

# WunderPass-White-Paper

G. Fricke, S.Tschurilin

March 15, 2022, Berlin

## Contents

<b>1 Abstract</b>	<b>2</b>
<b>2 Einleitung</b>	<b>3</b>
2.1 Identität . . . . .	3
2.2 Verständnis der digitalen Identität . . . . .	4
2.3 Missstände der digitalen Identität . . . . .	6
<b>3 Vision</b>	<b>10</b>
<b>4 Unser Ansatz</b>	<b>13</b>
<b>5 Economics</b>	<b>13</b>
5.1 Einleitung . . . . .	13
5.2 Goals . . . . .	18
5.3 Quantifizierung . . . . .	18
5.3.1 Grundlegende Definitionen . . . . .	18
5.3.2 Zustandsbeschreibung der digitalen Welt . . . . .	20
5.3.3 Zustandsbeschreibung WunderPass - simple Betrachtung . . . . .	22
5.3.4 Zustandsbeschreibung WunderPass - detaillierte Sicht . . . . .	30
5.3.5 Other Stuff . . . . .	40
5.3.6 Business-Plan in Mathematics . . . . .	44
5.3.7 Quantifizierung des Status quo . . . . .	44
5.3.8 Individuelle Wertschöpfung der Teilnehmer . . . . .	46
5.4 Token-Economics (WPT) . . . . .	46
5.4.1 Einleitung . . . . .	46
5.4.2 Lösungsideen . . . . .	49
5.4.3 Einbindung der Investing-Pools . . . . .	49
5.4.4 Bonding-Curves . . . . .	53
5.4.5 Lösungsidee 2 . . . . .	61
5.4.6 Kreislauf . . . . .	64
5.4.7 Token-Design . . . . .	64

5.4.8	Incentivierung . . . . .	64
5.4.9	Milestones-Reward-Pool . . . . .	64
5.4.10	WPT in Zahlen . . . . .	64
5.4.11	Fazit . . . . .	64
5.5	Fazit . . . . .	64
<b>6</b>	<b>NFT-Pass</b>	<b>64</b>
6.1	Konzeption . . . . .	65
6.1.1	Status-Property . . . . .	66
6.1.2	Hologramm . . . . .	67
6.1.3	Pattern-Property . . . . .	70
6.1.4	Edition . . . . .	71
6.1.5	Design . . . . .	73
6.1.6	Beispielhafte Analyse der Collection . . . . .	74
6.1.7	Intrinsischer Wert . . . . .	77
6.2	Technische Umsetzung . . . . .	79
<b>7</b>	<b>Abgrenzung zu SSI</b>	<b>81</b>
<b>8</b>	<b>Project 'Guard'</b>	<b>81</b>
<b>9</b>	<b>Project 'Pools'</b>	<b>81</b>
9.1	Einleitung . . . . .	81
9.2	Formalisierungen . . . . .	83
9.3	Pool-Erzeugung . . . . .	84
9.4	Pool-Lifetime . . . . .	86
9.5	Pool-Liquidierung . . . . .	88
9.6	Pool-Vertrag . . . . .	89
9.7	Pool-Economics . . . . .	90
<b>10</b>	<b>Community</b>	<b>97</b>
<b>11</b>	<b>Zusammenfassung</b>	<b>97</b>
<b>12</b>	<b>Anhang</b>	<b>97</b>

## 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. Zum mindesten 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 **einzigem 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 längst 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 Iden-

tität 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 hinwiegtauschen, 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 erzwungenen 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-Lieferservice 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 verwaltung 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-ins**).
- 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-ins**).

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 Konsenses, 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 Phishing 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

### 5.1 Einleitung

Wir beginnen mit einer gewagten Behauptung:

#### Hypothese 1: Daten haben einen Wert

**Digitale Daten besitzen einen realen** (nicht leicht zu beziffernden) **Value** - zumindest für die von ihnen direkt oder indirekt adressierten digitalen Individuen (User und Service-Provider). Dieser Value existiert bereits in Isolation des einzelnen

Datensatzes, wird aber mit Zunahme der verfügbaren Gesamtdaten innerhalb eines Netzwerks durch entstehende Synergien nicht nur in Summe sondern zudem ebenfalls pro einzelnen Datensatz stets größer (Netzwerkeffekt). Eine einzelne Information - ein Datensatz - besitzt also bereits einen isolierten Mehrwert - anfangs vielleicht nur für sehr wenige Teilnehmer des Netzwerks - und gewinnt zudem zunehmend weiter an Wert mit Wachstum des "Wissens" des Gesamtnetzwerks und verhilft auch anderen Dateninformationen zu deren Wertsteigerung.

Wir behaupten damit also, jeder digitale Datensatz habe sogar einen Value über die von ihm adressierten digitalen Individuen hinaus. Und zwar für die Gesamtheit des Netzwerks und all seiner Teilnehmer. Dies jedoch natürlich nicht im gleichen Maße für alle.

Damit ist **digitale Datenerfassung und -auswertung wertschöpfend** für die gesamte digitale Welt und wünschenswert. Lediglich die **Verteilung des geschöpften Values muss hinterfragt werden**. Wir möchten ein Ökosystem definieren, der genau dies gerecht und transparent tut.

Rein formal mathematisch betrachtet, ist die formulierte Behauptung ziemlich einleuchtend - zumindest wenn man auf die Forderung, dieser "Value" (sei er mit  $v_{data}$  bezeichnet) habe ein positives Vorzeichen, verzichtet. Als "Value" also zunächst lediglich abstrakt einen "Impact" annimmt (der auch einen "Schaden" mit  $v_{data} < 0$  darstellen könnte, wenn die Daten in irgendeiner Weise missbraucht werden). Von

$$|v_{data}| > 0$$

können wir also ziemlich bedenkenlos ausgehen.

Auf der gesellschaftlich/sozialen Ebene wird man dagegen deutlich mehr Widerspruch zur getätigten Hypothese ernten (bzw. von abstrakt-denken-könnenden Menschen zumindest das negative Vorzeichen von  $v_{data}$  vorgehalten bekommen). Denn leider ist die elektronische Datenverarbeitung - in ihrem wahren Sinne des Wortes - ziemlich in Verruf geraten. Man hört den Tadel von mit Datenschutz in Verbindung gebrachten Missständen deutlich lauter als die Anerkennung des Nutzens von Datenerfassung und ihrer Verarbeitung - auf die im Übrigen so gut wie niemand mehr verzichten können würde. Weil Menschen eben schnell vergessen und zudem in der Regel kein ausreichendes technisches Verständnis besitzen.

Kein Mensch würde doch heute wieder bei Taxizentralen anrufen wollen und seine Abholadresse durchgeben, weil GPS-Lokalisierungen unterbunden werden sollen. Gleichermaßen bei Food-Lieferanten. Und auch nur die Wenigsten auf die Intelligenz von Google, weil Google nur das für uns tun kann, was sie für uns tun, weil sie das über uns wissen, was sie eben über uns wissen. Der Zug in diesem Kontext ist bereits unumkehrbar abgefahren. Weil eben selbst so gut wie in jeder Lebenssituation von dem besagten Daten-Value  $v_{data}$  profitieren. Und zwar mit unbestreitbarem positiven Vorzeichen.

Was die besagten Datenschutz-Skeptiker da beanstanden, ist tatsächlich etwas ganz anderes als sie glauben: Es ist nicht die Datenerfassung, -verarbeitung und -monetarisierung,

sondern die teils unfaire Verteilung von  $v_{data}$  an die Netzwerkteilnehmer (insbesondere die beteiligten). Das ist auch genau das Problem, was wir mit WunderPass zu lösen versuchen.

Aber zunächst einmal zurück zu unserer einleitenden Hypothese. Sie formal zu beweisen ist äußerst schwer - wenn nicht gar unmöglich. Sie ist aber - laut unserer festen Überzeugung - trotzdem wahr, was wir an folgendem vielschichtigem (zugegeben ziemlich konstruiertem) Beispiel - bestehend aus "Journeys" mehrerer User - veranschaulichen möchten.

### Beispiel 1: Ökosystem von Datensätzen

#### Setup:

- User A plant im Zeitraum x eine Reise von Berlin nach London.
  - User A hat bereits seinen Flug bei einem Flug-Provider gebucht (z. B. EasyJet).
  - User A hat ebenso ein Hotel gebucht (z. B. über HRS).
  - User A besitzt einen Airbnb-Account und hat in dem letzten Jahr bereits häufig Wohnungen im Ausland angemietet.
- User B plant in demselben (oder zumindest stark überlappenden) Zeitraum x eine Reise von London nach Berlin.
  - User B hat ebenso seinen Flug gebucht - und zwar bei demselben Flug-Provider wie User A.
  - User B hat für den Zeitraum seiner Abwesenheit seine Wohnung in London bei Airbnb zur Vermietung eingestellt, jedoch bisher kein Angebot erhalten.
  - User B hat für seinen Aufenthalt in Berlin ein Auto bei einem Autovermietung-Provider (z. B. Sixt) reserviert.
  - User B scheint keinen Account bei Providern privaten Car-Sharings (wie Drivy) zu besitzen.
- User C wohnt in Berlin, besitzt ein Auto, welches er im Zeitraum x (oder einem überlappenden Zeitraum) nicht benötigt, und es deshalb bei einem Provider von privatem Car-Sharing (z. B. Drivy) zur Vermietung angeboten, ohne jedoch bisher ein Angebot erhalten zu haben.

#### Informationsgehalt & -value:

Wir wollen an dieser Stelle den gänzlich offensichtlichen (und tendenziell isolierten) Informationsgehalt/Datenverarbeitung - wie z. B. Reservierungsbestätigungen, Rechnungen oder schlichtweg zusammenfassende "Reminder" - der im obigen Setup-Kontext stehenden Daten ignorieren und diese stattdessen in einem deutlich stärker "rausgezoomten" und übergeordnetem Kontext betrachten und auf mögliche Synergien auswerten.

Im Folgenden eine punktuelle Zusammenfassung der relevanten Informationen bzw. vorliegenden Datensätzen unseres Beispiel-Szenarios - teils samt erfolgter Interpretation:

insight	Information	time	data owner
<b>info 1</b>	[Berlin → London] zu Zeitraum x	x	EasyJet und User A
<b>info 2</b>	[London → Berlin] zu Zeitraum x	x	EasyJet und User B
<b>info 3</b>	User A benötigt Unterkunft in London	x	1st: User A 2nd: EasyJet & HRS
<b>info 4</b>	User A hat Unterkunft in London	x	HRS und User A
<b>info 5</b>	User A hätte theoretisch Interesse an Airbnb- Wohnung in London	x	Airbnb und User A
<b>info 6</b>	User B sucht einen Mieter für Wohnung in London	≈ x	Airbnb und User B
<b>info 7</b>	User B benötigt ein Auto in Berlin	≈ x	Sixt und User B
<b>info 8</b>	User C möchte sein Auto in Berlin vermieten	≈ x	Drivy und User C

Aus obiger Auflistung wird bereits ersichtlich, worauf wir hier eigentlich hinauswollen: Nämlich die offensichtliche Tatsache, die tatsächliche "Journey" weiche möglicherweise stark von der optimalen "Journey" (optimal im Sinne der Gesamtheit aller betroffenen Teilnehmer unseres Beispiel-Cases) ab, weil kein *vollumfängliches Wissen aller beteiligten Teilnehmer über alle Gegebenheiten besteht*. Das Problem hierbei ist schlichtweg die Tatsache, dass oben aufgezählte *Insights* nur einigen der Teilnehmer bekannt sind, jedoch auch andere Teilnehmer betreffen. Wir können hierbei von *Informations-Vor- und nachteilen* bestimmter Teilnehmer sprechen.

Angenommen obige *Insights* lägen allen Teilnehmern vor. Dann ergäben sich folgende zusätzliche *Insights*:

insight	Information	owner
info 9	User A könnte Wohnung von User B in London mieten	"Gott"
info 10	<b>gegeben Info 9:</b> (1) Stornierungsrisiko der HRS-Buchung seitens User A (2) HRS könnte u. U. das Zimmer von User A gewinnbringender weitervermieten (bei großer Nachfrage)	"Gott"
info 11	User B könnte den Wagen von User C in Berlin anmieten	"Gott"
info 12	<b>gegeben Info 11:</b> (1) Stornierungsrisiko der Sixt-Reservierung seitens User B (2) Sixt könnte u. U. den reservierten Wagen von User B gewinnbringender vermieten (bei großer Nachfrage)	"Gott"

Zusammenfassend stellen wir den bisher aufgearbeiteten Informationsgehalt pro betroffenen Teilnehmer auf.

Legende:

User A sei abgekürzt mit **A**, User B mit **B** und User C mit **C**.

EasyJet sei mit **EJ**, HRS mit **HRS**, Airbnb mit **ABN**, Sixt mit **SX** und Drivy mit **DRV**.

info	owner	A	B	C	EJ	HRS	ABN	SX	DRV
1	<b>A + EJ</b>	✓	+	(o)	✓	+	+	+	+
2	<b>B + EJ</b>	(o)	✓	+	✓	+	+	+	+
3	<b>A + evtl. (EJ+HRS)</b>	✓	++	(o)	(o)	++	++	(o)	(o)
4	<b>A + HRS</b>	✓	?	(o)	(o)	✓	?	(o)	(o)
5	<b>A + ABN</b>	✓	++	(o)	(o)	?	✓	(o)	(o)
6	<b>B + ABN</b>	++	✓	(o)	(o)	(o)	✓	(o)	(o)
7	<b>B + SX</b>	(o)	✓	++	(o)	(o)	(o)	✓	++
8	<b>C + DRV</b>	(o)	++	✓	(o)	(o)	(o)	(o)	✓
9	—	+++	+++	(o)	(o)	--	++	(o)	(o)
10	—	✓	✓	(o)	(o)	+++	(o)	(o)	(o)
11	—	(o)	+++	+++	(o)	(o)	(o)	--	++
12	—	(o)	✓	✓	(o)	(o)	(o)	+++	(o)

Interpretation Verlierer/Gewinner der zusätzlichen Insights:

- Info 9 ist zwar absolut nicht im Sinne von HRS, kann HRS jedoch das Bekanntwerden dieser Info nicht verhindern, bekommt Info 10 für sie an signifikanter Relevanz (Value).
- Gleiches gilt für die Infos 11 und 12 aus Sicht von Sixt.

Gesamt-Value mit zusätzlichen Insights vs. ohne

WIP

## 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 verkonsument
- 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 verrechnet 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 5.4.9 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

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

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

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  $t \in \mathbf{T}$  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

$$U^{(t)} = \{u_1^{(t)}; u_2^{(t)}; \dots; u_n^{(t)}\}$$

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

### Definition 2

$$S^{(t)} = \{s_1^{(t)}; s_2^{(t)}; \dots; s_m^{(t)}\}$$

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 Funk-

tion  $\alpha^{(t)}$ , die über über die Tatsache "*is connected*" bzw. "*is not connected*" entscheidet:

### Definition 3

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

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

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

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

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  $u_{n^{(t)}}^{(t)}$  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

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

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  $(n^{(t)}, m^{(t)}) = dP^{(t)}$  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

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

nicht ganz abwegig. Genauso wenig unvernünftig scheint die Annahme, WunderPass begäne seine Weltoberung mit einem MVP mit lediglich einem einzigen Service-Provider - z. B. dem Guard (siehe Kap. 8] - und einer überschaubaren Anzahl an angepeilten Usern, also

$$n^{(t_0)} \approx 1.000 \text{ und } m^{(t_0)} = 1 \text{ bzw.} \\ dP^{(t_0)} \approx (1.000, 1) \quad (\text{iii})$$

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  $(n^{(t)}, m^{(t)}) = dP^{(t)}$  gilt:

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

Wir fassen Annahme 2 in einer abschließenden Definition zusammen:

#### Definition 4

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

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

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

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

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

Für die diskrete/sortierte Variante ist dies wieder gleichbedeutend mit

$$\widehat{U}^{(t)} = \left\{ \widehat{u}_1^{(t)}; \widehat{u}_2^{(t)}; \dots; \widehat{u}_{\widehat{n}}^{(t)} \right\} \quad (\text{iii})$$

$$\widehat{S}^{(t)} = \left\{ \widehat{s}_1^{(t)}; \widehat{s}_2^{(t)}; \dots; \widehat{s}_{\widehat{m}}^{(t)} \right\} \quad (\text{iv})$$

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"

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

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:

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

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

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

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

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

Nun beweisen wir folgende sich ergebende Zusammenhänge:

### Theorem 2

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

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

$$\Gamma(t) = \sum_{i=1}^{\hat{n}} \sum_{j=1}^{\hat{m}} \hat{\alpha}_{ij}^{(t)} \quad (\text{i})$$

$$\hat{n} \leq \Gamma(t) \leq \hat{n} * \hat{m} \quad (\text{ii})$$

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

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

Man beachte, Aussage (ii) impliziert insbesondere

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

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):

$\Gamma(t) \leq \hat{n} * \hat{m}$  ergibt sich aus

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

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

$$\begin{aligned} \Gamma(t) &\stackrel{(\text{i})}{=} \sum_{i=1}^{\hat{n}} \sum_{j=1}^{\hat{m}} \hat{\alpha}_{ij}^{(t)} \\ &\stackrel{(\text{Def 5})}{\geq} \sum_{i=1}^{\hat{n}} 1 = \hat{n} \end{aligned}$$

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

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

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

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

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

Widerspruch!

□

## Messbarkeit Status quo

Kommend von der intuitiven Annahme, die Größe der definierten "connected Pools"  $\hat{U}^{(t)}$  und  $\hat{S}^{(t)}$  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

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

seien umso besser je größer sie seien. Alle der eben genannten Größen, denen wir hier eine intuitiv spürbare "Erstrebenswertigkeit" beimesse, 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:

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

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

Mittels  $R_{\leq}$  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  $(t_1, t_2) \in R_{\leq}$  gilt.

Wir schreiben fortan statt  $(t_1, t_2) \in R_{\leq}$  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 " $\leq$ ", 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  $\hat{n}$  und  $\hat{m}$  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  $\hat{m} = 5$  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  $\hat{n} = 50.000$  angebundenen Usern ausgehen, von denen je 10.000 mit je einem einzigen der  $\hat{m} = 5$  Provider connectet wären und keinem anderem.
2. Genauso könnten dieselben  $\hat{n} = 50.000$  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  $\hat{n} \approx 25.000$ , 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  $\hat{n}$ ,  $\hat{m}$ ,  $\Gamma(t)$  gemessen, scheint Fall (3) aufgrund von  $\hat{n} = 25.000$  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.  $\Gamma_1(t) = 50.000, \hat{n}_1 = 50.000$  und  $\hat{m}_1 = 5$
2.  $\Gamma_2(t) = 50.000, \hat{n}_2 = 50.000$  und  $\hat{m}_2 = 1$
3.  $\Gamma_3(t) = 50.000, \hat{n}_3 = 25.000$  und  $\hat{m}_3 = 2$

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  $\hat{u} \in \hat{U}^{(t)}$  und Service-Providern  $\hat{s} \in \hat{S}^{(t)}$ . Jedoch bestehen ebenfalls signifikante Unterschiede jeweils innerhalb der beiden Teilnehmerklassen  $\hat{U}^{(t)}$  und  $\hat{S}^{(t)}$  (siehe [TODO: Links]). Um dieser Unterscheidung unserer Teilnehmer gerecht zu werden, definieren wir "connected Pools" pro individuellen Teilnehmer als

#### Definition 9

Sei  $t \in T$ ,  $\hat{U}^{(t)}$  und  $\hat{S}^{(t)}$  die übergeordneten "connected" User- und Provider-Pools und  $\hat{u}_* \in \hat{U}^{(t)}$  und  $\hat{s}_* \in \hat{S}^{(t)}$  die entsprechenden Teilnehmer, für deren individuelle "connected Pools" wir uns an dieser Stelle interessieren. Wir definieren die genannten "connected Pools" als

$$\begin{aligned} accounts : \hat{U}^{(t)} &\rightarrow \mathcal{P}(\hat{S}^{(t)}) \\ accounts^{(t)}(\hat{u}_*) &= \left\{ \hat{s} \in \hat{S}^{(t)} \mid \alpha^{(t)}(\hat{u}_*, \hat{s}) = 1 \right\} \end{aligned}$$

und

$$userbase : \widehat{S}^{(t)} \rightarrow \mathcal{P}(\widehat{U}^{(t)})$$

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

### Lemma 1

$$\bigcup_{\widehat{u} \in \widehat{U}^{(t)}} \left( accounts^{(t)}(\widehat{u}) \right) = \widehat{S}^{(t)} \quad (\text{i})$$

$$\bigcup_{\widehat{s} \in \widehat{S}^{(t)}} \left( userbase^{(t)}(\widehat{s}) \right) = \widehat{U}^{(t)} \quad (\text{ii})$$

*Beweis.*

zu (i): Es ist

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

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

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

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 könnte nicht alleinig an  $\hat{n}$ ,  $\hat{m}$  und  $\Gamma(t)$  gemessen werden. Diese geben zwar einen guten Anhaltspunkt, lassen jedoch in einer einzigen gegebenen Ausprägung  $[\hat{n}, \hat{m}, \Gamma(t)]$  eine enorme Vielzahl an durch  $\hat{U}^{(t)}, \hat{S}^{(t)}$  beschriebenen Szenarien zu, die allesamt die Vorgabe  $[\hat{n}, \hat{m}, \Gamma(t)]$  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  $[\hat{n}, \hat{m}, \Gamma(t)]$  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  $\text{accounts}^{(t)}(\hat{u})$  der angebundenen User  $\hat{u} \in \hat{U}^{(t)}$ ?

- (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  $userbase^{(t)}(\hat{s})$  der angebundenen Service-Provider  $\hat{s} \in \hat{S}^{(t)}$ ?
  - (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  $\hat{s}_* \in \hat{S}^{(t)}$  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  $[\hat{U}^{(t_0)}, \hat{S}^{(t_0)}, \Gamma(t_0)]$  mit  $[\hat{U}^{(t_1)}, \hat{S}^{(t_0)} \setminus \{\hat{s}_*\}, \Gamma(t_1)]$ ?

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

Wir definieren

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

$$\omega_i := |accounts^{(t)}(\hat{u}_i)|. \quad (i)$$

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

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

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

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

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

$$\Omega_k := \left| \widehat{U}_k \right| \text{ für } k \in \{1, \dots, \widehat{m}\}, \quad (\text{iii})$$

für die konsequenterweise

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

WIP

#### Theorem 4

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

$$1 = 1 \quad (\text{ii})$$

#### Theorem 5

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

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

Und ganz insbesondere

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

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

*Beweis.*

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

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

Nun zeigen wir die zweite Ungleichung von (ii):

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

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

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

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

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

(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  $j = m - 1$ .  $\square$

### [Beispiel]

#### **Beispiel 1**

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

	<b>s<sub>1</sub></b>	<b>s<sub>2</sub></b>	<b>s<sub>3</sub></b>
<b>u<sub>1</sub></b>	x		
<b>u<sub>2</sub></b>	x		
<b>u<sub>3</sub></b>	x	x	x
<b>u<sub>4</sub></b>		x	
<b>u<sub>5</sub></b>			x
<b>u<sub>6</sub></b>	x	x	
<b>u<sub>7</sub></b>		x	x
<b>u<sub>8</sub></b>	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:

	<b>s<sub>1</sub></b>	<b>s<sub>2</sub></b>	<b>s<sub>3</sub></b>
<b>u<sub>1</sub></b>	x		
<b>u<sub>2</sub></b>	x		
<b>u<sub>3</sub></b>			x
<b>u<sub>4</sub></b>		x	
<b>u<sub>5</sub></b>			x
<b>u<sub>6</sub></b>	x		
<b>u<sub>7</sub></b>		x	x
<b>u<sub>8</sub></b>	x		x

Damit ergeben sich die oben definierten

Größen als

Größen als

$$\widehat{U}^{(t)} = \{u_1; \dots; u_8\}$$

$$\widehat{S}^{(t)} = \{s_1; s_2; s_3\}$$

$$n = 8$$

$$m = 3$$

$$\Gamma(t) = 14$$

$$\widehat{U}^{(t)} = \{u_1; \dots; u_8\}$$

$$\widehat{S}^{(t)} = \{s_1; s_2; s_3\}$$

$$n = 8$$

$$m = 3$$

$$\Gamma(t) = 10$$

$$acc.(^{(t)})(u_1) = acc.(^{(t)})(u_2) = \{s_1\}$$

$$acc.(^{(t)})(u_3) = acc.(^{(t)})(u_8) = \{s_1; s_2; s_3\}$$

$$acc.(^{(t)})(u_4) = \{s_2\}$$

$$acc.(^{(t)})(u_5) = \{s_3\}$$

$$acc.(^{(t)})(u_6) = \{s_1; s_2\}$$

$$acc.(^{(t)})(u_7) = \{s_2; s_3\}$$

$$acc.(^{(t)})(u_1) = acc.(^{(t)})(u_2) = acc.(^{(t)})(u_6) = \{s_1\}$$

$$acc.(^{(t)})(u_3) = acc.(^{(t)})(u_5) = \{s_3\}$$

$$acc.(^{(t)})(u_4) = \{s_2\}$$

$$acc.(^{(t)})(u_7) = \{s_2; s_3\}$$

$$acc.(^{(t)})(u_8) = \{s_1; s_3\}$$

$$userbase^{(t)}(s_1) = \{u_1; u_2; u_3; u_6; u_8\}$$

$$userbase^{(t)}(s_2) = \{u_3; u_4; u_6; u_7; u_8\}$$

$$userbase^{(t)}(s_3) = \{u_3; u_5; u_7; u_8\}$$

$$userbase^{(t)}(s_1) = \{u_1; u_2; u_6; u_8\}$$

$$userbase^{(t)}(s_2) = \{u_4; u_7\}$$

$$userbase^{(t)}(s_3) = \{u_3; u_5; u_7; u_8\}$$

$$\omega_1 = \omega_2 = \omega_4 = \omega_5 = 1$$

$$\omega_6 = \omega_7 = 2$$

$$\omega_3 = \omega_8 = 3$$

$$\omega_1 = \omega_2 = \omega_3 = \omega_4 = \omega_5 = \omega_6 = 1$$

$$\omega_7 = \omega_8 = 2$$

$$\widehat{U}_1 = \{u_1; u_2; u_4; u_5\}$$

$$\widehat{U}_2 = \{u_6; u_7\}$$

$$\widehat{U}_3 = \{u_3; u_8\} \text{ mit}$$

$$\bigcup_{k=1}^m \widehat{U}_k = \widehat{U}^{(t)}$$

$$\widehat{U}_1 = \{u_1; u_2; u_3; u_4; u_5; u_6\}$$

$$\widehat{U}_2 = \{u_7; u_8\}$$

$$\widehat{U}_3 = \emptyset \text{ mit}$$

$$\bigcup_{k=1}^m \widehat{U}_k = \widehat{U}^{(t)}$$

$$\Omega_1 = |\widehat{U}_1| = 4$$

$$\Omega_2 = |\widehat{U}_2| = 2$$

$$\Omega_3 = |\widehat{U}_3| = 2 \text{ mit}$$

$$\sum_{k=1}^m \Omega_k = n$$

$$\Omega_1 = |\widehat{U}_1| = 6$$

$$\Omega_2 = |\widehat{U}_2| = 1$$

$$\Omega_3 = |\widehat{U}_3| = 1 \text{ mit}$$

$$\sum_{k=1}^m \Omega_k = n$$

### 5.3.5 Other Stuff

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

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

$$\begin{aligned}\hat{n} &= \sum_{k=1}^{\hat{m}} \Omega_k \leq \hat{m} * \max_{j \in \{1, \dots, \hat{m}\}} \Omega_j \\ \Leftrightarrow \frac{\hat{n}}{\hat{m}} &\leq \max_{j \in \{1, \dots, \hat{m}\}} \Omega_j\end{aligned}$$

Weiterverarbeitung von Theorem 5:

#### Theorem 6

Theorem 5 lieferte uns

$$\begin{aligned}2 * \hat{n} - \Gamma(t) &\leq \Omega_1 \leq \frac{\hat{m} * \hat{n} - \Gamma(t)}{\hat{m} - 1} \\ \Gamma(t) - (\hat{m} - 1) * \hat{n} &\leq \Omega_{\hat{m}} \leq \frac{\Gamma(t) - \hat{n}}{\hat{m} - 1}\end{aligned}$$

Der Übersicht halber setzen wir

$$\begin{aligned}A &:= 2 * \hat{n} - \Gamma(t) \\ B &:= \Gamma(t) - (\hat{m} - 1) * \hat{n} \\ C &:= \frac{\hat{m} * \hat{n} - \Gamma(t)}{\hat{m} - 1} \\ D &:= \frac{\Gamma(t) - \hat{n}}{\hat{m} - 1}\end{aligned}$$

womit sich nun obige Aussage ausdrückt als

$$\begin{aligned} A &\leq \Omega_1 \leq C \\ B &\leq \Omega_{\hat{m}} \leq D \end{aligned}$$

Damit lassen sich besondere zu untersuchende Grenzfälle formulieren:

$$A \leq B \Leftrightarrow \Gamma(t) \geq (\hat{m} - 1) * \frac{\hat{n}}{2} \quad (i)$$

$$A \leq C \Leftrightarrow 1 = 1 \quad (1)$$

$$A \leq D \Leftrightarrow \Gamma(t) \geq (2\hat{m} - 1) * \frac{\hat{n}}{\hat{m}} \quad (iii)$$

$$B \leq C \Leftrightarrow \Gamma(t) \leq (\hat{m} + (\hat{m} - 1)^2) * \frac{\hat{n}}{\hat{m}} \quad (iv)$$

$$B \leq D \Leftrightarrow 1 = 1 \quad (v)$$

$$C \leq D \Leftrightarrow \Gamma(t) \geq (\hat{m} - 1) * \frac{\hat{n}}{2} \quad (vi)$$

[ende TODO2]

[TODO3][”Verdichtung”]

Die Maße  $\hat{n}$ ,  $\hat{m}$  und  $\Gamma(t)$  sind sehr objektiv und teils zielführend. Sie scheinen aber nicht zu reichen. So kann es z. B. User  $\hat{u} \in \hat{U}^{(t)}$  geben, die im worst case ausschließlich zu einem einzigen Provider  $\hat{s} \in \hat{S}^{(t)}$  connectet sind (und somit aber trotzdem den Wert von  $\hat{n}$  beeinflussen, oder noch schlimmer analog Provider  $\hat{s} \in \hat{S}^{(t)}$ , 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  $\hat{U}^{(t)}$  und  $\hat{S}^{(t)}$  so modifiziert/verkleinert, dass  $\Gamma(t)$  davon kaum einen Einfluss spürt (sich lediglich um einen marginalen Prozentsatz verringert).
- Formeln auf die davon modifizierten Größen  $\hat{n}$  und  $\hat{m}$  anpassen.
- $\Rightarrow$  Die Grenzen von [Theorem 2][Aussage (ii)] werden damit deutlich schärfter.
- $\Rightarrow$  kann sicherlich in Abschnitt 5.3.6 für den Umgang mit dem Verhältnis  $\frac{\hat{n}}{\hat{m}}$  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  $n_{nexcl} \geq \Gamma(t) - \hat{n}$  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

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

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

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

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

Damit liefert uns die definierte  $\Gamma$ -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 Zielreichungs-Maß auszuweiten:

### Definition 13

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

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

[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

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

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 Teilnehmer

TODO

## 5.4 Token-Economics (WPT)

### 5.4.1 Einleitung

WIP

#### Prämissen 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

### Prämissse 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 verkonsument

- 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 verrechnet werden.

## 5.4.2 Lösungsideen

Smart Markets for Stablecoins  
Token Engineering Research  
A Token Engineering Process

- Staken von Sub-Projects.
  - Teilprojekt wird nach **Bonding-Curves-Modell** implementiert und bekommt damit seinen eigenen Token.
  - Die Projekteinlage erfolge in WUNDER-Tokens (Staking).
  - Investoren von WUNDER hätten damit die Möglichkeit, die für sie besonders interessanten Projekte stärker zu unterstützen als lediglich das übergeordnete WunderPass-Projekt.
  - Der WUNDER bekäme damit einen intrinsischen Wert: Man braucht ihn, um sich an den Teilprojekten zu beteiligen.
  - Teilprojekte könnten outgesourcet und ausschließlich mittels einer größeren WUNDER-Einlage in den Contract des neuen Projekts incentiviert werden. Die Voraussetzung dafür wäre die Einbindung des neuen Projekts und seines Tokens in das WunderPass-Ökosystem und die Nutzung der Wunder-Identity.

## 5.4.3 Einbindung der Investing-Pools

- Das Pool-Projekt wird als **Curation Market** implementiert und bekommt seinen eigenen Token (IPT).
- Der IPT wird mittels (**Augmented**) **Bonding-Curves** implementiert, ist also gegen eine Einlage für jeden und immer mintbar.
- Die Einlage für den IPT ist in WUNDER zu erbringen (**Es ist noch unklar, wie man an WUNDER kommt, wenn es vorher keinen Token-Sale gegeben hat. Ob der WUNDER ebenfalls mittels Bonding-Curves abzubilden wäre, sei hier erst einmal mehr als unklar.**)
- Der erste und größere Investor für das Pool-Projekt wäre WunderPass selbst. Für die erfolgte Einlage in den Projekt-Pool bekäme WunderPass IPT, die es für Incentivierungen und Rewards für die Nutzung von Pools verwenden könnte. Dieses Invest könnte (im Gegensatz zu den Einlagen anderer Investoren) zB. auch einem Locking unterliegen, um eine gewisse Preisstabilität des IPS zu gewährleisten.

- Der Pool-Initiator müsste bei der Pool-Eröffnung IPT staken, die er unter bestimmten Umständen verlieren könnte, wenn sein Pool z.B. ungenutzt bleibt. So könnte man sicherstellen, dass ernste Absichten hinter den Pools stecken und diese auch genutzt werden.
- Der Initiator wäre damit gleichzeitig auch Investor in das gesamte Pool-Projekt (da er ja für die Poolerstellung IPT kaufen muss).
- Gleichzeitig müsste der Initiator jedoch auch für sein Staken (ins Risiko gehen) belohnt werden, falls der Pool läuft und genutzt wird. Diese Belohnung würde in Form von zusätzlichen IPT (Stake-Rewards) erfolgen und z.B. durch WunderPass und/oder den anderen Poolteilnehmern als eine Art Gebühr getragen werden und dabei folgenden Faktoren folgen:
  - Pool-Lifetime
  - Anzahl Teilnehmer
  - Pool-Einsatz/-Umsatz
  - etwaiger Gewinn aus Invests
  - NFT-Pass-Status
  - Upvoting durch andere IPT-Holder (als ein Art *Master Pool-Creator*)
- In jedem Fall sollte der Staker im Normalfall (falls er nicht irgendwie Scheiße baut) bei der Auflösung des Pools mindestens seinen Einsatz zurückerhalten (also keinerlei Gebühren für die Nutzung des Pool-Service zahlen). In aller Regel sollte er mit mehr als dem ursprünglich gestakten Betrag rausgehen.
- Der nötige Staking-Betrag könnte fix pro Pool sein oder aber variabel und dabei von folgenden Kriterien abhängen:
  - geplante Pool-Lifetime
  - Anzahl Teilnehmer (min/max)
  - Pool-Einsatz pro Teilnehmer (min/max)
  - etwaige abgegeben Garantien seitens Pool-Creator (*der Pool muss mindestens x, y und z erfüllen..., bei deren Verfehlungen der Staker bestraft und im Erfolgsfall besonders entlohnt wird*)
  - NFT-Pass-Status
  - Reputation in der Community (als ein Art *Master Pool-Creator*)

Die entscheidende Frage beim zu entrichtenden Stake-Betrag, ist die Klärung, ob es im Interesse des Stakers (Pool-Creator) sei, besonders viel (um größere Staking-Rewards zu erhalten) oder besonders wenig (um kein Risiko zu tragen) zu staken / staken zu müssen.

- Ein weiterer sehr essenzieller Faktor für die Größe des zu stakenden Betrags könnte der Kurs des IPTs sein. Denn laut der **Bonding-Curves**-Implementierung würde der IPT-Preis mit steigender Zirkulation steigen, was mit der Zunahme von existierende Pools geschähe. Damit wäre die Erstellung neuer Pools mit ihrer zahlenmäßigen Zunahme stets kapital-intensiver (aber nicht gleichbedeutend teurer). **Die Frage hierbei ist also, ob der zu erbringende Stake des Pool-Creators auf den Total-Supply des IPTs normiert werden sollte oder nicht**, die gänzlich mit der obigen Fragestellung einhergeht, ob der Pool-Creator eigentlich staken möchte oder das nur tun muss.
  - Gegen eine Normierung spricht die Annahme/Hoffnung, ein Pool-Creator sei gleichzeitig auch ein großer Supporter des gesamten Projekt und glaube daran. Wenn der IPT-Preis steigt, ist dies gleichbedeutend mit der Zunahme an genutzten Pools, an denen der Pool-Creator als Staker, Besitzer von IPT und damit Projekt-Investor auch selbst (finanziell) profitiert.
  - Für eine Normierung spricht dagegen die potenzielle Gefahr, neue oder bestehende User durch eine zu hohe finanzielle Sicherheitseinlage davon abzuschrecken neue Pools zu erstellen.
- Die Antwort auf diese Fragestellung könnte auch darin liegen, ob wir uns besonders viele oder lieber weniger aber besonders Teilnehmer-starke Pools wünschen.
- Alle anderen Pool-Teilnehmer müssen eine Gebühr für ihre Teilnahme am Pool (und die Nutzung des Service) erbringen. Auch das hat in IPT zu erfolgen. **Ob die Gebühr bei Pool-Beitritt gewissermaßen als *prepaid* zu erbringen ist oder aber *on demand*** für eine anfallende Aktion bleibt zunächst unklar. Die Gebühren könnten sich nach folgenden Faktoren bzw. Features richten und könnten sowohl voraussehbar sein (dann beim Pool-Beitritt zu entrichten) als auch *on demand* anfallen:
  - pro Zeiteinheit (Vorauszahlung für einen gewissen Zeitraum als prepaid; danach Zahlungsaufforderung um im Pool zu bleiben)
  - abhängig vom Einsatz (multiplikativ zum ersten Punkt)
  - abhängig vom etwaigen Gewinn aus Invests (on demand)
  - abhängig vom Pool-Creator (Community-/Staking-Status als Invest-Guru; prepaid)
  - bei Aufstockung des Invests (on demand)
  - bei Vorzeitigem Ausbezahlen und Verlassen des Pools (on demand)
  - gekoppelt an Beteiligung am Staken (prozentual auf die vorigen Punkte anzurechnen)
  - abhängig vom NFT-Pass-Status (prozentual auf die vorigen Punkte anzurechnen)
- Die Teilnehmer können bei dieser Logik aber nicht wie nicht wie die Staker zusätzlich als Projekt-Investoren angesehen werden, weil sie IPTs kaufen, da die gekauften

IPTs direkt als Gebühr entrichtet werden. Für die Pool-Teilnehmer stellt der IPT also eher einen Utility- bzw. Purpose-Token dar weshalb die Höhe der zu entrichtenden Gebühr zweifelsfrei auf Basis von *Total-Supply des IPTs* normiert werden muss (die Gebühr darf keinesfalls mit Zunahme von Pools steigen).

- Die entrichteten **Gebühren gehen zu einem relevanten Teil in die Treasury des gemeinschaftlichen Investing-Pools-Contracts** und stellen damit eine gemeinschaftliche Projekt-Erwirtschaftung dar. Der verbleibende Teil der Gebühren geht an den Pool-Staker. Die Aufschlüsselung der Verteilung auf Project-Treasury und Pool-Staker könnte halbwegs komplex werden und folgende Festlegungen folgen bzw. Gegebenheiten berücksichtigen:
  - Verteilung nach einem simplen prozentualen Schlüssel (zB. 50-50)
  - Absolute Mindest- und Obergrenzen des Projekt-Pool-Anteils (mindestens Betrag  $x$  geht an den Projekt-Pool; wenn es nicht reicht, alles; ab der Mindestgrenze erfolgt eine prozentuale Verteilung bis zu einer Maximalgrenze  $y$  für den Projekt-Pool; alles darüber geht an den Staker)
  - progressive Verteilung abhängig des erbrachten Staking-Betrags (so könnte der Staker pro gestaktem IPT einen prozentualen Anteil  $x \in [0; 1]$  pro IPT an Gebühren für sich beanspruchen, wobei das  $x$  mit Größe des gestakten Betrags progressiv stiege)
  - Begünstigung des Stakers in Abhängigkeit seines NFT-Pass-Status.
- Folgende Auswahl sollte vermutlich bei der Pool-Erstellung angeboten werden:
  - [Pool-Creator erbringt den Stake; alle anderen Teilnehmer bezahlen die Gebühren]
  - [Alle Pool-Teilnehmer teilen sich den zu erbringenden Stake und alle anfallenden Gebühren]
- Bedingt durch den Gebühren-Mechanismus erwirtschaften das Pool-Projekt Einnahme für die gemeinschaftliche Pool-Treasury, womit auch der IPT auf natürliche Weise im Wert steigt (ohne dass neue Investoren hinzukommen müssen, die einen höheren Tokenpreis bezahlen müssen). Jeder IPT-Holder - also auch insbesondere die Pool-Staker - profitiert also an der Erstellung neuer Pools (der Staker also indirekt an seinem eigenen Pool als auch an den fremden, was additiv zu seinen direkten Stake-Rewards hinzukommt). Das fördert also Word-of-Mouth, was sowohl auf die Preissteigerung des IPTs durch neue IPT-Holder einzahlt, als auch die Pool-Treasury durch neue Pools und die dafür anfallenden Gebühren füttert, was wiederum den IPT-Kurs befeuert.
-

#### 5.4.4 Bonding-Curves

- [Gute Einführung](#)
- [Anwendungsbeispiel](#)
- [White-Paper](#)
- [Smart-Contract](#)

Zunächst einmal eine Formalisierung einer Token-Distribution mittels Bonding-Curves:

##### Definition 15: Token-Distribution mittels Bonding-Curves

Angenommen man möchte einen Projekt-Token **TKN** herausgeben und dieses im Markt distribuieren. Der Mechanismus der *Bonding-Curves* stellt hierbei ein alternatives Modell zu gängigen Tokensales (z.B. ICO) dar und folgt dabei einigen wesentlich Merkmalen, die ihn teils grundlegend von herkömmlichen Tokensales abgrenzen.

- TKN wird von einem Smart-Contract verwaltet, der wesentlich mehr Logik implementiert als ein herkömmlicher ERC20-Contract.
- TKN kann jederzeit und von jedem gemintet werden. Dies geschieht gegen eine Einlage/Bezahlung in einer dafür definierten Währung (z.B. ETH oder USDT). Der Token wird quasi von dem Verwalter-Contract verkauft.
- Es existiert damit keine initiale bevorzugte Token-Ausgabe beim Contact-Launch an etwaige bevorzugte Parteien (Contract-Owner, Herausgeber, Investoren etc.). Die Ausgabe erfolgt ausschließlich gegen Einlage und kennt keine Bevorzugung entgegen der Contract-Logik.
- Die Einnahmen aus der Tokenausgabe kommen ausschließlich der Token-Contract-Treasury  $\mathcal{T}$  zugute anstatt wie bei herkömmlichen Tokensales bestimmten Begünstigten (wie z.B. der Herausgeber-Company oder deren Gründern).
- TKN unterliegt keinem maximalen Gesamt-Supply. Es können stets neue Tokens ausgegeben werden, solange Interessenten existieren, die die Einlage für die Token-Ausgabe erbringen.
- Tokens können jederzeit von ihren Besitzern gegen einen - einer bestimmten Contract-Logik folgenden - Rückkaufpreis an den Token-Contract zurückgegeben werden. Zurückgegebene Tokens werden dabei sofort von dem Verwalter-Contract geburnt und somit aus der Zirkulation genommen.

- TKN kann selbstverständlich auch am Sekundärmarkt gehandelt werden (falls dieser bessere Konditionen hergibt als die Aussage bzw. Rücknahme durch den Token-Contract selbst).

Sei  $i \in \mathbb{N}$  der aktuelle Gesamt-Supply von TKR (wir nehmen hier mal an, TKR sei atomar) und  $\$$  die Tausch- bzw. Einlage-Währung ( $\$$  ist hier abstrakt und nicht als US-Dollar zu verstehen).

Dann werden die durch die Token-Contract vorgegebenen Ausgabepreis (Kaufpreis)  $\mathcal{K}$ , Rücknahmepreis (Verkaufspreis)  $\mathcal{V}$  und Contract-Treasury-Inhalt  $\mathcal{T}$  für den zuletzt ausgegebenen Token  $i$  - jeweils in der Einheit  $\$$  - durch die jeweils supply-abhängigen Funktionen beschrieben:

$$\mathcal{K}, \mathcal{V}, \mathcal{T} : \mathbb{N} \rightarrow \mathbb{Q}^+$$

$\mathcal{K}(i)$  := Letzter Token-Ausgabepreis in  $\$$  bei einem Gesamt-Supply von  $i$

$\mathcal{V}(i)$  := Aktueller Token-Rückkaufkurs in  $\$$  bei einem Gesamt-Supply von  $i$

$$\mathcal{T}(i) := \sum_{j=1}^i \mathcal{K}(j)$$

Die definierende Logik unseres Tokens lässt sich damit also formal als

$$TKR = (\mathcal{K}, \mathcal{V}, \$)$$

schreiben, wobei hierbei  $\mathcal{T}$  ausgespart bleibt, da es implizit durch  $\mathcal{K}$  gegeben ist.

Sicherlich können und werden bei einer konkreten Implementierung eines mittels der durch  $\mathcal{K}$  und  $\mathcal{V}$  gegebenen *Bonding-Curves* beschriebenen Tokens noch andere zu formalisierende Faktoren und Mechanismen eine Rolle spielen. Für die simpelste abstrakte Definition reichen die genannten Größen jedoch für den Moment aus.

Die eben - auf diskrete Weise - definierten Funktionen  $\mathcal{K}(i)$  und  $\mathcal{V}(i)$  erfordern insofern noch eine zusätzliche Bemerkung, als dass diese explizit nur eine Token-weise Auskunft über Ausgabe- und Rücknahmepreis geben. Möchte man mehrere Token minten oder zurückgeben, muss der Preis für jeden der Tokens separat ausgerechnet und anschließend addiert werden. Möchte man bei einem aktuellen Supply von  $i \in \mathbb{N}$  nicht einen sondern  $k \in \mathbb{N}$  mit  $k \leq i$  Tokens minten bzw. zurückgeben, beläuft sich der gesamte Kauf- bzw- Verkaufspreis auf

$$\mathcal{K}_k(i) := \sum_{j=i+1}^{i+k} \mathcal{K}(j)$$

$$\mathcal{V}_k(i) := \sum_{j=i-k+1}^i \mathcal{V}(j).$$

Das besonders Hervorhebenswerte an diesem Token-Ausgabemodell ist zweifelsfrei die gemeinschaftliche aus der Token-Ausgabe gefütterte Contract-Treasury aus echten Geldeinlagen, die nicht etwa einer dritten (Ausgabe-)Partei zugute kommt, sondern de facto den Tokeninhabern gehört. Die Existenz dieser Rücklagen gibt den ausgegebenen Tokens theoretisch einen realen Wert und ermöglicht einzig und allein die Implementierung des Rückkauf-Mechanismus. Der Gebrauch von dieser Möglichkeit und die Verankerung der Rückkauffunktion  $\mathcal{V}$  in der Logik des Token-Contracts realisiert den besagten realen Wert dann auch in der Praxis und nennt sich "***market maker of last resort***". Denn wenn ich eine definitive - in Contract-Logik verankerte - Sicherheit habe, ein Asset jederzeit verkaufen zu können, besitzt dieses Asset auch einen echten, intrinsischen Value, der nicht zwingend den marktwirtschaftlichen Mechanismen unterliegt - und somit auch keinen etwaigen Hypes um einen gut vermarktetem Tokensale ohne dahinterliegende Substanz. Vielmehr folgt der Tokenpreis der gemeinschaftlichen Projekt-Treasury  $\mathcal{T}$ , die ihrerseits substanziel mit dem Projekterfolg einhergeht.

Die letzte Einsicht lässt uns zu zwei wesentlichen Gedanken gelangen, die die entscheidenden Argumente für das *Bonding-Curves*-Modell liefern könnten:

- Der Rückgabepreis  $\mathcal{V}(i)$  sollte eine direkte Abhängigkeit vom Treasury-Inhalt  $\mathcal{T}(i)$  aufweisen.
- Nach bisheriger Definition hängt der Treasury-Inhalt  $\mathcal{T}(i)$  ausschließlich vom aktuellen Supply  $i \in \mathbb{N}$  (und den damit einhergehenden Ausgabepreisen  $\mathcal{K}(j)$  für  $j \leq i$ ) ab. Gepaart mit der ersten Forderung bedeutete dies implizit nichts anderes, als dass der aktuelle Rücknahmepreis ausschließlich von den Ausgabepreisen der bisherigen Tokens abhinge. Dies ist schlecht und ein sehr großes Problem der gängigen *Bonding-Curves*-Implementierungen, da Koppelung des Rücknahmepreises - also des intrinsischen Werts des Tokens - ausschließlich an den Kaufpreis voriger Tokens - und die Wertentwicklung damit an den Kaufpreis etwaiger zukünftig ausgegebener Tokens, würde mathematisch alternativlos eine monoton steigende Ausgabepreis-Funktion  $\mathcal{K}(i)$  erfordern. Ohne eine sehr stark fundierte projekt-bezogene Argumentation für ein monoton steigendes  $\mathcal{K}(i)$  schrie das gesamte Modell nur so nach *Pump & Dump* und *Hot Potatoe*. Und tatsächlich ist es so, dass nahezu alle *Bonding-Curves*-Implementierungen Gebrauch von einer (streng) monoton steigenden Ausgabepreis-Kurve  $\mathcal{K}(i)$  machen. Sie argumentieren mit anderem generierten Projekt-Value, der nicht durch die Contract-Treasury  $\mathcal{T}(i)$  gemessen werden kann und diese Argumentation muss nicht zwingend falsch oder ungenügend sein. Uns

reicht dies aber nicht - zumal es mehr als gute Gründe für ein monoton steigendes  $\mathcal{K}(i)$  gibt (dazu später mehr). Somit bleibt uns nichts anderes als die - zumindest teilweise - Abkoppelung von  $\mathcal{T}(i)$  und  $\mathcal{K}(i)$ , womit wir auch unsere obige Definition von  $\mathcal{T}(i) = \sum_{j=1}^i \mathcal{K}(j)$  wieder teils verwerfen müssen.

Wir fassen zusammen:

#### Conclusion 4: Contract-Treasury als wichtigster Baustein zum Erfolg

Wie sind der Überzeugung, der Contract-Treasury-Inhalt - gemessen als  $\mathcal{T}(i)$  - sei der entscheidende Baustein für einen soliden *Bonding-Curves*-Token.  $\mathcal{T}(i)$  beeinflusst direkt den Rücknahmepreis  $\mathcal{V}(i)$ , verleiht dem Token damit einen echten geldwerten Value, was wiederum als Kaufargument für neue Tokens gilt und damit implizit auch zur Beurteilung des Ausgabepreises  $\mathcal{K}(i)$  seitens etwaiger neuer Investoren hinzugezogen wird.

Konkret auf den Rücknahmepreis  $\mathcal{V}(i)$  bezogen sehen wir kaum sinnvollere Alternativen als der gängigen Definition

$$\mathcal{V}(i) = \frac{\mathcal{T}(i)}{i}$$

zu folgen, was gleichbedeutend damit ist, dass der Besitz am Contract-Treasury-Inhalt pro rata auf die sich in Zirkulation befindenden Token verteilt wird, was sich konsequenterweise im Rücknahmepreis  $\mathcal{V}(i)$  widerspiegelt. Mit der in Definition 15 beschriebenen Treasury-Funktion  $\mathcal{T}(i)$  ergibt sich damit für den Rücknahmepreis  $\mathcal{V}(i)$

$$\mathcal{V}(i) = \frac{\mathcal{T}(i)}{i} = \frac{\sum_{j=1}^i \mathcal{K}(j)}{i}.$$

Um einen Kauf bei aktuellem Supply von  $i \in \mathbb{N}$  zu dem Preis von  $\mathcal{K}(i)$  für sich als Investor zu rechtfertigen, muss man argumentieren, man könne den gekauften Token irgendwann zu einem höheren Preis wieder zurückgeben:

$$\exists k > i, \text{ so dass } \mathcal{V}(k) > \mathcal{K}(i)$$

$$\Leftrightarrow \sum_{j=1}^k \mathcal{K}(j) > k \cdot \mathcal{K}(i)$$

Gleichzeitig sollte  $\mathcal{V}(i) \leq \mathcal{K}(i)$  für alle Supplies  $i$  selbstverständlich angenommen werden können, da sonst Arbitrage entstünde, was sofort vom Markt aufgefressen werden würde.

Solche Anforderungen gehen alternativlos mit einem zwingend monoton steigenden  $\mathcal{K}(i)$  einher ('monoton steigend' wäre hierbei noch zu präzisieren, da es nicht zu hundert Prozent dem mathematischen Verständnis gleicht und die Aussage wahrscheinlich noch zu beweisen; intuitiv ist es aber klar). Da eine zwingend monoton steigende Preiskurve als Investitionsmotivation - in einem abstrakt stehenden Kontext und ohne zusätzliche Argumente - schlichtweg unseriös ist, fordern wir für den *Contract-Treasury-Inhalt*

$$\mathcal{T}(i) > \sum_{j=1}^i \mathcal{K}(j),$$

bzw.

$$\mathcal{T}(i) = \sum_{j=1}^i \mathcal{K}(j) + f(t, i) \text{ mit } f(t, i) > 0,$$

wobei  $f(t, i)$  eine nicht genau präzisierte, positive *Value-Funktion* unseres Projekts darstellt. Also so eine Art Gradmesser der (externen) Wertschöpfung/Wirtschaftlichkeit unseres Projekts, die nicht in direktem Bezug zum Projekt-Kontrakt steht. Man könnte  $f(t, i)$  vielleicht ***Of-Contract-EBIT*** unseres Projekt nennen - wie auch immer dieses erwirtschaftet wird.

Wie durch das  $t$  angedeutet, bringt das  $f(t, i)$  die zeitliche Dimension in unsere *Contract-Treasury-Rechnung*, die externen (wirtschaftlichen) Einflüssen unterliegt und nicht mehr ausschließlich vom GesamtSupply  $i$  abhängt - gleichwohl der GesamtSupply  $i$  durchaus auch die genannten externen Einflüsse und damit auch  $f(t, i)$  begünstigen kann.

Der *Of-Contract-EBIT* muss zwar nicht, kann aber durchaus auch aus anderen Smart-Contracts fließen. Solche Inter-Contract-Geldflüsse sind natürlich - falls möglich - eine stets bevorzugte Variante.

Ist dies nicht möglich - und etwaige finanzielle Projekteinnahmen tatsächlich gänzlich *off-chain*, bedarf es eines definierten und vertrauensvollen Mechanismus, der dafür sorge, dass die erzielten Projekterlöte in die gemeinschaftliche Projekt-Treasury eingezahlt werden. Dies könnte entweder durch eine gesonderte Contract-Function dargestellt werden, oder aber durch den allgemeingültigen Weg mittels Tokenkaufen. Im zweiten Fall würden die gegen die extern erwirtschaftete Einlage ausgegebenen Tokens pro rata auf alle aktuellen Tokenhalter verteilt werden.

Mit einer nachweislich existenten *externen projektbezogenen Profit-Funktion*  $f(t, i)$  bekäme ein einem Projekt zugrunde liegendes *Bonding-Curves-Token-Modell* das ihm noch fehlende - und aus unserer Sicht unverzichtbare - Merkmal: Nämlich eine gewisse Abkopplung des realen Tokenwerts - gemessen durch  $\mathcal{V}(i)$  - von der oft - zurecht als scheiball-artig kritisierten - Ausgabepreis-Kurve  $\mathcal{K}(i)$ .

Damit liefern wir aus unserer Sicht den bisher bei dem meisten *Bonding-Curves-*

*Implementierungen fehlenden Baustein für eine solide und fundierte Token-Distribution mittels eines *Bonding-Curves-Modells* und entgegen damit - zumindest auf abstrakt Weise - dem bestehenden Hauptproblem der *Bonding-Curves*: Nämlich *Ponzi*, *Pump & Dump* oder *Hot Potatoe* zu sein.*

Wir behaupten hierbei keinesfalls, den heiligen Gral für das Funktionieren von *Bonding-Curves-gestützten Token-Modellen* gefunden zu haben. Denn schließlich ist die Existenz des von uns eingeführten  $f(t, i)$  alles andere als gegeben, äußerst projekt-abhängig und zudem in der Regel vermutlich nicht leicht zu formalisieren - geschweige denn ohne optimistische Annahmen zu beweisen. Denn nicht zuletzt argumentieren viele auf *Bonding-Curves-Token-Modelle* gestützte Projekte genau wie wir hier an dieser Stelle: *Es existiere ein externer Projekt-Value, von welchem die Tokeninhaber profitieren!* Nur geben diese Argumentationen diesem Value nicht den Namen  $f(t, i)$  und verpassen damit eine formal abstrakte Verallgemeinerung.

Wir fassen zusammen:

#### Conclusion 5: Token-externer Projekt-Value

Wir reduzieren das bestehende Problem von *Bonding-Curves-Token-Modellen* hinsichtlich '*Ponzi*' und '*Pump & Dump*' auf den Nachweis der Existenz einer ***Of-Contract-EBIT-Funktion***  $f(t, i) > 0$  und deren Formalisierung anstatt von undefiniertem *externen Projekt-Value* zu sprechen.

Idealerweise wird  $f(t, i) > 0$  durch unbestreitbare Logik eines Smart-Contracts begründet, der in wertschöpfender Interaktion mit unserem Token-Contract steht (Profite in seine Treasury einzahlt). Andernfalls erschwert sich die Argumentation und muss solide begründet und formalisiert werden.

Um das  $f(t, i)$  nicht ganz als abstraktes Mysterium dastehen zu lassen und Zweifel an dessen Existenz zu zerstreuen:

#### Beispiel 2: DeFi-Projekte besitzen stets ein $f(t, i) > 0$

Jedes DeFi-Projekt besitzt ein  $f(t, i) > 0$ ! Ob

- DEX-Provider à la *Balancer*,
- Market-Places à la *OpenSea*,
- Lending-Platforms

oder viele andere agieren wirtschaftlich, indem sie in der Regel Provisionen auf ihre Dienstleistung veranschlagen. Diese Gebühren sind unmissverständlich in ihrer Contract-Logik verankert und gänzlich transparent.

Würden solche Projekte einen *Bonding-Curves-gestützten* Utility-Token herausgeben und einen gewissen Abfluss ihrer Provisions-Profite in die Contract-Treasury dieses Tokens implementieren, würde solch ein Mechanismus auf ganz natürlich Weise das von uns geforderte  $f(t, i) > 0$  definieren. Jeder Tokeninhaber würde damit jeder gebühren-pflichtigen Transaktion mit partizipieren.

Wie nun bereits mehrfach betont, ist und bleibt das von uns eingeführte  $f(t, i)$  projektbezogen. Wir wollen an dieser Stelle dagegen weiterhin möglichst abstrakt und allgemein bleiben und uns im folgenden der Ausgabepreis-Kurve  $\mathcal{K}(i)$  widmen - insbesondere auch mit der Zielsetzung die Anforderungen an das  $f(t, i)$  so gering zu gestalten, wie nur möglich.

Wie ebenfalls bereits herausgearbeitet, ist die verwendete Implementierung des  $\mathcal{K}(i)$  ohne nachweisbare Existenz eines  $f(t, i) > 0$  in vielen *Bonding-Curves-Projekten* als ein teils unseriöser Preistreiber zu sehen. Dies resultierte aus der bereits oben formalisierten Kaufentscheidung eines jeden potenziellen Tokenkäufers:

$$\text{Ich sollte kaufen } \Leftrightarrow \exists k > i, \text{ so dass } \mathcal{V}(k) > \mathcal{K}(i)$$

Und zwar **Preistreiber** deswegen, weil die Kaufentscheidung eines Tokens bei aktuellem Supply  $i \in \mathbb{N}$  ohne fundiertes  $f(t, i)$  von Kaufentscheidungen Anderer bei größerem Supply  $i, i+1, \dots, k$  abhängt. Man sollte also genau dann kaufen, wenn man davon ausgeht, das andere später auch kaufen - und das noch zu einem höheren Preis. Diese müssten dann davon ausgehen, dass wiederum andere noch später zu einem noch höheren Kurs einsteigen und so weiter.

An bier WIP

Und obwohl wir die Existenz eines  $f(t, i) > 0$  nicht allgemein sicherstellen und es erst recht nicht konkret benennen können, so können wir zumindest eine Mindestanforderung herleiten und diese dabei zusätzlich ins Verhältnis zum Risiko eines potenziellen Investors setzen.

Dazu wollen wir das  $\mathcal{V}(i)$  von etwaigen künftigen Käufen abkoppeln und seine Abhängigkeit von  $\mathcal{K}(j)$  auf ausschließlich vergangene Käufe  $\mathcal{K}(j)$  mit  $j \leq i$  reduzieren.

### Prämissse 3: Risiko eines Tokenkaufs

Wir definieren eine zusätzliche Abhängigkeit zwischen Ausgabepreis-Kurve  $\mathcal{K}(i)$  und Rücknahmepreis-Kurve  $\mathcal{V}(i)$ :

$$\mathcal{K}(i) = (1 + \rho) \cdot \mathcal{V}(i) = (1 + \rho) \cdot \frac{\mathcal{T}(i)}{i} = (1 + \rho) \cdot \frac{\sum_{j=1}^i \mathcal{K}(j)}{i} \text{ mit } \rho > 0$$

Neu an dieser Forderung ist hierbei lediglich die erste Gleichheit. Die anderen sind

Resultat unserer bereits weiter oben definierten Anforderungen an die Rücknahmepreis-Kurve  $\mathcal{V}(i)$ .

Das  $\rho > 0$  beschreibt hierbei das Invest-Risiko eines Tokenkaufs bei Supply von  $i \in \mathbb{N}$ . Unsere Forderung ist also wie folgt zu interpretieren:  $\rho$  beziffert den prozentualen Höchstverlust, den ein potenzieller Investor bei einem Kauf eines Tokens zum Preis von  $\mathcal{K}(i)$  bei einem Supply von  $i \in \mathbb{N}$  im schlimmsten Fall zu tragen hätte. Denn er könnte den gekauften Token jederzeit zum Preis von  $\mathcal{V}(i) = \frac{\mathcal{K}(i)}{1+\rho}$  wieder an den Contract zurückgeben und sich dafür auszahlen lassen.

Hinsichtlich dieser Interpretation wird das  $\rho > 0$  in der Praxis also vermutlich tendenziell sehr klein zu wählen sein:  $0 < \rho \ll 1$ .

Die konkrete Wahl von  $\rho$  wird hierbei in starker Wechselwirkung zum projektbezogenen  $f(t, i) > 0$  stehen. Je vielversprechender der durch  $f(t, i)$  beschriebe *Off-Contract-EBIT* des Projekts ausfällt, desto größeres Risiko und damit  $\rho$  ist einem Tokenkäufer zuzumuten und umgekehrt.

Am Ende gilt wahrscheinlich sogar

$$\text{Es existiert kein } f(t, i) > 0 \Leftrightarrow \rho = 0 \Leftrightarrow \mathcal{V}(i) = \mathcal{K}(i) \quad \forall i \in \mathbb{N}$$

Das Risiko ist mit der gemachten Vorgabe an die Rücknahmepreis-Kurve ist insofern mit gegebener Sicherheit gedeckelt als das  $\mathcal{V}(i)$  für  $\rho > 0$  stark monoton steigend ist

Zudem kann man bei gegebenem  $\rho > 0$  seine durch

$$\exists k > i, \text{ so dass } \mathcal{V}(k) > \mathcal{K}(i)$$

gechallengte Kaufentscheidung validieren und nicht nur die Existenz eines solchen  $k > i$  beweisen, sondern dieses  $k$  auch konkret in Abhängigkeit des  $\rho$  berechnen.

WIP

Begünstigte formalisieren (mit zusätzlicher Funktion). Begünstigte erhalten einen Teil der Projekt-Treasury zu ihrer freien Verfügung.

### 5.4.5 Lösungsidee 2

TODO

#### 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  **$2 * x \text{ WPT}$**  in den Lookup-Contract einzahlen.
- Die eingebrachten  **$2 * x \text{ WPT}$**  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 Bestätigungszeugnis von B.
- Mit dem Bestätigungszeugnis 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  **$2 * x \text{ WPT}$**  - also  **$x \text{ WPT}$** ) ausgeschüttet. Und zwar zur Hälfte an Provider A und zur andern Hälfte an den User.
- **$x \text{ WPT}$**  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  $z$  releasest immer wieder die Hälfte des verbliebenen gelockten Deposits.
- Nach Ablauf des definierten **Zeitraums  $z$** 
  - bekommt B den verbliebenen (nicht ausgeschütteten) Teil seines Deposits zurückgestattet.
  - 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 (→ 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 Dienstleistung, 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 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

#### **5.4.6 Kreislauf**

TODO

#### **5.4.7 Token-Design**

TODO

#### **5.4.8 Incentivierung**

TODO

#### **5.4.9 Milestones-Reward-Pool**

TODO

#### **5.4.10 WPT in Zahlen**

TODO

#### **5.4.11 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* genannt)

#### **Conclusion 6: 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/machen können" und diesen nicht "lediglich besitzen", um ihn ausschließlich mit einer gewissen Wahrscheinlichkeit gewinnbringend weiterverkaufen zu können ("Hot Potato"). Der Token bedarf also gewisser Eigenschaften eines *Governance-Tokens* (DAO) oder Ähnlichem.
- Der *NFT-Pass* braucht ungeachtet des vorigen Bullet-Points 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-Sets** 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 ein (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 zehn-millionste 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.

In den kommenden Abschnitten folgt ein initialer Abriss unserer Vorstellung des *NFT-Pass*:

### 6.1.1 Status-Property

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 einenrareren 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.

#### NFT-Property 1: Pass-Status

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 (**Pearl**)
  - Anzahl Pässe: 12.800
  - Gemintet an Nummer: 1801 bis 14.600
- Status D (**Platin**)
  - Anzahl Pässe: 102.400
  - Gemintet an Nummer: 14.601 bis 117.000
- Status E (**Ruby**)
  - Anzahl Pässe: 819.200
  - Gemintet an Nummer: 117.001 bis 936.200
- Status F (**Gold**)
  - Anzahl Pässe: 6.553.600
  - Gemintet an Nummer: 936.201 bis 7.489.800
- Status G (**Silver**)
  - Anzahl Pässe: 52.428.800

- Gemintet an Nummer: 7.489.801 bis 59.918.600
- Status H (**Bronze**)
  - Anzahl Pässe: 419.430.400
  - Gemintet an Nummer: 59.918.601 bis 479.349.000
- Status I (**White**)
  - Anzahl Pässe:  $\infty$
  - Gemintet an Nummer: 479.349.001 bis  $\infty$

Diese NFT-Property ist per Definition trivialerweise **deterministisch**: Es ist stets zweifellos klar, welchen Status ein an x-ter Stelle geminterter *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.

### 6.1.2 Hologramm

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.)

#### NFT-Property 2: Hologramm (Welt-Wunder)

Wir definieren folgende *NFT-Pass-Hologramme* mit den dazugehörigen Eigenschaften:

- WW1
  - Mögliche Ausprägung: **Pyramids of Giza**
  - Anteil Pässe: 0,390625% ( $\frac{1}{256}$ )
- WW2
  - Mögliche Ausprägung: **Great Wall of China**
  - Anteil Pässe: 0,78125% ( $\frac{1}{128}$ )

- WW3
  - Mögliche Ausprägung: **Petra**
  - Anteil Pässe: 1,5625% ( $\frac{1}{64}$ )
- WW4
  - Mögliche Ausprägung: **Colosseum**
  - Anteil Pässe: 3,125% ( $\frac{1}{32}$ )
- WW5
  - Mögliche Ausprägung: **Chichén Itzá**
  - Anteil Pässe: 6,25% ( $\frac{1}{16}$ )
- WW6
  - Mögliche Ausprägung: **Machu Picchu**
  - Anteil Pässe: 12,5% ( $\frac{1}{8}$ )
- WW7
  - Mögliche Ausprägung: **Taj Mahal**
  - Anteil Pässe: 25% ( $\frac{1}{4}$ )
- WW8
  - Mögliche Ausprägung: **Christ the Redeemer**
  - 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 unumkehrbar 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 betroffenen 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  $n$ .
- Gleichermaßen tue man nun für die Counts der geminteten Pässe pro Ausprägung der

Hologramm-Property WW1 bis WW8 als entsprechende Größen  $n_1, n_2, \dots, n_8$ .

- Und damit anschließend die aktuelle prozentuale Verteilung der Ausprägung auf die aktuell geminteten Pässe als  $\sigma_i := \frac{n_i}{n}$  für  $i \in \{1, \dots, 8\}$  berechnen.
- Seien  $\Theta_i$  für  $i \in \{1, \dots, 8\}$  die oben definierten **relativen** Obergrenzen der Ausprägungen der Hologramm-Property WW1 bis WW8.
- 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  $\rho_i$  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, auch für die neuen Wahrscheinlichkeiten gelte

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

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

Was hier so kompliziert klingt, lässt sich aber super simpel veranschaulichen:

Die *Verlosung* der Wunder erfolgt in einem periodischen 256er-Turnus ( $256 = 2^n$  mit  $n = 8$  für die acht bereitgestellten Hologramme). Nach jedem 256. geminteten Pass schmeißt man 256 Lose in eine Lostrommel: Ein Los für die *Pyramiden*, zwei für die *Chinesische Mauer*, vier für *Petra* etc. Die *Jesus-Statue* kommt letztendlich mit 129 Losen in die Trommel.

Nun ziehen wir blind ein Los und vergeben das gezogene Hologramm an den nächsten zu mintenden NFT-Pass. Wir tun dies solange, bis die Trommel leer ist. Anschließend fangen wir wieder von Vorne an und befüllen die Trommel erneut mit denselben 256 Losen.

**Achtung:** Wir befüllen die Trommel ausschließlich nachdem sie komplett leer geworden ist und nicht etwa zwischendurch mal.

### 6.1.3 Pattern-Property

Diese NFT-Property soll ebenso wie die beiden vorigen einem abstufernden Raritätsprinzip zu Grunde liegen - und zwar ausschließlich dem Zufall folgend.

Im Gegensatz zu den beiden vorigen Properties obliegt die *Pattern-Property* keiner absoluten Obergrenze - insbesondere auch dann nicht, falls einige Pattern zu einem Zeitpunkt verhältnismäßig unter- oder überrepräsentiert sind.

#### NFT-Property 3: Background (Pattern)

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

- P1
  - Mögliche Ausprägung: **Safari Fun**
  - Wahrscheinlichkeit: 0,1953125% ( $\frac{1}{512}$ )
- P2
  - Mögliche Ausprägung: **Triangular Bars**
  - Wahrscheinlichkeit: 0,390625% ( $\frac{1}{256}$ )
- P3
  - Mögliche Ausprägung: **Pointillism**
  - Wahrscheinlichkeit: 0,78125% ( $\frac{1}{128}$ )
- P4
  - Mögliche Ausprägung: **Wavy waves**
  - Wahrscheinlichkeit: 1,5625% ( $\frac{1}{64}$ )
- P5
  - Mögliche Ausprägung: **Stony desert**
  - Wahrscheinlichkeit: 3,125% ( $\frac{1}{32}$ )
- P6
  - Mögliche Ausprägung: **WunderPass**
  - Wahrscheinlichkeit: 6,25% ( $\frac{1}{16}$ )
- P7
  - Mögliche Ausprägung: **Zigzag**
  - Wahrscheinlichkeit: 12,5% ( $\frac{1}{8}$ )

- P8
  - Mögliche Ausprägung: **Linear**
  - Wahrscheinlichkeit: 25% ( $\frac{1}{4}$ )
- P9
  - Mögliche Ausprägung: **Curves**
  - Wahrscheinlichkeit: 50,1953125% ( $\frac{257}{512}$ )

#### 6.1.4 Edition

Die Edition unseres WunderPasses soll als Property auf die anfangs geforderte Möglichkeit einer gewissen Individualisierung des WunderPasses durch seinen Besitzer einzahlen. Zu individuell darf eine solche NFT-Property aber auch nicht sein, da der NFT zwingend seinen Eigentümer wechseln können soll, da das ganze Unterfangen mit dem NFT-Pass andernfalls ad absurdum führte.

Um die Edition-Property noch etwas interessanter zu gestalten, sollen Exemplare jeder Edition nicht endlos verfügbar sein, sondern stattdessen irgendwann einmal *aufgebraucht*. In solch einem Fall soll sich der User aber nicht einfach irgendeiner anderer Edition bedienen, sondern erhält die "*Oberedition*" (Parent) seiner ursprünglich gewünschten Edition. Und sollte auch diese *aufgebraucht* sein, dann wiederum die "*Oberedition*" der "*Oberedition*" usw.

#### NFT-Property 4: Edition

Als Ausprägung der WunderPass-NFT-**Edition** haben wir uns für **Städte** der Welt entschieden. Die **Parent-Edition** einer Stadt ist das dazugehörige **Land**, deren Parent-Edition wiederum der entsprechende **Kontinent** und als **oberste Editions-Ebene** dann die **Welt-Edition**. Letztere unterliegt folglich dann auch keiner stückweisen Obergrenze mehr.

#### Beispiel einer Edition-Kette:

Berlin → Germany → Europe → World

Es gilt das folgende grobe Regel-Set, was jedoch explizit auch nach Launch modifizierbar bleiben soll:

- Die möglichen Editionen werden von uns bestimmt. Diese müssen nicht zwingend beim Launch des NFT vollständig benannt werden, sondern können stattdessen auch nachträglich eingepflegt werden. User-Wünsche (in welcher Form auch immer) sind dabei explizit erwünscht.

- Jede berücksichtigte *Städte-Edition* ist genau **100** Mal verfügbar. Sind alle 100 Exemplare einer *Städte-Edition* bereits gemintet (verbraucht), erhält die nächste Mint-Anfrage nach einem WunderPass derselben Edition automatisch die zu dieser Städte-Edition gehörende *Landes-Edition*.
- Die *Landes-Editionen* sind in einer maximalen Stückzahl von je **10.000** pro berücksichtigtem Land verfügbar. Sind auch diese aufgebraucht, wird die durch den User ausgewählte Stadt auf die ihrem Land übergeordnete *Kontinent-Edition* gemappt.
- Die *Kontinent-Editionen* sind in einer maximalen Stückzahl von je **1.000.000** für jeden Kontinent (außer der Antarktis) vorgesehen. Sollte auch diese Menge irgendwann erschöpfen, greifen wir zu der übergeordneten *Welt-Edition*.

### Quantitative Daten zu den Editionen:

- Nach aktuellem Stand sind mindestens 693 *Städte-Edition* vorgesehen.
- Die genannten *Städte-Edition* verteilen sich dabei aktuell auf 179 *Landes-Edition*.
- Die unterschiedlichen *Kontinent-Edition* belaufen sich auf 6 (Nord- und Südamerika, Europa, Afrika, Asien und Australien).
- Die übergeordnete *Welt-Edition* ist in ihrer Stückzahl unbegrenzt.
- Die Auswahl der angebotenen *Städte-Editionen* folgt (mit Augenmaß) in etwa folgender Logik:
  - Die Hauptstadt eines jeden mit einer *Landes-Edition* versehenen Landes ist gleichzeitig auch eine verfügbare *Städte-Edition*.
  - Mit Ausnahme der Hauptstädte erfordert die Größe einer Stadt (nach Einwohnern) ein Mindestmaß  $m_1$ , um als *Städte-Edition* aufgenommen zu werden.
  - Sofern es das vorige Kriterium hergibt, sollen nach Möglichkeit für jedes Land mit einer eigenen *Landes-Edition* mindestens seine 5 größten Städte mit einer eigenen *Städte-Edition* versehen werden.
  - Überschreiten die  $n$  größten Städte eines in die *Landes-Editionen* aufgenommenen Landes eine bestimmte Mindestgröße  $m_2$  (nach Einwohnern), werden alle  $n$  Städte in die verfügbaren *Städte-Editionen* aufgenommen. Dieses Kriterium wird aufgrund des vorigen ausschließlich für  $n > 5$  relevant.
  - Städte der G7-Länder werden (ungeachtet etwaiger Mindestgröße) vermehrt in die *Städte-Editionen* aufgenommen (bis zu 25 *Städte-Editionen* pro G7-Land).
- Einzelne Städte können bei Bedarf auch bei Missachtung aller vorigen Kriterien aufgenommen werden.

### 6.1.5 Design

Dem teils trockenen Text der vorigen Kapitel sollen hier einfach wortlos einige denkbare Ausprägungen unseres WunderPasses in Bild folgen:

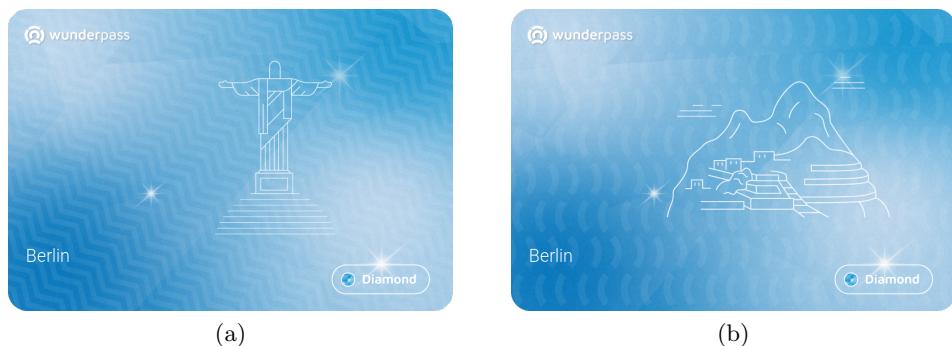


Figure 1: zwei *diamond* Pässe mit je unterschiedlichen Hologrammen und Pattern



Figure 2: Pässe des Status *black* und *pearl*



Figure 3: rechts ein bronzer Pass mit den sehr sehr seltenen *Pyramiden von Gizeh* als Hologramm

#### 6.1.6 Beispielhafte Analyse der Collection

Aus der in den vorigen Kapiteln formulierten Logik ergibt sich gleich vorweg folgende Implikation:

##### Conclusion 7: Vielfalt der Variationen

Bei aktuellem Setting ergeben sich in Summe

$$9 \cdot 8 \cdot 9 \cdot (693 + 179 + 6 + 1) = \mathbf{569.592}$$

unterschiedliche Kombinationen an möglichen NFT-Pässen.

Um ein besseres Gefühl über die formulierte Logik unseres NFTs zu bekommen, wollen wir ein Beispiel mit konkreten Zahlen rechnen und begeben uns dazu eine gute Weile in die Zukunft - zu einem Zeitpunkt, zu dem bereits genau 316.157 NFT-Pässe gemintet worden sind. Ich als potenzieller Interessent an einem Pass-NFT möchte verstehen, welchen Pass ich als nächsten in etwa zu erwarten hätte.

Wir analysieren die 316.157 bereits geminteten Pässe.

##### Status:

- Es wurden 200 Pässe des Status *diamond* gemintet.
- Es wurden 1.600 Pässe des Status *black* gemintet.
- Es wurden 12.800 Pässe des Status *pearl* gemintet.
- Es wurden 102.400 Pässe des Status *platin* gemintet.

- Es wurden 199.157 Pässe des Status *ruby* gemintet.
- Von den insgesamt 819.200 vorgesehenen *ruby* Pässen sind demnach noch 620.043 verfügbar.

***Unser Pass wird also definitiv den Status 'Ruby' haben!***

### **Hologramm:**

Hinsichtlich der Hologramme können wir nur über die ersten 315.904 der 316.157 bisher geminteten Pässe eine definitive Aussage treffen. Die übrigen 253 folgen einer gewissen Wahrscheinlichkeitsverteilung. Zunächst zu den ersten 315.904:

- Es wurden 159.186 Pässe mit dem Hologramm der *Jesus-Statue* gemintet.
- Es wurden 78.976 Pässe mit dem Hologramm des *Maj Mahal* gemintet.
- Es wurden 39.488 Pässe mit dem Hologramm des *Machu Picchu* gemintet.
- Es wurden 19.744 Pässe mit dem Hologramm der *Chichén Itzá* gemintet.
- Es wurden 9.872 Pässe mit dem Hologramm des *Kolosseum* gemintet.
- Es wurden 4.936 Pässe mit dem Hologramm der *Petra* gemintet.
- Es wurden 2.468 Pässe mit dem Hologramm der *Chinesischen Mauer* gemintet.
- Es wurden immerhin stolze 1.234 Pässe mit dem seltensten Hologramm der *Pyramiden von Gizeh* gemintet.

Die Evaluierung der übrigen 253 ist insofern recht dankbar, als dass die 253 schon sehr nah an der zyklischen 256 liegt ( $= 2^n$ , wobei  $n = 8$  für die acht verfügbaren Hologramme steht). Damit beschränkt sich die Analyse eigentlich lediglich auf die nächsten drei Pässe, von denen der erste unserer ist.

Die Auswahl der möglichen Hologramme für die nächsten 3 Pässe bis zum Abschluss des aktuellen 256er-Zyklus ist recht begrenzt. Zum besseren Verständnis dessen vergegenwärtige man sich noch einmal die Veranschaulichung mit der Lostrommel aus Abschnitt [6.1.2](#). Stattdessen erscheint bei der Vergabe-Logik der Hologramme ein Szenario nicht ganz unwahrscheinlich, bei dem für die restlichen drei Pässe des Zyklus noch 1-2 *Jesus-Statuen* verfügbar sind, im Falle nur einer *Jesus-Statue* zusätzlich ein *Taj-Mahal-Hologramm* und das dritte und letzte Hologramm mit etwas Glück auf ein etwas selteneres entfällt.

Wir setzen der Einfachheit halber voraus, im Besitz von Gottes Würfel gewesen zu sein und legen das eingetroffene Szenario auf folgendes fest:

- Unter den 253 geminteten Hologrammen des aktuellen Zyklus sind: Eine Pyramide, 2 Chinesische Mauern, 4 Petras, 8 Kolosseen, **15 Chichén Itzás**, 32 Machu Picchus, 64 Taj Mahals und **127 Jesus-Statuen**.
- Für die letzten drei Pässe des aktuellen Zyklus sind als Hologramme also noch einmal die *Chichén Itzá* und zweimal die *Jesus-Statue* verfügbar.

*Die Wahrscheinlichkeit für unseren NFT-Pass, als Hologramm die Chichén Itzá zu erhalten, liegt also bei 33,33 % und für die Jesus-Statue bei 66,67 %.*

#### Pattern:

Da die *Pattern*-Property einer trivialen Wahrscheinlichkeitsverteilung unterliegt, ist es bei dieser Property unmöglich, eine exakte Angabe zu der tatsächlichen Verteilung der *Pattern* auf die 316.157 bisher geminteten Pässe machen zu können. Da die Zahl der geminteten Pässe jedoch sehr groß ist, liege es nahe, die tatsächliche Verteilung entspräche nahezu exakt der in Property 3 angegebenen Wahrscheinlichkeitsverteilung. Für eine Prognose über etwaige Wahrscheinlichkeiten von möglichen Pattern für sowohl die nächsten 3 Pässe als auch den tatsächlich nächsten bleibt uns nichts anderes übrig, als mit denselben Wahrscheinlichkeits-Angaben aus Property 3 zu kalkulieren.

*Wir gehen stillschweigend davon aus, hinsichtlich Pattern bei unserem zu mintenden NFT-Pass Pech zu haben, und eines der beiden häufigsten aller verfügbaren Pattern zu erwischen: Nämlich die 'Curves' oder das 'Linear'.*

#### Edition:

*Als Edition wählen wir 'Berlin', von dem wir ausgehen, es sei noch verfügbar.*

#### Unser NFT-Pass:

Unter Berücksichtigung der bisher zusammengetragenen Ergebnisse und Wahrscheinlichkeits-Annahmen, erhalten wir mit 75-prozentiger Wahrscheinlichkeit einen der folgenden 4 Pässe:



Figure 4: mit einer Wahrscheinlichkeit von 50 % bekommen wir einen dieser beiden Pässe (zu 33,33 % den linken und zu 16,67 % den rechten)



Figure 5: mit einer Wahrscheinlichkeit von 25 % bekommen wir einen dieser beiden Pässe (zu 16,67 % den linken und zu 8,33 % den rechten)

Die restlichen 25 % der hier nicht berücksichtigten Fälle unterscheiden sich von den oben dargestellten schlichtweg in den (sel teneren) *Pass-Pattern*.

### 6.1.7 Intrinsischer Wert

Abschließend möchten wir an dieser Stelle an die anfangs formulierte zentrale Forderung nach einem **intrinsischen Wert** unseres Pass-NFTs anknüpfen und im folgenden einen Abriss zu denkbaren Einsatzmöglichkeiten des WunderPass-NFTs und seinen potenziellen Vorteilen für seinen Besitzer darlegen.

Konsequenterweise folgen wir bei der Erarbeitung solcher User-Nutzen & -Vorteile der Devise, ein seltenerer NFT-Pass solle als *gut* gelten und damit auch mit einem größeren **intrinsischen Wert** einhergehen. Die Seltenheit ist bei unserem NFT einerseits durch Zufall (*Hologramm & Pattern*) aber auch durch First-Mover-Sein (*Status*) gesteuert.

Wenn es um das Beimessung von Vorzügen und Einsatzmöglichkeiten eines *guten* Pass-NFTs geht, erscheint es irgendwie sinnvoll, eher First-Mover zu begünstigen als etwaige Glückspilze, weshalb wir in der folgenden „*Vorteile-Tabelle*“ das Augenmerk tendenziell auf den *Status* des Pass-NFTs legen möchten. Bei einigen der gleich zu listenenden Vorteilen erscheint jedoch auch der ausschließliche oder zusätzliche Glücksfaktor als ebenfalls sehr charmant, weshalb an solchen Stellen das *Hologramm* des Pass-NFTs zur Beimessung der Vorzüge hinzugezogen wird. Insbesondere möchten wir dem *Pyramiden-Hologramm* explizit und per default dasselbe Statussymbol im Sinne der zu definierenden Vorzüge beimessen wie dem *Diamond-Status*.

**Das *Pattern* findet nach aktuellem Stand jedoch nirgends Berücksichtigung hinsichtlich des intrinsischen Werts eines Pass-NFTs.** Dieses bleibt also zunächst pure Spielerei im Sinne des Pass-NFTs als reines Sammlerstück.

Bei der folgenden Auflistung der Vorzüge und Einsatzmöglichkeiten kategorisieren wir nach **Status-Vorteilen**, **finanziellen Anreizen** sowie **Mitgestaltungsspielraum** innerhalb der WunderPass-Company, die an den zugehörigen Farben zu erkennen sind.

	<i>diamond</i>	<i>black</i>	<i>pearl</i>	<i>pyramid</i>	<i>wall</i>	<i>petra</i>
Weihnachtsfeier	✓✓✓				✓✓✓	
Workshops	✓✓✓	✓			✓✓✓	
Hackathons						
private Discord	✓✓✓	✓✓✓			✓✓✓	
Metallkarte	✓✓✓	✓✓	✓		✓✓✓	
Goodies					✓✓✓	✓✓
Priorisierung	✓✓✓	✓✓	✓		✓✓✓	
Airdrops (Utility Token)					✓✓✓	✓✓
Rewards	✓✓✓	✓✓	✓		✓✓✓	
Staking-Zinsen	+++	++	+		+++	
Beteiligung an NFT-Verkäufen	✓✓✓				✓✓✓	
Dividende	✓✓✓				✓✓✓	
early Access	✓✓✓	✓✓✓			✓✓✓	
Voting for Product/Features	✓	✓	✓		✓	✓
Govern. Tokens (DAO- Membership)	✓✓✓	✓✓	✓		✓✓✓	
<b>Backlog</b>						
exklusiveres Naming						
Zugang zu Interna						
Vergünstigung für Wunder-Dienste						

## 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 verändert 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 Constraints
    - 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 publisiert 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 geparsst 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 Project 'Guard'

TODO

## 9 Project 'Pools'

### 9.1 Einleitung

Die Idee hinter den sogenannten *Wunder-Pools* ist das Bündeln von Liquidität mehrerer User/Teilnehmer bzw. eine Art 'Treuehandverwahrung' in einem gemeinsamen Pool. Die Anwendungsfälle solche Pools können sehr zahlreich sein. Um im Folgenden nur einige Beispiele zu nennen:

- Gemeinsame Invests in (Crypto-)Assets.
- Pool für ein gemeinsames (Geburtstags-)Geschenk.
- Kicktipp-Pool (der über die gesamte Saison verwahrt werden muss).
- Wetten unter Freunden.
- Ausgleichspool für Auslagen von Geld an Freunde (Splitwise).

Das besondere an dem in den folgenden Abschnitten genauer zu beschreibenden Modell, ist sein sehr allgemein gehaltener Ansatz, mit dem sich gleichzeitig Cases umsetzen

lassen, die auf den ersten Blick sehr verschieden zu sein scheinen. Genauer genommen lassen sich solche Pools mit speziellen *DAO-Strukturen* beschreiben.

Abgesehen von der den Pools zugrundeliegenden Geschäftslogik, besteht der zentrale Ansatz unserer *Wunder-Pools* darin, dem User ein rundes Produkt anzubieten - und zwar ganz unabhängig dessen, welcher der oben genannten Cases nun tatsächlich umgesetzt wird. An dieser Stelle möchten wir uns daher ganz explizit von dem Status quo der heute gängigen UX in der Web3-Welt abgrenzen.

Ganz grob beschrieben, streben wir in etwa folgende Geschäftslogik an:

- Ein User erstellt einen Pool (in einer dafür implementierten Wunder-Pool-Applikation).
- Derselbe User definiert die Pool-Art, ein etwaiges dazugehöriges Regelwerk und fordert andere User auf, dem Pool beizutreten. Idealerweise erfolgt die Einladung mittels Suche nach der Wunder-ID des einzuladenden Teilnehmers (und nicht etwa anhand seiner Ethereum-Adresse oder sonstigem).
- Die eingeladenen Teilnehmer erhalten die Einladung (in der WunderPass-App oder der Wunder-Pool-Applikation) und können entscheiden, ob sie dem Pool beitreten möchten oder nicht.
- In der Regel ist sofort beim Beitritt des Pools der definierte Einsatz zu entrichten (der anschließend in die Pool-Treasury geht). In einigen Cases kann der Einsatz evtl. zu einem späteren Zeitpunkt erfolgen oder gar ganz entfallen (z.B. beim Case *Splitwise*).
- Der Pool ist eingerichtet und "kommt zu Einsatz", wie in etwa
  - zum gemeinschaftlichen Investieren in (Crypto-)Assets,
  - zum Verwahren "in Treuhand" bei einer oder mehreren abgeschlossenen Wetten (oder auch z. B. Kicktipp)
  - etc.
- Der Pool wird liquidiert und das Geld nach dem vorher festgelegten Regelwerk auf alle Pool-Teilnehmer (nach einem aus dem Regelwerk folgenden Verteilungsschlüssel) verteilt. Die Liquidierung selbst kann entweder ebenfalls durch das Regelwerk auf einen bestimmten Zeitpunkt und/oder Ereignis terminiert werden (z.B. Ende einer BuLi-Saison beim Case *Kicktipp*) oder aber durch die Teilnehmer beschlossen werden (mittels einer DAO-Abstimmung). Die Errechnung des genannten Verteilungsschlüssels möchten wir möglichst allgemein halten und übertragen diese Verantwortlichkeit einem *abstrakten Oracle*, welches es stets Case-spezifisch zu definieren (und zu implementieren) gilt.

### Product-Sicht

Abschließend sei noch einmal betont, dass wir das/die aus den Wunder-Pools hervorgehende(n) Product(s) (mittelfristig) alternativlos user-friendly sehen. Ohne notwendigen

Bezug zur Crypto-Szene, ohne MetaMask und ohne kryptische hexadezimale Wallet-Adressen. Stattdessen clean und simpel.

## 9.2 Formalisierungen

Zunächst einmal benötigen wir einige formale Werkzeuge und bedienen uns dafür folgender Definition:

### Definition 16

Im folgenden setzen wir Voraus, die Nutzung der Pools seitens der User erfordert zwingend den Besitz eines WunderPass (bzw. Wunder-ID) und betrachten von daher auch nur solche User.

$$U := \{u_1; u_2; \dots; u_n \mid u_i \text{ besitzt eine Wunder-ID}\}$$

Wir stellen zusätzlich, dass der vorausgesetzte Besitz einer Wunder-ID mit dem Besitz von unterschiedlichen Wallets bzw. anderen durch die Wunder-ID implizierten Dingen einhergeht. So hat jeder User  $u_i$  z.B. eine Telefonnummer mit seiner Wunder-ID verknüpft (anhand derer er mittels Kontakte-Scan auf dem Smartphone als Inhaber einer Wunder-ID und damit potenzieller Pool-Teilnehmer erkannt werden kann und soll). Des weiteren kann  $u_i$  einen NFT-Pass (siehe Kapitel 6) besitzen und/oder unser ERC20-Utility-Token (im Folgenden als *WPT* bezeichnet; siehe Kapitel **TODO: verlinken**).

Wir formalisieren den in Kapitel 6 definierten NFT-Pass als die (geordnete) Menge aller bisher geminteter NFT-Pässe:

$$\begin{aligned} WPN &:= \{wpn_1; wpn_2; \dots\} \text{ mit} \\ wpn_i &:= (s_i, w_i, m_i) \end{aligned}$$

Dabei repräsentiert  $s_i$  den Status des NFT-Passes,  $m_i$  sein Muster und  $w_i$  das sich auf ihm abgebildete Weltwunder.

Den Besitz eines Pass-NFTs beschreiben wir durch die Funktion

$$\omega : U \rightarrow \mathcal{P}(WPN)$$

$$\omega(u) := \{wpn \in WPN \mid \text{User } u \text{ besitzt den Pass-NFT } wpn\}.$$

Analog dazu definieren wir auch den Besitz am *WPT* eines Users - mit dem Unterschied, dass der Funktionsbereich dieser Funktion aufgrund der Fungibilität von einer Potenzmenge auf einen simplen numerischen Wert zusammenfällt:

$$\varphi : U \rightarrow \mathbb{Q}$$

$$\varphi(u) := \text{Balance des Users } u \text{ am ERC20-Token WPT}.$$

### 9.3 Pool-Erzeugung

Die Erzeugung des Pools findet in zwei Phasen statt: Der *Initialisierungs-Phase* und der *Teilnahme-Phase*

#### Initialisierungs-Phase

Die Initialisierungs-Phase läuft in etwa in folgenden Schritten ab:

- Ein Initiator (Admin)  $u_A \in U$  erzeugt den Pool in einer dafür vorgesehenen *Pool-Applikation* (vergleichbar mit der Erstellung einer WhatsApp-Gruppe). Der Initiator  $u_A$  ist dabei selbst ein Teilnehmer des Pools. Unsere klare Absicht hierbei ist jedoch keine "gesonderten" Pool-Teilnehmer zu haben bzw. mit besonderen Rechten auszustatten. Die Unterscheidung zwischen dem Admin  $u_A$  und anderen Pool-Teilnehmern  $u \in U$  ist idealerweise - sofern es denn der spezielle Case zulässt - nur für die Initialisierungs-Phase von Nöten und kann anschließend entfallen.
- Der Admin definiert das Regelwerk für den zu erstellenden Pool:
  - Art des Pools (Invest-Pool, Wette, Spende, Kicktipp, Splitwise etc.)
  - privater oder öffentlich zugänglicher Pool
  - etwaige Obergrenze an Teilnehmern
  - Einsatz (minimaler, maximaler oder exakter Einsatz pro Teilnehmer und Währung des Einsatzes)
  - Auszahlungslogik (per Abstimmung oder Adresse eines Oracle-Smart-Contracts, der abhängig seiner Contract-Logik einen Auszahlungsschlüssel bereitstellt)

#### Teilnahme-Phase

Die Teilnahme-Phase besteht grob aus folgenden Schritten:

- Der Admin verliert seine Sonderstellung und wird stattdessen zum ersten Teilnehmer seines eigens initiierten Pools.

- Der (ursprüngliche) Admin lädt Teilnehmer ein, sich am Pool zu beteiligen. Die Beteiligung erfordert dabei einen WunderPass (= Wunder-ID) seitens des Teilnehmers. Idealerweise sind die Wunder-IDs mit Telefonnummern verknüpft, sodass sich die einzuladenden User in den Kontakten des Admins erkennbar als potenzielle Teilnehmer wiederfinden.
- Alternativ kann der (ursprüngliche) Admin (oder auch jeder andere bereits beigetretenen Teilnehmer) einen Teilnahme-Link an (weitere) potenzielle Teilnehmer verschicken.
- Jeder adressierte User erhält die Einladung mit allen relevanten Informationen zum eingeladenen Pool (insbesondere auch dem zu entwendenden Einsatz) in seiner Wunder-Pool-Applikation, und muss diese lediglich entweder bestätigen oder ablehnen (Pull-Prinzip). Insbesondere braucht der User für den Beitritt zum Pool kein Meta-Mask oder Sonstiges (Push-Prinzip wie aktuell bei DAOs üblich).
- Auch der Einsatz des neuen Teilnehmers muss nicht aktiv erbrachtet (an eine Wallet) werden, sondern wird stattdessen im Zuge des vorigen Schritts nach Bestätigung der Teilnahme am Pool automatisch eingezogen.

Wir fassen die bisher erzielten Ergebnisse etwas formaler zusammen:

### Definition 17

Ein (jungfräulicher) Pool im Sinne der oben Aufgezählten Eigenschaften und Anforderungen lässt sich formal schreiben als

$$Pool := (\mathcal{U}, \mathcal{R}, \mathcal{T}, \mathcal{G}) \text{ mit}$$

$\mathcal{U} = \{u_1; u_2; \dots; u_n\} \subseteq U$  die Menge der n Pool-Teilnehmer,  
 $\mathcal{R}$  das Regelset des Pools, was es gesondert zu formalisieren gilt,  
 $\mathcal{T} = \{s_1; \dots; s_n\}$  mit  $s_i \in \mathbb{Q}$  die Treasury des Pools und  
 $\mathcal{G} = \{g_1; \dots; g_n\}$  mit  $g_i \in \mathbb{N}$  die Governance des Pools.

Dabei beschreibt jedes  $s_i$  den Einsatz des Teilnehmers  $u_i \in \mathcal{U}$  ( $s$  für Stake). Dieser Einsatz liegt dabei in einem vom Regelset  $\mathcal{R}$  definierten Intervall  $\mathcal{I} \subseteq \mathbb{Q}$ . Damit haben wir bereits an dieser Stelle einen kleinen Teil der noch fehlenden Formalisierung von  $\mathcal{R}$  identifiziert. Bei genauer Betrachtung fehlt uns noch die Einheit der Einsätze  $s_i$ . Diese wird sehr wahrscheinlich *USDT* sein oder ein anderer Stable-Coin.

Zudem beachte man an dieser Stelle zusätzlich, die Definition von  $\mathcal{T}$  werde im Verlaufe der Lifetime eines Pools nicht so simpel bleiben können, als nur aus dem eingebrachten Einsätzen der Teilnehmer zu bestehen. Die Pool-Treasury bedeutet

nämlich mehr als nur die Menge der initialen Stakes. Etwaige Invests aus der Treasury heraus würden nämlich ebenfalls in der Treasury landen.

Die  $g_i$  dagegen beschreiben ganz simpel die Anzahl der Governance-Tokens pro User  $u_i \in \mathcal{U}$ . Man kann diese auch als Gesellschaftsanteile einer GbR betrachten. Das Stammkapital dieser Gesellschaft würde sich in diesem Vergleich auf

$$\kappa := \sum_{i=1}^n g_i$$

belaufen. Der prozentuale Stimmrecht-Anteil eines Users  $u_i \in \mathcal{U}$  ergäbe sich damit als

$$\rho_i = \frac{g_i}{\kappa}, \quad \forall i = 1, 2, \dots, n.$$

Die zusammengetragenen Anforderungen für die Initialisierung eines WunderPools lassen sofort deutlich erkennen, **diese Pools könnten mittels DAO-ähnlicher Strukturen implementiert werden**. Dies erscheint insofern noch logischer, nachdem wir erkannt haben, die Pools stellen gesellschaftsrechtlich GbRs dar - also Gesellschaften und/oder Organisationen. Diese Erkenntnis wollen wir noch einmal als eine formale Annahme formulieren:

### Annahme 3: Ein WunderPool stellt eine GbR dar

Sei  $\mathcal{P} := (\mathcal{U}, \mathcal{R}, \mathcal{T}, \mathcal{G})$  ein WunderPool wie in Definition 17 beschrieben. Wir ziehen die Analogie zu einer **Gesellschaft** bürgerlichen Rechts:

- Die Menge  $\mathcal{U}$  der Pool-Teilnehmer ist der **Gesellschafterkreis der Gesellschaft**.
- $\mathcal{G}$  bildet den **Cap-Table der Gesellschaft** ab.
- Das Pool-Regelwerk  $\mathcal{R}$  ist der **Gesellschaftervertrag zur Gesellschaft**.
- Die Pool-Treasury  $\mathcal{S}$  ist das **Gesellschaftskonto und/oder -depot der Gesellschaft**.

## 9.4 Pool-Lifetime

Eine (allgemeine) funktionale Beschreibung derjenigen WunderPool-Funktionalität, die der Überschrift der gegenständigen Sektion gerecht wird, ist insofern sehr schwierig, als dass sich diese deutlich schwerer auf unterschiedliche Pool-Cases verallgemeinern lässt. Wie anfangs in dem Einführungskapitel 9.1 ist die möglichste Verallgemeinerung aller Cases oberste Prämisse gewesen. Hier müssen wir versuchen zu verallgemeinern, was nur geht, und den Rest eben Case-spezifisch lösen.

Wir schauen auf die Anfangs in Kapitel 9.1 hervorgehobenen Anwendungsfälle für die WunderPools an - nun mit kurzer Skizzierung ihrer Lifetime:

- **Social Investing:** Das ist mit der klarste Case für eine relevante Lifetime eines Pools. Während der Lifetime werden mögliche Invests vorgeschlagen, zur Abstimmung gestellt und im Erfolgsfall abgewickelt. Die Möglichkeiten zur Erweiterung von Investmöglichkeiten (Staking, Lending, Liquidity-Providing, Yield Farming, Aktien, ETFs etc.) scheinen schier unendlich. In diesem Case unterliegt **die Dauer der Lifetime auch keinerlei natürlicher Grenzen** - diese Art von Pool kann theoretisch ewig existieren.
- **Geschenk-Pool:** In diesem Case besteht die Daseinsberechtigung des Pools eigentlich lediglich darin, bequem und einfach Geld einzusammeln und evtl. bis zum Kauf des Geschenks "in Treuhand" zu verwahren. Sind alle gewünschten Teilnehmer beigetreten (und somit ihren Beitrag zum Geschenk entrichtet), hat der Pool eigentlich bereits seinen Zweck erfüllt. Man kann zwar argumentieren, man könne die Auswahl des Geschenks mit DAO-Mitteln zur Abstimmung stellen, dies bleibt jedoch an den Haaren herbeigezogen, solange das Geschenk kein auf der Blockchain erwerbbares Asset ist. **Die Dauer der Lifetime der Pools in diesem Case sind also klar begrenzt:** Spätestens bis zu dem Moment des Kaufs des Geschenks.
- **Kicktipp-Pool:** Das ist der Bilderbuch-Case für den Pool im Sinne der Treuhand-Verwahrung (eines Spieleinsatzes) über einen längeren Zeitraum. Hier wird eingezahlt, über einen Zeitraum (außerhalb des Pools) gespielt und am Ende - je nach Ergebnis - wieder ausgezahlt. Das Geld wird vom Pool also lediglich verwahrt und umverteilt. In der sogenannten *Lifetime* des Pools passiert faktisch gar nichts. Man könnte sich sicherlich kreative Möglichkeiten zur Interaktion mit dem Pool überlegen (wie z.B. Abstimmungen über etwaige Regeländerungen oder über das Nachtragen von verspätet abgegebenen Tipps), dies beträfe aber nie die relevante Kernfunktionalität des Pools innerhalb dieses Cases. Die defacto '*leere Lifetime*' des Pools endet in diesem Case mit Ablauf der Spielzeit, für die die Kicktipp-Runde eingerichtet wurde. Ihre **Dauer ist also begrenzt**.
- **Wetten:** Dieser Case verhält sich sehr analog zum *Kicktipp-Case*. Dazu muss jedoch klargestellt sein, dass wir den Case als eine einzige Wette (zwischen zwei oder mehr Leuten) verstehen, bei der der Pool der Treuhand-Verwahrung dient, und nicht etwa eine "Wett-Gruppe", wo immer mal wieder neue Wetten vorgeschlagen und umgesetzt werden. Der Pool dieses Cases bildet also eine einzige Wette ab und seine **Lifetime endet in dem Moment, wo das Ergebnis der Wette feststeht**.
- **Splitwise:** Dies ist der außergewöhnlichste aller Cases. Hier existieren de facto weder eine echte Treasury noch eine Lifetime. Für Splitwise wird erst die Umverteilung interessant, wobei hier genau genommen der Betrag von 0 auf die Teilnehmer umverteilt wird. Da hier aber - im Gegensatz zu allen obigen Cases - auch negative

Withdraws zulässig sind (also genau genommen eine Einzahlung von denjenigen Teilnehmern, die anderen Teilnehmern etwas schulden), klingt die Umverteilung des Betrags 0 plötzlich doch nicht mehr so abwegig. Die 0 signalisiert nur die Forderung, die verteilten Beträge (Schulden und Auslagen mit entsprechendem Vorzeichen) müssen sich auf 0 summieren. Da der Pool in diesem Case faktisch gar keine Lifetime besitzt, ist **die Dauer der Lifetime konsequenterweise begrenzt**.

Zusammenfassend halten wir fest, die Dauer der Pool-Lifetime ist nur für den *Social-Investing-Case* theoretisch unbegrenzt. Bei allen anderen Cases wird der Pool nach einer bestimmten Zeit oder bei Eintreten eines bestimmten Ereignisses obsolet und muss/sollte anschließend aufgelöst werden. Und auch hinsichtlich relevanter Funktionalität während der *Lifetime* scheint der *Social-Investing-Case* ebenfalls der einzig interessante zu sein.

Eine Verallgemeinerung erscheint also - zumindest für die zuletzt genannten vier Cases - evtl. doch im Rahmen des Möglichen.

**Etwaiges Austreten bestehender Teilnehmer oder Eintreten neuer Teilnehmer würde sich während der 'Lifetime' abspielen.**

## 9.5 Pool-Liquidierung

Für eine etwaige Pool-Liquidierung stellen sich exakt zwei Fragen: **”Wann** wird liquidiert?” und **”Wie** wird liquidiert?” Das **Wann** ist hierbei schnell geklärt. Es gibt grob folgende drei Möglichkeiten, von denen eine durch das in Definition 17 definierte Regelset  $\mathcal{R}$  zu spezifizieren ist:

- $\mathcal{R}$  legt einen exakten Zeitpunkt fest, zu dem der Pool liquidiert werden soll.
- $\mathcal{R}$  definiert ein bestimmtes Ereignis, bei deren Eintreten der Pool liquidiert werden soll.
- $\mathcal{R}$  regelt, dass die Pool-Liquidierung per (DAO-)Abstimmung beschlossen werden muss.

Bullet 2 klingt hier leider noch nicht ausreichend abstrakt. Daher abstrahieren wir die genannten Forderungen in einer einzigen:

### Conclusion 8: Liquidierungsentscheidung-Oracle

Das in Definition 17 definierte Regelset  $\mathcal{R}$  definiert ein Oracle, welches zu jedem Zeitpunkt die Frage beantworten kann, ob der Pool zum jetzigen Zeitpunkt liquidiert werden soll oder nicht.

Dieses Oracle kann beliebig einfach gestrickt sein (z.B. im Falle des obigen Bullet 1

einfach anhand " $SYSDATE <= T_{END}$ " über das Fortbestehen des Pools entscheidet) oder aber auch beliebig komplex. Dies braucht uns aber an dieser Stelle nicht weiter weiter interessieren.

Und da die Abstraktion mittels Oracle so bequem scheint, tun wir das Gleiche ebenfalls für das oben genannte **Wie**:

### Conclusion 9: Auszahlungsschlüssel-Oracle

Seien  $\mathcal{P} = (\mathcal{U}, \mathcal{R}, \mathcal{T}, \mathcal{G})$  der Pool und  $\mathcal{U} = \{u_1; u_2; \dots; u_n\}$  die Menge seiner  $n$  Teilnehmer wie in Definition 17 beschrieben und  $v_{\mathcal{T}}$  der sich zum Liquidierungszeitpunkt in der Pool-Treasury  $\mathcal{T}$  befindende Value.

Falls der Pool lediglich als Treuhand-Verwahrung diente (also über die Zeit keine Veränderung der Treasury stattfand) ergibt sich  $v_{\mathcal{T}}$  als

$$v_{\mathcal{T}} = \sum_{i=1}^n s_i \text{ mit } s_i \text{ wie in Definition 17}$$

Wir definieren einen Auszahlungsvektor als

$$\varphi_{\mathcal{P}} = [\varphi_1, \varphi_2, \dots, \varphi_n] \text{ mit } \sum_{i=1}^n \varphi_i = v_{\mathcal{T}}$$

Ein mögliches  $\varphi_{\mathcal{P}}$  ist tatsächlich  $\mathcal{G}$

$\mathcal{R}$  definiert das Oracle und sagt, ob die  $\varphi_i$  negativ sein dürfen

Oracle verteilt anhand von  $\mathcal{T}$  und  $\mathcal{G}$

TODO

## 9.6 Pool-Vertrag

Herausgearbeitete Dinge zu  $\mathcal{R}$  zusammentragen

- Vorgabe zur Teilnehmer-Menge  $\mathcal{U}$
- Vorgabe zur Pool-Treasury  $\mathcal{S}$ :
  - Währung (zB *USDT*)
  - Intervall  $\mathcal{I}$  für  $s_i \in \mathcal{I}$
- Definition der *Liquidierungsentscheidung-Oracle*

- Definition der *Auszahlungsschlüssel-Oracle*
- Optionale Forderung  $\varphi_i \geq 0$
- etc.

## 9.7 Pool-Economics

So könnte ein Pool-Utility-Token umgesetzt werden.

- Utility-Token: WunderPool-Tolen (PLT)
- Bonding-Curves-Modell
- Bezug zum WunderToken herstellen
- Daten, Zahlen, Fakten
- Business-Case (aus Investoren-Sicht)
  - Wirtschaftlichkeit und Preisentwicklung vorrechnen
  - (praktische) Obergrenze des eingebrachten Gesamtkapitals annehmen, mit der eine plausible und attraktive Rendite vorgerechnet werden kann.

## Einleitung: Einführung des WunderPool-Tokens: W-PLT

### Prämissen 4: Cash-Flow

- Deposit/Invest erfolgt in einem Stable-Coin (z.B. *USDT*). Es sind aber auch mehrere zulässige Währungen zulässig.
- Cashout erfolgt in derselben Währung wie der Deposit (oder zumindest in einer der zulässigen Währungen).
- Fees werden in aller Regel prozentual am Volumen (also in *USDT*) berechnet, jedoch in **W-PLT** veranschlagt, bei dem man von Kursschwankungen ausgehen muss und ausgehen will. (Das muss sowohl bei der Token-Modellierung als evtl. auch bei der Gebührenordnung berücksichtigt werden.)
- Ein Teil der Fees soll direkt an den (Bonding-Curves-basierten) *W-PLT*-Contract gehen und damit die *W-PLT*-Investoren/-Hodler belohnen.
- Die Fees sollen (aufgrund des genauer zu erklärenden Stakings) erst bei der Liquidierung des Pools entrichtet werden.
- Die Fees sollen von allen Pool-Teilnehmern außer des Pool-Creators getragen werden.
- Für den Pool-Creator soll folgendes gelten:
  - (Muss einen PassNFT besitzen.)
  - Soll einen prozentual an den geschätzten gesamten Pool-Fees gemessenen Betrag  $x$  als Sicherheit staken ( $x \in [50\%; 200\%]$ ). Kann theoretisch auch einer absoluten oder relativen Obergrenze unterliegen.
  - Soll selbst keine Fees bezahlen.
  - Soll für das Staken mit einem Teil der erwirtschafteten Gebühren entlohnt werden.

### Annahme 4: Gebühren

Es sollen in etwa folgende *Basic-Fees* anfallen:

- Grundgebühr von 1 % auf den Deposit (für jeden Pool-Teilnehmer außer des Pool-Creators).
- Tradinggebühr von 0.1 % auf jede Kauf- oder Verkaufsorder.
- Gewinnprovision von 4.9 % auf einen durch den Pool erwirtschafteten **positiven** Wert.

tiven EBIT (bei Liquidierung des Pools).

Ergänzt werde diese durch etwaige *Service-Fees*:

- Erweiterte Grundgebühr von zusätzlichen 1.5 % auf den Deposit bei einem späteren Pool-Beitritt (additiv zu der obigen Basis-Grundgebühr).
- *Leaving-Gebühr* von 6.9 % auf den Cashout-Betrag bei vorzeitigem Verlassen des Pools und Cashout seitens eines Pool-Teilnehmers, falls der Cashout über den Pool-Contract erfolgt (und nicht z.B. mittels Verkaufs der Shares an einen anderen Pool-Teilnehmer oder am Sekundär-Markt).

Zudem sind folgende *Benefits* hinsichtlich der Gebührenordnung für Inhaber eines Pass-NFTs ([Kapitel verlinken](#)) vorgesehen:

- Wegfall der Deposit-Grundgebühr für Inhaber eines PassNFTs des Status *Diamond*.
- Reduzierung sämtlicher Gebühren, die auf User- und nicht Pool-Basis anfallen um
  - 50 % für Teilnehmer mit PassNFT-Status *Diamond*,
  - 30 % für Teilnehmer mit PassNFT-Status *Black*,
  - 20 % für Teilnehmer mit PassNFT-Status *Pearl*,
  - 10 % für Teilnehmer mit PassNFT-Status *Platin*.

Aktuell nicht berücksichtigt jedoch grundsätzlich spannend sind die folgenden Gebühren-Aspekte und -Varianten:

- Eine mögliche *Trial-vs-Pro-Gebührenordnung*, bei der (stark) limitierte Pools (sowohl finanziell als auch feature-technisch) gänzlich kostenlos bleiben könnten, während eine unlimitierte Nutzung mit höheren Gebühren als den obigen einhergehen würde.
- *Managed-Pools*: Pools, die von einem erprobten und erfolgreichen Pool-Creator hinsichtlich der Invests gesteuert, könnten eine höhere Teilnahme-Gebühr erfordern, an der auch der Creator maßgeblich beteiligt wird.

Abgerechnet werden die auf den Pool anfallenden Fees (selbst die ausschließlich User-basierten) aufgrund von *Mechanism-Design*-Überlegungen erst bei seiner Liquidierung.

### Prämissen 5: Abrechnung

Sämtliche für einen Pool angefallenen Fees werden (ungeachtet ihres Fälligkeitszeitpunkts) fließen erst bei seiner Liquidierung und werden zwischen Fälligkeit und Entrichtung in einem gesonderten Teil der *Pool-Treasury* vorgehalten (ähnlich dessen, wo der gestakte Betrag des Pool-Creators verwahrt wird).

Wir werden diese finanziellen Mittel im weiteren Verlauf auch als **Pending-Fees** bezeichnen.

In Analogie dazu werden wir an geeigneter Stelle folgend auch von **Staked-Fees** sprechen - gleichwohl es sich dabei eher um eine Sicherheit als um tatsächliche Fees handelt.

Der Gebührenordnung folgen einige Annahmen hinsichtlich des **Business-Plans** für eine Größenordnung von zwölf Monaten.

### Annahme 5: Business-Plan

Zunächst schätzen wir einige KPI ab, die es natürlich zu validieren gilt:

- Wir gehen im Mittel von ca. 4-5 Teilnehmern je Pool aus.
- Wir gehen von einem durchschnittlichen Deposit von 200\$ je Teilnehmer und Pool aus - also einem durchschnittlichen initialen Pool-Kapital von 800-1000\$.
- Wir gehen des Weiteren von einer durchschnittlichen *Pool-Lifetime* von ca. 6 Monaten aus,
- schätzen die durchschnittliche Anzahl an Tradings während der Pool-Lifetime auf 10-15,
- deren Trading-Volumen auf etwa  $\frac{1}{3}$  des initialen Pool-Kapitals und schließlich
- und einen daraus resultierenden konservativen mittleren Profit von 2 % (auf die Pool-Lifetime von 6 Monaten also 4-5 % p.a.).
- Zuletzt schätzen wir, jeder User betreibe im Mittel 2-3 Pools gleichzeitig.

Diesen geschätzten KPI zugrundeliegend setzen wir uns folgende Ziele hinsichtlich initiierten (gebührenpflichtiger) Pools - ungeachtet dessen, ob diese zu dem gegebenen Zeitpunkt noch existieren oder bereits liquidiert wurden:

- 50 initiierte Pools nach 3 Monaten

- 150 initiierte Pools nach 6 Monaten
- 500 initiierte Pools nach 12 Monaten

Damit ergeben sich folgende Business-Key-KPI:

#### Conclusion 10: Umsätze & Forecast

Für einen durchschnittlichen Pool  $\mathcal{P}$  mit dem initialen Pool-Kapital

$$vol^{\mathcal{P}} = 4.5 \cdot 200\$ = 900\$$$

approximieren wir die anfallenden Fees als Summe der Fee-Bestandteile

- Grundgebühren:  $fees_G^{\mathcal{P}} = \rho(nft) \cdot 0.01 \cdot (4.5 - 1) \cdot 200\$$
- Trading-Gebühren:  $fees_T^{\mathcal{P}} = \phi(nft) \cdot 0.001 \cdot 12.5 \cdot vol^{\mathcal{P}}$
- Profit-Beteiligung:  $fees_P^{\mathcal{P}} = \phi(nft) \cdot 0.02 \cdot vol^{\mathcal{P}}$

wobei  $\rho(nft)$  und  $\phi(nft)$  Normierungsfaktoren darstellen, die die in Annahme 4 beschriebenen *Benefits für PassNFT-Besitzer* berücksichtigen sollen, und von uns als

- $\rho(nft) \approx \frac{2}{3}$  und
- $\phi(nft) \approx \frac{3}{4}$

geschätzt werden sollen.

Damit belaufen sich die einzelnen Fees-Bestandteile auf

- Grundgebühren:  $fees_G^{\mathcal{P}} \approx 4.67\$$
- Trading-Gebühren:  $fees_T^{\mathcal{P}} \approx 8.44\$$
- Profit-Beteiligung:  $fees_P^{\mathcal{P}} \approx 13.50\$$

und damit die im Mittel erwarteten Gesamt-Fees pro Pool auf

$$fees^{\mathcal{P}} = fees_G^{\mathcal{P}} + fees_T^{\mathcal{P}} + fees_P^{\mathcal{P}} \approx 26.61\$.$$

Bei einer Staking-Anforderung von 200 % der geschätzten Pool-Fees ([auf Staking verlinken](#)) und den in 5 getroffenen Business-Plan-Annahmen ergeben sich folgende näherungsweisen Forecasts:

- Nach 3 Monaten: ca. 40 noch aktive und bereits ca. 10 liquidierte Pools.
  - bereits *umgesetzte Fees*: 266 \$
  - *Pending-Fees*: 1.064 \$
  - *Staked-Fees*: 2.129 \$
- Nach 6 Monaten: ca. 100 noch aktive und bereits ca. 50 liquidierte Pools.
  - bereits *umgesetzte Fees*: 1.330 \$
  - *Pending-Fees*: 2.661 \$
  - *Staked-Fees*: 5.322 \$
- Nach 12 Monaten: ca. 300 noch aktive und bereits ca. 200 liquidierte Pools.
  - bereits *umgesetzte Fees*: 5.322 \$
  - *Pending-Fees*: 7.983 \$
  - *Staked-Fees*: 15.966 \$

Zu guter Letzt noch eine sehr bullishe Prognose:

- Nach 5 Jahren: 450.000 noch aktive und bereits 550.000 liquidierte Pools.
  - bereits *umgesetzte Fees*:  $\approx$  15 Mio. \$
  - *Pending-Fees*:  $\approx$  12 Mio. \$
  - *Staked-Fees*:  $\approx$  24 Mio. \$

Wir rechnen ein bisschen rum, um ein Gefühl für den nötigen Token-Supply zu bekommen:

### Beispiel 3: Rechnerei zum Token-Supply

Wir peilen den Token-Contract so zu stricken, dass wir im eingeschwungenen Zustand einen Tokenwert des *W-PLT* von  $\approx$  1 Cent anpeilen, aber gleichzeitig auch die Grenzen [0.5 Cent; 2 Cent] im Auge behalten.

Im Folgenden wieder die obige Forecast-Ausstellung - nun aus Token-Sicht:

- Nach 3 Monaten: ca. 40 noch aktive und bereits ca. 10 liquidierte Pools.
  - bereits *umgesetzte Fees*: 25.000 *W-PLT*
  - mindestens bereits geburnte Tokens: 12.500 *W-PLT*
  - *Pending-Fees*: 100.000 *W-PLT*
  - *Staked-Fees*: 200.000 *W-PLT*

- Nach 6 Monaten: ca. 100 noch aktive und bereits ca. 50 liquidierte Pools.
  - bereits *umgesetzte Fees*: 130.000 *W-PLT*
  - mindestens bereits geburnte Tokens: 65.000 *W-PLT*
  - *Pending-Fees*: 250.000 *W-PLT*
  - *Staked-Fees*: 500.000 *W-PLT*
- Nach 12 Monaten: ca. 300 noch aktive und bereits ca. 200 liquidierte Pools.
  - bereits *umgesetzte Fees*: 500.000 *W-PLT*
  - mindestens bereits geburnte Tokens: 250.000 *W-PLT*
  - *Pending-Fees*: 800.000 *W-PLT*
  - *Staked-Fees*: 1.6 Mio. *W-PLT*
- Nach 5 Jahren: 450.000 noch aktive und bereits 550.000 liquidierte Pools.
  - bereits *umgesetzte Fees*: 1.5 Mrd. *W-PLT*
  - mindestens bereits geburnte Tokens: 750 Mio. *W-PLT*
  - *Pending-Fees*: 1.2 Mrd. *W-PLT*
  - *Staked-Fees*: 2.4 Mrd. *W-PLT*

## WIP

- Wann bezahlen die User die Fees?
- In welcher Form/Währung dürfen die Fees von den Usern erbracht/verrechnet werden und wird dann alles im Hintergrund sofort in *W-PLT* umgewandelt?
- Ist es denkbar die Fees aus dem Stake-Pool des Creators zu verwenden und diesem seinen Stake in einer anderen Währung zurückzuerstatten?
- Wie schafft man die Brücke zwischen Fees in *USDT* und *W-PLT*?

## 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 verfügt 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-Profil. 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 für 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 differenzierteres Bild über die Vor- und Nachteile dieser Techniken verschafft haben, erhalten für sie speziell zusam-

mengestellte 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 beispielweise – 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
  - erschwerete 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 Identitätsmanagement. 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, Kontaktdata 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, **Ergebnisse 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 11: 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 grundsätzliche 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 12: Link zu WunderPass**

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

### **Conclusion 13: Aufwand beim User**

Die Forderung nach oben zitierte 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 zurückzahlt.