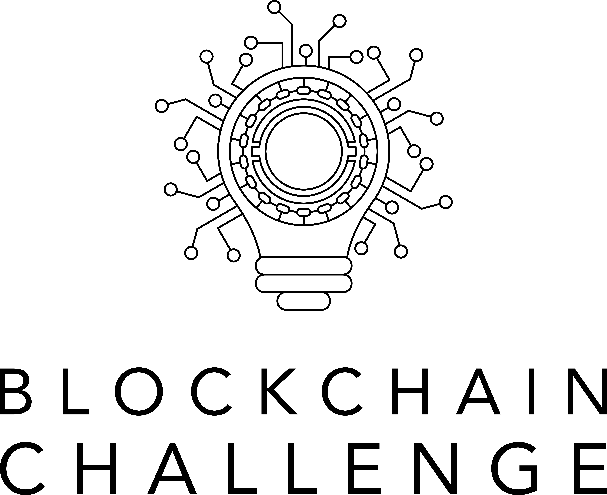
**Blockchain Plattform als Zahlungsarchiv**

Ein Auftrag des Verein Vorsorge Schweiz (VVS) im Rahmen der Blockchain Challenge

Center for Innovative Finance

University of Basel



Mit der Übersicht von:

Prof. Dr. Aleksander Berentsen

Prof. Dr. Walter Dettling

Prof Dr. Fabian Schär

Autoren:

Julian Mordig

[Julian.mordig@stud.unibas.ch](mailto:Julian.mordig@stud.unibas.ch)

Tim Keller

[Tim.keller@unibas.ch](mailto:Tim.keller@unibas.ch)

Alexander Walter

Alexander.walter@students.fhnw.ch

Eingereicht am 4. Dezember 2019

Inhalt

[1. Einleitung 1](#_Toc26290801)

[2. Erklärung des Case und Marktrechte 1](#_Toc26290802)

[3. Blockchain und Ökosystem 9](#_Toc26290803)

[4. Konsensprotokolle 11](#_Toc26290804)

[5. Datenmodell und Architektur 13](#_Toc26290805)

[6. Ökosystem 14](#_Toc26290806)

[7. Technische und Graphische Ausarbeitung 15](#_Toc26290807)

[8. Die Struktur des Smart Contracts 18](#_Toc26290808)

[9. Auswahl der geeigneten Investitionsstrategie 20](#_Toc26290809)

[10. Identifikationsprozess 21](#_Toc26290810)

[11. Das MockUp 22](#_Toc26290811)

[12. Schlusswort 24](#_Toc26290812)

[13. Abbildungsverzeichnis 25](#_Toc26290813)

[14. Literaturverzeichnis 25](#_Toc26290814)

[15. Anhang 26](#_Toc26290815)

[15.1. MockUp-Applikation 26](#_Toc26290816)

[15.2. Der Smart Contract 27](#_Toc26290817)

# Einleitung

Die heutige Welt ist zunehmend geprägt von Digitalisierung und Nachhaltigkeit. Immer öfter wird die Frage gestellt, wie man Prozesse optimieren und dabei nachhaltig agieren kann. Dies betrifft auch das Vorsorgewesen, also die Pensionskassen und die Freizügigkeitsstiftungen. Dieser Sektor leidet unter einem hohen administrativen Aufwand und beachtlichen Briefverkehr. Der aktuelle Trend von zentralen Systemarchitekturen zu Blockchain lässt auch hier Optimierungsprozesse zu. In diesem Auftrag des Vereins Vorsorge Schweiz (VVS) haben wir genau dies versucht. Im Folgenden werden die einzelnen Schritte in der Ausarbeitung aufgezeigt und die Lösung wird am Schluss in Form eines mehr oder weniger fertig ausgearbeiteten Systems präsentiert. Unsere Implementierung soll dazu dienen, den Briefverkehr auf ein Minimum zu reduzieren und Systemabläufe deutlich zu optimieren.

# Erklärung des Case und Marktrechte

Der Auftrag ersucht die Reduktion respektive die Eliminierung des Postversands zwischen Vorsorgenehmer, Pensionskassen und Freizügigkeitsstiftungen. Zudem sollen die Informationen über Kontostand sowie weiteren gesetzlichen Angaben jederzeit abrufbar zur Verfügung stehen für alle Parteien. Damit sollen die verschiedenen Zahlungsaufträge vereinfacht werden. Das Lösungskonzept sollte kosteneffizienter und ökologischer sein als die bisherige Methode. Der Zielmarkt des Auftrages sind die Stiftungen.

Der Verein Vorsorge Schweiz wurde 2014 gegründet und dient als Dachverband der Freizügigkeitsstiftungen und der Säule 3a Stiftungen in der Schweiz. Er vertritt die Interessen jener gegenüber Behörden, der Verwaltung und anderen Institutionen. Der Verein dient zur Orientierung und Beratung der Mitglieder und zur Informierung der Öffentlichkeit. Sein Hauptziel ist die Steigerung der Systemeffizienz. Dies geschieht anhand Empfehlungen und Richtlinien aus Vorschriften und den Lehren aus der Praxis. Des Weiteren herrscht eine zehnjährige Aufbewahrungspflicht der gesetzlich bedingten Informationen eines Versicherten. Ein Freizügigkeitskonto dient dazu, dass man seinen Vorsorgeschutz im Rahmen der 2. Säule (BVG) aufrechterhält. In speziellen Lebenssituationen, beispielsweise einer Unterbrechung oder Aufgabe der Erwerbstätigkeit, kann oder muss man sein erworbenes Kapital aus der beruflichen Vorsorge auf ein Freizügigkeitskonto überweisen.

Anhand Abbildung 1 lässt sich die Ausgangslage aufzeigen. Der Kunde, respektive der Vorsorgenehmer, arbeitet bei der Firma ABC in Periode t. Viele Firmen weisen eine individuelle Pensionskasse auf bei der das Pensionskassenvermögen ihrer Arbeitnehmer versichert ist. Nun ist der Kunde beispielsweise während eines gewissen Zeitraums t+1 nicht berufstätig aufgrund eines Jobwechsels, dem Verlust seines Jobs oder eines Sabbaticals. Nach diesem Unterbruch fängt der Vorsorgenehmer nun einen neuen Job bei Firma XYZ in Periode t+2 an.

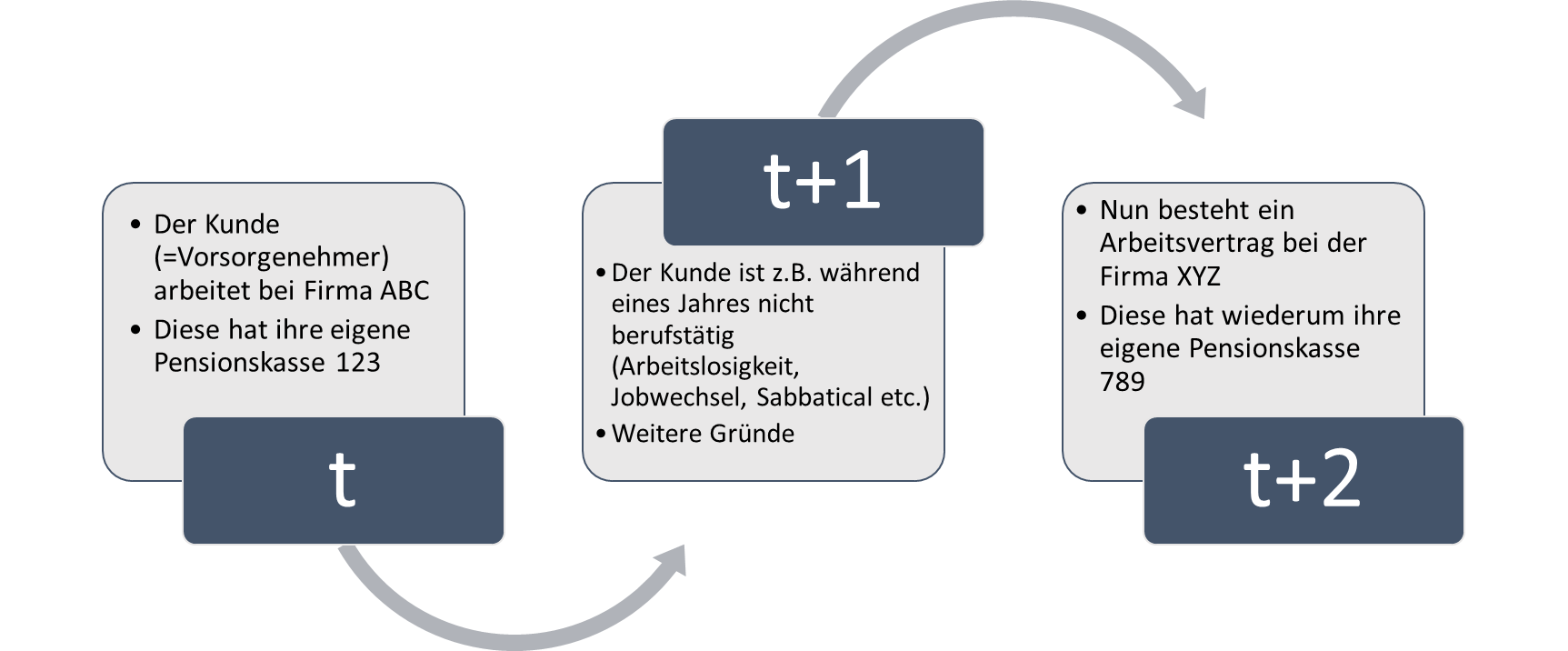
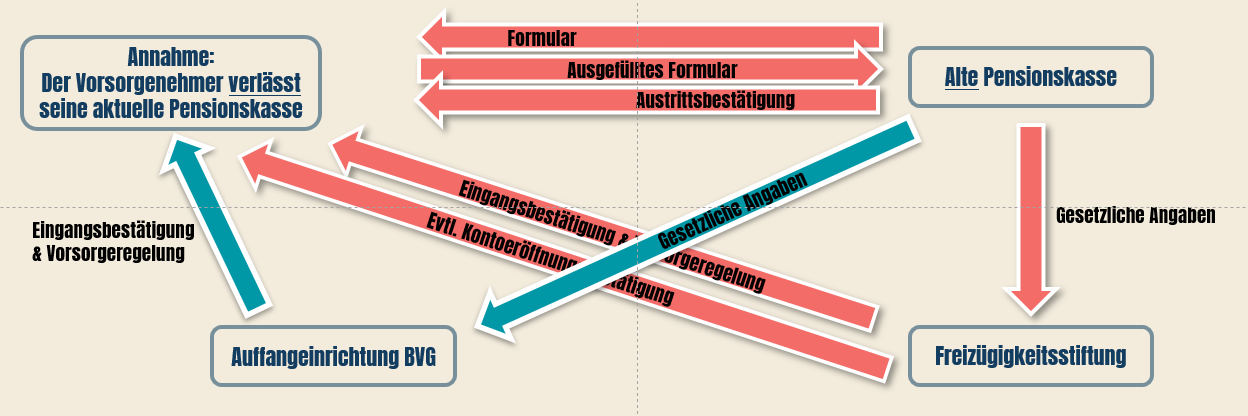
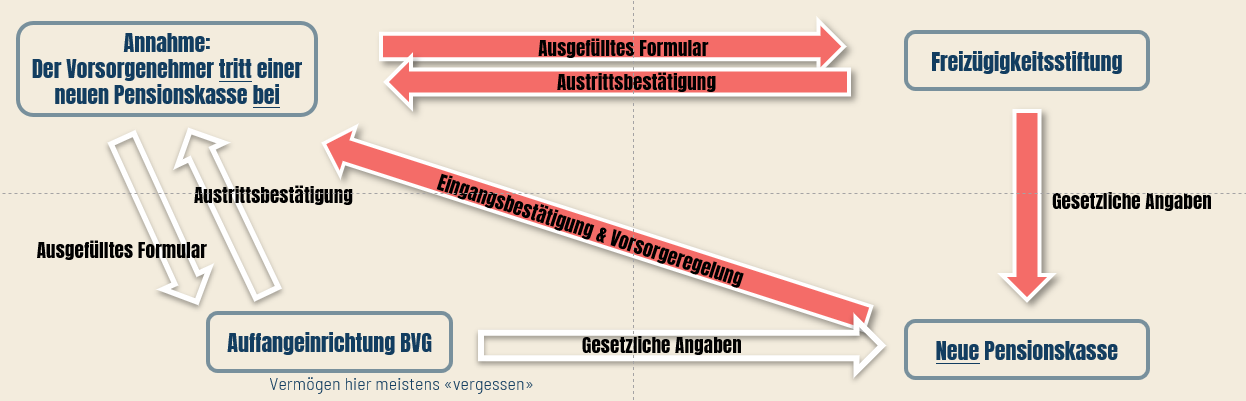


Abbildung 1: Illustration der zeitlichen Abfolge. Quelle: Eigene Darstellung

Als Interessengruppen lassen sich folgende Akteure definieren. Erstens die Pensionskassen der betroffenen Betriebe. Zweitens die Kunden respektive die Vorsorgenehmer und drittens betrachten wir die Freizügigkeitsstiftungen, welche das Geld der Kunden während einer Auszeit zwischenlagern. Viertens kann auch die «Auffangeinrichtung BVG» einbezogen werden.

Im Falle eines Unterbruchs im Berufsleben kontaktiert die Pensionskasse des ursprünglichen Betriebes den ehemaligen Kunden per Post, da diese nun nicht mehr für dieses Geld verantwortlich ist. Daraufhin kommuniziert der Kunde seiner ehemaligen Pensionskasse die Zahlungsverbindung der Freizügigkeitsstiftung, auf der sein Pensionskassenvermögen in der Transitionsphase „parkiert“ werden soll. Die von ihm gewählte Freizügigkeitsstiftung erhält sein Pensionskassenvermögen und verbucht es inklusive Vermerk einer Vielzahl von gesetzlich Mitteilungspflichten wie beispielsweise Name, Vorname, Geburtsdatum, Sozialversicherungsnummer etc. Bei Antritt einer neuen Arbeitsstelle muss die Freizügigkeitsstiftung wiederum das Pensionskassenvermögen an die Pensionskasse des neuen Arbeitgebers übergeben und der ganze Prozess der brieflichen Kommunikation beginnt von Neuem. Im Folgenden wird der gesamte Briefablauf detailliert dargestellt (siehe Abbildung 2). Es resultieren heutzutage im normalen Fall, d.h. wenn man alle roten Pfeile addiert, 10 Briefe.

Abbildung 2: Der postalische Ablauf. Quelle: Eigene Darstellung



Die Relevanz unseres Cases ist signifikant und wird verstärkt durch die allgegenwärtige Erhöhung des Umweltschutzes und der Nachhaltigkeit. Total existieren 2‘000 Pensionskassen in der Schweiz mit etwa einer Billion CHF verwaltetem Vermögen. Zudem sind die Pensionskassen gesetzlich dazu verpflichtet, das Guthaben eines austretenden Mitarbeiters an die nächste Pensionskasse zu überweisen. Trotzdem ist jeder Versicherte rechtlich gesehen selber verantwortlich für die verschiedenen Transfers. Falls keine Angabe erfolgt, landet das Geld nach spätestens 2 Jahren bei der Stiftung „Auffangeinrichtung BVG“. Hier existieren schlechthin etwa 800‘000 „vergessene“ Konten mit total 3 Milliarden Franken, die darauf warten, in die Hände ihres rechtmässigen Besitzer zu gelangen. Mithilfe einer adäquaten Lösung des Cases könnte man nicht nur die schriftliche Korrespondenz auf ein Minimum reduzieren, sondern auch dieses letztgenannte Problem in den Griff bekommen.

Unser Lösungskonzept baut auf verschiedenen Komponenten auf, aber grundsätzlich ist es unser Ziel, die komplette Struktur der Zahlungs- und Kommunikationsvorgänge der Pensionskassen zu modernisieren und auch kosteneffizienter zu gestalten. Mit einem Smart Contract als zentrales Element wollen wir die Kommunikation zwischen Pensionskassen, Freizügigkeitsstiftungen und Kunden komplett digital gestalten. Damit die ganzen verschiedenen Postsendungen effektiv ersetzt werden können, muss ein einfach bedienbares, zuverlässiges und selbstverständlich elektronisches Kommunikationssystem entwickelt werden, während es einen deutlichen Mehrwert zum alten System liefert.

Der Smart Contract soll dann die verschiedenen Phasen des Ablaufes regeln und hat mehrere Schnittstellen: ausgelöst wird er zum Beispiel dadurch, dass eine Person beim aktuellen Arbeitgeber kündigt und deshalb die aktuelle Pensionskasse wechseln will. Der Kunde wird darüber informiert, wie groß die Geldsumme ist und dass diese bewegt werden muss. Die Optionen werden auch dargelegt und der Kunde kann selbständig wählen, wo die Gelder hingehen sollen. Die Information des Kunden ist über ein Webinterface geplant, allerdings muss der Kunde irgendwie an seine Zugangsdaten kommen und zusätzlich muss ein Sicherheitsmechanismus entwickelt werden, der die Identität bestätigen kann und alle Datenschutz-Rahmenbedingungen einhält. An dieser Stelle, wie generell bei der ersten Nutzung des Systems, ist die Wahrscheinlichkeit am Größten, dass noch ein Teil der Kommunikation per Post passieren muss, falls kein anderer zuverlässiger Weg vorhanden ist, die Zugangsdaten zu übermitteln. Das Auslösen des Smart Contracts kann von Pensionskassen-Seite geschehen über ein Interface, welches auch zur Informationsgewinnung benutzt werden soll. Generell brauchen alle Parteien Schnittstellen für die Kommunikation der Prozesse, aber auch um Zugriff auf ältere Daten haben zu können. Denn die 10 Jahre gesetzlich festgelegte Aufbewahrungsbestimmung soll auch durch einen Mehrwert für alle Parteien eingebaut werden, indem auch die Information dezentral auf eine Blockchain geschrieben werden soll und so alle Parteien Zugriff auf die für sie relevanten Daten haben.

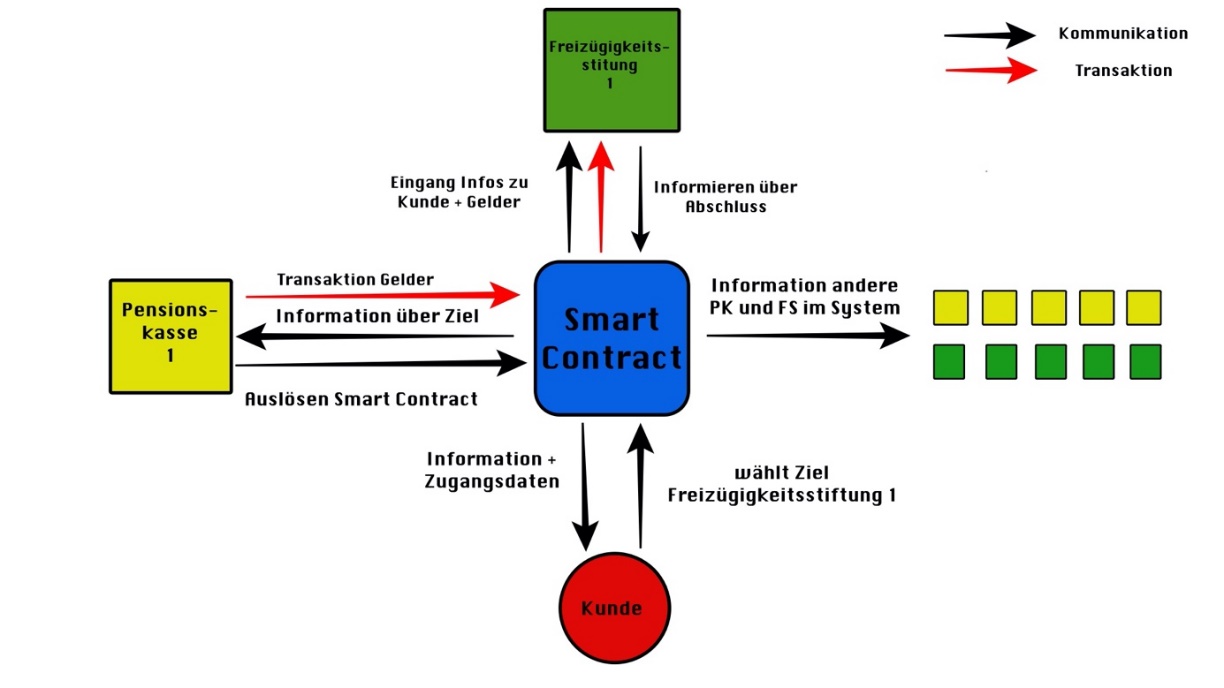
Damit das Konzept auf Zustimmung und Interesse stösst, muss auf jeden Fall ein finanzieller Vorteil gegenüber dem alten System vorhanden sein. Falls von uns kein signifikanter Mehrwert gegenüber dem alten System erarbeitet wird, hält sich die Zahlungsbereitschaft in Grenzen. Falls diese Schwelle jedoch überschritten wird und das System sich bewährt als Neuerung, dann ist die Zahlungsbereitschaft sehr groß, da das System mehrere Milliarden Schweizer Franken verwaltet und so die Bereitschaft, ein effektives System aufzustellen, sicherlich auch vorhanden ist. Deshalb ist es auch wichtig, herauszufinden, in welchem Rahmen unser Projekt rentabler ist als das aktuell bestehende System. Durch die dezentrale, digitale Dokumentation werden bei den Pensionskassen sicherlich über die Jahre Lagerkosten für die Dokumente eingespart, aber gleichzeitig werden auch Kosten anfallen für die Anschaffung und den Betrieb für Server-Einheiten. Weiterhin ist es allerdings so, dass durch die direktere und gezieltere Kommunikation die Arbeitsprozesse angekurbelt werden und so ein Mehrwert entsteht durch verkleinerten Arbeitsaufwand und somit Arbeitskräfte frei werden, die in anderen Aufgabenbereichen benutzt werden können. Kosten für Postversand und -papier können großflächig eingespart, allerdings entstehen natürlich durch den Betrieb des Blockchain-Systems neben administrativen Kosten auch Stromkosten.

Abbildung 3: Illustration der Verbindungen zwischen den Akteuren. Quelle: Eigene Darstellung

Also kann man sagen, wenn die entsprechenden neuen Kosten durch Verlagerungen und die neuen Mehrwerte gedeckt werden oder bestenfalls sogar übertroffen werden, dann sind alle Stakeholder Profiteure des Systems. Der Kunde ist besser informiert über seine Optionen, die Pensionskassen und Freizügigkeitsstiftungen haben ihre Informationen effektiver gespeichert und haben damit auch eine bessere Kommunikation mit gekoppelten Transaktionen verbunden. Wenig Datenverlust und User-Bindung sollen für weniger vergessene Konten sorgen und gleichzeitig den Kassen und Stiftungen einen zusätzlichen Mehrwert bilden.

Allerdings ist diese Fantasie-Vorstellung nach einem profitablen System für alle Parteien noch sehr weit entfernt davon, dass man sie umsetzen kann. Es gibt nämlich noch einige Hürden, die man bis dorthin überwinden muss. Wie angesprochen muss in allen Prozessen die Datenschutzkomponente sowie die Identitätssicherung eingehalten werden, damit alles mit rechten Dingen zugeht und niemand den Datenverkehr von außen einsehen oder sogar beeinflussen kann. Lösungsansätze wären hier die verschlüsselte Speicherung auf der Blockchain durch kryptografische Hashfunktionen, so wären die Informationen zwar öffentlich verfügbar, aber nur für die Personen mit den entsprechenden Entschlüsselungsmöglichkeiten lesbar. Auch ein verifizierbarer Weg muss gefunden werden, um dem Kunden einen Zugriff möglich zu machen, während die ganze Prozedur trotzdem relativ einfach und vor allem verständlich ist. Erste Überlegungen haben ergeben, dass hier möglicherweise der Briefverkehr noch ein Teil des Ganzen sein könnte zur Übermittlung der Zugangsdaten. Eine weitere Hürde ist die Umsetzung des Transaktionsverkehrs, dabei müssen die Transaktionskosten so klein wie möglich gehalten werden und es muss natürlich, auch für eine ordnungsgemäße Zahlung, der Preis stabil gehalten werden, damit man weiterhin sicher gehen kann, dass keinerlei Geldmittel verloren gehen.

Die Marktsituation der Freizügigkeitsstiftungen ist wie folgt definiert. Die Anzahl der Freizügigkeitskassen beträgt 54 Stück. Die grossen Finanzinstitute sowie Kantonalbanken betreuen eigene Freizügigkeitskassen. Die jährliche Spannweite der Zinsrendite beträgt 0.100% - 0.050%. Im Rahmen der weniger restriktiven Investitionspolitik auf Seite der Kassen kann der Kunde das Risiko minimieren, indem er die höhere Streuung der Pensionskassengelder in Anspruch nimmt. Somit können die Pensionsgelder in aggressivere Investitionen investiert werden. Die Investitionsinstrumente sind im Rahmen der Renditestrategie wählbar zwischen Obligationen, Aktien und alternativen Investment. Im Normallfall werden alle Pensionskassengelder in eine Kasse einbezahlt, jedoch ist es gesetzlich erlaubt, seine Pensionskassenguthaben auf zwei verschiedene Kassen aufzuteilen, um das Risiko eines Komplettausfall im Falle einer Liquidierung der Aktiven zu minimieren.

Bei Überweisungen des Altersguthaben von Pensionskasse zu Pensionskasse oder von Pensionskasse zu Freizügigkeitsstiftung bzw. Freizügigkeitsstiftung zur Pensionskasse gibt es gewisse gesetzliche Mitteilungspflichten. Diese sind:

- Angabe zur Person (Name, Vorname, Geburtsdatum, AHV-Nummer) Adresse und Wohnort, Zivilstand (Kann auf der Erstregistration mit QR Code auf der Plattform eingetragen werden, dazu noch einen Persönlichen Login Code zugeschickt, womöglich via TAN)

- Summe Altersguthaben und deren Aufteilung in obligatorischen Teil und überobligatorischen Teil (Bei Aufteilung der PK Gelder auf zwei verschiedene Freizügigkeitskassen wird die Rendite verglichen und das Restguthaben angezeigt und zusammengerechnet.)

- Erste gemeldete Freizügigkeitsleistung (=Altersguthaben) per 1.1.1995 (dann wurde das Freizügigkeitsgesetz in Kraft gesetzt)

- Gemeldete Freizügigkeitsleistung bei Heirat (sofern zutreffend, kein Zugriff auf Daten des Ehepartners) - Gemeldete Freizügigkeitsleistung im Alter 50 (sofern zutreffend)

- Vorbezug für Wohneigentum (sofern zutreffend) wann und welche Höhe

- Ist das Altersguthaben verpfändet (für Wohneigentum) Ja/Nein

- Wurden in den letzten drei Jahren Einkäufe getätigt Ja/Nein, wenn Ja, wann und in welcher Höhe?

- Im Falle einer Scheidung und Überweisung eines Teils des Altersguthabens an eine andere Stiftung würde bei einem Transfer des verbleibenden Teils des Altersguthabens diese Scheidungsüberweisung ebenfalls angegeben werden (denn der Vorsorgenehmer kann auch diese Lücke wieder durch Einkäufe auffüllen).

**Bisheriger Lösungsansatz:**

Momentan gibt es wenige Freizügigkeitskassen, welche im Rahmen einer Kooperation eine zentrale Datenverarbeitungsstelle aufbauen. Die Aufgabe besteht darin, den Verwaltungsaufwand zu reduzieren und die Kosten dafür zu teilen. Eine Blockchain Lösung für das Problem besteht momentan nicht. Die meisten Kassen unterhalten den Kundenkontakt mithilfe von Briefverkehr und Angestellten für die Koordination der Transaktionen. Die Schwäche der momentanen Verarbeitung ist, dass sie sehr kostenintensiv und personalintensiv ist, was sich auf die Renditen der Konsumenten ausweitet. Das verwaltete Vermögen beträgt rund 10% der verwalteten Vermögen der Pensionskassen.

# Blockchain und Ökosystem

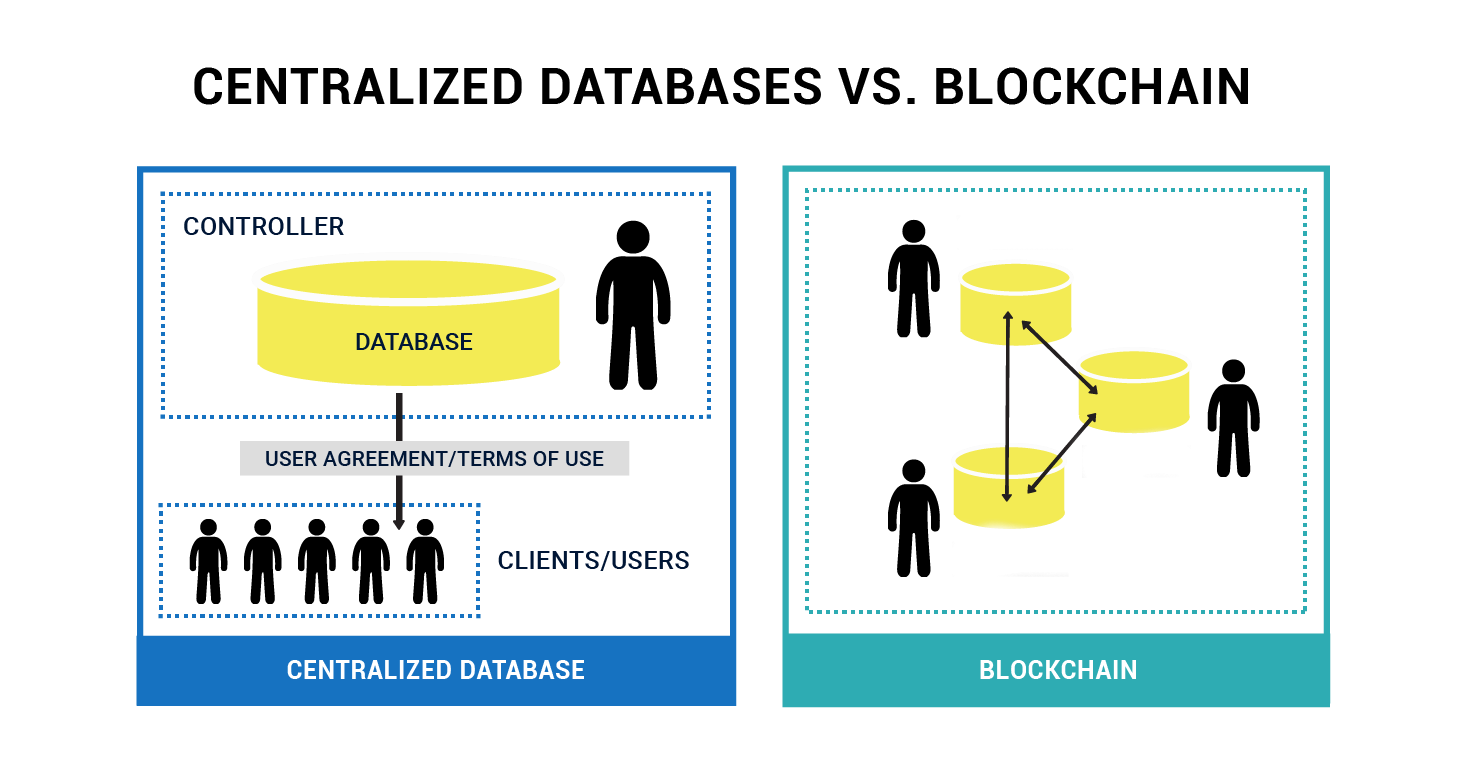


Abbildung 4: Ein Vergleich der Blockchain-Technologie mit einer zentralisierten Datenbank. Quelle: CoinRevolution

Da die Blockchain so eingerichtet werden kann, dass nur bestimmte Personen Zugriff auf die Daten haben und man trotzdem das weltweit verteilte Netz verwenden kann um die Daten zu lagern, ist es perfekt dazu geeignet, sensible Daten von Vorsorgenehmern zu speichern. Somit können Informationen über Kontostände, Kontaktdaten, gesetzliche Pflichtangaben, Präferenzen über allfällige Freizügigkeitsstiftungen und vieles weiteres in der Blockchain gespeichert werden und nur dann für jemanden sichtbar sein, wenn dieser auch über jene Informationen verfügen darf. Zudem besteht die Möglichkeit, Änderungen schnell und unkompliziert online zu tätigen ohne dass man wieder auf den Briefverkehr zurückgreifen muss. Die Blockchain kommt somit in unserem Case bei der Datenerfassung und der Kommunikation bezüglich Änderungen zwischen den verschiedenen Parteien ins Spiel.

Um den Unterschied zwischen einer normalen Datenbank und einer Blockchain aufzuzeigen, kann Abbildung 4 zur Hilfe ziehen. Eine normale Datenbank verwendet eine Client-Server Netzwerkarchitektur. Am besten lässt sie sich definieren als Sammlung von organisierten Daten auf zentraler Ebene. Der Client kann Daten in der Datenbank leicht abändern und mit neuen Einträgen aktualisieren. Die Verwaltung der Datenbank erfolgt zentral durch einen Administrator (z.B. eine Institution). Dieser authentifiziert den Eingriff eines Benutzers bevor der Eingriff auf die Datenbank gewährt wird. Falls die Verwaltung nicht lückenlos funktioniert, kann dies u.a. dazu führen, dass Daten gelöscht oder geändert werden.

Die Blockchain-Technologie ermöglicht hingegen eine dezentrale Speicherung aller Daten. Die Blockchain selber ist nur ein Register aller akzeptierten, validierten, signierten und verarbeiteten Transaktionen. Dieses Register ist dezentral auf verschiedenen Knoten, also bei den Teilnehmern dieser spezifischen Blockchain, abgelegt. Zur Sicherstellung einer korrekten Dokumentation dient der Konsens. Der Konsens kann durch Blockchain-Konsensus-Algorithmen erreicht werden. Einige Beispiele sind der Proof-of-Work (PoW) und der Proof-of-Stake (PoS). Mehr dazu später. Die Blockchain hat den grossen Vorteil, dass sie für eine hohe Integrität der Daten sorgt, da letztere unverändert und unverfälscht sind. Zudem ist die Blockchain von hoher Transparenz geprägt. Jede Transaktion kann nachverfolgt werden und überprüft werden. Somit verfügt jeder Nutzer/Knoten über die aktuelle Version der Blockchain und neue Daten, respektive Änderungen bestehender Daten können nur mit der Zustimmung der anderen betroffenen Parteien erfolgen.

Mit der Implementierung der Blockchain könnten folgende Probleme in unserem Case gelöst werden. Primär geht es darum, den Briefversand stark zu reduzieren oder sogar komplett einzustellen. Dies kann geschehen, indem der Zugriff auf die jeweiligen Daten eines Vorsorgenehmers mithilfe eines Webinterface erfolgt. Wie bereits im vorigen Kapitel beschrieben, kann die Initialzündung eines Smart Contracts daraus bestehen, dass die ehemalige Pensionskasse den austretenden Mitarbeiter kontaktiert und der Vorsorgenehmer somit die Möglichkeit erhält, im Webinterface seine Präferenzen bezüglich einer allfälligen Freizügigkeitsstiftung zu definieren. Zudem könnte er weitere, praktischere Kommunikationsschnittstelle hinzufügen wie zum Beispiel E-Mail-Adresse oder Telefonnummer. Dies dient auch unter anderem als Verifizierungsmöglichkeit bei darauffolgenden Anmeldeversuchen des Vorsorgenehmers. Des Weiteren können jegliche Informationen eines Vorsorgenehmers für jede betroffene Partei zur Verfügung gestellt werden über das auf der Blockchain-Technologie basierte Webinterface. Somit integriert das System nun alle betroffenen Parteien ohne Divergenzen in ein einziges Ökosystem. Diesbezüglich könnten Zahlungsaufträge nun einfacherer veranlasst werden als mit der aktuellen Lösung.

# Konsensprotokolle

Die Blockchain soll so eingerichtet werden, dass sie mit einem minimalen administrativen Aufwand aufgebaut und gepflegt werden kann. Bei dieser Fragestellung muss analysiert werden, welche Blockchain oder Datenbank am besten für dieses System geeignet ist. Wichtige Kriterien zur Auswahl der richtigen Blockchain sind die Sicherheitsaspekte der Datensensibilität welche auf der Blockchain gespeichert werden. Insbesondere Informationen über Kontostände, Kontaktdaten, gesetzliche Pflichtangaben dürfen nur für die berechtigten Parteien eingesehen werden.

Die Frage stellt sich, welche Art von Protokoll für diese Aufgabenstellung am besten geeignet ist. Eine erste Auswahl ist, ob eine öffentliche oder private Blockchain aufgebaut werden soll. Public sowie Private Blockchains sind verteilte Peer-to-Peer-Netzwerke, bei welchen jeder Teilnehmer eine Kopie des gemeinsamen Registers führt. Ob eine Public oder eine Private Blockchain besser geeignet ist, lässt sich anhand der folgenden Fragen ermitteln:

**1. Wer darf am Netzwerk teilnehmen?**

Am Netzwerk nimmt nur Teil, wer eine Überweisung an eine Freizügigkeitsstiftung als Einlagentransfer von einer Pensionskasse vornimmt. Somit ist das konsensberechtigten Ledger bei den drei verschiedenen Parteien gespeichert. Eine private Blockchain wird von einem Netzwerkadministratoren geführt, in diesem Falle der VVS, und steht nur einer bestimmten Gruppe von zugelassenen Teilnehmern zur Verfügung. Der Netzwerkadministrator hat also eine wichtige Funktion inne: er gewährt oder verweigert Teilnehmern den Zutritt zum Netzwerk. Somit sind dem Netzwerkadministrator die Teilnehmer an einer privaten Blockchain bekannt. Sodann sind die Informationen zu einer Transaktion auch nicht öffentlich einsehbar, sondern nur die involvierten Transaktionsteilnehmer können die Informationen einsehen. Ferner kann der Netzwerkadministrator bestimmte Privilegien an Teilnehmer erteilen oder verweigern, wie z.B. Schreib- oder Leserechte.

**2. Wer darf Blockchain-Einträge gemäss dem Konsensus-Mechanismus validieren?**

Die Teilnehmer selbst können eine Validierung durchführen für diese bestimmte Stelle im Smart-Contract wo sie eine Schreibberechtigung besitzen um die Vollständigkeit ihres Abschnittes zu bestätigen. Deshalb gilt, dass von einer gewissen Gruppe gemäss den individuell festgelegten Validierungsregeln die Rechte vorgenommen werden.

**3. Wo befindet sich das dezentrale Register?**

Die dezentrale Registerführung obliegt den Teilnehmern des Smart-Contracts also allen Personen, welche auch eine Validierungsbefugnis haben.

Aus dieser Fragestellung ist die Beurteilung möglich, dass eine private Blockchain die kosten- und sicherheitseffizienteste Lösung. Die Auswahl der Blockchain-Plattform für diese Problemstellung basiert auf einer privaten Blockchain. Beispiele für Plattformen auf welcher private Blockchains erstellt werden können sind Hyperledger, sowie bekannte Kryptowährungen wie Ripple und Ethereum.

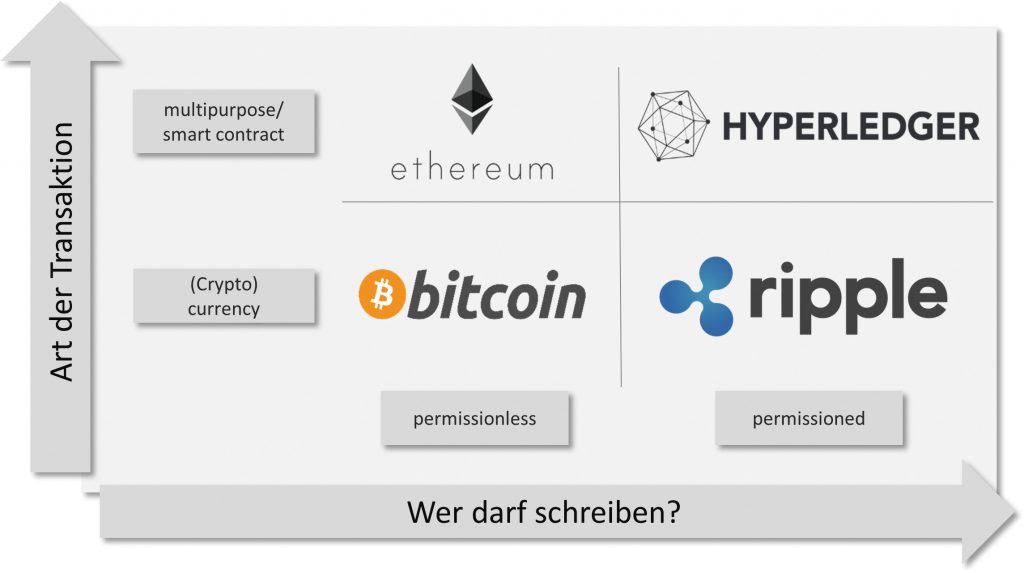


Abbildung 5: Übersicht über die verschiedenen Technologien. Quelle: IT-Produktion

# Datenmodell und Architektur

Wir haben beschlossen, das Konzept „Proof of delegated Stake“ zu benutzen. Also wird immer über eine anteilmässige Wahl innerhalb des Systems bestimmt, wer den nächsten Block bauen darf. So werden die Transaktionen festgehalten und die Aufbewahrungspflicht für alle Parteien rechtens eingehalten. Der Stake für die Wahl wird für Knoten daraus bestimmt, ob und an wie vielen der letzten Transaktionen ein Knoten beteiligt war.

Die gespeicherten Daten wären dann: Die Sozialversicherungsnummer des Kunden, der Ursprung und das Ziel der Transaktionen sowie ein Zeitstempel. Die Zuordnung zu den Personen passiert folglich über die Benutzerkonten auf der Weboberfläche. Zugang zu den Daten haben alle, die einen Knoten im System bilden. Dies sind unter anderem die Pensionskassen und Freizügigkeitsstiftungen. Somit erfüllen alle gemeinsam ihre Aufbewahrungspflichten. Jede Transaktion soll einen einzigartigen Zeitstempel haben, welcher als Referenz in den Blöcken auftritt. Bei unserem Datenmodell ist es so, dass es kaum ungültige Transaktionen gibt. Trotzdem, falls eine Zahlung rückgängig gemacht werden muss, dann referenziert man innerhalb eines Blocks denselben Input bestehend aus dem Ursprung.

Der Smart Contract hat grundsätzlich drei verschiedene Funktionen: Einerseits spielt der Smart Contract eine Rolle in der Abwicklung eines Wechsels von einer Pensionskasse zu einer Anderen oder einer Freizügigkeitsstiftung. Der Contract stellt über eine Weboberfläche die Anfrage beim Kunden, wohin sein Vermögen bei der Pensionskasse transferiert werden soll. Der Contract gibt diese Informationen weiter und leitet somit die Transaktion ein. Andererseits können beim Contract auch Informationen angefragt werden, welche der Contract dann von der Blockchain holt. Diese Funktion ist hauptsächlich für Kunden wichtig, weil diese nur so Informationen über vergangene Transaktionen erlangen können. Die Institutionen haben dadurch, dass sie Teil der Wir-Blockchain Struktur sind, welche wir benutzen in diesem Case. Die dritte Funktion ist ein wichtiger Teil der anderen zwei Funktionen. Der Smart Contract ist auch zuständig für die Koordination der Identitätsüberprüfung: Er sammelt die notwendigen Informationen bei der Anmeldung und leitet diese weiter via Schnittstelle zu einer Online-Identifikationsprüfung wie sie von Swisscom angeboten wird. Das Ergebnis wird dann vom Smart Contract wieder ausgewertet und die entsprechenden Aktionen werden durchgeführt oder abgeblockt. Die Funktion der Identitätsüberprüfung wird bei den beiden anderen Funktionen mitgenutzt.

# Ökosystem

In Abbildung 6 sieht man das hieraus resultierende Ökosystem. Der Vorsorgenehmer nimmt eine dominante Position gegenüber den Freizügigkeitsstiftungen ein bezüglich der Auswahl einer individuellen Anlagestrategie. Aufgrund der Abwesenheit des Postversands kann er nun ziemlich einfach auf dem Web-Interface auswählen, bei welcher Pensionskasse sein PK-Vermögen aufbewahrt werden soll. Die Freizügigkeitsstiftungen haben ab Einführung des vereinfachten Zugangs der Vorsorgenehmer mehr Möglichkeit mit attraktiven Konditionen neue Kunden zu generieren. Hiermit besteht auch die Möglichkeit den Umsatz zu steigern, da jeder Kunde eine Verwaltungsgebühr zahlt. Diesbezüglich wird wahrscheinlich die Konkurrenzsituation unter den Freizügigkeitsstiftungen verstärkt. Rein marktwirtschaftlich betrachtet sorgt steigende Konkurrenz für effizientere Abläufe und besser positionierte Unternehmen. Des Weiteren und betreffend des Cases sehr wichtig sind die möglichen Kosteneinsparungen der Pensionskassen durch eine Reduktion des administrativen Aufwands. Die Blockchain und auch der Smart Contract erlauben nun effizientere Prozesse, die deutlich weniger Zeit und Ressourcen benötigen. Zudem ist zu erwähnen, dass ein Vorsorgenehmer ab seiner Erstregistration für immer im System aufzufinden ist und somit bei Antritt einer neuen Arbeitsstelle keinen grösseren Aufwand für die Pensionskasse mehr verursacht. Ferner können in einem weiteren Schritt die Zahlungsaufträge zwischen den Pensionskassen und den Freizügigkeitsstiftungen vereinfacht werden durch eine Automatisierung des Zahlungsprozesses.

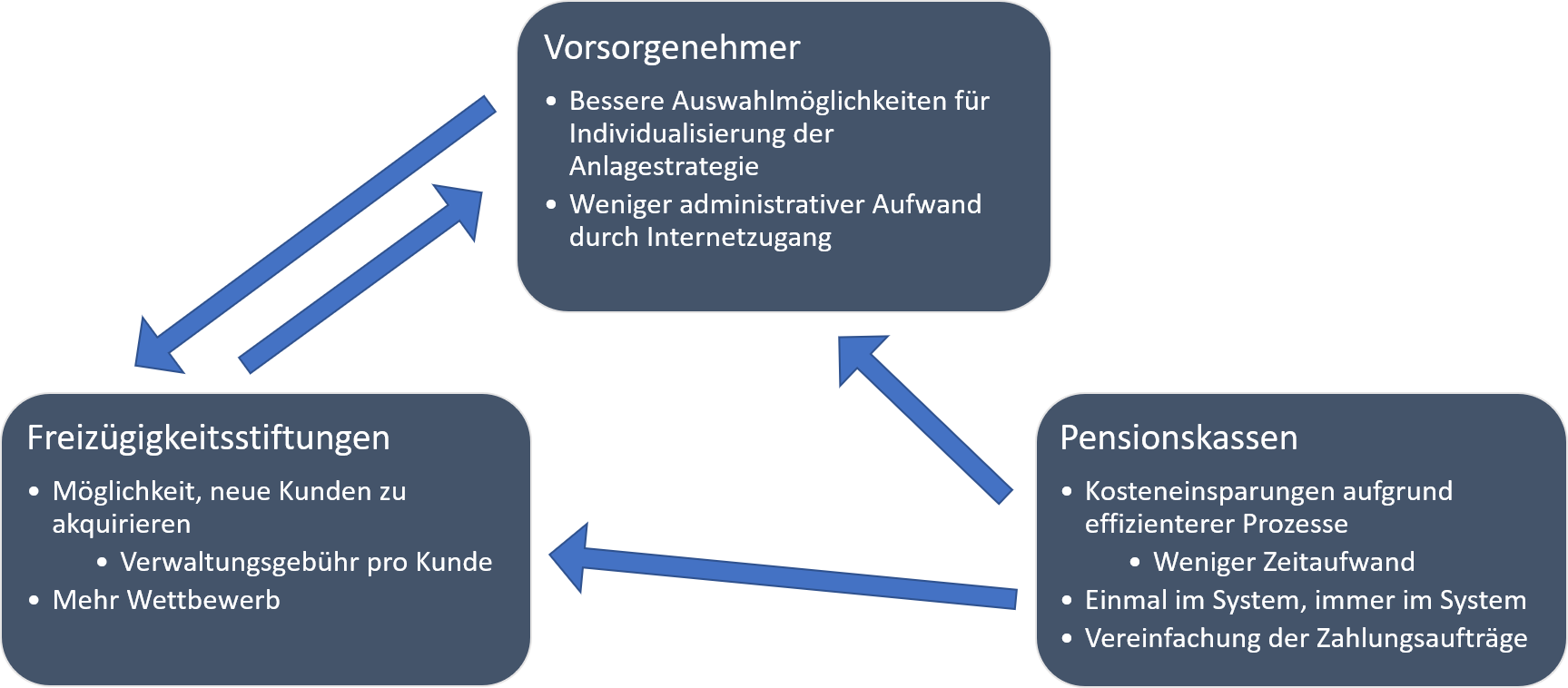


Abbildung 6: Das resultierende Ökosystem mit den Vorteilen der jeweiligen Parteien. Quelle: Eigene Darstellung

# Technische und Graphische Ausarbeitung

In dem folgenden Teil der Blockchain Challenge geht es um die Verfeinerung gewisser Aspekte der bisherigen Überlegungen. Im Fokus steht eine Verbesserung der Systemarchitektur und eine Ausarbeitung der resultierenden Möglichkeiten nach einer Implementierung unseres Projektes. Des Weiteren befassen wir uns nun mit der Erstellung einer Mock-up Applikation und der Programmierung des betreffenden Smart Contracts.

In folgender Grafik (siehe Abbildung 7) sollen die verschiedenen Beziehungen zwischen den betroffenen Akteuren detailliert aufgezeigt werden und präzis beschrieben werden. Aufgrund der letzten Analysen und Besprechungen wird die von uns genutzte Lösung auf einer privaten Ethereum-Instanz basieren. Die Netzwerkknoten respektive die Teilnehmer bestehen nun aus den Pensionskassen und den Freizügigkeitsstiftungen. Der Vorsorgenehmer verfügt über keinen eigenen Netzwerkknoten in der Block Chain. Als Betreiber der Blockchain schlagen wir den Verein Vorsorge Schweiz (VVS) vor. Ob dies rechtlich gesehen möglich ist, oder ob ein neuer Verein gegründet werden muss, ist noch nicht geklärt.

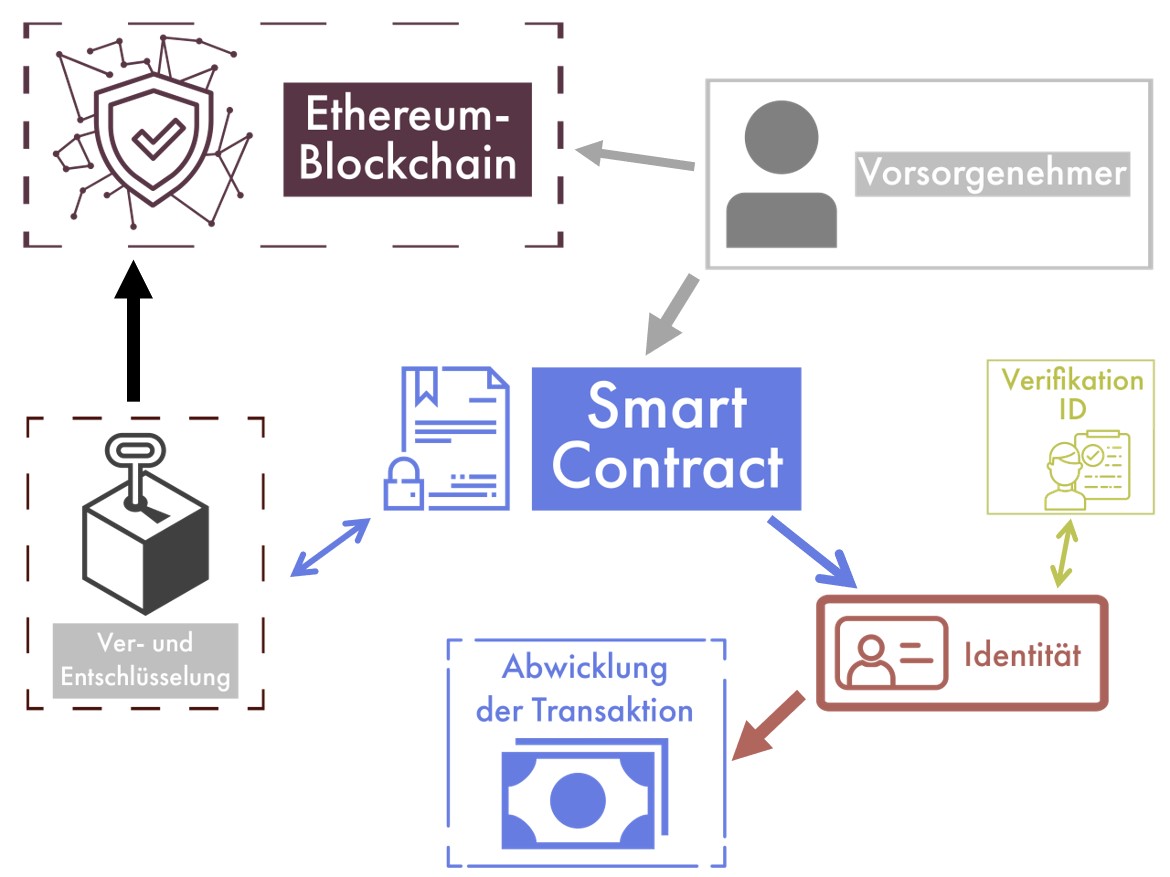


Abbildung 7: Eine Übersicht der Beziehungen zwischen den Akteuren. Quelle: Eigene Darstellung

Die entstehenden Kosten sollen durch Mitgliederbeiträge gedeckt werden und es herrscht aufgrund der Blockchain-Topologie eine gegenseitige Aufsicht vor. In diesem Case wird eine private Ethereum Instanz als Blockchain Technologie verwendet. Ferner können die verschiedenen Netzwerkknoten nur die für sie relevanten Informationen sehen. Diesbezüglich können die Kunden/Vorsorgenehmer über das Web Interface auch nur die Daten betrachten, die sie selbst betreffen. Da auch die Frage bezüglich Umweltfreundlichkeit im Raum steht, wird als Konsensprotokoll das „Proof of delegated Stake“ benutzt. Verglichen zum „Proof of work“-Protokoll wird hierbei deutlich weniger Strom benutzt.

Der Vorsorgenehmer kann im ganzen System nur eine einzige „Variable“ verändern, nämlich das Ziel der Transaktion respektive die zu empfangende Freizügigkeitsstiftung. Wie bereits erwähnt, kann er sonst nur seine Daten im System abrufen. Sinngemäss ist eine Abwicklung der Smart Contracts nur möglich, wenn man über eine genaue Identifikation des Vorsorgenehmers verfügen kann. Somit ist dieser Case nur relevant, wenn eine neue Art der Identifikation eingesetzt werden kann. Sozusagen spielt eine Online-Identifikation hier eine essentielle Rolle. Korrespondierend existieren schon mehrere Firmen, die eine Online-Identifikation zulassen. Da unser Auftrag zukunftsorientiert ist, folgen die nächsten Prozesse unter der Annahme, dass eine verlässliche Identifikation des Vorsorgenehmer stets möglich ist. Da die Implementierung einer solchen Verifikationsmöglichkeit den aktuellen Rahmen des Auftrags deutlich vergrössern würde, wird hierbei einfach ein binärer Dummy-Wert benutzt. Dieser nimmt somit entweder den Wert „Verifiziert“ (=1) oder den Wert „Nicht verifiziert“ (=0) ein. Um allfällige Missverständnisse bezüglich des Smart Contracts aus dem Weg zu räumen, figuriert der Smart Contract nur noch als Framework für alle Zahlungen und nicht mehr für jeden Kunden einzeln. Bei jedem Zahlungsauftrag wird der Smart Contract mit der jeweiligen State-Variable gespeist, um die anderen Teile des Ablaufs in Gang zu bringen. Ferner ist der Smart Contract nach seinem Deployment auf der Blockchain nicht mehr im Ganzen veränderbar.

# Die Struktur des Smart Contracts

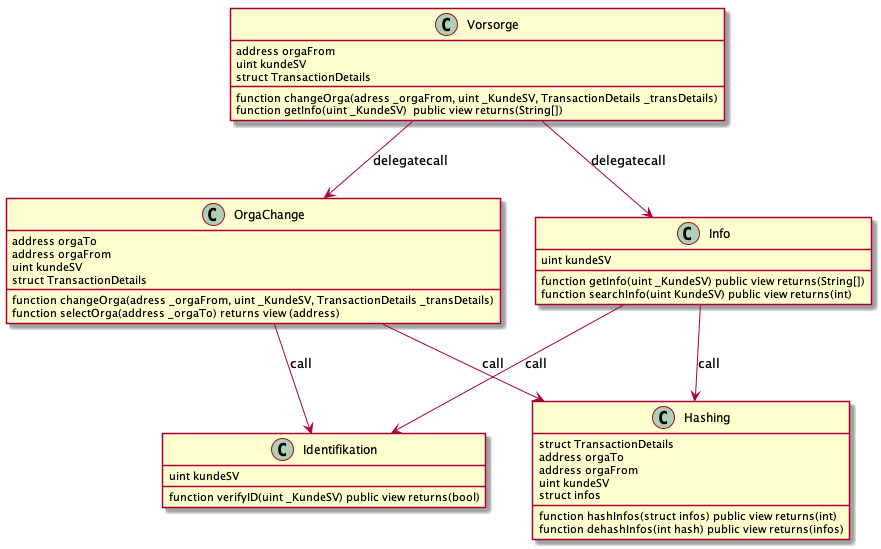


Abbildung 8: UML-Klassendiagramm der Smart Contract Struktur. Quelle: Eigene Darstellung erstellt mit plantUML

Das oben dargestellte UML-Klassendiagramm zeigt unsere Struktur für die Umsetzung unseres Konzepts mit Smart-Contracts dar. Dabei gibt es einen zentralen Smart Contract «Vorsorge», welcher zur Liveschaltung des kompletten Systems «deployed» wird und dann immer wieder angesprochen werden kann. Die zwei zentralen Aufgaben des Smart Contracts, das Wechseln der aktuellen Organisation eines Vorsorgenehmers und die Einsicht von Informationen können dort ausgelöst werden.

Die Funktionen an sich werden aber nicht im Contract Vorsorge implementiert, sondern werden via delegatecall von anderen Contracts ausgeführt. Dies dient zur besseren Wartbarkeit des Contracts und sorgt dafür, dass bei einer Veränderung der komplette Contract mit allen Funktionen neu deployed werden muss, sondern durch die Modularität können einzelne Bausteine, falls es notwendig ist, ausgetauscht werden.

Der Contract OrgaChange regelt den kompletten Ablauf des von der Ausgangs-Organisation ausgelösten Organisationswechsel. Dabei wird dann innerhalb der Funktion changeOrga auch eine weitere Methode ausgelöst namens selectOrga, welche via eine Schnittstelle zu einem Webinterface dem Vorsorgenehmer die Möglichkeit gibt, seine Zielorganisation auszuwählen. In der Methode selectOrga wird auch die Identitätsüberprüfung durchgeführt durch eine externe Identitäts-Verifizierung. Falls diese fehlschlägt, wird der komplette Prozess abgebrochen.

Sobald die Organisation ausgewählt und die Identitätsüberprüfung abgeschlossen ist, wird der Wechsel der Organisation weitergeführt. Die hashInfos Funktion der Hashing Klasse wird ausgelöst und die Informationen des Wechsels also die Teilnehmer sowie die Transaktionsinfos werden als kryptographischer Hash verschlüsselt. Danach werden die gehashten Infos und die Sozialversicherungsnummer, sowie ein Zeitstempel zur Referenzierung an die Ethereum-Instanz geschickt und sind bereit zur Blockbildung. Nun wird der Zeitstempel zur Referenzierung an die alte Organisation, die neue Organisation und an den Vorsorgenehmer geschickt. Damit es für alle Parteien ordentlich referenziert werden kann. Die Ausgangsorganisation bekommt auch noch die Information, wohin die Transaktion gehen soll und die neue Organisation wird informiert über einen einkommenden Vorsorgenehmer.

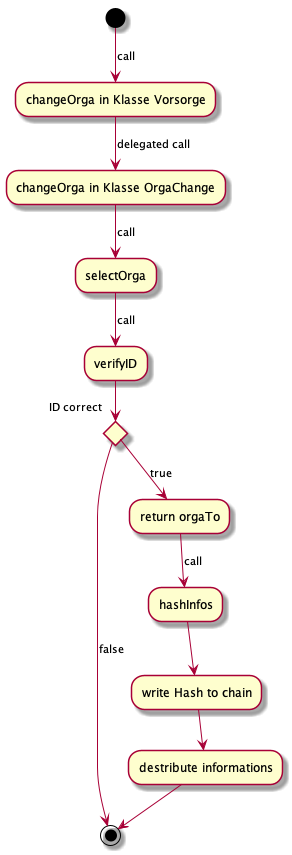
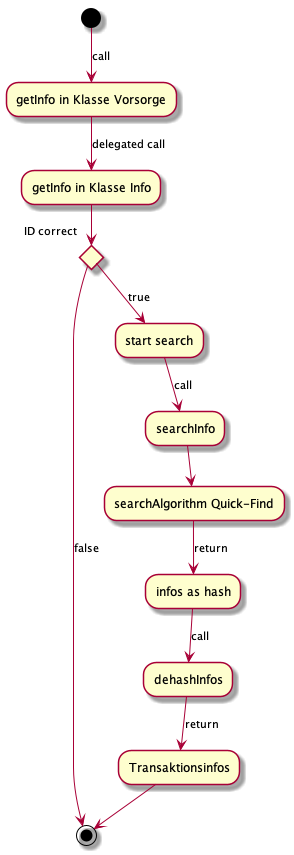


Abbildung 9: Aktivitätsdiagramme zum Ablauf der Funktionen Organisationswechsel und Informationsgewinnung. Quelle: Eigene Darstellung

Contract Info regelt den Erhalt von Infos, welcher über die Funktion getInfo im Vorsorge Contract angestoßen wird. Diese Funktion kann von Vorsorgenehmern oder Organisationen über ein Webinterface ausgelöst werden. Danach wird wieder über die Externe Identitätsüberprüfung ein Check durchgeführt. Falls dieser Check fehlschlägt, wird die komplette Aktion sofort abgebrochen. Ansonsten wird die Suche auf der Blockchain mithilfe der Referenzdaten und eines Quick-Find Algorithmus durchgeführt. Nachdem die gehashten Infos gefunden wurden, wird im Hashing Vertrag die Information entschlüsselt und dann in Klartext dargestellt auf der Webseitenschnittstelle.

Der gesamte Smart Contract ist im Anhang ersichtlich.

# Identifikationsprozess

Durch die Transaktion der Vermögen muss ein Identifikationsprozess gestaltet werden, welcher möglichst einfach für den Vorsorgenehmer ist und den höchst möglichen Sicherheitsstandard für das Implementierte System ermöglicht. Die nachfolgende Grafik bildet diesen Prozess bildlich ab.

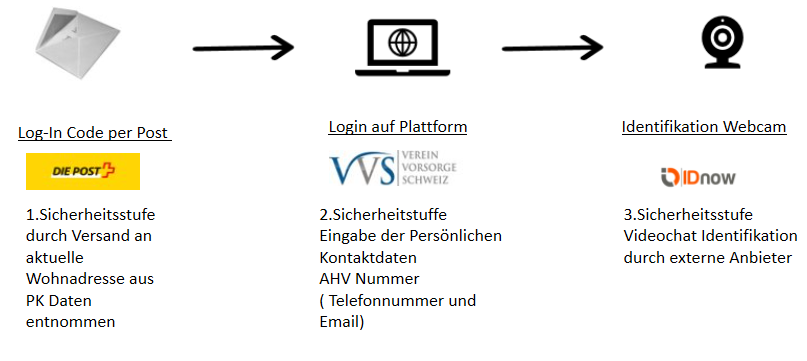


Abbildung 10: Übersicht über den Prozess Quelle: Eigene Darstellung

Bei Austritt aus der Pensionskasse wird das Vermögen auf eine Freizügigkeitsstiftung transferiert. Bei dem Erstkontakt mit dem Vorsorgenehmer wird dieser postalisch mit einem Log-In Code versorgt. Dieser berechtigt den Vorsorgenehmer in Verbindung mit seiner AHV-Nummer sich auf der Plattform Verein Vorsorge Schweiz einzuloggen. Nach Eingabe aller relevanten Daten wird dieser auf einen externeren Identifikationsdienst wie z.B. ID-NOW weitergeleitet. Diese überprüfen mittels Videochat und spezieller Erkennungssoftware für Pässe und ID Karten, ob die Person, die sich angemeldet hat, dazu berechtigt ist, diese Verschiebung zu autorisieren. Nach Abschluss der Überprüfung wird eine Identitätsbestätigung an die Plattform des Verein Vorsorge Schweiz (VVS) gesendet. Nach Erhalt dieser Bestätigung werden die Gelder auf die gewählte Freizügigkeitsstiftung überwiesen.

Durch die Abspaltung der Identifikationserkennung mindert sich der administrative Aufwand für die Plattform des VVS. Die Datensicherheit wird dadurch erhöht, weil bisher nicht miteinander verbundene Systeme zur Verschiebung der Gelder zu einem einzigen System komprimiert werden.

# Das MockUp

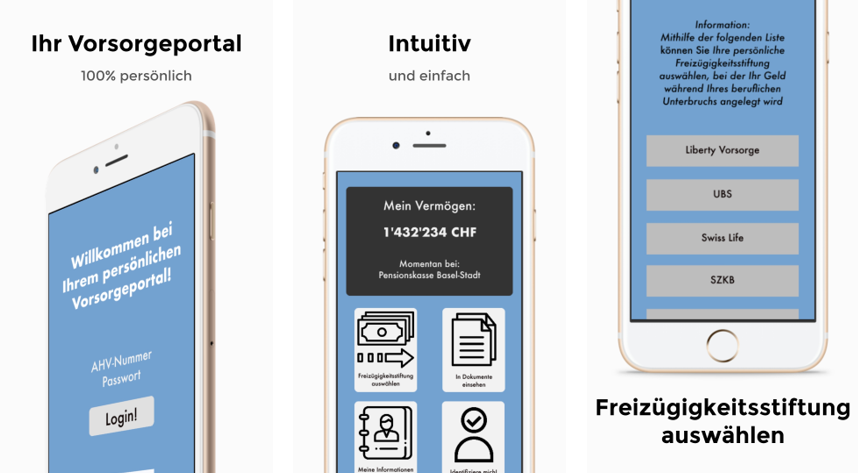
Dieser Teil dreht sich um die Beschreibung des erstellten Mockups. wie in der folgenden Abbildung zu erkennen ist, gibt es eine Anmeldeseite. Nach der Anmeldeseite kommt man zu einer Übersicht, auf der das Vermögen, der aktuelle Ort des Geldes und die verfügbaren Optionen ersichtlich sind. Es gibt 4 Auswahlmöglichkeiten: Freizügigkeitsstiftung auswählen, in Dokumente einsehen, meine Informationen abrufen und identifiziere mich. nachdem man die erste Option ausgewählt hat, gelangt man auf eine Seite, auf der man eine der möglichen Freizügigkeitsstiftungen auswählen kann. Bei der Auswahl wird dies auf der Blockchain vermerkt. Des Weiteren kann man in seine Dokumente einsehen. In dem Fenster lassen sich Eingangs- und Ausgangsbestätigungen, sowie die Vorsorgeregelung abrufen. Zudem lassen sich die individuellen Informationen über den Vorsorgenehmer abrufen. hier erscheinen Name, AHV Nummer, aktueller Ort des Vermögens und Zielort des Vermögens. Die letzte Funktion betrifft die Identifizierung des Vorsorgenehmers und leitet auf einen externen Anbieter weiter. das Mockup kann getestet werden unter folgendem Link: bit.ly/VVSApp.

Abbildung 11: Das MockUp. Quelle: Eigene Darstellung

# Schlusswort

# Abbildungsverzeichnis

[Abbildung 1: Illustration der zeitlichen Abfolge. Quelle: Eigene Darstellung 2](file:///C:\Users\Julian\Dropbox\BCC_2019\Paper%20VVS.docx#_Toc26290618)

[Abbildung 2: Der postalische Ablauf. Quelle: Eigene Darstellung 3](file:///C:\Users\Julian\Dropbox\BCC_2019\Paper%20VVS.docx#_Toc26290619)

[Abbildung 3: Illustration der Verbindungen zwischen den Akteuren. Quelle: Eigene Darstellung 5](file:///C:\Users\Julian\Dropbox\BCC_2019\Paper%20VVS.docx#_Toc26290620)

[Abbildung 4: Ein Vergleich der Blockchain-Technologie mit einer zentralisierten Datenbank. Quelle: CoinRevolution 9](file:///C:\Users\Julian\Dropbox\BCC_2019\Paper%20VVS.docx#_Toc26290621)

[Abbildung 5: Übersicht über die verschiedenen Technologien. Quelle: IT-Produktion 12](file:///C:\Users\Julian\Dropbox\BCC_2019\Paper%20VVS.docx#_Toc26290622)

[Abbildung 6: Das resultierende Ökosystem mit den Vorteilen der jeweiligen Parteien. Quelle: Eigene Darstellung 14](file:///C:\Users\Julian\Dropbox\BCC_2019\Paper%20VVS.docx#_Toc26290623)

[Abbildung 7: Eine Übersicht der Beziehungen zwischen den Akteuren. Quelle: Eigene Darstellung 16](file:///C:\Users\Julian\Dropbox\BCC_2019\Paper%20VVS.docx#_Toc26290624)

[Abbildung 8: UML-Klassendiagramm der Smart Contract Struktur. Quelle: Eigene Darstellung erstellt mit plantUML 18](file:///C:\Users\Julian\Dropbox\BCC_2019\Paper%20VVS.docx#_Toc26290625)

[Abbildung 9: Aktivitätsdiagramme zum Ablauf der Funktionen Organisationswechsel und Informationsgewinnung. Quelle: Eigene Darstellung 19](file:///C:\Users\Julian\Dropbox\BCC_2019\Paper%20VVS.docx#_Toc26290626)

[Abbildung 10: Übersicht über den Prozess Quelle: Eigene Darstellung 21](file:///C:\Users\Julian\Dropbox\BCC_2019\Paper%20VVS.docx#_Toc26290627)

[Abbildung 11: Das MockUp. Quelle: Eigene Darstellung 23](file:///C:\Users\Julian\Dropbox\BCC_2019\Paper%20VVS.docx#_Toc26290628)

# Literaturverzeichnis

Roos, N. (Februar 2016). *Vergessene Pensionskassen-Gelder: So forschen Sie nach*. Von https://www.srf.ch/sendungen/kassensturz-espresso/themen/geld/vergessene-pensionskassen-gelder-so-forschen-sie-nach abgerufen

# Anhang

Im Anhang findet man den Smart Contract sowie die Übersicht der Mock-Up-Applikation.

## 15.1. MockUp-Applikation



Das MockUp ist zudem abrufbar unter: bit.ly/VVSApp

## 15.2. Der Smart Contract