnis erkennt man sofort das aus der eben formulierten Definition resultierende Problem: **Diese ist nämlich in unserer aktuellen digitalen Welt alles andere als eindeutig**. Und zwar deshalb nicht, weil sie auf Datenmodellierungs-Ebene zu interpretieren ist, die jeder digitale Service-Provider für sich allein vornimmt. Der so simplen und unmissverständlich klaren Definition der *digitalen Identität* fehlt also eine winzige Kleinigkeit, deren Fehlen das Verständnis der *digitalen Identität* plötzlich von *trivial* zu *höchst komplex* hievt: **Der Forderung *global eindeutig* zu sein.**

Dieser Umstand verstärkt konsequenterweise sogar das im vorigen Abschnitt bereits aufgegriffene Problem hinsichtlich des komplexen *Identitäts-Verständnis*: **Das Identitäts-Verständnis ist stark Perspektive-abhängig**. Um dies zu verdeutlichen transformieren wir die (bereits unbefriedigende) Definition 2 in die digitale Welt und bekommen ein sehr sprechendes Analogon:

Definition 4: Online-Account = (eine) digitale Identität

Ich bin genau der, als den mich ein jeder Online-Provider in seinem Datenmodell modelliert.

Damit hat die Digitalisierung - gleichwohl sie die Mittel besäße, Abhilfe für viele Probleme im Kontext der *Identität* beizusteuern - das **Identitäts-Verständnis** sogar noch komplexer gemacht, als es vorher schon war.

Zusammengefasst:

Conclusion 1

- Eine **digitale Identität** entspricht einer (User-)Entität innerhalb der Datenmodells eines beliebigen digitalen Service-Provider.
- Es existiert keinerlei Forderung/Spezifikation/Konsens nach Einheitlichkeit oder gar Eindeutigkeit der **digitalen Identität**. Auf Grund dessen kann auch keinesfalls die Rede von **der** digitale Identität sein. Stattdessen besitzt ein Individuum zig - wenn nicht gar hunderte - digitale Identitäten.
- Es existieren keinerlei "Querverweise" zwischen der Vielzahl der digitale Identitäten eines Einzelnen, die es erlauben würden, die vielen Online-Account (= digitale Identitäten) zu einer **einzigen digitalen Identität** zu konsolidieren.

ab hier WIP

Anologie in die analoge Welt:

Aufgrund der gängigen Praxis nahezu aller Web-Service-Anbieter/Apps/Online-Shops existieren Zig - wenn nicht gar Hunderte - von digitalen Kopien meines Ichs.

Das eine Ich darf nur in dem einen Laden einkaufen, das andere nur in dem anderen. Die unterschiedlichen Ichs haben unterschiedliche Kreditkarten dabei (hinterlegte oder akzeptierte Zahlungsmittel bei unterschiedlichen Anbietern) - manche gar keine (Zahlungsmittel wird nicht akzeptiert). Einige Ichs haben ihren Ausweis dabei (Ident-Verfahren durchgeführt), andere wieder nicht. Gleiches gilt für den Führerschein (Anmeldung bei unterschiedlichen CarSharings). Und während das eine Ich bereits einen frischen Führerschein dabei hat, hat das andere noch den abgelaufenen (lange nicht benutzt und Führerschein abgelaufen). Die Ichs haben teils unterschiedliche Telefonnummern oder unterschiedliche Email-Adressen. Manche Ichs haben ihr Telefon komplett vergessen. Manche Ichs sind bereits längt tot oder kurz davor (Account verstaubt oder vergessen, überhaupt einen zu besitzen). Die Ichs sind gut vernetzt (Telefonnummern, WhatsApp, Facebook, LinkedIn, Xing), aber die einen Ichs kennen manche Leute nicht, die die anderen Ich kennen und umgekehrt. Und wenn sie irgendwie doch von der letzten Party erkennen, wissen sie plötzlich den Namen des Gegenüber nicht mehr oder auch nicht, worüber man bei genannter Party gesprochen hat.

Das alles ist eine metaphorisch polemische Darstellung des digitalen Status quo den vorherrschenden schier unendlichen Multi-Accountings in der Web2.0-Welt. Jeder Account ist das Abbild meiner Identität in die digitale Welt. Es bin immer ich, der hinter jeder dieser Identitäten steht. Jede dieser digitalen Identitäten ist fraglos eine Identität im Sinne der Definition. Sie kann gar ein detailliertes und durchaus sehr vertrauenswürdigen Abbild sein - um Fake-Identitäten soll es hierbei gar nicht gehen - aber sie ist stets eine weitere Kopie. Ich lasse also Zig und Hunderte Kopien meines Selbst in die digitale Welt raus, ohne dass sie als die Kopie derselben echten Identität erkennbar sind.

Dies kann natürlich an vielen Stellen sogar von Vorteil sein.

Einige meiner Ichs sind auf so weit voneinander entfernten Kontinenten unterwegs, dass sie sich niemals treffen oder von dem gegenseitigen Geschehen beeinflusst werden (Amazon vs. CarSharing). Andere Ichs sind wiederum so schüchtern, dass sie sehr gerne unerkannt bleiben (Datenschutz/Privatsphäre).

Alle meine Ichs, die aber stets ihre Brieftasche mit sich führen, werden gewissen Interesse daran haben, das dem einen dieser Ichs nicht das Bargeld, dem anderen die Kreditkarte und dem dritten der Ausweis fehlt. Sie würden gerne eine gemeinsame Brieftasche haben, in der ihre gemeinsame Identität für alle Zwecke bereitliegt.

TODO: Ggf. noch den Sign-Up/-In als Identifizierung einer Online-Identity einbeziehen und erklären.

2.3 Missstände der digitalen Identität

Das im letzte Kapitel beleuchtete Verständnis der *digitalen Identität* lässt bereits erahnen, dieses sei alles andere als optimal. Nicht aus technischer Sicht, nicht aus gesetzlicher Sicht und schon gar nicht aus Sicht des Anwenders. Profitierende Akteure des Status quo in diesem Kontext, sind bestenfalls diejenigen, die sich aufgrund einer etwaigen Vormachtstellung an Ineffizienzen des Gesamtsystems bereichern können, weil sie eben weniger Nachteile durch besagte Ineffizienzen erfahren als der restliche Markt. Also Google, Apple, Amazon, Facebook etc. Nur darf der Umstand, die größten Player da draußen, haben gar kein eigenes Interesse daran, das aktuelle Verständnis der *digitalen Identität* (öffentlich) zu hinterfragen, nicht darüber hinwegtäuschen, das dieses tatsächlich alles andere als optimal und sehr wohl zu hinterfragen sei.

Dies liegt in erster Linie daran, dass die Einsicht zur Notwendigkeit einer sauberen Spezifikation der digitalen Identität erst viel später reifte, als ihre praktische Notwendigkeit. Spätestens mit dem massentauglichen Vormarsch des Web 2.0, mussten von so gut wie jedem Online-Dienst Userdaten modelliert werden. Da wären Gedanken, wie wir diese hier anstellen, hellseherisch gewesen. Die heutigen Definitionen 3 und 4 entstanden also aus damaliger Sicht "by doing" und nicht etwa aus (dummen) Überlegungen.

Denn für Anbieter von Online-Diensten ist es schier unabdingbar, Daten des Users - also zumindest einen Teil der *Identität* - zu erfassen: Sei es

- im Falle eines Versandhandels: **die Lieferadresse**
- im Falle der Absicherung gegenüber Jugendlichen: **die Altersfreigabe**
- im Falle von Entgeltforderungen: **Konto- oder Kreditkartendaten**

Auch die für das Marketing Verantwortlichen eines solchen Anbieters sind vielmals an einem **registrierten und wiedererkennbaren Kunden** und an dessen Kaufverhalten interessiert. [Der letzte Absatz folgte vielen Formulierungen der Diplomarbeit "Identitäten und ihre Schnittstellen auf Basis von Ontologien in einer dezentralen Umgebung"].

Aber die ebenso suboptimale Fortentwicklung der eher ungesteuert geborenen *digitalen Identität* blieb fortan nicht nur dem "Ist-Eben-So-Gewachsen" geschuldet.

Im Gegensatz zum User war es für den Dienstanbieter meist interessanter, **Informationen über die Nutzer an zentraler Stelle vorzuhalten**, deren Kontrolle ihm selbst oblag. Denn besagte Datenerfassung - gegeben durch freiwilligen oder gar erzwungen durch verpflichtend eingeforderten Daten-Input seitens des Anwenders - ermöglichte dem Dienstanbieter die Wiedererkennung und Verfolgung des Users, bzw. das Speichern und Auslesen von identifizierenden Dateien – sogenannten Cookies – und die Vergabe von zusätzlich identifizierenden Session-IDs. Auf diese Weise ließen und lassen sich heute noch extrem große Mengen an Daten erfassen, verknüpfen und systematisch auswerten. [Der letzte Absatz folgte vielen Formulierungen der Diplomarbeit "Identitäten und ihre Schnittstellen auf Basis von Ontologien in einer dezentralen Umgebung"].

Ungeachtet dessen, wem oder was die besagte suboptimale "Geburt" und Fortentwicklung der digitalen Identität geschuldet sei, wollen wir im folgenden die konkreten Probleme und Missstände dieser aufarbeiten.

Problem 1: fehlende Eindeutigkeit

Das Problem der fehlenden Eindeutigkeit der Identität in der digitalen Welt wird am besten deutlich an dem Vergleich des sprachlichen Unterschieds zwischen den beiden Begriffen *"dasselbe"* und *"das Gleiche"*. Während ich im REWE-Supermarkt und am EasyJet-Terminal am Flughafen dieselbe Person darstelle, bin ich beim (online) REWE-Lieferdienst und beim Buchen eines Flugtickets auf der EasyJet-Homepage - aus Sicht der beiden Dienstleister - nur der gleiche Online-Konsument. Bestenfalls ist dies überhaupt erkennbar...

Ich bin mit *denselben* Personen befreundet, mit denen ich auch gleichzeitig auf WhatsApp, Facebook, LinkedIn etc. connectet, ohne dass die sichere - geschweige denn zweifellos logisch implizierte - Gewissheit besteht, dass es sich tatsächlich stets um dieselbe Person handelt. Es könnte theoretisch ja auch ein Fake-Account sein (Facebook) oder längst veraltete Telefonnummer (WhatsApp), die sich hinter der geglaubten Identität verbirgt.

Die Sicherstellung der Eindeutigkeit erfolgt stets analog: Z. B. aus einem (plausiblen) Chat-Verlauf bei WhatsApp oder einem Foto auf Instagram, wo man selbst drauf ist, was die geglaubte Identität beweist.

Dass diese *analoge Verifizierung* aber nichts taugt, zeigt spätestens das Beispiel, dass ich sowohl eine KFZ-Führerschein- als auch eine Motorboots-Führerschein-Identität habend, bei einem Alkohol-Vergehen - was gesetzlich beide Identitäten beträfe - nur an derjenigen Identität belangt werde, die im direkten Zusammenhang mit dem Vergehen stand. Weil es eben oft bürokratisch und schwierig ist zwei *gleiche* Datensätze aus unterschiedlichen digitalen Systemen zu *derselben* Person zusammenzuführen. Weil eben Gleichheit keine Eindeutigkeit garantiert.

Verkörpert wird das Problem der fehlenden Eindeutigkeit in der digitalen Welt durch den sogenannten "Sign-Up", wo ich mich mal mit meiner Email-Adresse, mal mit meiner Telefonnummer, mal mit einem frei wählbaren Nickname und mal mit Google oder Facebook registrieren kann.

Problem 2: Redundanz und fehlerbehaftete Daten

Kann heutzutage noch irgendeiner zählen, wie oft er schon sein Email-Adresse eingeben musste, um sich irgendwo zu registrieren? Und das trotz sämtlicher Browser-Autovervollständigung. Wie oft seine Adresse bei Versandhandeln? Seine Kreditkarten-Nummer oder zumindest -CVC? Ebenso werden die meisten die Konsequenzen von Umzügen in eine neue Wohnung, den Wechsel der Telefonnummer oder den Verlust

oder Ablauf einer Kreditkarte im Hinblick auf die bürokratischen Konsequenzen bei etwaigen Online-Diensten einzuordnen wissen. **Fuckup pur**.

Und das alles nur, weil unsere Daten abermals und abermals redundant von jedem Online-Service separat gespeichert werden. Ich ziehe nur einmal um, muss diese Info aber zig Mal mit Anderen teilen. ich verliere nur einmal meine Kreditkarte - und bekomme eine neue - muss dies aber an zig Stellen manuell aktualisieren. Ich wechsele meine Telefonnummer und es wird von 100 Kontakten trotzdem 10 geben, die mich deswegen nicht mehr erreichen können werden. Es wird Stellen geben, wo sich Typos in meine persönlichen Daten, meine Email-Adresse oder meine Telefonnummer einschleichen, von denen ich nichts ahne und andere Stellen, von denen ich noch nicht einmal mehr weiß, sie besäßen noch Daten von mir, die zu aktualisieren sind.

Dies ist nicht nur ein Problem beim User (Aufwand) sondern ebenso großes Problem beim Dienstleister (falsche Daten).

Problem 3: mangelhafte UX

Die heutige Existenz von zig, wenn nicht gar hunderten von Online-Accounts (= digitale Identitäten) pro User sehen wir nicht nur aufgrund der beiden eben formulierten Probleme der Uneindeutigkeit und Redundanz, sondern insbesondere auch aus User-Sicht als gänzlich unzeitgemäß und unzumutbar. Weil es eben nicht der Anspruch des digitalen Fortschritts unserer Zeit sein kann, zig und hunderte von Accounts und Passwörtern verwalten zu müssen, und diesen Missstand mit Verweis auf etwaige unterstützende Passwort-Manager auszublenden. **Was wir brauchen, sind keine Passwort-Manager oder Auto-Completion-Browser-Extensions, sondern ein grundlegendes Neudenken des digitalen Identifizierungs-Managements (Sign-up / Sign-in).**

Um den hiesigen Appell besser nachvollziehen zu können, brauchen wir einen etwas technischeren Blick auf den heute gängigen Sign-up-/Sign-in-Prozess. Für die Nutzung eines Online-Dienstes bedarf es folgender (simpler) Elemente:

- Anlegen einer neuen Online-Identität beim zugehörigen Online-Dienst (**Sign-up**) als Mapping zwischen
  - technischem Identifier beim zugehörigen Online-Dienst (Kundennummer/ Nickname/Telefonnummer/Emailadresse).
  - Userdaten
- Identifizierung mittels Eingabe des technischen Identifier, um dem zugehörigen Online-Dienst mitzuteilen, wer man ist (Teil des **Sing-in**s).
- Autorisierung mittels Eingabe des persönlichen Passworts (oder auch 2FA), um dem zugehörigen Online-Dienst zu beweisen, man sei auch tatsächlich

derjenige, als den man sich ausgibt (Teil des **Sing-in**s).

Alle dieser drei Elemente sind fraglos nötig (gleichwohl das erste genau genommen nur einmal universell für alle existierenden Online-Dienste nötig wäre; siehe auch die beiden oben adressierten Probleme), das Problem hier ist nur, dass hier viel zu viel manuelles Zutun vom User eingefordert wird und damit die besagte UX ruiniert.

Dabei ist der Status quo hinsichtlich der Autorisierung bereits auf ganz gutem (UX-)Weg. Der Stand hinsichtlich der Identifizierung ist dagegen weiterhin katastrophal! Und katastrophal heterogen und uneinheitlich noch dazu.

Problem 4: Datenschutz

TODO: ausformulieren

- meine Daten liegen an zig/hunderten Stellen gespeichert
- Hacks sind an zig/hunderten Stellen möglich

Problem 5: Daten werden nicht dort erfasst, wo sie gebraucht werden

TODO: ausformulieren

- Daten werden an anderer Stelle erhoben als sie gebraucht werden –¿ Beispiel mit der Supermarkt-Kassiererin bzw. Fluggesellschaften

Problem 6: Datenmissbrauch/Bereicherung

TODO: ausformulieren Big Tech nutzt meine Daten, um daran Geld zu verdienen. Und ich werde nicht an der Wertschöpfung beteiligt.

Problem 7: Abhängigkeit von Big Tech

TODO: ausformulieren Derzeit dominieren zentrale ID-Provider wie Google und Facebook die Verwaltung von Identitätsdaten sehr vieler IT-Dienste weltweit, was zu einer großen Abhängigkeit unserer Gesellschaft in Bezug auf den Fortgang der Digitalisierung führt.

Problem 8: Ungenutzte Möglichkeiten

TODO: ausformulieren Daten-Querverweise → Beispiel anführen
(zB aus Vorlesung zu SSI)

3 Vision

TODO: Einleitung ausformulieren

Wenn Personen auch im virtuellen Raum mehr sein wollen als Warenempfänger, Zahlende oder "Nicknames", nämlich individuelle und facettenreiche Kommunikationspartner, dann muss sich die Komplexität des digitalen Identitätskonzeptes derjenigen des realen annähern.

Im Bereich der realen Identität ist aber weder ein fest abgegrenzter Raum von zu berücksichtigenden Bereichen oder Themen, welche einer Identität zuzuweisen wären, benennbar, noch sind Standards definiert, auf denen der Informationsaustausch zwischen Individuen stattfindet. Dies macht ein umfassendes Konzept erforderlich mit den Möglichkeiten, die notwendige Flexibilität einerseits und eine Vereinheitlichung oder einen Abgleich des Informationsflusses andererseits zu gewährleisten. Dieses Konzept muss dem durch die Individualität der Identitäten gegebenen Mangel an Kompatibilität entgegentreten.

Die Umsetzung des realen Identitätskonzeptes in ein digitales Identitätskonzept muss [...] Umfassende ***Vernetzung mit direkten Verbindungen*** *und die Möglichkeit zur Nutzung von Daten in maschinenlesbarer Form erscheinen für einen möglichen Einsatz als vorteilhaft. Um dem Anwender keine Barriere in den Weg zu legen, ist es notwendig, möglichst viele Aspekte – gerade solche von struktureller und organisatorischer Natur –* ***so weit wie möglich transparent*** *zu halten.* ***Wenn der Anwender auf der einen Seite durch keinen oder nur einen minimalen Mehraufwand, aber auf der anderen Seite verschiedene Vorteile, Erleichterungen oder neue Dienste erlangt, die auf dem Konzept digitaler Identitäten aufsetzen, wäre dies eine Bewältigung eines ansonsten sicherlich auftretenden Akzeptanzproblems.*** [Auszug aus der Arbeit "Identitäten und ihre Schnittstellen auf Basis von Ontologien in einer dezentralen Umgebung"]

TODO: Aufgreifend aus vorigen Kapitel (verlinken)

Lösung 1: fehlende Eindeutigkeit

Um Eindeutigkeit der Identität bzw. Identifizierung herzustellen, bedarf es eines übereinstimmenden Konsens, welches ausreichend der relevanten digitalen Akteure

mittragen.

Der Status quo könnte in diesem Sinne gar nicht schlimmer sein. Meine digitale wird heutzutage gleichermaßen durch meine Email-Adresse, meine Telefonnummer, einen etwaigen frei wählbaren Nickname oder aber meinen Google- oder Facebook-Account repräsentiert. Wo es grad wem besser passt. Weniger eindeutig geht es also quasi kaum.

Die "Großen" haben das Problem bereits erkannt und forcieren die Eindeutigkeit gen Google-, Apple- oder Facebook-Account als eindeutige Identität. Nur ist es so, dass die sich unwahrscheinlich an einen Tisch setzen und ein gemeinsames Standard beschließen. Und wenn es am Ende nur die 4 großen GAFA-Identitäten gibt, sind es im Sinne der Eindeutigkeit 3 zu viel.

Und da eine kollaborative Festlegung auf eindeutige Identität völlig utopisch erscheint, muss eine von den Naturgesetzen vorgegebene gewählt werden. Eine, die jeder unmissverständlich und gleich interpretieren kann, ohne eine Kollaboration mit irgendwem eingehen zu müssen.

Das kryptografische Private-Public-Key-Pair scheint der perfekte Kandidat für diese Anforderung zu sein!

Lösung 2: Redundanz und fehlerbehaftete Daten

Wir möchten diesem Problem entgegnen, indem wir persönliche Daten nur an einer einzigen globalen Stelle speichern - einem Identity-Management-Service in der Blockchain.

Der User muss seine Daten dann nur an einer einzigen Stelle aktuell und sauber halten und die Datennutzer (z. B. Online-Services) können stets von Aktualität und Korrektheit ausgehen.

Lösung 3: mangelhafte UX

Wie auch bei obiger Lösung 1 sehen wir auch für dieses Problem **das kryptografische Private-Public-Key-Pair** als sehr aussichtsreiches Allheilmittel an.

Denn es ist geeignet als

- technischer Identifier mittels Public-Key,
- universelles und einheitliches Erkennungsmerkmal (**Identifizierung**) mittels Public-Key,
- sicherster "Identity-Proof" (**Autorisierung**) mittels kryptografischer Signatur (die zudem auch noch "zero-knowledge" ist, und nicht mittels Pishing gehackt werden kann).

Dies sichert uns schon einmal einen "Zero-Input-Sign-in" ("zero input" aus Usersicht; die Workflows laufen im Hintergrund ohne Zutuns des Users ab).

Gepaart mit obiger Lösung 2 kann zudem ebenso der Sign-up abgeschafft (bzw. auf eine einzige universelle und übergeordnete Registrierung für sämtliche Online-Dienste reduziert) werden - nämlich auf die einmalige Erstellung seines Wunder-Passes.

Lösung 4: Datenschutz

TODO: ausformulieren

- meine Daten liegen an einer einzigen Stelle gespeichert
- Daten sind verschlüsselt und unhackbar
- Derart ließen sich auch Identitätsdaten auf automatisierte Weise kontrolliert weitergeben. 'Kontrolliert' in diesem Zusammenhang bedeutet die Möglichkeit für den Anwender, selbst zu entscheiden, an wen er welche Daten wann und zu welchen Bedingungen übermittelt.

Lösung 5: Daten werden nicht dort erfasst, wo sie gebraucht werden

TODO: ausformulieren

- Beispiel mit der Supermarkt-Kassiererin
- Beispiel mit Amazon und der Post

Lösung 6: Datenmissbrauch/Bereicherung

TODO: ausformulieren Ich werde an der Verwendung meiner Daten monetär beteiligt (Token-Economics)

Lösung 7: Abhängigkeit von Big Tech

TODO: ausformulieren Bei Self-Sovereign Identity (SSI) oder selbstbestimmter Identität kontrollieren und besitzen Nutzer ihre digitalen Identitäten und weitere verifizierbare digitale Nachweise (Verifiable Credentials (VC)), ohne hierfür auf eine zentrale Stelle, wie etwa Facebook oder Google, angewiesen zu sein. Sie sind somit komplett unabhängig von Dritt-Instanzen und entscheiden vollkommen eigenständig, wer welche Identitätsdaten zur Verfügung gestellt bekommt, da alle Identitätsdaten ausschließlich bei ihnen gespeichert werden. Dadurch ist ein einfacher, flexibler,

sicherer und vertrauenswürdiger Austausch von manipulationssicheren digitalen Nachweisen zwischen Nutzer und Anwendungen möglich.

Lösung 8: Ungenutzte Möglichkeiten

TODO: ausformulieren Daten-Querverweise → Beispiel anführen
(zB aus Vorlesung zu SSI)

4 Unser Ansatz

TODO

5 Economics

TODO

5.1 Einleitung

Conclusion 2: unser Ökosystem generiert Value

- Wir schöpfen Mehrwert, indem wir Datenerfassung ermöglichen (die ja einen nachgewiesenen Value besitzen. Beispiele für Value durch Querverweise
- Besitzer der Daten werden entlohnt.
- Nutzer der Daten zahlen für Daten, generieren damit aber Value, der wiederum entlohnt wird.
- Am Ende haben alle Teilnehmer entweder Value generiert oder aber im Wert des values verkonsumiert
- Wir partizipieren am extrinsischen Wert des Tokens (Kurs-Entwicklung durch positive Wertschöpfung des gesamten Ökosystems).
- Incentives sind nötig, um das Henne-Ei-Problem zu lösen
- Incentives sollten nachträglich mit der dadurch geschaffenen Wertschöpfung verrechtet werden.

TODO

5.2 Goals

TODO

5.3 Quantifizierung

Einleitung - Start

Wir wollen den Mehrwert von User-Provider-Connections mittels Wunderpass einen bezifferbaren Mehrwert verleihen und diesen fundiert argumentieren. Dazu müssen wir diesen Value messen und beziffern können. Die Ergebnisse dieses Kapitels werden insbesondere für das im Kapitel 5.4.5 beleuchteten "Reward-Pools" von großer Bedeutung sein. Bzw. sogar im gesamten übergeordneten Kapitel 5.4. Einleitung - Ende

5.3.1 Grundlegende Definitionen

Sei t_0 der initiale Zeitpunkt all unserer Messungen und Betrachtungen (vermutlich der Zeitpunkt des MVP-Launches).

Darauf aufbauend betrachten wir das künftige Zeitintervall T, welches einzig an Relevanz für unser Vorhaben und alle in diesem Kapitel getätigten Ausführungen besitzt:

$$T = [t_0; \infty[$$

Der Zeitstrahl muss nicht zwingend unendlich sein. Er muss ebenfalls nicht zwingend infinitesimal fortlaufend sein und kann stattdessen je nach Kontext endlich und/oder diskret betrachtet werden. Also z. B. auch wahlweise als

$$T = [t_0; t_{ende}]$$

$$T = [t_0; t_1; ...; t_{ende}]$$

definiert sein. In letzteren beiden Fällen wird jedoch t_{ende} in aller Regel eine kontextbezogene (unverzichtbare) Bedeutung haben, die eine solche Definition des Zeitstrahls unverzichtbar macht. So könnte t_{ende} z. B. für eine mathematisch quantifizierbare Erreichung unserer Vision stehen.

Sei $\mathbf{t} \in \mathbf{T}$ fortan stets ein beliebiger Zeitpunkt, zu welchem wir eine Aussage treffen möchten.

Wir definieren die Anzahl aller zum Zeitpunkt t potenziellen User $U^{(t)}$ überhaupt und ihre (maximale) Anzahl $n^{(t)}$ als

Definition 1

$$U^{(t)} = \left\{ u_1^{(t)}; u_2^{(t)}; ...; u_n^{(t)} \right\}$$

Und ganz analog dazu ebenfalls die potenziellen Service-Provider $S^{(t)}$ und ihre (maximale) Anzahl $m^{(t)}$ als

Definition 2

$$S^{(t)} = \left\{ s_1^{(t)}; s_2^{(t)}; ...; s_m^{(t)} \right\}$$

Man beachte, dass die definierten Mengen $U^{(t)}$ und $S^{(t)}$ bzw. ihre Größe gewissermaßen den Fortschritt der Digitalisierung insgesamt beschreiben (potenzielle User brauchen einen Zugang zum digitalen Ökosystem und potenzielle Provider sind unabhängige Service-Dienstleister, die eigenmächtig darüber entscheiden, zu solchen zu werden) und in keiner Weise im Einfluss Wunderpasses stehen. Viel mehr beschreiben sie die "Umstände der Welt", mit denen WunderPass (wie alle anderen) "arbeiten" müssen.

Nun definieren den ***Connection-Koeffizienten*** zwischen den eben definierten potenziellen Usern $\mathbf{U^{(t)}}$ und den Service-Providern $\mathbf{S^{(t)}}$ zum Zeitpunkt t als boolesche Funktion $\alpha^{(\mathbf{t})}$, die über über die Tatsache *"is connected"* bzw. *"is not connected"* entscheidet:

Definition 3

$$\alpha^{(t)} : U^{(t)} \times S^{(t)} \to \{0; 1\}$$

$$\alpha^{(t)}(u, s) := \begin{cases} 1, & \text{falls User } u \in U^{(t)} \text{ mit mit Provider } s \in S^{(t)} \text{ connectet ist} \\ 0, & \text{andernfalls} \end{cases}$$

Bzw. wenn man die diskreten Auslegungen der Pools $U^{(t)} = \left\{ u_1^{(t)}; u_2^{(t)}; ...; u_n^{(t)} \right\}$ und $S^{(t)} = \left\{ s_1^{(t)}; s_2^{(t)}; ...; s_m^{(t)} \right\}$ heranzieht, alternativ als

$$\alpha_{ij}^{(t)} := \begin{cases} 1, & \text{falls User } u_i^{(t)} \in U^{(t)} \text{ mit mit Provider } s_j^{(t)} \in S^{(t)} \text{ connectet ist} \\ 0, & \text{andernfalls} \end{cases}$$

Man beachte, dass wir bei den diskreten/Aufzählungs-basierten Definitionen oben, der Übersicht halber etwas "geschlampt" haben, indem wir - klar zeitbedingte - Indizes stillschweigend als n und m bezeichnet haben, gleichwohl diese korrekterweise $n^{(t)}$ und $m^{(t)}$ lauten müssten. Nur verwirrt eben ein Ausdruck wie $u^{(t)}_{n^{(t)}}$ mehr, als dieser in seiner pedantischen Korrektheit einen Mehrwert generiert. Wir werden genannte Ungenauigkeit zudem im weiteren Verlauf in gleicher Weise fortführen und gehen davon aus, der Leser wisse damit umzugehen.

5.3.2 Zustandsbeschreibung der digitalen Welt

Mit diesen geschaffenen Formalisierungs-Werkzeugen lassen sich nun einige Dinge formal deutlich besser greifen. Und zwar zum einen im Folgenden die übergeordneten "Umstände der digitalen Welt" (auf die WunderPass bestenfalls sehr geringfügig Einfluss üben kann) aber zum anderen ebenfalls unser gesamtes Vorhaben inklusive der übergeordneten WunderPass-Vision, die in den darauf folgenden Kapitels beleuchtet wird.

Aufgrund der bereits weiter oben erwähnten nicht möglichen Einflussnahme auf die Mengen $U^{(t)}$ und $S^{(t)}$ benötigen wir noch ein weiteres Hilfsmittel, dessen Existenz wir im Folgenden einfach voraussetzen möchten - und diese mit Möglichkeiten der Markt-Analyse rechtfertigen.

Annahme 1: Digitalisierungs-Orakel

Sei $t \in T$. Anstatt die (nicht wirklich berechtigte) Kenntnis der Mengen $U^{(t)}$ und $S^{(t)}$ vorzugeben, wollen wir lieber die (realistischere) Existenz einer "Schätzfunktion" $dP^{(t)}$ (digital progress) annehmen. Wir definieren $dP^{(t)}$ als

$$dP : T \to \mathbb{N} \times \mathbb{N}$$
$$dP^{(t)} := \left(n^{(t)}, m^{(t)}\right)$$

wobei $n^{(t)} = |U^{(t)}|$ und $m^{(t)} = |S^{(t)}|$ darstellen sollen, ohne dafür zwingend die exakten Mengen $U^{(t)}$ und $S^{(t)}$ kennen zu müssen.

Und auf der letzten Annahme aufbauend der Vollständigkeit halber die aus praktischer Sicht vollkommen alternativlose Annahme ergänzen, laut der Service-Provider stets eine große Anzahl an Users ansprechen/bedienen und damit zahlenmäßig den Usern stark unterlegen sind.

[TODO1][Annahme 2 ist noch buggy]

Annahme 2: Verhältnismäßigkeit der Teilnehmer

Für alle $t \in T$ mit $\left(n^{(t)}, m^{(t)}\right) = dP^{(t)}$ gilt:

$$m^{(t)} << n^{(t)} \tag{i}$$

Diese Aussage mag zahlenmäßig noch etwas "griffiger" formuliert werden. Dafür möchten wir das Verhältnis der Größen $n^{(t)}$ und $m^{(t)}$ abschätzen: Für unseren Zeithorizont, an dessen Ende - einem ausreichend späten, aber auch nicht in unabsehbar fernen Zukunft liegenden Zeitpunkt $t_{end} \in T$ - wir von einer WunderWelt sprechen, sei die Annahme

$$\begin{aligned} n^{(t_{end})} &\approx 10 Mrd. \text{ und } m^{(t_{end})} \approx 10.000 \text{ bzw.} \\ dP^{(t_{end})} &\approx (10^{10}, 10^4) = 10^4 * (10^6, 1) \end{aligned} \tag{ii}$$

nicht ganz abwegig. Genauso wenig unvernünftig scheint die Annahme, WunderPass begänne seine Welteroberung mit einem MVP mit lediglich einem einzigen Service-Provider - z. B. dem Guard (siehe Kap. 9] - und einer überschaubaren Anzahl an angepeilten Usern, also

$$\begin{aligned} n^{(t_0)} &\approx 1.000 \text{ und } m^{(t_0)} = 1 \text{ bzw.} \\ dP^{(t_0)} &\approx (1.000, 1) \end{aligned} \tag{iii}$$

Mit den beiden zuletzt getroffenen (quantitativen) Annahmen (ii) und (iii) lässt sich auch die initiale (qualitative) Annahme (i) ebenfalls quantifizieren:

Für alle $t \in]t_0; t_{end}[$ mit $\left(n^{(t)}, m^{(t)}\right) = dP^{(t)}$ gilt:

$$1.000 = \frac{n^{(t_0)}}{m^{(t_0)}} < \frac{n^{(t)}}{m^{(t)}} < \frac{n^{(t_{end})}}{m^{(t_{end})}} = 1.000.000 \tag{iv}$$

Wir fassen Annahme 2 in einer abschließenden Definition zusammen:

Definition 4

Seien $t \in T$ und $dP^{(t)} = \left(n^{(t)}, m^{(t)}\right)$ wie in Annahme 1 beschrieben. Wie definieren die "Verhältnismäßigkeit der Teilnehmer" als

$$\sigma : T \to \mathbb{Q}$$
$$\sigma^{(t)} = \frac{n^{(t)}}{m^{(t)}}$$

Zudem halten wir fest, Annahme 2 lege nahe, man könne in der Praxis stets von

$$1.000 < \sigma^{(t)} < 1.000.000$$

ausgehen.

[ende TODO1]

5.3.3 Zustandsbeschreibung WunderPass - simple Betrachtung

Status quo

Aufbauend auf die bisher erzielten Ergebnisse, wollen wir nun auch dem Stand von WunderPass für einen beliebigen Zeitpunkt $t \in T$ einen formalisierten Charakter verleihen und definieren zunächst einmal mittels der in Def 3 beschriebenen Koeffizienten $\alpha_{ij}^{(t)}$ die sogenannten "connected Pools" von Usern und Service-Providern zum Zeitpunkt $t \in T$:

Definition 5

Wir definieren den "connected User-Pool" $\widehat{U}^{(t)} \subseteq U^{(t)}$ und den "connected Service-Provider-Pool" $\widehat{S}^{(t)} \subseteq S^{(t)}$ als

$$\widehat{U}^{(t)} := \left\{ u \in U^{(t)} \mid \exists s^* \in S^{(t)} \text{ mit } \alpha^{(t)}(u, s^*) = 1 \right\} \tag{i}$$
$$\widehat{S}^{(t)} := \left\{ s \in S^{(t)} \mid \exists u^* \in U^{(t)} \text{ mit } \alpha^{(t)}(u^*, s) = 1 \right\} \tag{ii}$$

Für die diskrete/sortierte Variante ist dies wieder gleichbedeutend mit

$$\widehat{U}^{(t)} = \left\{ \widehat{u}_1^{(t)}; \widehat{u}_2^{(t)}; ...; \widehat{u}_{\widehat{n}}^{(t)} \right\} \tag{iii}$$
$$\widehat{S}^{(t)} = \left\{ \widehat{s}_1^{(t)}; \widehat{s}_2^{(t)}; ...; \widehat{s}_{\widehat{m}}^{(t)} \right\} \tag{iv}$$

Der Wert $\widehat{n} \leq n$ beschreibt die Größe des connecteten User-Pools - also die Anzahl $\widehat{n}$ der tatsächlich mit WunderPass connecteten User unter den n potenziellen Usern.

Analog steht $\widehat{m} \leq m$ für die Anzahl der tatsächlich mit WunderPass connecteten Providern. Der Vollständigkeit halber übertragen wir das aus Def 3 stammende Verständnis der Connection-Koeffizienten auch auf die eben definierten "connected Pools"

$$\widehat{\alpha}_{ij}^{(t)} := \begin{cases} 1, & \text{falls User } \widehat{u}_i^{(t)} \in \widehat{U}^{(t)} \text{ mit mit Provider } \widehat{s}_j^{(t)} \in \widehat{S}^{(t)} \text{ connectet ist} \\ 0, & \text{andernfalls} \end{cases} \tag{v}$$

Man beachte bei den diskreten/sortierten Schreibweisen der definierten Mengen $U^{(t)}$, $\widehat{U}^{(t)}$, $S^{(t)}$ und $\widehat{S}^{(t)}$, dass in aller Regel $u_i^{(t)} \neq \widehat{u}_i^{(t)}$ und $s_j^{(t)} \neq \widehat{s}_j^{(t)}$ gelten. Die sich teils trivial aus den letzten Definitionen ergebenden Zusammenhänge fallen wir in Form eines Theorems zusammen:

Theorem 1

Seien $n = |U^{(t)}|$ und $m = |S^{(t)}|$ bzw. $(n, m) = dP^{(t)}$. Dann gelten folgende Aussagen:

$$\widehat{n} \leq n \tag{i.u}$$
$$\widehat{m} \leq m \tag{i.s}$$
$$\widehat{n} = n \Leftrightarrow \widehat{U}^{(t)} = U^{(t)} \tag{ii.u}$$
$$\widehat{m} = m \Leftrightarrow \widehat{S}^{(t)} = S^{(t)} \tag{ii.s}$$
$$\widehat{n} * \widehat{m} > 0 \Leftrightarrow \widehat{U}^{(t)} \neq \emptyset \Leftrightarrow \widehat{S}^{(t)} \neq \emptyset \tag{iii}$$
$$\widehat{n} * \widehat{m} = 0 \Leftrightarrow \widehat{U}^{(t)} = \emptyset = \widehat{S}^{(t)} \tag{iv}$$
$$\widehat{u}^{(t)} \in \widehat{U}^{(t)} \Leftrightarrow \exists \widehat{s} \in \widehat{S}^{(t)} \text{ mit } \alpha^{(t)}(\widehat{u}, \widehat{s}) = 1 \tag{v}$$
$$\widehat{s}^{(t)} \in \widehat{S}^{(t)} \Leftrightarrow \exists \widehat{u} \in \widehat{U}^{(t)} \text{ mit } \alpha^{(t)}(\widehat{u}, \widehat{s}) = 1 \tag{vi}$$

Beweis.

(i) und (ii) sind (in jeweils beiden Varianten) trivial!

zu (iii): Zunächst einmal ist

$$\begin{aligned} \widehat{n} * \widehat{m} > 0 &\Leftrightarrow \widehat{n}, \widehat{m} > 0 \\ &\Leftrightarrow |\widehat{U}^{(t)}|, |\widehat{S}^{(t)}| > 0 \\ &\Leftrightarrow \widehat{U}^{(t)}, \widehat{S}^{(t)} \neq \emptyset \end{aligned}$$

Es bleibt also nur noch $\widehat{U}^{(t)} \neq \emptyset \Leftrightarrow \widehat{S}^{(t)} \neq \emptyset$ zu beweisen. Wir beschränken uns hierbei lediglich auf "$\Rightarrow$". Die Rückrichtung erfolgt gänzlich analog. Sei also $\widehat{U}^{(t)} \neq \emptyset$.

$$\begin{aligned}\widehat{U}^{(t)} \neq \emptyset \Rightarrow \exists u^* \in \widehat{U}^{(t)} \\ \xRightarrow{Def 5} \exists s^* \in S^{(t)} \text{ mit } \alpha^{(t)}(u^*, s^*) = 1 \\ \Rightarrow s^* \in \widehat{S}^{(t)} \\ \Rightarrow \widehat{S}^{(t)} \neq \emptyset\end{aligned}$$

zu (iv): "$\Leftarrow$" ist gänzlich trivial. Die Richtung "$\Rightarrow$" folgt dagegen aus

$$\begin{aligned}\widehat{n} * \widehat{m} = 0 \Rightarrow \text{ mindestens eine der Mengen } \widehat{U}^{(t)}, \widehat{S}^{(t)} \text{ ist leer} \\ \xRightarrow{(iii)} \widehat{U}^{(t)}, \widehat{S}^{(t)} = \emptyset\end{aligned}$$

zu (v): Die Richtung "$\Leftarrow$" folgt trivial aus Def 5 und $\widehat{s} \in \widehat{S}^{(t)} \subseteq S^{(t)}$.
Für "$\Rightarrow$" mögen wir annehmen

$$\exists u^* \in \widehat{U}^{(t)} \text{ mit } \forall \widehat{s} \in \widehat{S}^{(t)} \text{ gilt } \alpha^{(t)}(u^*, \widehat{s}) = 0$$

Da jedoch laut Annahme $u^* \in \widehat{U}^{(t)}$, muss aufgrund von Def 5 ein $s^* \in S^{(t)} \setminus \widehat{S}^{(t)}$ mit $\alpha^{(t)}(u^*, s^*) = 1$ existieren. Da $u^* \in \widehat{U}^{(t)} \subseteq U^{(t)}$, muss s^* jedoch laut Def 5 auch in $\widehat{S}^{(t)}$ liegen. Im Widerspruch zu $s^* \in S^{(t)} \setminus \widehat{S}^{(t)}$.

Aussage (vi) ergibt sich ganz analog zu (v)!

□

Es ist klar, dass WunderPass sich in gewisser Weise an den definierten numerischen Messgrößen ihrer angebundenen Teilnehmer $\widehat{n}$ und $\widehat{m}$ messen können wird. Zusätzlich dazu möchten wir ein - womöglich deutlich relevanteres - numerisches Maß formalisieren. Nämlich die intuitive und sehr simple KPI "Gesamtzahl bestehender User-to-Provider-Connections" zum Zeitpunkt $t \in T$.

Definition 6

$$\Gamma : T \to \mathbb{N}$$

$$\Gamma(t) := \sum_{i=1}^{n} \sum_{j=1}^{m} \alpha_{ij}^{(t)} \text{ mit } (n, m) = \left(n^{(t)}, m^{(t)}\right) = dP^{(t)}$$

Nun beweisen wir folgende sich ergebende Zusammenhänge:

Theorem 2

Sei $t \in T$ ein beliebiger Zeitpunkt, $(n, m) = dP^{(t)}$ und $\widehat{U}^{(t)} = \left\{\widehat{u}_1^{(t)}; \widehat{u}_2^{(t)}; ...; \widehat{u}_{\widehat{n}}^{(t)}\right\}$ und $\widehat{S}^{(t)} = \left\{\widehat{s}_1^{(t)}; \widehat{s}_2^{(t)}; ...; \widehat{s}_{\widehat{m}}^{(t)}\right\}$ die connecteten Teilnehmer-Pools mit $\widehat{n} < n$ sowie $\widehat{m} < m$.

Zudem soll in Anlehnung an Annahme 2 $\widehat{m} << \widehat{n}$ gelten. Dann gelten zusätzlich auch folgende Aussagen:

$$\Gamma(t) = \sum_{i=1}^{\widehat{n}} \sum_{j=1}^{\widehat{m}} \widehat{\alpha}_{ij}^{(t)} \tag{i}$$

$$\widehat{n} \leq \Gamma(t) \leq \widehat{n} * \widehat{m} \tag{ii}$$

$$\widehat{n} = \Gamma(t) \Leftrightarrow \forall i \in \{1; ...; \widehat{n}\} \text{ gilt } \sum_{j=1}^{\widehat{m}} \widehat{\alpha}_{ij}^{(t)} = 1 \tag{iii}$$

$$\Gamma(t) = \widehat{n} * \widehat{m} \Leftrightarrow \widehat{\alpha}_{ij}^{(t)} = 1 \ \forall i \in \{1; ...; \widehat{n}\} \text{ und } \forall j \in \{1; ...; \widehat{m}\} \tag{iv}$$

Man beachte, Aussage (ii) impliziert insbesondere

$$\Gamma(t) = 0 \Leftrightarrow \widehat{n} = 0 \Leftrightarrow \widehat{U}^{(t)} = \emptyset \Leftrightarrow \widehat{S}^{(t)} = \emptyset$$

Aussage (iv) beschreibt dagegen quasi eine " ***Voll- Vernetzung***" der aktuell connecteten Teilnehmer!

Beweis.

Die Aussage (i) ist intuitiv nahezu trivial. Das explizite Vorrechnen dagegen etwas aufwendig, erfolgt aber in Grunde sehr ähnlich wie der Beweis der Aussagen (v) und (vi) des Theorems 1.

zu (ii):
$\Gamma(t) \leq \widehat{n} * \widehat{m}$ ergibt sich aus

$$\Gamma(t) = \sum_{i=1}^{\widehat{n}} \sum_{j=1}^{\widehat{m}} \widehat{\alpha}_{ij}^{(t)} \leq \sum_{i=1}^{\widehat{n}} \sum_{j=1}^{\widehat{m}} 1 = \widehat{n} * \widehat{m}$$

Nun zeigen wir $\widehat{n} \leq \Gamma(t)$. Für $n = 0$ ergibt sich die Aussage aus Punkt (iv) aus Theorem 1. Sei also $n > 0$. Dann ist

$$\Gamma(t) \overset{(i)}{=} \sum_{i=1}^{\widehat{n}} \sum_{j=1}^{\widehat{m}} \widehat{\alpha}_{ij}^{(t)}$$
$$\overset{(Def5)}{\geq} \sum_{i=1}^{\widehat{n}} 1 = \widehat{n}$$

zu (iii): "$\Leftarrow$" ist trivial.

Zu "$\Rightarrow$": Sei $\widehat{n} = \Gamma(t)$. Angenommen es gäbe ein $i^* \in \{1; ...; \widehat{n}\}$ mit $\sum_{j=1}^{\widehat{m}} \widehat{\alpha}_{i^*j}^{(t)} > 1$. Dann müsste es aufgrund der Annahme aber auch ein $i^{**} \in \{1; ...; \widehat{n}\}$ mit $\sum_{j=1}^{\widehat{m}} \widehat{\alpha}_{i^{**}j}^{(t)} < 1$ also $\sum_{j=1}^{\widehat{m}} \widehat{\alpha}_{i^{**}j}^{(t)} = 0$ geben. In diesem Fall wäre aber $\widehat{u}_{i^{**}}^{(t)} \notin \widehat{U}^{(t)}$ und somit auch $i^{**} \notin \{1; ...; \widehat{n}\}$. Widerspruch!

zu (iv): "$\Leftarrow$" ist wieder trivial.

Zu "$\Rightarrow$": Es gelte also $\Gamma(t) = \widehat{n} * \widehat{m}$. Angenommen es gäbe ein $i^* \in \{1, ..., \widehat{n}\}$ und ein $j^* \in \{1, ..., \widehat{m}\}$, sodass $\alpha_{i^*j^*}^{(t)} = 0$. Dann wäre unter Gültigkeit der Aussage (i)

$$\widehat{n} * \widehat{m} = \Gamma(t) = \sum_{i=1}^{\widehat{n}} \sum_{j=1}^{\widehat{m}} \widehat{\alpha}_{ij}^{(t)}$$
$$\leq \left(\sum_{i=1}^{\widehat{n}} \sum_{j=1}^{\widehat{m}} 1 \right) - 1 = \widehat{n} * \widehat{m} - 1 < \widehat{n} * \widehat{m}$$

Widerspruch!

□

Messbarkeit Status quo

Kommend von der intuitiven Annahme, die Größe der definierten "connected Pools" $\widehat{U}^{(t)}$ und $\widehat{S}^{(t)}$ sei irgendwie erstrebenswert in unserem Sinne, definierten wir im vorangehenden Abschnitt das - aus unserer Sicht fundierteres und geeigneteres - Maß $\Gamma(t)$, um dem Verständnis von "erstrebenswerter Zustand" besser gerecht zu werden.

In diesem Abschnitt wollen wir die - bisher eher wertfrei/objektiv formulierten - Ergebnisse des vorigen Abschnitts in den Kontext der "Erstrebenswertigkeit" stellen. Also eine formale und quantifizierbare Vergleichbarkeit unserer - ohnehin beim Lesen des letzten Abschnitts mitschwingender - Intuition schaffen, die Werte

- $\widehat{n} = |\widehat{U}^{(t)}|$,
- $\widehat{m} = |\widehat{S}^{(t)}|$ und vor allem
- $\Gamma(t)$

seien umso besser je größer sie seien. Alle der eben genannten Größen, denen wir hier eine intuitiv spürbare "Erstrebenswertigkeit" beimessen, besitzen einen klaren Zeitbezug. Daher überrascht es kaum, wir strebten die genannte quantifizierbare Vergleichbarkeit für je zwei beliebige Zeitpunkte $t_1, t_2 \in T$ an. Formale Vergleichbarkeit schreit nur so nach der mathematisch verstandenen "Ordnungsrelation":

Definition 7

Wir bedienen uns der in Definition 6 beschriebenen Funktion $\Gamma(t)$, um damit eine Ordnungsrelation auf unserem Zeitstrahl T für je zwei beliebige Zeitpunkte $t_1, t_2 \in T$ zu erhalten:

$$R_{\preceq} \subseteq T \times T \text{ mit}$$

$$R_{\preceq} := \{(t_1, t_2) \in T \times T \mid \Gamma(t_1) \leq \Gamma(t_2)\}$$

Mittels $R_{\preceq}$ erhalten wir eine Ordnung unseres Zeitstahls T und erklären zudem

insbesondere, was "erstrebenswert" bedeutet. Ein beliebiger Zeitpunkt $t_1 \in T$ ist nämlich verbal genau dann "nicht weniger erstrebenswert" in Sinne unserer Vision als ein beliebiger anderer Zeitpunkt $t_2 \in T$, falls $(t_1, t_2) \in R_{\preceq}$ gilt.

Wir schreiben fortan statt $(t_1, t_2) \in R_{\preceq}$ lieber $t_1 \preceq t_2$

Man beachte, dass es sich bei der definierten Ordnungsrelation gar um eine Totalordnung handelt! Der Form halber ergänzen wir an der Stelle noch um zwei weitere - schematisch induzierte - Relationen auf unserem Zeitstrahl T:

Definition 8

Um zusätzlich zur in Def 7 definierten Ordnungsrelation "$\preceq$", auch dem Verständnis von "echt besser" und "gleich gut" Rechnung zu tragen, definieren wir die beiden Relationen "$\prec$" und "$\simeq$"

$$R_{\prec} := \{(t_1, t_2) \in T \times T \mid \Gamma(t_1) < \Gamma(t_2)\}$$

$$R_{\simeq} := \{(t_1, t_2) \in T \times T \mid \Gamma(t_1) = \Gamma(t_2)\}$$

Bei $R_{\prec}$ handelt es sich im Übrigen wieder um eine Ordnungsrelation. Bei $R_{\simeq}$ dagegen nicht.

Auch für die letzten beiden Relationen wollen wir fortan die vereinfachte Schreibweise $t_1 \prec t_2$ und $t_1 \simeq t_2$ nutzen.

Fazit

Ungeachtet des Werts der bisher erzielten erfolgreichen Ergebnisse hinsichtlich der quantitativen Einordnung des WunderPass-Fortschritts zu einem Zeitpunkt $t \in T$, besitzt der Zusatz "...simple Betrachtung" innerhalb der Überschrift des gegenwärtigen Kapitels durchaus seine Rechtfertigung.

Wir haben zwar die Größe $\Gamma(t)$ als sehr gut geeigneten Gradmesser für den Fortschritt WunderPasses herausgearbeitet und dieses ebenfalls in Abhängigkeit der intuitiven Erfolgsmesser $\widehat{n}$ und $\widehat{m}$ gesetzt sowie nach unten und oben abgeschätzt. Jedoch scheint unser Ökosystem zu komplex und unsere bisherige Betrachtungsweise zu global geprägt, als dass wir guten Gewissens den besagten Zusatz "...simple Betrachtung" in der Überschrift des gegenwärtigen Kapitels weglassen könnten. Den geäußerten Zweifel verdeutlicht folgendes

Beispiel

Wir nehmen den Zustand zum Zeitpunkt $t \in T$ mit $\widehat{m} = 5$ angebundenen Service-Providern und als durch $\Gamma(t) \approx 50.000$ beschrieben an und schauen uns drei Szenarien an, die allesamt die getroffene Annahme hergeben:

1. Wir könnten von $\widehat{n} = 50.000$ angebundenen Usern ausgehen, von denen je 10.000 mit je einem einzigen der $\widehat{m} = 5$ Provider connectet wären und keinem anderem.

2. Genauso könnten dieselben $\widehat{n} = 50.000$ angebundene User so verteilt sein, dass 49.996 (quasi alle) mit demselben einzelnen Provider connectet sind, und die restlichen 4 (also quasi niemand) User mit je einem anderen der verbleibenden 4 Provider verbunden sind.

3. Ein ganz anderes Szenario wäre der Fall von $\widehat{n} \approx 25.000$, von denen jeder mit denselben zwei unserer fünf Service-Providern connectet wäre (und keinem anderen) und zudem ein paar vereinzelte zusätzliche User mit je einem der verbleibenden drei unserer fünf Provider.

Rein an den Größen $\widehat{n}$, $\widehat{m}$, $\Gamma(t)$ gemessen, scheint Fall (3) aufgrund von $\widehat{n} = 25.000$ der schlechteste zu sein. Rein intuitiv scheint genau dieser Fall aber der beste zu sein. Dies ist aber nur ein Gefühl. Es lassen sich ebenso gute Argumente finden, warum Fall (1) oder Fall (2) der beste sein könnten. Es kommt eben darauf an...Gleichwohl für alle der Fälle $\Gamma(t) = 50.000$ gilt, lässt sich zweifelsfrei entscheiden, welcher zwingend der beste sein soll.

Was sich jedoch objektiv beurteilen lässt, ist die Tatsache, dass in Fall (2) vier der fünf Service-Provider quasi "wertlos" sind. Und in Fall (3) immer noch drei von fünf!

Wir könnten also unsere Gegenüberstellung der drei angeführten Cases auch zur folgenden quantitativen Beurteilung stellen:

1. $\Gamma_1(t) = 50.000$, $\widehat{n}_1 = 50.000$ und $\widehat{m}_1 = 5$
2. $\Gamma_2(t) = 50.000$, $\widehat{n}_2 = 50.000$ und $\widehat{m}_2 = 1$
3. $\Gamma_3(t) = 50.000$, $\widehat{n}_3 = 25.000$ und $\widehat{m}_3 = 2$

Was ist also besser?

5.3.4 Zustandsbeschreibung WunderPass - detaillierte Sicht

Teilnehmer

Nicht alle angebundenen Teilnehmer innerhalb der WunderPass-Netzwerks sind gleichgestellt. Dies ist zweifelsfrei klar hinsichtlich der Unterscheidung zwischen connecteten Usern $\widehat{u} \in \widehat{U}^{(t)}$ und Service-Providern $\widehat{s} \in \widehat{S}^{(t)}$. Jedoch bestehen ebenfalls signifikante Unterschiede jeweils innerhalb der beiden Teilnehmerklassen $\widehat{U}^{(t)}$ und $\widehat{S}^{(t)}$ (siehe [TODO: Links]). Um dieser Unterscheidung unserer Teilnehmer gerecht zu werden, definieren wir "connected Pools" pro individuellen Teilnehmer als

Definition 9

Sei $t \in T$, $\widehat{U}^{(t)}$ und $\widehat{S}^{(t)}$ die übergeordneten "connected" User- und Provider-Pools und $\widehat{u}_* \in \widehat{U}^{(t)}$ und $\widehat{s}_* \in \widehat{S}^{(t)}$ die entsprechenden Teilnehmer, für deren individu-

elle "connected Pools" wir uns an dieser Stelle interessieren. Wir definieren die genannten "connected Pools" als

$$accounts : \widehat{U}^{(t)} \to \mathcal{P}\left(\widehat{S}^{(t)}\right)$$
$$accounts^{(t)}(\widehat{u}_*) = \left\{\widehat{s} \in \widehat{S}^{(t)} \mid \alpha^{(t)}(\widehat{u}_*, \widehat{s}) = 1\right\}$$

und

$$userbase : \widehat{S}^{(t)} \to \mathcal{P}\left(\widehat{U}^{(t)}\right)$$
$$userbase^{(t)}(\widehat{s}_*) = \left\{\widehat{u} \in \widehat{U}^{(t)} \mid \alpha^{(t)}(\widehat{u}, \widehat{s}_*) = 1\right\}$$

Lemma 1

$$\bigcup_{\widehat{u} \in \widehat{U}^{(t)}} \left(accounts^{(t)}(\widehat{u})\right) = \widehat{S}^{(t)} \tag{i}$$
$$\bigcup_{\widehat{s} \in \widehat{S}^{(t)}} \left(userbase^{(t)}(\widehat{s})\right) = \widehat{U}^{(t)} \tag{ii}$$

Beweis.

zu (i): Es ist

$$\bigcup_{\widehat{u} \in \widehat{U}^{(t)}} \left(accounts^{(t)}(\widehat{u})\right) \overset{\text{Def } 9}{=} \bigcup_{\widehat{u} \in \widehat{U}^{(t)}} \left\{\widehat{s} \in \widehat{S}^{(t)} \mid \alpha^{(t)}\left(\widehat{u}, \widehat{s}\right) = 1\right\}$$
$$\overset{(*)}{=} \left\{\widehat{s} \in \widehat{S}^{(t)} \mid \exists \widehat{u} \in \widehat{U}^{(t)} \text{ mit } \alpha^{(t)}\left(\widehat{u}, \widehat{s}\right) = 1\right\}$$
$$\overset{\text{Th. } 1 \text{ (vi)}}{=} \widehat{S}^{(t)}$$

Die Gleichheit zu (*) ergibt aus der Tatsache, Mengen-Vereinigungen ignorierten Doppelzählungen!

Aussage (ii) folgt ganz analog!

□

Theorem 3

$$\sum_{\widehat{u}\in\widehat{U}^{(t)}} |accounts^{(t)}(\widehat{u})| = \sum_{\widehat{s}\in\widehat{S}^{(t)}} |userbase^{(t)}(\widehat{s})| = \Gamma(t)$$

Beweis.

Es ist

$$\begin{aligned}
\Gamma(t) &\overset{\text{Th. 2 (i)}}{=} \sum_{i=1}^{\widehat{n}}\sum_{j=1}^{\widehat{m}} \widehat{\alpha}_{ij}^{(t)} \\
&= \sum_{\widehat{u}\in\widehat{U}^{(t)}} \sum_{\widehat{s}\in\widehat{S}^{(t)}} \alpha^{(t)}(\widehat{u},\widehat{s}) \\
&= \sum_{\widehat{u}\in\widehat{U}^{(t)}} \sum_{\widehat{s}\in\widehat{S}^{(t)} \text{ mit } \alpha^{(t)}(\widehat{u},\widehat{s})=1} 1 \\
&\overset{\text{Def 9}}{=} \sum_{\widehat{u}\in\widehat{U}^{(t)}} \sum_{s\in accounts^{(t)}(\widehat{u})} 1 \\
&= \sum_{\widehat{u}\in\widehat{U}^{(t)}} |accounts^{(t)}(\widehat{u})|
\end{aligned}$$

Die zweite Gleichheit folgt analog, falls man die Kommutativität der Def 6 beachtet:

$$\Gamma(t) = \sum_{i=1}^{n}\sum_{j=1}^{m} \alpha_{ij}^{(t)} = \sum_{j=1}^{m}\sum_{i=1}^{n} \alpha_{ij}^{(t)}$$

□

Spätestens bei der Verinnerlichung der eben erzielten Erkenntnisse, wird einem bewusst, die Bewertung unseres Fortschritts könne nicht alleinig an $\widehat{n}$, $\widehat{m}$ und $\Gamma(t)$ gemessen werden. Diese geben zwar einen guten Anhaltspunkt, lassen jedoch in einer einzigen gegebenen Ausprägung $[\widehat{n},\widehat{m},\Gamma(t)]$ eine enorme Vielzahl an durch $\widehat{U}^{(t)}, \widehat{S}^{(t)}$ beschriebenen Szenarien zu, die allesamt die Vorgabe $[\widehat{n},\widehat{m},\Gamma(t)]$ erfüllten.

Wir müssen also dringend die Ausprägungen und Unterschiede der einzelnen angebundenen Teilnehmer und deren Synergien untereinander verstehen und dieses Verständnis zwingend in die Messung unseres Fortschritts integrieren. Der bereits erarbeitete (für sich alleine noch ziemlichen wertlose) Input $[\widehat{n},\widehat{m},\Gamma(t)]$ ist dabei absolut nicht unbedeutend und liefert Eingrenzungen und Abschätzungen - wie bereits anhand von Lemma 1 und Theorem 3 zu sehen ist.

Sequenzierung

Zunächst einmal einige qualitative Gedanken, die die daran anschließende Formalisierungen motivieren:

- Welche Bedeutung haben die individuellen Account-Pools $accounts^{(t)}(\widehat{u})$ der angebundenen User $\widehat{u} \in \widehat{U}^{(t)}$?
  - (a) gemessen an ihrer bloßen Größe ($\rightarrow$ User mit besonders vielen/wenigen Providern verbunden)
    - (i) Welche besondere Bedeutung haben User, die mit nur einem einzigen Provider verbunden sind?
    - (ii) Welche besondere Bedeutung haben User, die mit allen Providern verbunden sind?
  - (b) gemessen an ihrem konkreten "Inhalt" ($\rightarrow$ User mit besonders "wertvollen"/"wertlosen" Providern verbunden)
- Welche Bedeutung haben die individuellen Userbases $userbase^{(t)}(\widehat{s})$ der angebundenen Service-Provider $\widehat{s} \in \widehat{S}^{(t)}$?
  - (a) gemessen an ihrer bloßen Größe ($\rightarrow$ Provider ist durch eine besonders stark/schwach ausgeprägte Userbase gekennzeichnet). Kann daraus bereits eine gewisse Relevanz des Service-Providers innerhalb der WunderPass-Universum abgeleitet werden?
  - (b) gemessen an ihrem konkreten "Inhalt" ($\rightarrow$ Ist der Provider mit bestimmten Usern verbunden, die eine besondere "Beachtung" erfordern?)
- Kann ein Provider $\widehat{s_*} \in \widehat{S}^{(t)}$ in seiner Wichtigkeit/Relevanz bereits daran gemessen werden, indem man seinen Verlust (also Verlassen der WunderWelt und "Zerstören" aller Connections) beziffert? Also mittels Vergleichs von $\left[\widehat{U}^{(t_0)}, \widehat{S}^{(t_0)}, \Gamma(t_0)\right]$ mit $\left[\widehat{U}^{(t_1)}, \widehat{S}^{(t_0)} \setminus \{\widehat{s_*}\}, \Gamma(t_1)\right]$?

Um diesen Fragen auf den Grund gehen zu können, benötigen wir zunächst eine Vielzahl von zusätzlichen Größen und Werkzeugen, die wir nun definieren wollen:

Definition 10

Sei $t \in T$ ein beliebiger Zeitpunkt, $\widehat{U}^{(t)} = \{\widehat{u}_1; \widehat{u}_2; ...; \widehat{u}_{\widehat{n}}\}$ und $\widehat{S}^{(t)} = \{\widehat{s}_1; \widehat{s}_2; ...; \widehat{s}_{\widehat{m}}\}$ sowie $accounts^{(t)}(\widehat{u}_i)$ für alle $i \in \{1, ..., \widehat{n}\}$ wie bekannt und zudem in Anlehnung an Annahme 2 $\widehat{m} << \widehat{n}$.

Wir definieren

Die Anzahl der connecteten Service-Provider pro User $\widehat{u}_i \in \widehat{U}^{(t)}$ als

$$\omega_i := \left| accounts^{(t)}(\widehat{u}_i) \right| . \tag{i}$$

Die (disjunkte) Partition des gesamten Connectet-User-Pools $\widehat{U}^{(t)}$

$$\widehat{U}^{(t)} = \left(\widehat{U}_1, ..., \widehat{U}_{\widehat{m}} \right) \text{ mit } \bigcup_{k=1}^{\widehat{m}} \widehat{U}_k = \widehat{U}^{(t)}$$

nach dem Kriterium "User ist mit k der insgesamt $\widehat{m}$ Provider verbunden" als

$$\widehat{U}_k := \left\{ \widehat{u}_i \in \widehat{U}^{(t)} \text{ mit } \omega_i = k \right\} \text{ für } k \in \{1, ..., \widehat{m}\} . \tag{ii}$$

Die (rein zahlenmäßige) Ausprägung der eben definierten Partition von $\widehat{U}^{(t)}$ als

$$\Omega_k := \left| \widehat{U}_k \right| \text{ für } k \in \{1, ..., \widehat{m}\} , \tag{iii}$$

für die konsequenterweise

$$\sum_{k=1}^{\widehat{m}} \Omega_k = \widehat{n} \text{ gilt.}$$

WIP

Theorem 4

$$\Gamma(t) = \sum_{k=1}^{\widehat{m}} k * \Omega_k \tag{i}$$

$$1 = 1 \tag{ii}$$

Theorem 5

$$\frac{(j+1)*\widehat{n}-\Gamma(t)}{j} \leq \sum_{k=1}^{j} \Omega_k \leq \frac{\widehat{m}*\widehat{n}-\Gamma(t)}{\widehat{m}-j} \text{ für } j \in \{1,...,\widehat{m}-1\} \tag{i}$$

$$\frac{\Gamma(t)-j*\widehat{n}}{\widehat{m}-j} \leq \sum_{k=j+1}^{\widehat{m}} \Omega_k \leq \frac{\Gamma(t)-\widehat{n}}{j} \text{ für } j \in \{1,...,\widehat{m}-1\} \tag{ii}$$

Und ganz insbesondere

$$2*\widehat{n}-\Gamma(t) \leq \Omega_1 \leq \frac{\widehat{m}*\widehat{n}-\Gamma(t)}{\widehat{m}-1} \tag{iii}$$

$$\Gamma(t)-(\widehat{m}-1)*\widehat{n} \leq \Omega_{\widehat{m}} \leq \frac{\Gamma(t)-\widehat{n}}{\widehat{m}-1} \tag{iv}$$

Beweis.

zu (i) und (ii): Zunächst zeigen wir die zweite Ungleichung von (i):

$$\begin{aligned}
\Gamma(t) &\overset{(Th.4)}{=} \sum_{k=1}^{\widehat{m}} k*\Omega_k = \sum_{k=1}^{j} k*\Omega_k + \sum_{k=j+1}^{\widehat{m}} k*\Omega_k \\
&\leq j*\sum_{k=1}^{j}\Omega_k + \widehat{m}*\sum_{k=j+1}^{\widehat{m}}\Omega_k \\
&= j*\sum_{k=1}^{j}\Omega_k + \widehat{m}*\left(n-\sum_{k=1}^{j}\Omega_k\right) \\
&= \widehat{m}*\widehat{n}-(\widehat{m}-j)*\sum_{k=1}^{j}\Omega_k \\
\Leftrightarrow (\widehat{m}-j)*\sum_{k=1}^{j}\Omega_k &\leq \widehat{m}*\widehat{n}-\Gamma(t) \\
\Leftrightarrow \sum_{k=1}^{j}\Omega_k &\leq \frac{\widehat{m}*\widehat{n}-\Gamma(t)}{\widehat{m}-j}
\end{aligned}$$

Nun zeigen wir die zweite Ungleichung von (ii):

$$\begin{aligned}
\Gamma(t) &\overset{(Th.4)}{=} \sum_{k=1}^{\widehat{m}} k * \Omega_k = \sum_{k=1}^{j} k * \Omega_k + \sum_{k=j+1}^{\widehat{m}} k * \Omega_k \\
&\geq 1 * \sum_{k=1}^{j} \Omega_k + (j+1) * \sum_{k=j+1}^{\widehat{m}} \Omega_k \\
&= \sum_{k=1}^{m} \Omega_k + j * \sum_{k=j+1}^{\widehat{m}} \Omega_k = \widehat{n} + j * \sum_{k=j+1}^{\widehat{m}} \Omega_k \\
\Leftrightarrow \Gamma(t) - \widehat{n} &\geq j * \sum_{k=j+1}^{\widehat{m}} \Omega_k \\
\Leftrightarrow \frac{\Gamma(t) - \widehat{n}}{j} &\geq \sum_{k=j+1}^{\widehat{m}} \Omega_k
\end{aligned}$$

Die erste Ungleichung von (i) folgt direkt aus der zweiten von (ii):

$$\begin{aligned}
\widehat{n} &= \sum_{k=1}^{\widehat{m}} \Omega_k = \sum_{k=1}^{j} \Omega_k + \sum_{k=j+1}^{\widehat{m}} \Omega_k \\
&\leq \sum_{k=1}^{j} \Omega_k + \frac{\Gamma(t) - \widehat{n}}{j} \\
\Leftrightarrow \widehat{n} - \frac{\Gamma(t) - \widehat{n}}{j} &\leq \sum_{k=1}^{j} \Omega_k \\
\Leftrightarrow \frac{j * \widehat{n} - \Gamma(t) + \widehat{n}}{j} &\leq \sum_{k=1}^{j} \Omega_k
\end{aligned}$$

Und gänzlich analog dazu die erste Ungleichung von (ii) aus der zweiten von (i):

$$\widehat{n} = \sum_{k=1}^{\widehat{m}} \Omega_k = \sum_{k=1}^{j} \Omega_k + \sum_{k=j+1}^{\widehat{m}} \Omega_k$$
$$\leq \frac{\widehat{m} * \widehat{n} - \Gamma(t)}{\widehat{m} - j} + \sum_{k=j+1}^{\widehat{m}} \Omega_k$$
$$\Leftrightarrow \frac{\widehat{m} * \widehat{n} - j * \widehat{n} - \widehat{m} * \widehat{n} + \Gamma(t)}{\widehat{m} - j} \leq \sum_{k=j+1}^{\widehat{m}} \Omega_k$$
$$\Leftrightarrow \frac{\Gamma(t) - j * \widehat{n}}{\widehat{m} - j} \leq \sum_{k=j+1}^{\widehat{m}} \Omega_k$$

(iii) und (iv) sind gänzlich trivial und eigentlich keine zusätzlichen Erkenntnisse zu (i) und (ii), sondern deren besonders relevanten Ausprägungen für $j = 1$ und $j = m - 1$, Man beachte hierfür höchstens die Tatsache $\Omega_m = \sum_{k=j+1}^{\widehat{m}} \Omega_k$ für $j = m - 1$.

□

[Beispiel]

Beispiel 1

Sei das Setting zu einem Zeitpunkt $t \in T$ durch die folgende Grafik der bestehenden User-Provider-Connections gegeben:

	s_1	s_2	s_3
u_1	x		
u_2	x		
u_3	x	x	x
u_4		x	
u_5			x
u_6	x	x	
u_7		x	x
u_8	x	x	x

Damit ergeben sich die oben definierten

Beispiel 2

Sei das Setting zu einem Zeitpunkt $t \in T$ durch die folgende Grafik der bestehenden User-Provider-Connections gegeben:

	s_1	s_2	s_3
u_1	x		
u_2	x		
u_3			x
u_4		x	
u_5			x
u_6	x		
u_7		x	x
u_8	x		x

Damit ergeben sich die oben definierten

Größen als

Größen als

$$\widehat{U}^{(t)} = \{u_1; ...; u_8\}$$
$$\widehat{S}^{(t)} = \{s_1; s_2; s_3\}$$
$$n = 8$$
$$m = 3$$
$$\Gamma(t) = 14$$

$$acc.^{(t)}(u_1) = acc.^{(t)}(u_2) = \{s_1\}$$
$$acc.^{(t)}(u_3) = acc.^{(t)}(u_8) = \{s_1; s_2; s_3\}$$
$$acc.^{(t)}(u_4) = \{s_2\}$$
$$acc.^{(t)}(u_5) = \{s_3\}$$
$$acc.^{(t)}(u_6) = \{s_1; s_2\}$$
$$acc.^{(t)}(u_7) = \{s_2; s_3\}$$

$$userbase^{(t)}(s_1) = \{u_1; u_2; u_3; u_6; u_8\}$$
$$userbase^{(t)}(s_2) = \{u_3; u_4; u_6; u_7; u_8\}$$
$$userbase^{(t)}(s_3) = \{u_3; u_5; u_7; u_8\}$$

$$\omega_1 = \omega_2 = \omega_4 = \omega_5 = 1$$
$$\omega_6 = \omega_7 = 2$$
$$\omega_3 = \omega_8 = 3$$

$$\widehat{U}_1 = \{u_1; u_2; u_4; u_5\}$$
$$\widehat{U}_2 = \{u_6; u_7\}$$
$$\widehat{U}_3 = \{u_3; u_8\} \text{ mit}$$
$$\bigcup_{k=1}^{m} \widehat{U}_k = \widehat{U}^{(t)}$$

$$\Omega_1 = \left|\widehat{U}_1\right| = 4$$
$$\Omega_2 = \left|\widehat{U}_2\right| = 2$$
$$\Omega_3 = \left|\widehat{U}_3\right| = 2 \text{ mit}$$
$$\sum_{k=1}^{m} \Omega_k = n$$

$$\widehat{U}^{(t)} = \{u_1; ...; u_8\}$$
$$\widehat{S}^{(t)} = \{s_1; s_2; s_3\}$$
$$n = 8$$
$$m = 3$$
$$\Gamma(t) = 10$$

$$acc.^{(t)}(u_1) = acc.^{(t)}(u_2) = acc.^{(t)}(u_6) = \{s_1\}$$
$$acc.^{(t)}(u_3) = acc.^{(t)}(u_5) = \{s_3\}$$
$$acc.^{(t)}(u_4) = \{s_2\}$$
$$acc.^{(t)}(u_7) = \{s_2; s_3\}$$
$$acc.^{(t)}(u_8) = \{s_1; s_3\}$$

$$userbase^{(t)}(s_1) = \{u_1; u_2; u_6; u_8\}$$
$$userbase^{(t)}(s_2) = \{u_4; u_7\}$$
$$userbase^{(t)}(s_3) = \{u_3; u_5; u_7; u_8\}$$

$$\omega_1 = \omega_2 = \omega_3 = \omega_4 = \omega_5 = \omega_6 = 1$$
$$\omega_7 = \omega_8 = 2$$

$$\widehat{U}_1 = \{u_1; u_2; u_3; u_4; u_5; u_6\}$$
$$\widehat{U}_2 = \{u_7; u_8\}$$
$$\widehat{U}_3 = \emptyset \text{ mit}$$
$$\bigcup_{k=1}^{m} \widehat{U}_k = \widehat{U}^{(t)}$$

$$\Omega_1 = \left|\widehat{U}_1\right| = 6$$
$$\Omega_2 = \left|\widehat{U}_2\right| = 1$$
$$\Omega_3 = \left|\widehat{U}_3\right| = 1 \text{ mit}$$
$$\sum_{k=1}^{m} \Omega_k = n$$

5.3.5 Other Stuff

[TODO2][Abschätzung $\frac{\widehat{n}}{\widehat{m}}$]

Aussagen aus Annahme 2 und Theorem 2 - Aussage (ii) - verwerten und Annahme 2 deutlich verschärfen.

$$\widehat{n} = \sum_{k=1}^{\widehat{m}} \Omega_k \leq \widehat{m} * \max_{j \in \{1;\ldots;\widehat{m}\}} \Omega_j$$
$$\Leftrightarrow \frac{\widehat{n}}{\widehat{m}} \leq \max_{j \in \{1;\ldots;\widehat{m}\}} \Omega_j$$

Weiterverarbeitung von Theorem 5:

Theorem 6

Theorem 5 lieferte uns

$$2 * \widehat{n} - \Gamma(t) \leq \Omega_1 \leq \frac{\widehat{m} * \widehat{n} - \Gamma(t)}{\widehat{m} - 1}$$
$$\Gamma(t) - (\widehat{m} - 1) * \widehat{n} \leq \Omega_{\widehat{m}} \leq \frac{\Gamma(t) - \widehat{n}}{\widehat{m} - 1}$$

Der Übersicht halber setzen wir

$$A := 2 * \widehat{n} - \Gamma(t)$$
$$B := \Gamma(t) - (\widehat{m} - 1) * \widehat{n}$$
$$C := \frac{\widehat{m} * \widehat{n} - \Gamma(t)}{\widehat{m} - 1}$$
$$D := \frac{\Gamma(t) - \widehat{n}}{\widehat{m} - 1}$$

womit sich nun obige Aussage ausdrückt als

$$A \leq \Omega_1 \leq C$$
$$B \leq \Omega_{\widehat{m}} \leq D$$

Damit lassen sich besondere zu untersuchende Grenzfälle formulieren:

$$A \leq B \Leftrightarrow \Gamma(t) \geq (\widehat{m} - 1) * \frac{\widehat{n}}{2} \quad \text{(i)}$$
$$A \leq C \Leftrightarrow 1 = 1 \quad (1)$$
$$A \leq D \Leftrightarrow \Gamma(t) \geq (2\widehat{m} - 1) * \frac{\widehat{n}}{\widehat{m}} \quad \text{(iii)}$$
$$B \leq C \Leftrightarrow \Gamma(t) \leq (\widehat{m} + (\widehat{m} - 1)^2) * \frac{\widehat{n}}{\widehat{m}} \quad \text{(iv)}$$
$$B \leq D \Leftrightarrow 1 = 1 \quad (v)$$
$$C \leq D \Leftrightarrow \Gamma(t) \geq (\widehat{m} - 1) * \frac{\widehat{n}}{2} \quad \text{(vi)}$$

[ende TODO2]

[TODO3]["Verdichtung"]

Die Maße $\widehat{n}$, $\widehat{m}$ und $\Gamma(t)$ sind sehr objektiv und teils zielführend. Sie scheinen aber nicht zu reichen. So kann es z. B. User $\widehat{u} \in \widehat{U}^{(t)}$ geben, die im worst case ausschließlich zu einem einzigen Provider $\widehat{s} \in \widehat{S}^{(t)}$ connectet sind (und somit aber trotzdem den Wert von $\widehat{n}$ beeinflussen, oder noch schlimmer analog Provider $\widehat{s} \in \widehat{S}^{(t)}$, die als "angebunden" gelten, weil sie mit marginal wenigen Usern (im worst case mit einem einzigen) connectet sind. Solche Teilnehmer spielen eigentlich für den zahlenmäßigen WunderPass-Fortschritt keinerlei Rolle, beeinflussen jedoch unsere relevanten Messgrößen (KPI).

Von daher benötigen wir noch eine weitere Präzisierung in Form von

- "80-20-Regel" heranziehen, indem man die Mengen $\widehat{U}^{(t)}$ und $\widehat{S}^{(t)}$ so modifiziert/verkleinert, dass $\Gamma(t)$ davon kaum einen Einfluss spürt (sich lediglich um einen marginalen Prozentsatz verringert).
- Formeln auf die davon modifizierten Größen $\widehat{\widehat{n}}$ und $\widehat{\widehat{m}}$ anpassen.
- $\Rightarrow$ Die Grenzen von [Theorem 2][Aussage (ii)] werden damit deutlich schärfer.
- $\Rightarrow$ kann sicherlich in Abschnitt 5.3.6 für den Umgang mit dem Verhältnis $\frac{\widehat{n}}{\widehat{m}}$ genutzt werden.
- Wird vermutlich auch Relevanz bei den "individuellen" (Definition erfolgt noch) User- und Provider-Pools zum Einsatz kommen.

[ende TODO3]

[TODO4.1]["Exklusive Connections"]

- Eine Connection zu einem Service-Provider ist exklusiv, wenn der zugehörige User zu keinem anderen Service-Provider connectet ist.
- Es gibt mindestens $n_{excl} \geq \Gamma(t) - \widehat{n}$ nicht exklusive Connections.

[ende TODO3.1]

[TODO6][deprecated Inhalt verarbeiten]

Mit diesen geschaffenen Formalisierungs-Werkzeugen lässt sich nun auch die übergeordnete WunderPass-Vision formal erfassen - und zwar indem man den Zeitpunkt $t_* \in T$ ihrer Erreichung benennt:

Definition 11

Wir betrachten die WunderPass-Vision zu einem Zeitpunkt $t_* \in T$ als erreicht, falls

$$\alpha_{ij}^{(t_*)} = 1 \text{ für alle } i \in \{1, ..., n\} \text{ und } j \in \{1, ..., m\} \tag{2}$$

erfüllt ist. Darüber hinaus ist es noch nicht ganz klar, welche Aussage für die Zeitpunkte $t > t_*$ hinsichtlich der Visions-Erreichung zu treffen sei. Grundsätzlich ist es ja durchaus denkbar, die obige Voraussetzung gelte für $t > t_*$ nicht mehr. Bleibt die Vision in diesem Fall trotzdem als 'erreicht' zu betrachten?

Die gelungene Formalisierung unserer Vision mittels Definition 11 mag einen Fortschritt hinsichtlich unserer "Business-Mathematics" darstellen, bleibt jedoch losgelöst zunächst einmal ziemlich wertlos. Zum einen ist das Erreichen der Vision im formellen Sinne der Definition 11 weder praxistauglich noch akribisch erforderlich. Zudem bleibt zum anderen der resultierende (intrinsische) Business-Value der Visions-Erreichung bisher weiterhin nicht ohne Weiteres erkennbar. Vielmehr sollten wir die Anforderung von Gleichung (2) als eine Messlatte unseres Fortschritts heranziehen, und eher als (unerreichbare) 100%-Zielerreichungs-Marke betrachten. Zudem müssen wir zeitnah - obgleich die vollständige oder nur fortschreitend partielle - Zielerreichung unserer Vision in klaren, quantifizierbaren Business-Value übersetzen.

Dazu definieren wir als erstes ein intuitives Maß der Zielerreichung:

Definition 12

$$\Gamma : T \to \mathbb{N}$$

$$\Gamma(t) := \sum_{i=1}^{n} \sum_{j=1}^{m} \alpha_{ij}^{(t)}$$

Damit liefert uns die definierte Γ-Funktion aber auch ein extrem greifbares und intuitiv nachvollziehbares Fortschrittsmaß unseres Vorhabens. Zudem fügt sich dieses perfekt in unsere mittels Definition 11 quantifizierte Unternehmens-Vision und unterliegt einer fundamentalen (bezifferbaren) Obergrenze. Dies zeigt folgendes Lemma:

Lemma 2

Es gelten folgende Aussagen:

$$\Gamma(t) \leq n^{(t)} * m^{(t)} \text{ für alle } t \in T \quad \text{(i)}$$

$$\text{es gilt Gleichheit bei (i)} \Leftrightarrow \text{ es gilt Gleichung (2) aus Def 11} \quad \text{(ii)}$$

Gleichung (ii) ermöglicht uns die Definition 6 auf ein relatives Zielereichungs-Maß auszuweiten:

Definition 13

$$\gamma : T \to [0; 1]$$

$$\gamma(t) := \frac{\Gamma(t)}{n^{(t)} * m^{(t)}}$$

[ende TODO6]

Ab hier WIP

5.3.6 Business-Plan in Mathematics

Diese letzten Werkzeuge lassen und Begriffe wie "Zielsetzung" bzw. "Milestone" einführen.

Definition 14

Seien $t \in T$ und zudem entsprechend $(n^{(t)}, m^{(t)}) = dP^{(t)}$ der angenommene Zustand der digitalen Welt zu einem beliebig gewählten Zeitpunkt. Wir definieren die - allein durch WunderPass zu bestimmende - Zielfunktion als

5.3.7 Quantifizierung des Status quo

Vernetzung & Netzwerk-Effekt

Die WunderPass-Vision steht in ihrer Formulierung ganz klar im Sinne einer gewissen "Vernetzung". Wir möchten, dass möglichst viele User sich mit möglichst vielen Service-Providern "connecten" (bzw. connectet sind/bleiben). Schränkt man seine Sichtweise alleinig auf diese Vision (ohne diese zunächst zu hinterfragen), liefern uns die zuletzt eingeführten Größen $\alpha_{ij}^{(t)}$, $\Gamma(t)$ und $\gamma(t)$ ziemlich gute Gradmesser, um zweifelsfreie Aussagen hinsichtlich der Vergleichbarkeit zweier Zeitpunkte $t_1, t_2 \in T$ treffen zu können. Es ist irgendwie klar, $\alpha_{ij}^{(t)} = 1$ sei im Sinne unserer Vision irgendwie besser als $\alpha_{ij}^{(t)} = 0$.

Aus diesem Blickwinkel (in dem die Vision zunächst ein Selbstzweck bleibt) erscheint die folgende Definition mehr als intuitiv einleuchtend, um die obige Formulierung "irgendwie besser" zu formalisieren und vor allem zu quantifizieren.

WIP: Hier stand vorher Definition 7

Man beachte, dass es sich bei der definierten Ordnungsrelation gar um eine Totalordnung handelt! Der Form halber ergänzen wir an der Stelle noch um zwei weitere - schematisch induzierte - Relationen auf unserem Zeitstrahl T:

WIP: Hier stand vorher Definition 8

Auch für die letzten beiden Relationen wollen wir fortan die vereinfachte Schreibweise $t_1 \prec t_2$ und $t_1 \simeq t_2$ nutzen.

Diese Netzwerk-Bewertungs-Modell besitzt jedoch im aktuellen Zustand drei wesentliche Schwachstellen:

- Es beschreibt uns misst weiterhin ausschließlich den intrinsischen Wert der Vernetzung innerhalb unserer kleinen "Visions-Welt", dem es noch an Bezug zur "Außenwelt" und dem Business-Case fehlt. Diesen Umstand wollen wir weiterhin zunächst einmal ignorieren.

- Es bewertet in der aktuellen Form ausschließlich "unsere Welt" bzw. unseren Fortschritt als Ganzes. Die definierte "besser"-Relation misst das "Besser" aus Sicht der Allgemeinheit. Der einzelne Teilnehmer bleibt individuell unberücksichtigt. Es ist schwer vorstellbar, ein Ökosystem zu designen, welches intrinsisch nach dem Wohl/Optimum Aller strebt (und damit eben einmal einen formalen Beweis für das Funktionieren des Kommunismus zu liefern.)

- Es lässt den sogenannten Netzwerkeffekt außer Acht! Denn selbst wenn man eben einmal das Problem des Bullet 1 aus der Welt schafft, und ein Preisschild an den Mehrwert einer Connection zwischen User und Provider bekommt. Die Literatur zum besagten Netzwerkeffekt liefert gute Argumente für die Annahme, eine von uns anvisierte User-Provider-Connection kann nur sehr selten alleinstehend in ihrem Mehrwert bewertet werden. Vielmehr bemisst sich dieser etwaige Mehrwert in dem Zusammenspiel und den Synergien mit anderen User-Provider-Connections. Es lassen sich viele Beispiele finden, um diesen Umstand zu begründen. So kann es z. B. sein, dass ein Finance-Aggregator-Service für einen User um so wertvoller wird, je mehr Finance-Provider der User selbst mit seiner WunderIdentity connectet. Hierbei wird es kaum einen Unterschied für ihn machen, ob die genannten Finance-Provider mit 100 anderen WunderPass-Usern connectet seien oder mit 10 Mio. Im Case einer Splitwise-Connection (oder auch einer etwaigen EventsWithFriends-App) dagegen entsteht der Mehrwert erst dann, wenn auch ganz viele Freunde des Users diese Splitwise-Connection mit WunderPass besitzen. Andernfalls beläuft sich der Mehrwert seiner eigenen Connection so ziemlich gen Null.

Insbesondere der letzte Punkt wirft einige interessante Fragen auf, zu denen wir eine Antwort finden werden müssen. Oder zumindest Hypothesen und Annahmen treffen. Was bedeutet eigentlich

$\alpha_{kj}^{(t)} * \alpha_{lj}^{(t)} = 1$ für zwei User $u_k^{(t)}, u_l^{(t)} \in U^{(t)}$ die beide mit Provider $s_j^{(t)} \in S^{(t)}$ connectet sind?

Sind diese dann damit gleichbedeutend in irgendeiner Weise ebenfalls "*miteinander connectet*"? Und was würde eine solche Implikation für unser bisheriges Modell bedeuten? Wie (un)abhängig ist eine solche "indirekte Connection" von ihrer "Brücke" - dem Service-Provider? All diese Fragen lassen sich zudem analog auf "indirekte Connections" zwischen Providern übertragen - die dann etwaige User als "Brücke" nützten. Zu guter Letzt ließe sich diese neue Komplexität beliebig potenzieren, indem man mittels Rekursion indirekte Connections "zweitens, drittens,... Grades" definiert.

Um der aufkommenden Komplexität Herr zu werden, wollen wir uns zunächst einmal dem zweiten der oben genannten Schwachstellen unseres bisherigen Modells zuwenden, und dieses idealerweise dahingehend erweitern, auch individuelle Bewertungen unserer Teilnehmer $u \in U^{(t)}$ und $s \in S^{(t)}$ zu erfassen.

5.3.8 Individuelle Wertschöpfung der Teilneher

TODO

5.4 Token-Economics (WPT)

WIP

Prämisse 1: generelle Anforderungen an den Token

- Der Token soll ein **echter** Utility-Token sein. Er braucht also zwingend einen **intrinsischen Wert**.

Die Teilnehmer (User und Provider) müssen einen intrinsischen Vorteil am Besitz von Tokens innerhalb des Ökosystems erfahren. Sie müssen quasi "irgendwas mit dem Token machen können" - und zwar innerhalb des Ökosystems und nicht mittels "Verkaufs nach außen". Wenn man als Teilnehmer die Möglichkeit besitzt, Tokens für/durch irgendetwas zu erwerben, muss auch die Möglichkeit bestehen, diesen für irgendetwas (anderes; "nützliches") innerhalb des Ökosystems auszugeben. Idealerweise verhält sich unser Token zur Euro, wie sich der Euro zum nicht existenten "Weltall-Taler" verhält - also ohne Rechtfertigung zu besitzen, das Ökosystem verlassen zu müssen.

Falls die Schaffung einer solchen Ökonomie nicht gelingen sollte - weil z.B. die Service-Provider mehr Value generieren, als sie innerhalb des Ökosystems "konsumieren" können - sollte diese Forderung zumindest für den Teilnehmer "User" sichergestellt werden. Denn der User partizipiert in seinem Dasein eher als Konsument innerhalb des Digital-Universums, als als Wertschöpfer, weshalb seinem intrinsischen Vorteil am Besitz von Tokens mit dem damit ermöglichten Konsum von digitalen Dienstleistungen Genüge getan sein sollte.

- Der Token sollte natürlich auch einen **extrinsischen** Wert besitzen.

Nicht all zu laut (der Community ggü.) kommuniziert, wäre unsere ganze Unternehmung im Falle des Fehlen des extrinsischen Werts nichts anderes als ein kommunistischer Akt. Nur diese Beschaffenheit des Tokens liefert uns ein Monetarisierungs-Modell. Und auch deutet zudem vieles darauf hin, die Service-Provider-Teilnehmer kämen ohne einen extrinsischen Wert nicht aus.

- Der Token soll **nicht inflationär** sein - also einen definierten Cap besitzen.

Mit voriger Forderung - laut der man "etwas mit dem Token innerhalb des Systems machen kann", verleiht die gegenständige Forderung das dieses "Etwas", was mittels des Tokens ermöglicht wird, einem gewissen Qualitätsanspruch genügen muss. Je

größer die Qualität dieses besagten "Etwas" - also z. B. einer Dienstleistung, die mit ausschließlich mit dem Token bezahlt werden kann - ist, desto *wertvoller* wird auch der Besitz des Tokens. Und damit auch sowohl sein intrinsischer als auch extrinsischer Wert. Schlichtweg deshalb, weil der Token und somit der mögliche Konsum besagter Dienstleistung gecappt ist.

- Kreislauf.

Kreislauf-Beschreibung

Prämisse 2: Daten haben einen Wert

TODO: Evaluierung extrem schwierig. Folgende Aussagen/Antworten sind zu beweisen.

- Wer besitzt Daten/Informationen?
- Für wen sind diese Daten von "Wert" (Geld verdienen)?
- Wie kann der Wert der Daten maximiert werden? Wer profitiert im welchen Maße davon?
- Wer würde für diese Daten bezahlen und wie viel?
- Wie ist die (maximale) Wertschöpfung zu verteilen? Wer wird beteiligt? Wie wird die maximierende Rolle der Wertschöpfung belohnt?
- Wer trägt etwaige Risiken und in welchem Verhältnis?
- Wie ist das alles in die Token-Economics zu integrieren?

Conclusion 3: unser Ökosystem generiert Value

- Wir schöpfen Mehrwert, indem wir Datenerfassung ermöglichen (die ja einen nachgewiesenen Value besitzen?
- Besitzer der Daten werden entlohnt
- Nutzer der Daten zahlen für Daten, generieren damit aber Value, der wiederum entlohnt wird.
- Am Ende haben alle Teilnehmer entweder Value generiert oder aber im Wert des values verkonsumiert

- Wir partizipieren am extrinsischen Wert des Tokens (Kurs-Entwicklung durch positive Wertschöpfung des gesamten Ökosystems).
- Incentives sind nötig, um das Henne-Ei-Problem zu lösen
- Incentives sollten nachträglich mit der dadurch geschaffenen Wertschöpfung verrechtet werden.

Lösung 9: möglicher Token-Flow

- Ein User nutzt einen Service-Provider A, der WunderPass unterstützt, und ist auch mit seinem WunderPass bei Provider A eingeloggt.
  - Beispiel 1: Der Service-Provider A ist ein Identity-Data-Management-Service, der die persönlichen Daten des Users verwaltet und bei Bedarf Dritten zur Verfügung stellen kann.
  - Beispiel 2: Der Service-Provider A ist EasyJet.
- Der User und der Service-Provider A erzielen - wie auch immer - eine Übereinkunft darüber, dass die von Provider A verwalteten - den User betreffenden Daten - theoretisch mittels des WunderPass-Lookups mit Dritten geteilt werden können sollen.
  - Beispiel 1: Die Daseinsberechtigung des Identity-Data-Management-Service beschränkt sich eigentlich ausschließlich auf das Teilen von Daten mit Dritten. Hierbei ist die obige Anforderung also trivialerweise unabdingbar.
  - Beispiel 2: Beim Beispiel von EasyJet könnten die besagten Daten z. B. gebuchte Flugtickets sein, die man mit Drittdiensten teilt, um daran ausgerichtet gezielte Werbeangebote im zugehörigen Ausland zu ermöglichen.

  User und Provider einigen sich auf einen Preis/Preisformel für das Teilen dieser Daten - und zwar auf den konkreten Preis von **x WPT** (WunderPass-Utility-Token).
- Service-Provider B (der ebenfalls WunderPass unterstützt) möchte Userdaten des Service-Provider A nutzen, falls solche vorliegen.
  - Beispiel 1: Hierbei könnte Provider B so ziemlich jeder denkbare Online-Dienst sein, der irgendwelche persönlichen Userdaten benötigt (z. B. Adresse, Email, Kreditkarte etc.).
  - Beispiel 2: Hierbei könnte es sich z. B. um (schlecht ausgelastete) Hotels handeln, die anhand der EasyJet-Flugdaten über die Destination des Users wissend, besondere Angebote an ihn ausspielen wollen.

- Service-Provider B callt der WunderPass-Lookup-Service, um die Existenz etwaiger Daten und deren **Preis x WPT** in Erfahrung zu bringen.
- Liegen Lookup-Daten vor, kann Provider B entscheiden, ob er diese zum angegebenen Preis beziehen möchte.
- Möchte Service-Provider B Gebrauch vom Lookup machen, muss er in Vorleistung gehen und den Betrag von **2 * x WPT** in den Lookup-Contract einzahlen.
- Die eingebrachten **2 * x WPT** werden - abzüglich einer kleinen WunderPass-Fee - im Lookup-Contract gelockt. Service-Provider B erhält im Gegenzug einen *Berechtigungs-Token* für den Abruf von entsprechenden Daten von Provider A (hierbei ist eher ein technischer Security-Token und kein Crypto-Token gemeint).
- Die Zugriffsberechtigung für das Abrufen der Daten von Provider A soll dabei einer **zeitlichen Beschränkung z** unterliegen (z. B. "eine Woche"). **z** ist hierbei ebenso individuell (Teilnehmer- und Daten-abhängig) zu sehen wie **x**.
- Service-Provider B fragt unter Vorlage des Berechtigungs-Token die gewünschten Daten beim Service-Provider A an.
  - Provider A muss den Berechtigungs-Token validieren (beim Lookup-Service).
  - A muss unter Umständen die Freigabe beim User einfordern (ggf. sollte der User in irgendeiner Weise "bestraft" werden, falls er den Datenzugriff verwehrt).
  - Provider A und B müssen einen gewissen "Handshake" implementieren, der A bescheinigt, wie vereinbart die korrekten Daten an B ausgeliefert zu haben.
- Provider A liefert die Daten an Provider B aus und erhält im Gegenzug ein Bestätigungszertifikat von B.
- Mit dem Bestätigungszertifikat kann Provider A seine Vergütung beim Lookup-Contract einlösen. Dabei wird die Hälfte der gelockten Einlage von Provider B (also an dieser Stelle die Hälfte von **2 * x WPT** - also **x WPT**) ausgeschüttet. Und zwar zur Hälfte an Provider A und zur andern Hälfte an den User.
- **x WPT** des ursprünglich eingezahlten Deposits von B bleiben weiterhin im Lookup-Contract gelockt.
- Jede künftige Anfrage von B an A (bezüglich desselben Datensatzes) innerhalb des definierten Zeitraums **z** releast immer wieder die Hälfte des verbliebenen gelockten Deposits.

- Nach Ablauf des definierten **Zeitraums z**
  - bekommt B den verbliebenen (nicht ausgeschütteten) Teil seines Deposits zurückerstattet.
  - wird der *Berechtigungs-Token* ungültig.
  - hat A keinen Anspruch mehr, für die Datenauslieferung an B vergütet zu werden (auch dann, falls er Daten ausgeliefert, ohne vorher die abgelaufene Gültigkeit des Berechtigungs-Tokens zu validieren).
- Es ist denkbar, die an der User ausgezahlten Rewards in irgendeiner Weise (zeitlich) zu locken und deren Release an bestimmte Bedingungen zu knüpfen ($\rightarrow$ um den User zu incentivieren irgendetwas zu tun).

Cashflow:

- Provider B zahlt für den Lookup. Aber auch nur dann, falls er den Lookup nutzt. Andernfalls erhält er seinen getätigten Deposit (abzüglich einer kleinen Fee an WunderPass) zurück. Er zahlt in gleichem Teil an Provider A und den User. Aus der Verwertung der bezogenen Daten kreiert er einen Value (im Sinne seiner Dienstleistung). Einen Value, der auch durchaus im Sinne des Users sein könnte. Es ist also gut denkbar, dass Provider B eine Rechtfertigung besitzt, den User an seinen Kosten zu beteiligen (z. B. mittels einer Fee für die erbrachte Dienstleitung, die den gekauften Datensatz erforderte; idealerweise ebenfalls in **WPT** vom User zu erbringen).
- Provider A ist der klare Nutznießer des Datenaustauschs. Der "Daten-Trade" hat - direkt betrachtet - erst einmal gar nichts mit seinem Kerngeschäfts zu tun (es sei denn, A sei wie in Beispiel 1 ein Identity-Data-Management-Service, dessen Kerngeschäft ausschließlich darin besteht, Daten zur Verfügung zu stellen). In der perfekten WunderWelt kann Provider A in einem anderen Case, analog als Provider B auftreten, um seine erhaltenen Token-Rewards für für ihn relevante Daten auszugeben.
- Der User scheint hierbei auch der Nutznießer von etwaigen "Daten-Deals" zu sein. Seine Stellung als solcher ist aber weniger klar als diejenige von Provider A, da er von dem stattgefundenen Datenaustausch indirekt ebenso profitieren könnte, indem er z. B. auf Basis der Datennutzung eine bessere Dienstleistung von Provider B erhält. Der Pitch "der User monetarisiert seine Daten" kling zwar sehr attraktiv, muss man hierbei jedoch sehr aufpassen, den Bogen nicht zu überspannen. Denn - während die Rolle von Provider A als Profiteur unbestreitbar ist - wird die Zahlungsbereitschaft von Provider B von Fall zu Fall ganz unterschiedlich und nur bedingt vorhanden sein. Denn schließlich ist es alles andere als selbsterklärend, ein Online-Shop solle für Adressdaten des Users bezahlen, um seine Bestellung zustellen zu können,

während der User davon profitiert. In diesem Fall wäre es eher nachvollziehbar, Provider B und der User würden sich die an Provider A zu entrichtenden Fees für die Bereitstellung der Adressdaten teilen. Hierbei ist die **Verteilung der Fees leider extrem heterogen**.

TODO

5.4.1 Einleitung

TODO

5.4.2 Kreislauf

TODO

5.4.3 Token-Design

TODO

5.4.4 Incentivierung

TODO

5.4.5 Milestones-Reward-Pool

TODO

5.4.6 WPT in Zahlen

TODO

5.4.7 Fazit

TODO

5.5 Fazit

TODO

6 NFT-Pass

Ein exzellentes Mittel, um *WunderPass* als Geschäftsmodell, Unternehmung und Unternehmen ein symbolisches - gewissermaßen plastisches - Sinnbild einzuverleiben, ist die Repräsentation von *WunderPass* als Service/Protokoll mittels eines - eigens dafür kreierten - NFTs: **"Des WunderPass"** (im Folgenden auch *NFT-Pass*)

Conclusion 4: WunderPass deabstrahiert durch "den WunderPass" als NFT

"Ich nutze *WunderPass*" wird symbolisiert durch "Ich besitze **meinen WunderPass**"!

6.1 Konzeption

Unser Anspruch an den zu modellierenden *NFT-Pass* ist grob der folgende:

- Der *NFT-Pass* muss sich ganz klar von dem Großteil der heutigen - in größter Regel als Sammlerstück verstandenen - den Markt überflutenden NFTs abgrenzen. Er braucht einen klar ersichtlichen **intrinsischen Wert**. Man muss also "etwas mit dem *NFT-Pass* anfangen können" und diesen nicht "nur besitzen", um ihn ausschließlich mit einer gewissen Wahrscheinlichkeit gewinnbringend weiterverkaufen zu können ("Hot Potato"). Der Token bedarf also gewisse Eigenschaften eines *Governance-Tokens* (DAO) oder Ähnlichem.
- Der *NFT-Pass* braucht ungeachtet des vorigen Bullets jedoch trotzdem zusätzlich ebenso eine ähnliche Beschaffenheit - wie solche der aktuell üblichen marktbeherrschenden NFTs - als Sammlerstück - gleichwohl nicht erstrangig.
- Anders als die aktuell gängigen NFTs soll unser *NFT-Pass* **nicht begrenzt** in der Anzahl seiner Stücke sein. Stattdessen sollen theoretisch beliebig viele *NFT-Pässe* existieren können. Nichtsdestotrotz soll unser *NFT-Pass* ebenso die Eigenschaft der nicht "inflationären Begehrtheit" einverleibt bekommen. Dies möchten wir mittels einer ausgeklügelten Minting-Logik abbilden, die ein **endliches Sub-Set** an raren und begehrten *NFT-Pässen* innerhalb des **unendlichen Gesamt-Set** der *NFT-Pässe* sicherstellt. Soll heißen: Es werden einerseits *NFT-Pässe* existieren, die den heutigen NFTs - im Sinne ihres Sammlerwertes - gleichkommen, während die restlichen andererseits mit ihrer steigenden Gesamtanzahl zunehmend entwerten, bis sie irgendwann (als NFT betrachtet) nahezu wertlos und lediglich "funktional" werden.
- Die Rarität und Begehrtheit unseres *NFT-Pass* soll Gamification-Mechanismen folgen:

  - Wir brauchen an etwaigen Stellen das (wertbestimmendes) first-come-first-serve-Prinzip.
  - Wir brauchen an anderen Stellen ein (ebenso wertbestimmendes) Zufallsprinzip.
  - Wir brauchen irgendwo ebenso ein (geringes) Maß an persönlicher Individualisierung des *NFT-Pass* - ausschließlich durch den User gesteuert.
  - Abrundend könnte ein **gemeinnützig wertbestimmendes** (randomisiertes) Merkmal wirken. (Beispiel: Wenn die *NFT-Pässe* irgendwann inflationär geworden sind, könnte der 10-Mio-ste plötzlich wieder richtig krass sein.)
- Der *NFT-Pass* muss gänzlich transparent und vor allem verständlich für den interessierten - gleichwohl vielleicht technisch nicht bewandertsten - User sein.

TODO: "Monalisa-Prinzip" (→ NFT ganz neu gedacht → USP)

Im folgenden ein initialer Abriss unserer Vorstellung des *NFT-Pass*:

NFT-Property 1: Pass-Status

Diese NFT-Property - die wir gleichzeitig als die Main-Property unseres *NFT-Pass* ansehen - soll der oben formulierten Anforderung nach einem first-come-first-serve-Prinzip Rechnung tragen. Zeitlich früher *ausgestellte NFT-Pässe* sollen einen rareren und begehrteren *Pass-Status* inne haben als die späteren. Und vor allem sollen die *NFT-Pässe* eines bestimmten ausgestellten Status in ihrer Anzahl begrenzt sein und nach Erreichen einer zu definierenden Höchstgrenze fortan nie wieder ausgestellt (gemintet) werden können.

Wir definieren folgende *NFT-Pass-Status* mit den dazugehörenden Eigenschaften:

- Status A (Diamond)
  - Anzahl Pässe: 200
  - Gemintet an Nummer: 1 bis 200
- Status B (Black)
  - Anzahl Pässe: 1.600
  - Gemintet an Nummer: 201 bis 1800
- Status C (Platin)
  - Anzahl Pässe: 12.800
  - Gemintet an Nummer: 1801 bis 14.600
- Status D (Rubin)
  - Anzahl Pässe: 102.400

  - Gemintet an Nummer: 14.601 bis 117.000
- Status E (Gold)
  - Anzahl Pässe: 819.200
  - Gemintet an Nummer: 117.001 bis 936.200
- Status F (Silver)
  - Anzahl Pässe: 6.553.600
  - Gemintet an Nummer: 936.201 bis 7.489.800
- Status G (Bronze)
  - Anzahl Pässe: 52.428.800
  - Gemintet an Nummer: 7.489.801 bis 59.918.600
- Status H (Pearl)
  - Anzahl Pässe: 419.430.400
  - Gemintet an Nummer: 59.918.601 bis 479.349.000
- Status I (White)
  - Anzahl Pässe: ∞
  - Gemintet an Nummer: 479.349.001 bis ∞

Diese NFT-Property ist per Definition trivialerweise **deterministisch**: Es ist stets zweifellos klar, welchen Status ein an x-ter Stelle geminteter *NFT-Pass* haben wird. Die hinzugezogene "Reverse-Halving-Logik" **belohnt die Early-Adopter** mit einem begehrten NFT, dessen Rarität per Protokoll mit der Zeit stets abnimmt.

Die Beschaffenheit dieser first-come-first-serve-Property soll jedoch einzigartig bleiben. Die folgenden Properties werden nicht mehr deterministisch sein, um unserem *NFT-Pass* ein **unvorherbestimmbares "Eigenleben"** einzuverleiben.

NFT-Property 2: Hologramm (Welt-Wunder)

Diese NFT-Property soll zwar einem ähnlichen abstufenden Raritätsprinzip zu Grunde liegen wie die Main-Property, dies jedoch nicht mehr einem first-come-first-serve- sondern stattdessen einem Zufallsprinzip folgend.

Ebenfalls abweichend von der Beschaffenheit der Main-Property soll bei dieser Property die Rarität nicht mittels einer absoluten Obergrenze abgebildet werden, sondern mittels einer relativen. (Dies zahlt auf die oben formulierte Anforderung nach einem **gemeinnützig gewinnbringendem Value** unseres *NFT-Pass* ein.

Wir definieren folgende *NFT-Pass-Hologramme* mit den dazugehörenden Eigen-

schaften:

- WW1
  - Mögliche Ausprägung: **Pyramiden von Gizeh**
  - Anteil Pässe: 0,390625% $\left(\frac{1}{256}\right)$
- WW2
  - Mögliche Ausprägung: **Chinesische Mauer**
  - Anteil Pässe: 0,78125% $\left(\frac{1}{128}\right)$
- WW3
  - Mögliche Ausprägung: **Steinstadt Petra**
  - Anteil Pässe: 1,5625% $\left(\frac{1}{64}\right)$
- WW4
  - Mögliche Ausprägung: **Kolosseum**
  - Anteil Pässe: 3,125% $\left(\frac{1}{32}\right)$
- WW5
  - Mögliche Ausprägung: **Chichén Itzá**
  - Anteil Pässe: 6,25% $\left(\frac{1}{16}\right)$
- WW6
  - Mögliche Ausprägung: **Machu Picchu**
  - Anteil Pässe: 12,5% $\left(\frac{1}{8}\right)$
- WW7
  - Mögliche Ausprägung: **Taj Mahal**
  - Anteil Pässe: 25% $\left(\frac{1}{4}\right)$
- WW8
  - Mögliche Ausprägung: **Christus-Statue Corcovado**
  - Anteil Pässe: 50% + x $\left(\frac{1}{2} + \frac{1}{256}\right)$

Das Besondere an dieser Property spiegelt sich in der Tatsache wider, gewisse rar beschaffene Ausprägungen seien nur "zeitweise" ausgeschöpft, da sich ihre (rare) Anzahl lediglich **relativ** an der Gesamtzahl der aktuell *ausgestellten NFT-Pässe* bemisst und nicht wie die Main-Property einer absoluten Obergrenze obliegt, deren Erreichung nicht wieder umkehrbar ist. Soll heißen: Ist die prozentuale Obergrenze an Pässen mit einer bestimmten Ausprägung der gegenwärtigen Property zu einem bestimmten Zeitpunkt erreicht, kann zwar für einen gewissen Zeitraum kein Pass mit dieser Ausprägung

mehr ausgestellt werden. Sobald jedoch die Gesamtanzahl der *ausgestellten NFT-Pässe* wieder groß genug ist - sodass die Anzahl der vorhandenen *NFT-Pässe* mit der besagten Ausprägung wieder die prozentuale Obergrenze unterschreitet - werden Pässe der besagten Ausprägung "wieder verfügbar".

Algorithmus 1: Verlosungs-Mechanismus für Hologramm-Property

- Zunächst bestimme man die Gesamtanzahl aller bisher geminteter Pässe n.
- Gleiches tue man nun für die Counts der geminteten Pässe pro Ausprägung der Hologramm-Property WW1 bis WW7 als entsprechende Größen $n_1, n_2, ..., n_7$.
- Und damit anschließend die aktuelle prozentuale Verteilung der Ausprägung auf die aktuell geminteten Pässe als $\sigma_i := \frac{n_i}{n}$ für $i \in \{1, ...7\}$ berechnen.
- Seien Θ_i für $i \in \{1, ...7\}$ die oben definierten **relativen** Obergrenzen der Ausprägungen der Hologramm-Property WW1 bis WW7.
- Alle Ausprägungen mit $\sigma_i \geq \Theta_i$ können zum aktuellen Zeitpunkt nicht vergeben werden und damit auch nicht beim Minting eines neuen Pass berücksichtigt werden.
- Für die Ausprägungen mit $\sigma_i < \Theta_i$ berechnen wir den Normierungsfaktor

$$\omega := \sum_{\sigma_i < \Theta_i} \Theta_i \ \leq 1$$

- Damit errechnen wir die aktuell vorliegenden Wahrscheinlichkeiten ρ_i für unsere Hologramm-Ausprägungen als

$$\rho_i := \begin{cases} 0, & \text{falls } \sigma_i \geq \Theta_i \\ \frac{\Theta_i}{\omega}, & \text{falls } \sigma_i < \Theta_i \end{cases}$$

Man vergewissere sich an dieser Stelle gedanklich, dass auch für die neuen Wahrscheinlichkeiten

$$\sum_{i=1}^{7} \rho_i \ = 1$$

gilt.

- Am Ende bestimme man mittels Randomisierung anhand der Wahrscheinlichkeiten ρ_i für $i \in \{1, ...7\}$ die zu vergebende Hologramm-Ausprägung.

NFT-Property 3: Background (Muster)

Diese NFT-Property soll ebenso wie die vorige einem ähnlichen abstufenden Raritätsprinzip zu Grunde liegen wie die Main-Property, dies jedoch ebenso nicht einem first-come-first-serve- sondern stattdessen einem Zufallsprinzip folgend.

Genauso wie bei der Main-Property soll die Rarität dieser Property einer absoluten Obergrenze obliegen, bei deren Erreichung fortan keine *NFT-Pässe* mit der erschöpften Property-Ausprägung mehr ausgestellt/gemintet werden können.

Wir definieren folgende *NFT-Pass-Background-Muster* mit den dazugehörenden Eigenschaften:

- M1
  - Mögliche Ausprägung: Muster festlegen
  - maximale Anzahl Pässe: 256
  - Wahrscheinlichkeit falls noch nicht aufgebraucht: 1,5625% $\left(\frac{1}{64}\right)$
- M2
  - Mögliche Ausprägung: Muster festlegen
  - maximale Anzahl Pässe: 4.096
  - Wahrscheinlichkeit falls noch nicht aufgebraucht: 3,125% $\left(\frac{1}{32}\right)$
- M3
  - Mögliche Ausprägung: Muster festlegen
  - maximale Anzahl Pässe: 65.536
  - Wahrscheinlichkeit falls noch nicht aufgebraucht: 6,25% $\left(\frac{1}{16}\right)$
- M4
  - Mögliche Ausprägung: Muster festlegen
  - maximale Anzahl Pässe: 1.048.576
  - Wahrscheinlichkeit falls noch nicht aufgebraucht: 12,5% $\left(\frac{1}{8}\right)$
- M5
  - Mögliche Ausprägung: Muster festlegen
  - maximale Anzahl Pässe: 16.777.216
  - Wahrscheinlichkeit falls noch nicht aufgebraucht: 25% $\left(\frac{1}{4}\right)$
- M6
  - Mögliche Ausprägung: Muster festlegen

- maximale Anzahl Pässe: unbegrenzt
- Wahrscheinlichkeit: 50% + x mit stets größer werdendem $x \in \left[\frac{1}{64}; \frac{1}{2}\right]$

Werden Pässe der Ausprägungen M1 bis M5 (aufgrund ihres Caps) im Laufe der Zeit aufgebraucht, geht deren Wahrscheinlichkeit auf die Property-Ausprägung M6 über. Für das x aus der Beschreibung der Ausprägung M6 gilt also:

$$x = \frac{1}{64} + \sum_{aufgebrauchte\ M \in \{M1;...;M5\}} Wahrscheinlichkeit(M)$$

Algorithmus 2: Verlosungs-Mechanismus für Background-Property

- Zunächst bestimme man die Gesamtanzahl aller bisher geminteter Pässe n.
- Gleiches tue man nun für die Counts der geminteten Pässe pro Ausprägung der Background-Property M1 bis M6 als entsprechende Größen $n_1, n_2, ..., n_6$.
- Seien Θ_i für $i \in \{1, ...6\}$ die oben definierten **absoluten** Obergrenzen der Ausprägungen der Background-Property M1 bis M6.
- Seien ρ_i für $i \in \{1, ...6\}$ die oben definierten Wahrscheinlichkeiten der Ausprägungen der Background-Property M1 bis M6, deren Auswahl wir hier zusätzlich formalisieren wollen:

$$\rho_i := \begin{cases} \frac{1}{2^{7-i}}, & \text{für } i = 1, ..., 5 \\ \frac{1}{2} + \frac{1}{2^6}, & \text{für } i = 6 \end{cases}$$

- Alle Ausprägungen mit $n_i \geq \Theta_i$ sind aufgebraucht und können weder zum aktuellen Zeitpunkt noch in der Zukunft vergeben werden und damit fortan auch nicht beim Minting eines neuen Pass berücksichtigt werden.
- Wir unterteilen die Ausprägungen der Background-Property in *"verbraucht"* und *"verfügbar"*:

$$\overline{M} := \{i \in \{1, ..., 6\} \mid n_i \geq \Theta_i\} \text{ [verbraucht]}$$
$$M := \{i \in \{1, ..., 6\} \mid n_i < \Theta_i\} \text{ [verfügbar]}$$

Man vergewissere sich an dieser Stelle gedanklich, dass $M \cap \overline{M} = \emptyset$, $M \cup \overline{M} = \{1, ..., 6\}$ und $6 \in M$ gelten.

- Ist eine bestimmte Ausprägung $i \in \{1, ..., 5\}$ verbraucht, soll ihre Wahrscheinlichkeit ρ_i auf die Ausprägung M6 übertragen werden (damit wir bei 100% bleiben).

- Damit errechnen wir die aktuell vorliegenden neuen Wahrscheinlichkeiten $\widehat{\rho}_i$ für unsere Background-Ausprägungen als

$$\widehat{\rho}_i := \begin{cases} 0, & \text{für } i \in \overline{M} \\ \rho_i, & \text{für } i \in M,\ i \neq 6 \\ \rho_1 + \sum_{i \in \overline{M}} \rho_i, & \text{für } i = 6 \end{cases}$$

Man vergewissere sich an dieser Stelle gedanklich, dass auch für die neuen Wahrscheinlichkeiten

$$\sum_{i=1}^{6} \widehat{\rho}_i \ = 1$$

gilt.

- Am Ende bestimme man mittels Randomisierung anhand der Wahrscheinlichkeiten $\widehat{\rho}_i$ für $i \in \{1, ...6\}$ die zu vergebende Background-Ausprägung.

NFT-Property 4: Community

TODO

Wrangel-Kiez → Berlin → Germany → Europe → WunderWorld → Sonnensystem → Milchstraße

TODO: Beispielrechnung für geminteten NFT-Pass mit der Nummer x

Angenommen x sei 1.005.965.

- vorrechnet, welche ersten 1.005.964 NFT-Pässe schon weggemintet sein könnten und Wahrscheinlichkeiten für den neu zu mintenden NFT-Pass erklären.

- neuen NFT-Pass unter Einbindung der Wahrscheinlichkeiten und vorgegaukelten Zufalls errechnet.

- geminteten neuen NFT-Pass als exakte Grafik in unserem Design hier abbilden.

TODO: Design
TODO: intrinsischer Wert mittels Berechtigungen als Governance-Token

TODO: Strategie des Minting und der Vergabe (Exploit-Prävention)

TODOs könnten als Teil der Tech-Deep-Dive-Termine erarbeitet werden.

6.2 Technische Umsetzung

TODO: technische Implementierung

- Abwandlung des ERC721-Standard, um unsere Metadaten-Logik zu bändigen.
- Die Metadaten werden wohl auch einem ähnlichen Konstrukt wie IPFS (off-chain) gespeichert werden und lediglich deren Hash als Datenfeld im Smart-Contract (on-chain), damit die Metadaten nicht nachträglich verändern werden können (dieses Vorgehen wird der absolute Standard sein).
- Unsere Metadaten sind jedoch so komplex, das deren Erzeugung (beim Minten) wohl einen zweiten Smart-Contract erfordern wird. Wir haben also quasi einen "Metadaten-Hybriden":
  - Erzeugung on-chain
  - Storing off-chain
- Der Metadaten-Smart-Contract wird die oben skizzierte Logik implementieren
  - Wie viele Pässe gibts es bereits und welche (hinsichtlich Properties)?
  - Wie sind die aktuellen Verteilungen der Properties und deren Contstraints
  - Einbindung von Randomisierungs-Orakeln
  - Sicherstellung, dass die erzeugten Metadaten auch tatsächlich vom Caller (ERC721-Contract) verwendet wurden und keine nachträgliche Manipulation stattgefunden hat.
- Es muss geklärt werden, ob hinsichtlich des Gedanken an den besagten "zweiten Smart-Contract" Standards/Best-Practices existieren, damit wir hier nicht das Rad neu erfinden.
- Es bleibt noch nicht ganz klar, wie die Metadaten nach ihrer Erzeugung nach IPFS gelangen, da dies laut meinem Verständnis ein Smart-Contract nicht selbst gewährleisten kann. Moritz Idee war grob die Folgende
  - Der Minting-Contract erzeugt den NFT, lässt seine Metadaten-Referenz jedoch zunächst ungesetzt (der NFT ist damit in gewisser Weise noch "unfertig"; kann in dem Zustand auch noch Constraints unterstellt sein).
  - Der Minting-Contract callt den Metadaten-Contract mit dem Anliegen, Metadaten zu dem "unfertigen" NFT mit der zugehörigen ID zu erzeugen.

- Der Metadaten-Contract erzeugt die Metadaten, hasht diese und gibt den Hash zurück an den Minting-Contract. Gleichzeitig publisht er ein Create-Event mit der Token-ID und den zugehörigen erzeugten Metadaten.
- Der Minting-Contract speichert den erhaltenen Metadaten-Hash und wartet auf "approvement".
- Das forcierte Event wird von einem dafür bestimmten (off-chain) Web3-Service vernommen und weiterverarbeitet: Die Metadaten werden geparst und nach IPFS gepusht. Als Ergebnis bekommen wir eine entsprechende IPFS-URI.
- Unser Web3-Service stößt anschließend eine "Set-URI"-Transaktion mit den entsprechenden Input-Daten (Token-ID; IPFS-URI) beim Minting-Contract an, um den gesamten Minting-Prozess für den neuen Token abzuschließen.
- Der Minting-Contract verifiziert die Metadaten mittels des gespeicherten Meta-Daten-Hashs (Hier ist nicht nicht ganz klar, wie. Ich weiß nicht, ob der Contract einfach die Daten von IPFS laden kann, um den Hash abzugleichen oder ob er vorher die URI implizit vorgeben muss, die irgendwie im Hash berücksichtigt werden muss, oder wie auch immer hier die Best-Practise aussieht) und updatet die NFT-URI auf den Wert der übergebenen IPFS-URI.
- Hiermit ist der Minting-Prozess abgeschlossen, der NFT "fertig" gemintet und kann von etwaigen "Temporary-Locked-Constraint" entbunden werden und vom neuen Besitzer frei verfügt werden.

- **Ein etwaiger Crypto-Freelancer muss auf die skizzierten Herausforderungen gechallenget werden.**

7 Abgrenzung zu SSI

TODO

TODO: DID scheint für uns eine zentralere Rolle zu spielen als SSI. DID sollten wir also eher in WunderPass einbinden, als uns davon distanzieren zu versuchen.

8 Dinge

TODO

9 Project 'Guard'

TODO

10 Community

TODO

11 Zusammenfassung

TODO

12 Anhang

Eine schöne Definition der Identität laut Döring, N. (1999). Sozialpsychologie des Internet.

Definition 5: Identität laut Döring, N. (1999). Sozialpsychologie des Internet.

Identität wird heute als komplexe Struktur aufgefasst, die aus einer Vielzahl einzelner Elemente besteht (Multiplizität), von denen in konkreten Situationen jeweils Teilmengen aktiviert sind oder aktiviert werden (Flexibilität). Eine Person hat aus dieser Perspektive nicht nur eine "wahre" Identität, sondern verfugt über eine Vielzahl an gruppen-, rollen-, raum-, körper- oder tätigkeitsbezogenen Teil-Identitäten.

Folgende hilfreiche Zitate, Aussagen und Formulierungen entstammen der Diplomarbeit "Identitäten und ihre Schnittstellen auf Basis von Ontologien in einer dezentralen Umgebung".

Zitat 1: Betrachtungsweise der digitalen Identität

In der Informatik finden sowohl der rein mathematische Identitätsbegriff Verwendung – ein Standardkonzept in den meisten Programmiersprachen –, als auch der sozialpsychologische Aspekt dieses Begriffs. In dieser Arbeit ist ein Identitätsbegriff der Betrachtungsgegenstand, der von beiden Seiten inspiriert ist. Der mathematische Identitätsbegriff bildet die Grundlage: Anhand eines Identifikators ist eine Identität eindeutig bestimmbar. Dieser Identifikator wird angereichert durch eine beliebige Vielfalt an ergänzenden Attributen und ihre situationsbedingt eingeschränkte Verwendung.

Zitat 2: Avatar

Diesem Vorbild der Newsgroup-Nutzer folgend unterstützen viele Foren-Systeme im ¨ World Wide Web von vornherein das Anlegen eines Identitäts-Profils. Neben diversen Identitäts- und Nutzungsdaten kann hier oft ein **Bild als Stellvertreter und Wiedererkennungsmerkmal und emotionale Botschaft eingesetzt** werden, für welches der Begriff **"Avatar"** geprägt wurde. [...]

Einen Nachteil neben der mangelnden Standardisierbarkeit und dem demzufolge bestehenden Mangel an automatischer Auswertbarkeit weist die Identitätsdarstellung im World Wide Web ebenfalls noch auf: Es gibt keine praktikable Möglichkeit, zu bestimmen, wer auf diese Daten zugreifen kann und wer nicht. Daten, die sich im World Wide Web befinden, sind im Allgemeinen für jeden einsehbar.

Zitat 3: Web-Visitenkarte

Im Rahmen des World Wide Webs hat sich eine Variante privater Homepages herausgebildet, die als Hauptmerkmal die Darstellung der eigenen Person aufweist. Die starke Verbreitung dieser persönlichen Homepages oder Web-Visitenkarten ist [...] ein Indiz fur den starken Bedarf nach individueller Darstellung der eigenen Identität im virtuellen Raum.

Zitat 4: Skepsis hinsichtlich Datenerfassung

Als Reaktion auf solche - in Abschnitt 2.3 zitierte - oftmals ungefragt oder aber vom Anwender ungewünscht erfolgenden Datenerfassungsmethoden werden Gegenmaßnahmen eingesetzt: Bei der Dateneingabe werden **bewusst Falschangaben vorgenommen** oder Cookies und die Quellen von Web-Bugs werden blockiert. Dies geschieht insbesondere bei **Anbietern, bei denen die Daten nicht zwingend benötigt werden** oder deren Notwendigkeit zur Erfassung dem Nutzer nicht einsichtig ist. Insgesamt hat das Vorgehen vieler Anbieter zumindest bei kritischen

Nutzern des Internets ein starkes Misstrauen gegenüber diesen Techniken geweckt. So finden die Gegenmaßnahmen – zum Beispiel die Blockade von Cookies – auch dann leicht statt, wenn sie unbegründet wäre und vielmehr ein echter Vorteil dadurch ermöglicht wurde. Ein Beispiel für einen solchen Vorteil ist die Vereinfachung und Individualisierung von Informationsangeboten durch personalisierte Darstellung.

Zitat 5: Misstrauen vernichtet Value

Insgesamt hat das Vorgehen vieler Anbieter zumindest bei kritischen Nutzern des Internets ein starkes Misstrauen gegenüber diesen Techniken geweckt. So finden die Gegenmaßnahmen – zum Beispiel die Blockade von Cookies – auch dann leicht statt, wenn sie unbegründet wäre und vielmehr ein echter Vorteil dadurch ermöglicht wurde. Ein Beispiel für einen solchen Vorteil ist die Vereinfachung und Individualisierung von Informationsangeboten durch personalisierte Darstellung.

Weniger kritische Nutzer und solche, die sich ein differenziertes Bild über die Vor- und Nachteile dieser Techniken verschafft haben, erhalten für sie speziell zusammengestellte Inhalte, bekommen relevante Angebote unterbreitet oder haben die Möglichkeit, mit anderen Nutzern mit ähnlichen Interessen oder mit entsprechend ähnlichen Fähigkeiten in Kontakt zu treten. Dieser Nutzen gilt allerdings immer nur im eingeschränkten Bereich innerhalb eines Angebotes.

Zitat 6: Synonymisierung

[...] Dabei geht es nicht immer um eine der Wirklichkeit entsprechende Darstellung, sondern oftmals auch um **spielerische** oder die reale Identität **verschleiernde Pseudonyme** und Rollen-Repräsentationen. Manche Dienste – Online-Spiele beispielsweise – fordern dies sogar explizit ein, während andere – zum Beispiel Instant Messenger – dies problemlos ermöglichen. Wesentlich ist bei beiden die Kontinuität der Identifizierbarkeit. **Auch hier gilt die Beschränkung der Nutzbarkeit der Identitätsdaten auf einen Dienst**. Dies ist beim Beispiel des Online-Spiels wohl auch grundsätzlich sinnvoll – die erschaffene Spiel-Identität hat schließlich oftmals wenig mit der realen Identität gemein –, beim Instant Messaging aber schon **weniger gewünscht**.

Zitat 7: Identitätsdaten

Identitätsdaten sind variantenreich und individuell und beschränken sich nicht auf einen Kundendatensatz oder Anmeldedaten für Online-Dienste. Dies sind allerdings bisher die ¨ Hauptbereiche, in denen Identitätsdaten heute zum Einsatz kommen. Die Daten einer Identität müssen aber alle Aspekte einer solchen abbilden können. Diese Vielzahl an persönlichen und auch personengebundenen Daten kann

viele **Erleichterungen und Automatisierungen** mit sich bringen, birgt aber **auch Risiken** und **erschwert die Handhabung**. So ist bei einer Betrachtung von Konzepten zu einem Identitätsmanagement immer auch der Blick zu richten auf die **Frage nach der Kontrolle der Daten** durch den Anwender, nach den **Verwendungsmöglichkeiten durch zur Nutzung dieser Daten** berechtigte Personen und nach Möglichkeiten des **unvorhergesehenen Missbrauchs**. Als noch entscheidenderes Kriterium für die **Akzeptanz durch die Anwender** ist aber sicherlich die Frage nach dem **Mehraufwand**: Kann ein Konzept, beziehungsweise seine Umsetzung in einer Anwendung gewisse Kriterien erfüllen, **dass es der Anwender als vorteilhaft und nicht als belastend wertet**? [...]

Wichtige Aspekte aus dem letzten Zitat:

- Pros
  - Erleichterungen und Automatisierungen
  - Kontrolle der Daten beim User
  - Verwendungsmöglichkeiten durch Nutzung der Daten
- Kontras
  - Risiken
  - erschwerte Handhabe
  - Kontrolle der Daten beim Provider
  - unvorhergesehener Missbrauch
- Akzeptanz → Rechtfertigt der Nutzen den Mehraufwand?

Zitat 8: E-Mail (auch als Identifier)

Der E-Mail-Standard ist sicher kein Standard für ein Identiätsmanagement. Er sei hier aber erwähnt, da es sich um den ältesten und am weitesten verbreiteten digitalen Standard handelt, der sich primär auf Individuen und somit Identitäten bezieht. [...]

Neben dem reinen Aspekt der gegenseitigen Erreichbarkeit weist eine E-Mail-Adresse nur durch die – heute oft freie – Wahl der Kennung Individualität auf. Die meisten E-Mail-Systeme interpretieren ebenfalls zusätzliche Angaben des vollen Namens und der Organisation. Neben der eher "seriösen" Variante, den eigenen Namen in voller oder teilweise abgekürzter Form zu verwenden, versuchen viele Personen eine bestimmte Geisteshaltung, Zuneigung oder Gruppenzugehörigkeit durch die Wahl der richtigen Kennung auszudrücken. Genau hier ist aber auch schon die Grenze des E-Mail-Standards als Identitätskonzept erreicht: Weder lässt sich eine Namenswahl klar deuten – es sei denn, man ist mit dem weiteren Kontext des Anwenders vertraut –, noch lässt sich dieses durch automatische Prozesse sinnvoll

auswerten. **Eine E-Mail-Adresse bleibt als Identitätskonzept das, was sie von Anfang an auch nur sein sollte: Ein eindeutiges Identifizierungszeichen, um der damit verknüpften Identität Daten zukommen lassen zu können.**

Zitat 9: Workaround im Status quo

Die wenigen bisherigen Standards und auch andere Konzepte ermöglichen nicht mehr als die Speicherung der eigenen Kennung, Kontaktdaten oder Daten zum Bezahlen. [...]

Viele Anwender verwalten schon heute eine Reihe von Daten, die auf Basis einer digitalen Identitäten-Infrastruktur zusammengefasst betrachtet werden könnten: Dazu zählen solche Dinge wie das digitale Adressbuch, ein Kalender, die Lesezeichen, Verwaltungsdaten von Sammlungen (beispielsweise Fotos, Bücher oder Musik), ¨ Wunschlisten (beispielsweise bei Onlineshops), Lebensläufe, **Ergebnisstände von Computerspielen** und vieles mehr. All diese Daten liegen bisher in verschiedenen Strukturen vor, ohne Gesamtstruktur und **ohne, dass sich automatisierte Querbezüge bei Bedarf herstellen ließen, obwohl es alles Daten sind, die sich der Identität des Anwenders zuordnen ließen**. Diese fehlende Gesamtstruktur kann zur Folge unerwünschte **Redundanzen und auch Inkonsistenzen** mit sich bringen.

Zitat 10: Übergeordnete Struktur → "Querverweise"

[...] Notwendig ist hierbei eine zusätzliche Struktur, die – ohne die bestehenden Daten und ihren eventuell aktuellen Bezug zueinander zu verändern – diesen Daten eine Gesamtstruktur verleiht: eine Identitätsdatengesamtstruktur. Auf diese Weise ließen sich Daten wie bisher speichern. Zusätzlich ließen sich mittels dieser Struktur aber auch Zusammenhänge herstellen, die unabhängig von der ursprünglichen Gebundenheit der Daten bestünden.

Derart ließen sich auch Identitätsdaten auf automatisierte Weise kontrolliert weitergeben. **"Kontrolliert" in diesem Zusammenhang bedeutet die Möglichkeit für den Anwender, selbst zu entscheiden, an wen er welche Daten wann und zu welchen Bedingungen übermittelt.** Dies ließe sich leicht bewerkstelligen, indem er Teile der Struktur mit entsprechenden Freigaben oder Einschränkungen versähe. Einen geeigneten Kommunikations- oder Kooperationsdienst vorausgesetzt, könnte der Anwender so bestimmten anderen Anwendern gezielt Daten über sich zukommen lassen, ohne sich selbst um die Zusammenstellung dieser Daten oder deren Übertragung kümmern zu müssen.

Conclusion 5: Link zu WunderPass

Insbesondere das letzte Zitat schreit förmlich nach WunderPass. Die "Struktur", von der dort abstrakt die Rede ist, heißt "WunderPass" (zumindest auf den Aspekt der "Querverweise" bezogen).

Zitat 11: Herausforderung

Der Ansatz, einen Großteil der persönlichen Daten strukturell der Identität zuzuordnen, bietet ein großes Potenzial für die Personalisierung und Individualisierung in Datennetzen. Es bestehen allerdings auch grunds¨atzliche Probleme, die ein solches Konzept überwinden muss: Wenn individuelle und umfassende Strukturen die Identitätsdaten in einen Gesamtzusammenhang bringen sollen, so müssen diese Strukturen erstellt werden. Wenn die Strukturen die Kommunikation unterstützen sollen, muss die individuelle ¨ Struktur auf Empfängerseite bekannt sein, um dort von Vorteil sein zu können.

Conclusion 6: Link zu WunderPass

Das letzte Zitat beschreibt nicht anderes als unser "Henne-Ei-Problem" hinsichtlich der Anbindung WunderPasses an Drittanbieter.

Conclusion 7: Aufwand beim User

Die Forderung nach oben zitierter Struktur (aka WunderPass) erfordert aber das Zutun des Users, welches mit nicht unerheblichem Aufwand einhergeht. Die Vorteile genannter Struktur werden dabei nicht zwangsläufig von Anfang an für den User ersichtlich sein. Das bedeutet im Umkehrschluss, er müsse zu einem Aufwand gedrängt werden, dessen Mehrwert sich für ihn kaum erschließt.

Es erfordert als eines Incentivierungs-Mechanismus (z. B. als Bestandteil etwaiger Token-Economics). Gleichzeitig ist es aus dem Blickwinkel des gesamten Ökosystems nicht zu rechtfertigen, der User werde ausschließlich aufgrund seiner Ignoranz - nämlich seine eigenen Vorteile aus obiger Struktur nicht erkennen zu können - Nutznießer von (vom Ökosystem gemeinschaftlich getragenen) Incentives. Daher wäre ein Hebel innerhalb der Token-Economics wünschenswert, der den User - ab Eintreten persönlicher Vorteile durch die "Querverweise" - die ausgeschütteten Incentives wieder zurückzahlen lässt.