



BERNER FACHHOCHSCHULE - DEPARTEMENT WIRTSCHAFT

MASTER-THESIS

POLIT-ÖKONOMISCHE EVALUATION EINER BLOCKCHAIN-BASIERTEN IDENTITÄTSNACHWEISLÖSUNG

**Die Blockchain-ID: Eine mehrheitsfähige Lösung  
für den digitalen Identitätsnachweis innerhalb  
der schweizerischen Demokratie?**

*Tim Wackernagel*

Studiengang: Master of Science in Business Administration

Betreuer:in: Dr. Daniel Schwarz Badertscher

Expert:innen: Dr. Daniel Schwarz Badertscher, Prof. Dr. Thomas Gees

---

## Abstract

Am 7. März 2021 hat die schweizerische Bevölkerung im Rahmen einer eidgenössischen Volksabstimmung die Gesetzesgrundlage für einen elektronischen Identitätsnachweis (*E-ID*) abgelehnt. Ein alternativer E-ID-Lösungsansatz könnte auf der Blockchain-Technologie basieren. Im Rahmen dieser Master-Thesis wird empirisch geprüft, ob eine digitale ID-Lösung basierend auf der Blockchain-Technologie beim schweizerischen Stimmvolk auf Akzeptanz stossen würde. Die empirischen Forschungsergebnisse zeigen, dass die schweizerische Bevölkerung einer derartigen E-ID-Lösung verhältnismässig positiv gegenübersteht. Sowohl geschlechter-, sprach- als auch weitgehend parteiübergreifend scheint eine vergleichsweise hohe Offenheit und Zustimmung gegenüber einer staatlichen und Blockchain-basierten ID im Rahmen einer Volksabstimmung möglich. Trotz Ausschluss des Anspruchs auf Repräsentativität der Ergebnisse scheint die Schlussfolgerung legitim, dass eine rein staatliche und Blockchain-basierte E-ID innerhalb der Schweizerischen Eidgenossenschaft zumindest realistische Aussichten auf das Erreichen einer demokratischen Volksmehrheit vorweist. Damit kann dieser Lösungsansatz zur Umsetzung einer digitalen ID innerhalb der Schweizerischen Eidgenossenschaft als mehrheitsfähige Option in Erwägung gezogen werden.

---

## Management Summary

Viele Expert:innen betrachten eine digitale ID als Zugangsschlüssel zu ökonomischen, sozialen und politischen Bereichen und Potenzialen in einer digitalen Welt. Am 7. März 2021 hat die schweizerische Bevölkerung im Rahmen einer eidgenössischen Volksabstimmung die Gesetzesgrundlage für einen elektronischen Identitätsnachweis (*E-ID*) abgelehnt. Im Rahmen der Konzeption neuer E-ID-Lösungen versucht die schweizerische Politik seither, das Fachwissen und die Interessen von Wissenschaft, Wirtschaft, Zivilgesellschaft und Politik besser berücksichtigen zu können.

Wie die vergangene Volksabstimmung gezeigt hat, muss eine E-ID-Lösung letztlich das schweizerische Stimmvolk überzeugen. Ein alternativer E-ID-Lösungsansatz könnte auf der Blockchain-Technologie basieren. Im Rahmen dieser Master-Thesis wird empirisch geprüft, ob eine digitale ID-Lösung basierend auf der Blockchain-Technologie beim schweizerischen Stimmvolk auf Akzeptanz stossen würde.

In einer quantitativen Umfrage mit 1'730 Teilnehmenden wird die Einstellung von in der Schweiz stimmberechtigten Personen gegenüber einer solchen E-ID-Lösung erhoben und analysiert. Daraus werden Erkenntnisse gewonnen, ob das Konzept einer Blockchain-Lösung zum Identitätsnachweis in der Schweizerischen Eidgenossenschaft bei einer erneuten Volksabstimmung Erfolgschancen hätte. Aus forschungsoökonomischen Gründen ist eine für die schweizerische Bevölkerung repräsentative Datengrundlage nicht realisierbar. Stattdessen wird die Stichprobe durch Gewichtungsverfahren bestmöglich an die Bevölkerungsstruktur angeglichen.

Die empirischen Forschungsergebnisse zeigen, dass die schweizerische Bevölkerung einer derartigen E-ID-Lösung verhältnismässig positiv gegenübersteht. Sowohl geschlechter-, sprach- als auch beinahe parteiübergreifend scheint eine vergleichsweise hohe Offenheit und Zustimmung gegenüber einer staatlichen und Blockchain-basierten ID im Rahmen einer Volksabstimmung möglich. Hauptgrund für diese Zustimmung stellt die Ermöglichung der vollständig selbstbestimmten Verwaltung der eigenen Identität dar. Auf der Gegenseite stehen hauptsächlich Datenschutz- und Sicherheitsbedenken gegenüber einer E-ID im Allgemeinen als auch gegenüber dem Einsatz von Blockchain-Technologie im Zentrum.

Trotz Ausschluss des Anspruchs auf Repräsentativität der Ergebnisse bezogen auf die schweizerische Gesamtbevölkerung scheint die Schlussfolgerung legitim, dass eine rein staatliche und Blockchain-basierte E-ID innerhalb der Schweizerischen Eidgenossenschaft zumindest realistische Aussichten auf das Erreichen einer demokratischen Volksmehrheit vorweist. Damit kann dieser Lösungsansatz zur Umsetzung einer digitalen ID innerhalb der Schweizerischen Eidgenossenschaft als mehrheitsfähige Option unter anderen Umsetzungsmöglichkeiten in Erwägung gezogen werden.

# Inhaltsverzeichnis

<b>1 Einleitung</b>	<b>1</b>
1.1 Ausgangslage . . . . .	1
1.2 Forschungsziele . . . . .	2
1.3 Forschungsfragen . . . . .	3
1.4 Wissenschaftliche Relevanz . . . . .	3
<b>2 Theoretischer Teil</b>	<b>4</b>
2.1 Theoretischer Rahmen & Begriffsdefinitionen . . . . .	4
2.1.1 Identitätsbegriff . . . . .	4
2.1.2 Digitale Identität & digitales Identitätsmanagement . . . . .	6
2.1.3 Blockchain-Technologie . . . . .	13
2.1.4 Digitale Demokratie & Krypto-Demokratie . . . . .	20
2.2 Fokussierung & Abgrenzung . . . . .	23
2.3 Aktueller Identitätsnachweis in der Schweiz . . . . .	24
2.4 Digitale Demokratie & die Identität ihrer Bürger:innen . . . . .	27
2.4.1 Demokratische Triebkräfte des digitalen Identitätsnachweises .	28
2.4.2 E-Government-Strategie Schweiz 2020-2023 & Strategie Digitale Schweiz . . . . .	32
2.4.3 Anwendungsbereiche einer digitalen ID für Dienstleistungen im öffentlichen Sektor und der Demokratie . . . . .	33
2.5 Eidgenössische Abstimmung zur E-ID 2020 . . . . .	37
2.6 Blockchain-Technologie & Self-Sovereign Identity . . . . .	40
2.6.1 Theoretische Konzepte zum Blockchain-Identitätsnachweis .	41
2.6.2 Chancen & Vorteile des Blockchain-Identitätsnachweises .	46
2.6.3 Hürden & Risiken des Blockchain-Identitätsnachweises .	49
2.7 Blockchain-Identitätsnachweis in der Praxis . . . . .	55
<b>3 Empirischer Teil</b>	<b>59</b>
3.1 Ziele der Forschung . . . . .	59
3.1.1 Hypothesen . . . . .	60
3.2 Datenerhebung . . . . .	61
3.2.1 Umfrageverlauf . . . . .	61
3.3 Analyse & Gewichtung der Stichprobe . . . . .	63
3.3.1 Analyse der persönlichen Merkmale . . . . .	65
3.3.2 Güte der Gewichtung . . . . .	70

## INHALTSVERZEICHNIS

---

3.4	Deskriptive Datenauswertungen . . . . .	72
3.4.1	Vertrauen in den Staat . . . . .	73
3.4.2	Wahrnehmung & Einordnung der digitalen ID . . . . .	75
3.4.3	Anwendungsbereiche der digitalen ID im öffentlichen Sektor & in der digitalen Demokratie . . . . .	77
3.4.4	Vorkenntnisse & Einstellung gegenüber der Blockchain-Technologie . . . . .	78
3.4.5	Einstellung gegenüber der Self-Sovereign Identity . . . . .	82
3.4.6	Einstellung gegenüber einer digitalen ID auf Basis von Blockchain-Technologie . . . . .	84
3.4.7	Abstimmungsabsicht bezüglich einer staatlichen & Blockchain-basierten ID-Lösung . . . . .	86
3.4.8	Gründe für und gegen eine staatliche & Blockchain-basierte ID-Lösung . . . . .	90
3.5	Inferenzstatistische Datenauswertungen . . . . .	95
3.5.1	Hypothese 1: Blockchain-Kompetenz & Stimmabsicht . . . . .	95
3.5.2	Hypothese 2: Wichtigkeit von öffentlichen Dienstleistungen & Stimmabsicht . . . . .	97
3.5.3	Hypothese 3: Kantonale Unterschiede bezüglich Stimmabsicht	101
3.5.4	Multivariate Datenanalyse - Entscheidungsbaum . . . . .	103
<b>4</b>	<b>Konklusion</b>	<b>106</b>
4.1	Diskussion der Resultate . . . . .	106
4.1.1	Bezug zu den Forschungsfragen . . . . .	112
4.1.2	Handlungsempfehlungen . . . . .	113
4.2	Ausblick & künftige Forschung . . . . .	114
<b>Literaturverzeichnis</b>		<b>115</b>

## Abbildungsverzeichnis

1	Funktionsweise der Blockchain schematisch erklärt [Schweizerischer Baumeisterverband 2020], bearbeitet.	16
2	Asymmetrische Verschlüsselung schematisch erklärt [Ledger Academia 2019].	17
3	Trapdoor function von Schlüsseln bei asymmetrischer Verschlüsselung [Ledger Academia 2019].	17
4	Die vier Entwicklungsstufen der digitalen Identität, eigene Darstellung in Anlehnung an Bakre et al. 2017, S. 379.	42
5	Die 10 Prinzipien der Self-Sovereign Identity nach Christopher Allen [Jolocom 2018], bearbeitet.	43
6	Schiefe der Stichprobe am Beispiel der Fragestellung Q5.2.	72
7	Auswertung der Fragestellung Q5.2.	74
8	Auswertung der Fragestellung Q5.3.	74
9	Auswertung der Fragestellung Q5.5.	75
10	Auswertung der Fragestellung Q6.2.	76
11	Auswertung der Fragestellung Q6.3.	76
12	Auswertung der Fragestellung Q6.4.	77
13	Auswertung der Fragestellung Q7.3.	78
14	Auswertung der Fragestellung Q7.4.	78
15	Auswertung der Fragestellung Q8.1.	79
16	Auswertung der Fragestellung Q8.3.	80
17	Auswertung der Fragestellung Q8.4.	80
18	Auswertung der Fragestellung Q8.5.	81
19	Auswertung der Fragestellung Q8.7.	82
20	Auswertung der Fragestellung Q9.1.	83
21	Auswertung der Fragestellung Q10.2.	84
22	Auswertung der Fragestellung Q10.7.	85
23	Auswertung der Fragestellung Q11.2 - Total.	86
24	Auswertung der Fragestellung Q11.2 nach Geschlecht.	87
25	Auswertung der Fragestellung Q11.2 nach Sprache.	88
26	Auswertung der Fragestellung Q11.2 nach Partei.	89
27	Auswertung der Fragestellung Q11.3.	90
28	Auswertung der Fragestellungen Q11.4, Q11.7 und Q11.8 nach Stimmabsicht.	91

## ABBILDUNGSVERZEICHNIS

---

29	Auswertung der Fragestellungen Q11.5, Q11.6 und Q11.9 nach Stimmabsicht. . . . .	93
30	Visualisierung Hypothese 1 - Rangkorrelation nach Spearman von Kompetenz und Zustimmung. . . . .	96
31	Auswertung der Fragestellung Q10.8. . . . .	97
32	Visualisierung Hypothese 2 - Rangkorrelation nach Spearman von Wichtigkeit und Zustimmung. . . . .	99
33	Visualisierung Hypothese 2 - Rangkorrelation nach Spearman von Voraussetzungsbewusstsein und Zustimmung. . . . .	100
34	Visualisierung Hypothese 3 - Unterschiede in der Zustimmung zwischen ZG und SH im Vergleich zu den restlichen Kantonen. . . . .	102
35	Multivariate Datenanalyse - Entscheidungsbaum. . . . .	104

## Tabellenverzeichnis

1	Abstimmungsverhalten beim E-ID-Gesetz 2020 von Stichprobe und Bevölkerung. . . . .	65
2	Vergleich von Stichprobe und Bevölkerungsstruktur nach Geschlecht. . . . .	65
3	Vergleich von Stichprobe und Bevölkerungsstruktur nach Sprachregion. . . . .	66
4	Vergleich von Stichprobe und Bevölkerungsstruktur nach Altersgruppen. . . . .	67
5	Vergleich von Stichprobe und Bevölkerungsstruktur nach Bildungsabschluss. . . . .	68
6	Vergleich von Stichprobe und Bevölkerungsstruktur nach Parteinähe. . . . .	69
7	Abstimmungsverhalten beim E-ID-Gesetz 2020 zwischen gewichteter Stichprobe und Bevölkerung. . . . .	70

# 1 Einleitung

Die vorliegende Master-Thesis wird im Rahmen des Studiengangs *Master of Science in Business Administration* der Berner Fachhochschule verfasst. Die Thesis widmet sich dem Digitalisierungstrend der Demokratie in der Schweizerischen Eidgenossenschaft und der damit einhergehenden Herausforderung zur staatlichen Lösungsentwicklung eines digitalen Identitätsnachweises. Die Begriffe *elektronisch* und *digital* lassen sich im Kontext des Identitätsnachweises als Synonyme verstehen.

Unterschiedlichste Prozesse der schweizerischen Demokratie setzen voraus, dass die Identität von Bürger:innen eindeutig verifiziert werden kann. Am 7. März 2021 hat die schweizerische Bevölkerung im Rahmen einer eidgenössischen Volksabstimmung eine Gesetzesgrundlage für einen vom Bund anerkannten, elektronischen Identitätsnachweis (*E-ID*) abgelehnt. Der Mangel einer solchen Lösung betrifft neben dem Privatsektor verschiedenste Bereiche des öffentlichen Sektors und der digitalen Demokratie. Eine Alternative zu der im abgelehnten Gesetz ursprünglich vorgesehenen Lösung könnte auf der Blockchain-Technologie basieren. Ob allerdings eine digitale Identitätsnachweislösung basierend auf der aufstrebenden und von Vorurteilen geprägten Blockchain-Technologie beim schweizerischen Stimmvolk auf Akzeptanz stossen würde, ist unklar.

## 1.1 Ausgangslage

In einer immer stärker digitalisierten Gesellschaft wird die Einführung von Lösungen zum eindeutigen und sicheren digitalen Identitätsnachweis unausweichlich. Die Notwendigkeit und die Vorteile einer E-ID im privatwirtschaftlichen als auch im öffentlichen Sektor werden im Zuge der fortschreitenden Digitalisierung immer offensichtlicher. Das McKinsey Global Institute [2019, S. vi] attribuiert die digitale Identifikation als einen Schlüssel für inklusives Wachstum einer Gesellschaft. Der Report zur *Digital Identification* beschreibt die digitale ID als Mittel, um eindeutige Identifikation über digitale Kanäle zu ermöglichen und so Zugang zu Bankgeschäften, Behörden, Bildung und vielen weiteren Dienstleistungen zu erhalten [McKinsey Global Institute 2019, S. vi].

Eine digitale ID-Lösung kann also der Zugangsschlüssel zu ökonomischen, sozialen und politischen Bereichen in einer digitalen Welt sein. Beim ökonomischen Potenzial beschreibt das McKinsey Global Institute [2019, S. 51] eine global betrachtet durchschnittlich mögliche Steigerung des Bruttoinlandsprodukts (BIP) von rund 6 % pro Land bis 2030, rein basierend auf der Einführung einer digitalen Identitätsnachweislösung. Gleichzeitig erwähnt der Bericht auch nicht-ökonomische Potenziale einer digitalen ID wie politische und soziale Inklusion, den Schutz von

Menschenrechten oder die Erhöhung von Transparenz [McKinsey Global Institute 2019, S. 51]. Insgesamt macht der Bericht des McKinsey Global Instituts klar, dass der digitalen Identität in den kommenden Jahren eine immer grösser werdende Bedeutung zukommen wird.

Durch die Ablehnung der gesetzlichen Grundlage für eine staatliche elektronische Identität an der Urne wurde die Einführung einer digitalen Lösung zum Identitätsnachweis in der Schweizerischen Eidgenossenschaft auf unbestimmte Zeit verschoben. Für Schweizer:innen existiert somit nach wie vor keine vom Bund offiziell anerkannte Möglichkeit zum digitalen Identitätsnachweis. Dies betrifft auch verschiedenste Bereiche der digitalen Demokratie und des öffentlichen Sektors, welche für vollständig digitale Behördendienstleistungen auf eine digitale ID angewiesen sind. Für den schweizerischen Bundesrat ist deshalb trotz der Ablehnung der E-ID-Vorlage an der Urne klar, dass künftig eine Lösung zum digitalen Identitätsnachweis in der Schweiz unumgänglich ist. Bereits drei Tage nach der Volksabstimmung haben alle politischen Fraktionen der Schweiz Motionen für eine *vertrauenswürdige, staatliche E-ID* eingereicht [Eidgenössisches Justiz- und Polizeidepartement 2021a]. Bundesrätin Keller-Sutter hat in der Folge am 2. September 2021 eine öffentliche Konsultation gestartet, um möglichst rasch eine überarbeitete gesetzliche Grundlage für eine staatliche, digitale ID schaffen zu können [Eidgenössisches Justiz- und Polizeidepartement 2021c]. Das Ziel ist dabei, die breite Öffentlichkeit in die Konzeption einer neuen E-ID-Lösung miteinzubeziehen, um so die Interessen und Bedürfnisse der Wissenschaft, Wirtschaft, Zivilgesellschaft und Politik berücksichtigen zu können.

## 1.2 Forschungsziele

Das Vorgehen des Bundesrats zeigt, dass die Einführung einer Lösung zum digitalen Identitätsnachweis in der Schweizerischen Eidgenossenschaft keinesfalls ad acta gelegt wurde. Für einen erneuten Anlauf sollen nun verschiedenste Möglichkeiten zur Umsetzung einer digitalen ID geprüft werden. Wie die vergangene Volksabstimmung gezeigt hat, muss eine neue E-ID-Lösung neben den Bedürfnissen der Privatwirtschaft und des öffentlichen Sektors letztlich vor allem auch das schweizerische Stimmvolk überzeugen können. Die vorliegende Master-Thesis widmet sich vorwiegend den Themenfeldern der digitalen Demokratie, des digitalen Identitätsnachweises sowie der Blockchain-Technologie im Kontext der Schweizerischen Eidgenossenschaft. Ziel dieser Master-Thesis ist es, den digitalen Identitätsnachweis in einen theoretischen Rahmen einzuordnen, Blockchain-basierte Identitätsnachweiskonzepte im Hinblick auf ihre Vor- und Nachteile zu untersuchen und insbesondere einen Bezug zur Digitalisierung der schweizerischen Demokratie zu schaffen. In einer quantitativen Umfrage soll ausserdem die Einstellung von in der Schweiz stimmberechtigten

Personen gegenüber einer solchen Identitätslösung und deren Einsatzgebieten in der digitalen Demokratie empirisch erhoben und analysiert werden. Daraus sollen Erkenntnisse gewonnen werden, ob das Konzept einer Blockchain-Lösung zum Identitätsnachweis in der Schweizerischen Eidgenossenschaft bei einer erneuten Volksabstimmung Erfolgschancen hätte.

## 1.3 Forschungsfragen

Folgende Fragestellungen werden im Rahmen der Master-Thesis überprüft:

- Welche Chancen und Herausforderungen ergeben sich im Hinblick auf die Verwendung der Blockchain-Technologie im Bereich der digitalen Demokratie und insbesondere im Bereich eines digitalen Identitätsnachweises?
- Wie ist die Einstellung der schweizerischen Bevölkerung gegenüber der Blockchain-Technologie und insbesondere gegenüber dem Einsatz von Blockchain-Technologie zum Zwecke eines digitalen Identitätsnachweises?
- Ist eine auf der Blockchain-Technologie basierende E-ID-Lösung in der Schweizerischen Eidgenossenschaft mehrheitsfähiger als die in der Volksabstimmung zur *E-ID 2020* vorgeschlagene und von der Bevölkerung abgelehnte Lösung?

## 1.4 Wissenschaftliche Relevanz

Nach der gescheiterten Abstimmung zur Gesetzesgrundlage einer digitalen ID-Lösung versucht der schweizerische Bund möglichst rasch eine neue Lösung für den elektronischen Identitätsnachweis zu präsentieren. Dazu wurde am 02.09.2021 eine öffentliche Anhörung zum Diskussionspapier *Zielbild E-ID* eröffnet [Eidgenössisches Justiz- und Polizeidepartement 2021a; Eidgenössisches Justiz- und Polizeidepartement 2021c]. Die Aktualität der Thematik in der Schweiz unterstreicht die wissenschaftliche Relevanz der geplanten Forschung. Die Forschungsarbeit soll Erkenntnisse zur Wahrnehmung und Einstellung der Bevölkerung gegenüber einem möglichen Einsatz einer auf der Blockchain-Technologie basierenden Identitätsnachweislösung liefern. Diese Erkenntnisse sollen in der Praxis Hinweise darauf geben, ob eine Blockchain-basierte Herangehensweise reale Chancen hätte, von der Bevölkerung als elektronische Identitätsnachweislösung akzeptiert zu werden. Die wissenschaftliche Community soll von einem Erkenntnisgewinn über die Haltung der Bevölkerung gegenüber der Blockchain als unbekannte Technologie im Allgemeinen und über den Einsatz von Blockchain-Lösungen innerhalb der digitalen Demokratie und des öffentlichen Dienstleistungssektors profitieren.

## 2 Theoretischer Teil

### 2.1 Theoretischer Rahmen & Begriffsdefinitionen

Um einen theoretischen Wissensrahmen rund um die Thematik des digitalen Identitätsnachweises schaffen zu können, werden in den folgenden Kapiteln verschiedene Begriffe und Konzepte erläutert. Dabei handelt es sich um zentrale Kernelemente einer digitalen ID wie *Identität*, *digitale Identität* und *digitales Identitätsmanagement*. Weiter sind für diese Thesis die Kontexte von *Blockchain-Technologie*, *digitaler Demokratie* und *Krypto-Demokratie* von grosser Relevanz.

#### 2.1.1 Identitätsbegriff

Der Begriff der *Identität* wird in der Literatur als sehr vielschichtig und nicht eindeutig definierbar beschrieben. Wie die ideengeschichtliche Analyse des Begriffs von Nicke [2018] zeigt, handelt es sich bei der Identität um einen noch relativ jungen Begriff, welcher bis zum Ende des 19. Jahrhunderts als „*philosophisches Kunstwort*“ beschrieben wurde. Auch zeitgenössische Autor:innen wie Treiblmaier und Beck [2019, S. 235] beschreiben aus rechtlicher Sicht Identität als nebulösen Begriff, welcher gerade im Zuge von globalen Digitalisierungsfortschritten immer komplexer wird. Neben den rechtlichen Unschärfen in der Definition von Identität führen Zwitter et al. [2020, S. 3] ein ebenso vieldeutiges Verständnis des Begriffs aus philosophischer Sicht an.

Die Dudenredaktion weist der Identität zwei Bedeutungen zu: Zum einen die „*Echtheit einer Person oder Sache; völlige Übereinstimmung mit dem, was sie ist oder als was sie bezeichnet wird*“ und die „*als ‚Selbst‘ erlebte innere Einheit der Person*“, zum anderen die „*völlige Übereinstimmung mit jemandem, etwas in Bezug auf etwas; Gleichheit*“ [Duden 2022]. Der Begriff beschreibt demnach sowohl ein Bewusstseinskonzept als auch ein Echtheits- und Nämlichkeitskonzept.

Aus sozialwissenschaftlicher Sicht lässt sich die Identität in mindestens drei Kontextgruppen unterteilen: Identität kann einerseits als Zusammenhang von von aussen zugeschriebenen Merkmalen (Typisierung, Rollen, etc.), andererseits als Merkmalszusammenhang sozialer Systeme (bspw. nationale, kulturelle, ethnische Identitäten) verstanden werden [Heinzer und Reichenbach 2013, S. 12]. Die dritte Kontextgruppe gilt als Prozess der Selbstreflexion eines Individuums, wobei eine Person eine Identität durch Verarbeitung von Wissen und Erfahrungen über sich selbst herstellt. Wie diese Einteilung offenbart, wohnt dem Begriff der Identität neben einer philosophischen auch eine stark psychologisch geprägte Komponente inne.

Neben den beschriebenen Begriffseinordnungen existiert eine Vielzahl weiterer Perspektiven auf den Identitätsbegriff. Eine eindeutige und allgemeingültige Definition ist nur schwer zu fassen. Im Rahmen dieser Master-Thesis ist es dennoch wichtig, ein für in dieser Forschungsarbeit relevantes sowie einheitliches Verständnis des Begriffs zu schaffen.

Identität im Kontext dieser Forschungsarbeit soll als ein vielschichtiges Konzept verstanden werden, welches Individuen als einzigartig definiert. Identität besteht aus einer (u.U. dynamischen) Sammlung von Attributen, welche einer Entität zugeschrieben werden. Diese Entität wird dadurch eindeutig identifizierbar und von anderen Entitäten unterscheidbar gemacht [Mir et al. 2020, S. 1; Melin et al. 2016, S. 75]. Im Kontext von Identitätsnachweisen dominiert in der heutigen Zeit noch immer ein Verständnis, welches nach Cap und Maibaum [2001, S. 805] sehr eng an das physische Ausweisdokument des Passes gebunden ist. Ein Pass vereint unterschiedlichste Eigenschaften wie Namen, Geburtsdatum, Wohnort, Fotos oder auch biometrische Merkmale (Attribute) einer Person (Entität), um dadurch eine Person eindeutig identifizierbar zu machen. Durch die Assoziation des Identitätsnachweises mit einem Ausweisdokument verstehen die meisten Menschen Identität weiter als etwas, das mit dem Staat in Verbindung steht [Camp 2004, S. 35]. Die Regierung eines Landes besitzt dabei die Hauptverantwortlichkeit für die Erstellung, Implementierung, Pflege und Kontrolle von Identitätsnachweismitteln [Müller und Windisch 2018, S. 4].

Da sich diese Thesis mit neuen technischen Lösungen zum Identitätsnachweis von Menschen befasst, sind neben der Identität auch andere, mit dem Identifikationsprozess von Menschen zusammenhängende Begriffe relevant. Ein Identitätssystem besteht aus folgenden Elementen [Camp 2004, S. 35-36]:

- *Identität*: In einem Identitätssystem ist die Identität eine Menge von permanenten oder langlebigen Attributen, welche mit einer Entität assoziiert werden.
- *Identifizierer*: Ein Identifizierer unterscheidet eine eindeutige Person oder Sache im Kontext eines Namensraums (der Kontext, in welchem die Zuordnung gilt).
- *Attribute*: Ein Attribut ist eine Charakteristik, welche mit einer Entität (bspw. einem Individuum) assoziiert wird.
- *Identifikation*: Die Identifikation beschreibt die Assoziation eines Identifizierers mit einem Individuum, welches Attribute präsentiert („Deine Attribute zeigen eindeutig, dass du Max Muster bist.“).
- *Authentifizierung*: Unter Authentifizierung wird der Nachweis eines Attributs verstanden.

- *Identitätsauthentifizierung:* Die Identitätsauthentifizierung weist eine Assoziation zwischen einer Entität und einem Identifizierer nach.
- *Attributsauthentifizierung:* Die Attributsauthentifizierung weist eine Assoziation zwischen einer Entität und einem Attribut nach.
- *Autorisierung:* Mit Autorisierung wird die Entscheidung beschrieben, auf Basis von Identifizierern oder Attributen eine spezifische Handlung oder einen spezifischen Prozess zuzulassen.

Wie die vorgängige Auflistung zeigt, bestehen Identitätssysteme im Kontext von Identitätsnachweisen aus unterschiedlichsten Elementen. Identität wird im Rahmen dieser Thesis als ein Kernelement zur eindeutigen Identifikation von Menschen verstanden. Sie lässt sich im Kontext dieser Forschungsarbeit auch aus einer technischen Sicht einordnen, was sich im Begriff der *digitalen Identität* niederschlägt.

### 2.1.2 Digitale Identität & digitales Identitätsmanagement

Die *digitale Identität* (digitale ID) soll ein Schlüsselproblem der modernen Welt lösen: Die Identität einer Person im digitalen Raum einwandfrei und vertrauenswürdig nachweisbar zu machen. Wie vorgängig beschrieben, werden *elektronische Identität* und *digitale Identität* im Kontext dieser Arbeit als Synonyme behandelt.

Nach Goode [2019, S. 5] befinden sich technisch fortgeschritten entwickelte Staaten in einer Transitionsphase von physischen Identitätsdokumenten zu digitalen Identitätsnachweisen. Im Zentrum steht in der jetzigen Phase vorgängig die digitale Identität im Sinne einer Zugangsprämissen für digitale Dienstleistungen in Form eines Log-ins. Sullivan [2016, S. 475] erachtet es als unausweichlich, dass der künftige Standard für Transaktionen zwischen Individuen und Dienstleistungen des privaten oder öffentlichen Sektors eine digitale Identität voraussetzen wird. Die Relevanz der digitalen Identität beschreiben auch Müller und Windisch [2018, S. 2] als weitreichend: Anbieter:innen technischer Infrastruktur, staatliche Behörden, Banken, Unternehmen unterschiedlichster Branchen sowie natürlich auch Konsument:innen werden sich künftig mit digitaler Identität befassen müssen.

Das *National Institute of Standards and Technology* (NIST) der Vereinigten Staaten von Amerika definiert die digitale Identität generell als einzigartige Repräsentation eines in einer digitalen Transaktion beteiligten Subjekts [Grassi et al. 2017, S. 2]. Eine digitale Identität ist dabei im Kontext einer spezifischen digitalen Dienstleistung einzigartig (z.B. ein Log-in aus Benutzername und Passwort). Diese digitale Identität ist jedoch nicht zwingend in jedem Kontext eindeutig und es muss sich dabei auch nicht um eine real existierende Identität eines Menschen handeln. Mehrere digitale Identitäten für ein einzelnes Subjekt sind möglich

[Toth und Anderson-Priddy 2019, S 18]. Eine weitere, generalistische Auslegung von digitaler Identität der *International Organization for Standardization* (ISO) beschreibt diese als ein Element innerhalb oder ausserhalb eines Informations- und Kommunikationssystems, wie z. B. eine Person, eine Organisation, ein Gerät oder ein Teilsystem solcher Elemente, das eine erkennbare eigene Existenz hat [Mir et al. 2020, S. 1]. Das *World Economic Forum* (WEF) definiert die digitale Identität als Sammlung von Einzelattributen die eine Einheit beschreiben und die (digitalen) Transaktionen bestimmen, an denen diese Einheit teilnehmen kann [Mir et al. 2020, S. 1].

Mit digitaler Identität geht auch der Bedarf nach einem *digitalen Identitätsmanagement* einher. Digitales Identitätsmanagement wird von der OECD [2020] als fundamental für die Weiterentwicklung der Internetwirtschaft angesehen. Wie in der physischen Welt sind auch im digitalen Raum Identifikationsprozesse in hohem Masse von Vertrauen abhängig und müssen vertrauensvoll durchgeführt werden. Dieser Prozess beinhaltet beispielsweise die digitale Überprüfung, ob ein Subjekt ist, was es behauptet zu sein, ob eingegebene Authentikatoren valide sind und ob diese zur Nutzung von Dienstleistungen berechtigen. Die meisten digitalen Identifikationssysteme verifizieren eine Identität auf Basis von mehreren Faktoren: Etwas, das man ist (z.B. biometrische Merkmale), etwas, das man hat (z.B. einen digitalen Schlüssel) oder etwas, das man weiss (z.B. ein Passwort) [Treiblmaier und Beck 2019, S. 240-241]. Digitales Identitätsmanagement kann als Sammlung von Regeln, Prozeduren und technischen Mitteln verstanden werden, welche zur Ausstellung, Nutzung und zum Austausch von digitalen Identitätsinformationen eingesetzt werden, um auf digitale Dienstleistungen oder Ressourcen zugreifen zu können [Lips 2010, S. 276].

Wie die erste Einordnung der digitalen Identität zeigt, lässt sich diese exakter als der Begriff der allgemeinen Identität definieren. Digitale Identität ist primär maschinenbezogen und maschinengebunden [Zwitter et al. 2020, S. 2]. Es handelt sich bei einer digitalen Identität zusammengefasst um eine Entität, welcher Attribute zugewiesen werden. Diese Entität kann im digitalen Raum identifiziert werden und als Transaktions-Ermöglicher agieren. Dennoch unterliegt der Begriff der digitalen Identität einer eigenen Ambiguität.

Einerseits kann digitale Identität ein einfaches, anonymes und pseudonymisiertes Log-in im Sinne einer Authentifizierungsmethode beschreiben. Eine digitale Identität bestehend aus der Kombination eines pseudonymisierten Benutzernamens und eines Passworts kann als Identifikation ausreichen, um Zugriff auf digitale Dienstleistungen zu erhalten. Dabei kann die wahre Identität der agierenden Entität (Mensch oder Maschine) oftmals auch geheim gehalten werden, wie Peter Steiner bereits 1993 in seinem Cartoon [Fleishman 2000] treffend feststellte: „*On the Internet, nobody knows you're a dog.*“. Andererseits ist dem Konzept der digitalen Identität auch ein

Äquivalenzstatus zu einem staatlich anerkannten Ausweisdokument inhärent. Die vorgängige Auslegung des Begriffs als Benutzer-Passwort-Log-in unterscheidet sich grundlegend davon, wie wir Identität in der physischen Welt interpretieren und handhaben [Toth und Anderson-Priddy 2019, S. 18; Sullivan 2016, S. 475]. Im Gegensatz zum digitalen Raum basieren Transaktionen in der physischen Welt auf der Prämisse, dass eine Person legitimerweise genau eine Identität besitzt. Treiblmaier und Beck [2019, S. 234-235] beschreiben unter diesem Gesichtspunkt die digitale Identität als eine einem Individuum eindeutig zugewiesene und einzigartige Identität. Diese wird typischerweise staatlich ausgegeben und reguliert. Sie vereint verschiedenste Informationen eines physischen Ausweisdokuments, wird aber digital gespeichert und transferiert. In dieser Form ist die digitale Identität als eine dem physischen Ausweisdokument in Form eines Passes gleichwertige Identifikationsmöglichkeit zu betrachten.

Im weiteren Verlauf dieser Forschungsarbeit wird die digitale Identität hauptsächlich unter dem Aspekt der Blockchain-Technologie behandelt. An dieser Stelle wird deshalb auf die Chancen und Risiken der Umstellung von physischen Identitätsformen auf digitale Identitätsformen im Allgemeinen eingegangen. Die Digitalisierung der Identität birgt sowohl generelle Cybersicherheitsrisiken, welche für praktisch alle technologischen Produkte und Dienstleistungen gelten als auch spezifisch auf die digitale Identität bezogene Risiken. Die folgende, nicht abschliessende Auflistung behandelt die typischen Risiken einer digitalen Identität.

*Datensicherheit:* Bei Identitätsdaten handelt es sich um persönliche Daten und damit um besonders schützenswerte Daten. Digitale Ökosysteme müssen einem stetig wachsenden Risiko von Cybersecurity-Risiken unterschiedlichster Art begegnen und digitale Identitätssysteme stellen keine Ausnahme dar [McKinsey Global Institute 2019, S. 80; Dunphy und Petitcolas 2018, S. 20]. Diese inhärenten Gefahren digitaler Systeme betreffen Individuen beispielsweise durch unautorisierte Zugriffe auf persönliche Daten oder Institutionen durch unautorisierte Datenlecks in Form von Cyberattacken [McKinsey Global Institute 2019, S. 80]. Digitale Identitätsdaten und -systeme sind daher mindestens im selben Masse gegen allgegenwärtige Gefahren der technologischen Welt zu schützen, wie jegliche anderen Daten oder Systeme.

*Transaktionssicherheit:* Zusätzliche Risiken ergeben sich im digitalen Raum, wenn digitale Dienstleistungen aus der Ferne über Kanäle wie das Internet angeboten und genutzt werden. Die Transaktion von Identitätsdaten über ein digitales Netzwerk bietet Angreifern zusätzliche Möglichkeiten, diese Daten abzugreifen, zu manipulieren oder unautorisiert selbst zu verwenden [Grassi et al. 2017, S. iv]. Auch bereits Metadaten über die Existenz einer Transaktion können bei eindeutig identifizierenden Daten über ein enormes Schadenspotenzial verfügen. Denkbar ist beispielsweise ein Szenario, in welchem eine Person in einer Suchtklinik ihre digitale ID vorzeigt. Wird diese Transaktion des digitalen Vorzeigens der ID in einem System

protokolliert, so können theoretisch indirekt sensible Gesundheitsinformationen über eine Person gewonnen werden. Hier besteht ein fundamentaler Unterschied zu rein analogen Ausweisdokumenten, welche beim Vorzeigen oftmals keine Daten hinterlassen.

*Datenintegrität:* Hochsensible Personendaten, welche im Rahmen von Identitätsnachweisen allgegenwärtig sind, sind in hohem Masse von der Genauigkeit und Integrität der erfassten Daten abhängig. Allerdings sind digitale Systeme verwundbar gegenüber Fehlern bei der Datenerfassung oder Datenübertragung, wodurch die Integrität von Identitätsdaten gefährdet sein kann [Sullivan 2016, S. 475]. Obwohl digitale Systeme die Wahrscheinlichkeit von menschlichen Fehlern in der Datenhandhabung minimieren können, unterliegt die digitale ID und deren Integrität menschlichem Fehlerpotenzial [McKinsey Global Institute 2019, S. 82-83].

*Verfügbarkeit:* Die Infrastruktur, auf welcher eine digitale ID basiert, kann technischen Problemen oder Ausfällen unterliegen. Technische Störungen können auf der Hardware-Ebene (physische Komponenten) oder Software-Ebene (Programme und Betriebssysteme) eines digitalen ID-Systems auftreten, aber auch durch Ausfälle der Elektrizitäts- und Internet-Infrastruktur begründet sein [McKinsey Global Institute 2019, S. 77-79]. Auch Angriffe auf ID-Systeme oder deren tragende Infrastruktur besitzen Risikopotenzial. Durch technische Störungen kann die Möglichkeit für Anwender:innen, auf ihre digitale ID zuzugreifen, diese zu kontrollieren oder zu teilen, limitiert werden. Dies betrifft auch die eine digitale ID anfordernden Parteien, welche auf einwandfrei funktionierende ID-Systeme angewiesen sind, um Identitätsdaten erhalten und validieren zu können. Im Gegensatz zu analogen Identitätsdokumenten ist im Fall einer technischen Störung die Identifikation nicht mehr möglich. Damit können Individuen potenziell auf unbestimmte Zeit von wichtigen Dienstleistungen ausgeschlossen sein.

*Missbrauchspotenzial:* Wie andere technische Innovationen kann eine digitale ID aus ethischer Sicht korrekt und wertbringend oder aber missbräuchlich und schädigend eingesetzt werden [McKinsey Global Institute 2019, S. 31]. Kriminell motivierte Einzelpersonen oder Gruppen, welche bei Anbieter:innen von digitalen Identitätslösungen angestellt sind, können potenziell durch Administrationsrechte missbräuchlich mit Identitätsdaten umgehen [McKinsey Global Institute 2019, S. 81]. Besonders kritisch ist das Missbrauchspotenzial im Rahmen des Identitätsdiebstahls. Dabei können sich Personen im digitalen Raum als eine andere Person ausgeben, da sie über deren Identitätsdaten (illegalerweise) verfügen. Wenn im digitalen Raum per Definition unveränderbare biometrische Identifikationsmerkmale wie Fingerabdrücke zum Einsatz kommen, erhöht sich das Missbrauchsrisiko weiter [McKinsey Global Institute 2019, S. 82-83].

*Machtkonzentration:* Ein anders gelagertes Missbrauchspotenzial birgt eine mit digitalen ID-Systemen potenziell einhergehende Machtkonzentration. Die Digitalisierung und zentralisierte Speicherung von Identitätsdaten stellt ID-Anbieter:innen eine enorme Menge an persönlichen Informationen über Individuen bereit. Dies gilt insbesondere, wenn die digitale ID als staatliches Ausweisdokument für sämtliche Bürger:innen interpretiert wird. Bei solch tiefgreifenden Vorhaben zur Einführung der digitalen ID entsteht in Form der digitalen ID-Systeme eine beispiellose Sammlung von Identitätsdaten [McKinsey Global Institute 2019, S. 31]. Firmen oder Behörden in Besitz der Daten gewinnen dadurch sowohl Macht als auch Verantwortung, was saubere Kontrollmechanismen und robuste Governance im Umgang mit diesen Daten unabdingbar macht [McKinsey Global Institute 2019, S. 82]. Wo mit analogen Identitätsnachweisformen noch eine natürliche Grenze einherging, wie effizient, rasch und eindeutig die Identität von Individuen festgestellt werden konnte, ergeben sich durch die digitalisierte ID neue Möglichkeiten [McKinsey Global Institute 2019, S. 31]. Die Kontrollmöglichkeiten von Institutionen, welche durch effiziente digitale IDs Überwachung, politische Kontrolle oder auch Exklusion von Individuen neu manifestieren könnten, vervielfachen sich. Sullivan [2016, S. 475-476] schreibt der digitalen ID das Potenzial zu, die Balance von Verantwortlichkeit, Rechenschaft und Haftung zwischen Regierungen und Bürger:innen fundamental zu verändern. Für Dunphy und Petitcolas [2018, S. 20] steht auf der Risikoseite primär der mögliche Mangel an Kontrolle und Besitz über die eigenen digitalen Identitätsdaten für die Nutzer:innen im Zentrum.

Trotz dieser Vielzahl von Risiken bringt eine digitale ID auch enorme Chancen mit sich. Die digitale ID und neue Technologien, welche die digitale ID ermöglichen, verfügen über das revolutionäre Potenzial, das Hauptmittel künftiger kommerzieller und behördlicher Transaktionen zu werden [Dunphy und Petitcolas 2018, S. 20; Sullivan 2016, S. 475; Treiblmaier und Beck 2019, S. 235-236]. Chancen der digitalen ID zeigen sich hauptsächlich in den nachfolgend dargelegten Aspekten.

*Digitale Welt der Zukunft:* In hochgradig digitalisierten Ländern und Gesellschaften sind vollständig oder partiell digitale Dienstleistungen und Prozesse allgegenwärtig. Geht man davon aus, dass sich der Digitalisierungstrend sämtlicher Lebensbereiche künftig noch weiter verstärken wird, muss sich auch der Bereich der Identitätsnachweislösungen anpassen. Ohne digitale ID sind die vollständigen Potenziale der durchdringenden Digitalisierung nur begrenzt nutzbar [Deloitte 2022]. Eine digitale ID verkörpert den Katalysator für zahllose Anwendungsbereiche einer tiefgreifend digitalisierten Welt für Regierungen, Behörden, Bank- und Versicherungsgeschäfte, Handel, Tourismus, Arbeitsmarkt, Gesundheit und viele weitere Bereiche [PricewaterhouseCoopers 2022]. Auch die digitale Demokratie der Gegenwart und Zukunft stellt einen Bereich dar, welcher von einer digitalen ID stark profitieren könnte.

*Ökonomischer Mehrwert:* Eine der zentralsten Chancen einer digitalen ID liegt in Effizienz- und Produktivitätssteigerungen sowie in Kosteneinsparungen. Die digitale ID verspricht das Potenzial einer global betrachtet durchschnittlich möglichen Steigerung des Bruttoinlandsprodukts (BIP) von rund 6 % pro Land bis 2030 [McKinsey Global Institute 2019, S. 51]. Der Nachweis einer Identität durch eine Identitätsnachweislösung im digitalen Raum erlaubt es, vollständig digitale Dienstleistungen und Produkte effizient anbieten und nutzen zu können, ohne dass die physische Präsenz einer Person notwendig ist [Klenk 2022]. Viele manuelle und zeitintensive Schritte, welche die Verwendung von analogen Identitätsdokumenten mit sich bringt, entfallen. Als klassisches Beispiel gilt die Eröffnung eines Kontos bei einer Bank als Prozess, welcher mithilfe einer digitalen ID vollständig digital und ohne Notwendigkeit einer weiteren Identifikationsprozedur (z.B. das Senden eines Scans eines physischen Ausweisdokuments oder das Zeigen des Gesichts via Webcam) auskommen würde. Ein rein digitaler Prozess zum Identitätsnachweis steigert so die Effizienz für alle in den Prozess involvierten Subjekte. Außerdem kann ein digitaler Identitätsnachweis durch Vereinfachung und Aufwandsminderung des Identifikationsprozesses die Nutzungshürden von Dienstleistungen senken [McKinsey Global Institute 2019, S. 1].

*Neue Geschäftsmodelle:* Durch eine digitale ID kann eine Identitätsinfrastruktur aufgebaut werden, in welcher die Identität eine eigenständige Ebene im Internet-Ökosystem darstellt. Zusätzlich zum ökonomischen Mehrwert in Form von Effizienz- und Produktivitätssteigerung ist es vorstellbar, dass eine digitale ID vollständig neue Produkte, Dienstleistungen und Geschäftsmodelle ermöglicht [McKinsey Global Institute 2019, S. 51].

*Benutzer:innenfreundlichkeit:* Grundsätzlich digital konzipierte Prozesse, welche eine Identifikation der amtlichen Identität von Benutzer:innen voraussetzen, sind mit den heutigen ID-Lösungen umständlich. Sie bedürfen oftmals einer Kombination von digitalen und analogen Unterprozessen, wobei der Teil des Identitätsnachweises kaum ohne analoge Schritte erfolgen kann. Darunter leidet die Benutzer:innenfreundlichkeit von digitalen Transaktionen zwischen Anbieter:innen und Kund:innen. Gemäß Klenk [2022] haben aktuelle Studien gezeigt, dass zwei von drei Personen bei Online-Registrierungen mit Identitätsnachweisen den Prozess vorzeitig abbrechen. Die Gründe dafür liegen im Registrierungsprozess, welcher zu zeitaufwändig, beschwerlich und schwerfällig ist. Für künftige, vollständig digitale Dienstleistungen ist es wichtig, dass Identifikationsprozesse einfach und intuitiv ablaufen und die Benutzer:innenfreundlichkeit steigt. Die digitale ID kann bei entsprechender Umsetzung die nahtlose Integration von Identifikationsprozessen im digitalen Raum erlauben.

*Transparenz, Vertrauen und Sicherheit:* Trotz der Risiken, welchen die meisten Technikinnovationen unterliegen, ergibt sich aus einer digitalen ID auch das Potenzial, Transparenz, Vertrauen und Sicherheit zu fördern [McKinsey Global Institute 2019, S. 82-83]. Stärkere Formalisierung in digitalen Identifizierungsprozessen kann zur Verringerung von Betrug, zum Schutz von Rechten und zur Erhöhung der Transparenz beitragen [McKinsey Global Institute 2019, S. 1]. Obwohl in der Gegenwart physische ID-Lösungen noch geläufiger sind, stossen diese allmählich an ihre Grenzen [Ho 2021]. Mit heutigen technologischen Mitteln wird es immer einfacher, analoge ID-Lösungen zu manipulieren oder illegal zu erwerben. Wenn die Digitalisierung der Welt weiter in hohem Tempo voranschreitet, werden nach Ho [2021] nationale Programme für digitale ID's zur künftig weiterhin sicheren und schnellen Identifikation unumgänglich. Auch Camp [2004, S. 35] vertritt diese Ansicht. Die Konzepte und organisatorischen Modelle papierbasierter Identifikationssysteme schaffen gefährliche Fehlermöglichkeiten, wenn sie auf digitale Identitäten angewendet werden. Digitale ID bedeutet auch, bürgerliche Freiheiten zu schützen und die Kontrolle über persönliche Daten dorthin zurückzubringen, wo sie hingehört: In die Hände des Individuums [Identity2020 Systems 2022b]. Bestimmte Arten von technischer Implementation lassen mehr oder weniger Kontrolle über die eigenen Identitätsdaten zu. Grundsätzlich sind digitale ID-Lösungen denkbar, welche das Konzept der *Self-Sovereign Identity*, also einer vollständig selbstbestimmten Identität, ermöglichen.

*Inklusion:* Inklusion durch die digitale ID steht unter anderem auf der Agenda von Nichtregierungsorganisationen wie der *Identity2020 Systems Inc.*, welche sich nach eigenen Angaben für ethische, die Privatsphäre schützende Ansätze für die digitale Identität einsetzt [Identity2020 Systems 2022a]. Etwa eine Milliarde Menschen weltweit besitzen keine amtlich anerkannte Form von Identifikationsausweisen [McKinsey Global Institute 2019, S. 23]. Die digitale Identität kann künftig mehr Menschen ermöglichen, Zugang zum gesellschaftlichen und wirtschaftlichen Leben zu erhalten [Identity2020 Systems 2022b; Ho 2021]. Dazu gehört auch, Rechte als Bürger:innen und Wähler:innen wahrzunehmen und an der modernen Demokratie teilnehmen zu können [Identity2020 Systems 2022b]. Digitale ID-Systeme auf nationaler Ebene sind nach Klenk [2022] der erste Schritt zum Aufbau einer digital inklusiven Gesellschaft.

Wie die vorgenommene Einordnung des Begriffs der digitalen Identität zeigt, ist die Entwicklung und Einführung von digitalen ID-Lösungen in der antizipierten Welt und Gesellschaft der Zukunft nahezu unumgänglich. Um jedoch von den Chancen der digitalen Identität tatsächlich profitieren zu können, muss den damit einhergehenden Risiken durch qualifizierte und zweckmässige technische Konzeption begegnet werden.

### 2.1.3 Blockchain-Technologie

Der Kunstbegriff *Blockchain* beschreibt eine Technologie, welche Informationen als Kette (*Chain*) von Blöcken (*Block*) darstellt [Rauschenbach und Stucki 2020, S. 7]. Ihren Ursprung hat die Blockchain als die der digitalen (Krypto-)Währung *Bitcoin* zugrunde liegende Technologie, welche inmitten der Finanzkrise 2008 publiziert wurde [Ammous 2016, S. 1; Poblet et al. 2020, S. 1]. Als Schöpfer:in von Bitcoin und dem zugehörigen Blockchain-Protokoll gilt das Pseudonym *Satoshi Nakamoto*. Die hinter diesem Pseudonym stehende Person ist bis heute unbekannt. Lediglich einige Beiträge in einschlägigen Technikforen sowie ein Whitepaper mit dem Titel „*A Peer-to-Peer Electronic Cash System*“ [Nakamoto 2008] bilden die Grundlage all dessen, was der Bitcoin und die Blockchain-Technologie seit mehr als einem Jahrzehnt in der Welt bewegt haben.

Nakamoto [2008] beschreibt in diesem Whitepaper ein Peer-to-Peer-Konzept von elektronischem Geld. Das Konzept erlaubt es, Onlinezahlungen direkt von einer Partei zur anderen zu senden, ohne dass eine Drittpartei wie ein Finanzinstitut dazwischengeschaltet ist. Es basiert auf einem (internetbasierten) Netzwerk, in welchem Transaktionen zeitgestempelt durch sogenanntes *Hashing* (kryptografische Prozesse) an eine endlose Kette angegliedert werden. Geschichtlich betrachtet basiert die Blockchain-Technologie auf dem TCP/IP-Protokoll von 1974, welches bereits als Grundbaustein des Internets agiert [Pilkington 2016, S. 227]. Die neuartige Blockchain-Technologie gilt seit einigen Jahren als die potenziell wichtigste Erfindung seit der Erfindung des Internets selbst [Crosby et al. 2016, S. 8; Efanov und Roschin 2018, S. 116-120]. Während nach Efanov und Roschin [2018, S. 116-120] das Internet ermöglicht hat, digitale Geschäftsprozesse zu realisieren, könnte die Blockchain-Technologie das sogenannte *Problem of Trust* (Vertrauensproblematik) bei digitalen Transaktionen lösen und damit sämtliche Sphären unseres Lebens beeinflussen.

Die Blockchain-Technologie selbst befindet sich in praktischen Anwendungen allerdings noch immer in der Pionierphase und der Bitcoin stellt laut Treiblmaier und Beck [2019, S. 341] einen seltenen Fall dar, in welchem die praktische Anwendung der Theorie voraus zu sein scheint. Die Begriffe Blockchain und Bitcoin sind im Allgemeinverständnis der Gesellschaft eng miteinander verknüpft. Dennoch ist eine Unterscheidung zwischen dem Anwendungszweck einer digitalen Währung (Bitcoin) und der grundlegenden Technologie (Blockchain) essenziell. Obwohl die Blockchain-Technologie ursprünglich dazu entwickelt wurde, die Kryptowährung Bitcoin zu ermöglichen, sind die Potenziale der Blockchain als eigenständige technologische Entwicklung deutlich weitreichender [Ahram et al. 2017, S. 3; Biswas und Muthukumaraasamy 2016, S. 1392; Poblet et al. 2020, S. 1-2].

Die Blockchain-Technologie gilt als Technologie mit dem Versprechen, die digitale Welt zu revolutionieren [Ahram et al. 2017, S. 1; Underwood 2016, S. 15; Prashanth Joshi et al. 2018, S. 339]. Begründet wird diese Prognose durch eine zentrale Eigenschaft der Blockchain-Technologie: Sie gilt als Vertrauensmaschine (*Trust Machine*) [Poblet et al. 2020, S. 2]. Das Kernmerkmal der Blockchain-Technologie ist die Fähigkeit, sämtliche Transaktionen auf einer Datenbank in Form von aneinandergereihten Datenblöcken nachvollziehen zu können und damit vollständig vertrauensvolle Transaktionen ohne menschliche Überwachungs- und Kontrollnotwendigkeit zu ermöglichen [Efanov und Roschin 2018, S. 116-117]. Die absolute Immutabilität von Transaktionen auf einer Blockchain, also deren Widerstandsfähigkeit gegenüber Manipulationsversuchen, ermöglicht der Technologie, ohne Drittpartei zwischen zwei Parteien Authentizität zu proklamieren [Pilkington 2016, S. 234].

Die Glaubwürdigkeit dieses Versprechens der Blockchain-Technologie beweist die Blockchain-Anwendung Bitcoin dadurch, dass seit ihrer Einführung bis heute die Immutabilität gewährleistet ist [Pilkington 2016, S. 234]. Transaktionsprozesse auf einer Blockchain sind transparent, rückverfolgbar und manipulationssicher, womit durch die Nutzung einer Blockchain ein robustes Vertrauenssystem aufgebaut werden kann [Yang und Li 2020, S. 5]. Die Nutzung eines Vertrauenssystems ist auf ein breites Spektrum anwendbar. Es ermöglicht eine sichere Methode, um Güter, Dienstleistungen, Verträge oder Informationen jeglicher Art auszutauschen und dadurch neue, globale Netzwerke und Geschäftsmodelle aufzubauen [Ahram et al. 2017, S. 1-5; Underwood 2016, S. 15].

Bevor im Rahmen dieser Begriffseinordnung auf spezifische Einsatzbereiche der Blockchain eingegangen wird, wird im Folgenden die generelle Funktionsweise der Blockchain aus technischer Sicht beschrieben. Welche technologischen Eigenschaften der Blockchain geben ihr das Potenzial, eine Vertrauensmaschine zu sein? Eine Blockchain ist grundsätzlich eine digitale Datenbank, welche Datenbankeinträge validiert und diese Einträge mit sämtlichen Teilnehmenden der Datenbank teilt [Bakre et al. 2017, S. 381; Efanov und Roschin 2018, S. 116-117]. Diese Datenbank, auch *Ledger* genannt, wird im Kontext von Blockchain häufig als dezentrale und öffentliche Datenbank verstanden. Jedes digitale Gerät, welches am Blockchain-Netzwerk teilnimmt, wird als *Node* oder Knotenpunkt bezeichnet und enthält eine Kopie der aktuellen Blockchain-Datenbank [Crosby et al. 2016, S. 8; Prashanth Joshi et al. 2018, S. 122]. Wichtig ist zu beachten, dass es nicht *die eine* Blockchain gibt, sondern sich beliebig viele Blockchain-Datenbanken für unterschiedlichste Einsatzzwecke entwickeln und betreiben lassen.

Informationen werden in einer Blockchain in Form von Blöcken gespeichert und jede Transaktion zwischen zwei Blockchain-Teilnehmenden wird sämtlichen anderen Teilnehmenden (Nodes) der Blockchain angekündigt, von diesen verifiziert und in einen neuen Block eingeschrieben [Ammous 2016, S. 1; Crosby et al. 2016, S. 8]. Die Besonderheit ist dabei, dass in einer Blockchain jeder neue Block in einer linearen, chronologischen Reihenfolge an den vorgängigen Block angehängt wird, wodurch eine Kette von Datenblöcken entsteht [Crosby et al. 2016, S. 10; Hou 2017, S. 1]. Dieser Prozess resultiert in einer immer weiter wachsenden Liste oder Kette von Transaktionseinträgen in Form von Blöcken. In einem Block kann jeder Sachverhalt und somit jede beliebige Art von Daten festgeschrieben werden. Die Blöcke werden durch kryptografische Verfahren untrennbar miteinander verknüpft, da in jedem zusätzlichen Block ein Fingerabdruck (Hash) des vorgängigen Blocks festgeschrieben ist [Rauschenbach und Stucki 2020, S. 7; Prashanth Joshi et al. 2018, S. 125]. Wird ein Block an einer beliebigen Position der Kette nachträglich manipuliert, so fällt dies durch Abweichungen in den umliegend berechneten Hashes sofort auf.

So entsteht eine Blockchain-Datenbank, welche vertrauenswürdige, verifizierbare Einträge sowie gleichzeitig auch ein Buchungskonto sämtlicher je getätigter Transaktionen festhält, ohne dass eine separate Dokumentation notwendig ist [Crosby et al. 2016, S. 8; Prashanth Joshi et al. 2018, S. 122]. Die Transaktionen sind durch die technologischen Eigenschaften einer Blockchain manipulations-offenbarend sowie manipulationssicher und erlauben durch dezentrale Implementationsweise absolutes Vertrauen zwischen zwei Parteien ohne zentrale Autorität (bspw. eine Bank, Firma oder Behörde) [Yaga et al. 2018, S. iv]. Abb. 1 auf der nächsten Seite zeigt schematisch den Ablauf einer Transaktionsbuchung auf einer Blockchain.

Damit dieses Prinzip des Vertrauens funktioniert, muss der Prozess der Generierung, Validierung, Integration und Speicherung von Datenblöcken mit modernsten kryptografischen Methoden gesichert sein. Transaktionen auf einer Blockchain basieren auf durch Kryptografie garantierter Wahrheit [Crosby et al. 2016, S. 9]. Einfach erklärt basieren die eingesetzten kryptografischen Verfahren darauf, dass die mathematischen Verschlüsselungsprozesse relativ leicht lösbar sind, deren Umkehroperationen, also die Entschlüsselung, durch reines Ausprobieren beinahe unlösbar sind (sog. *Trapdoor functions*) [Pilkington 2016, S. 228].

Dieses kryptografische Absicherungskonzept wird *Public Key Cryptography* (PKC), *Public Key Infrastructure* (PKI) oder *asymmetrische Verschlüsselung* genannt [Sovrin Foundation 2018, S. 7; Ledger Academia 2019]. Asymmetrische Verschlüsselung beruht auf einem Zwei-Schlüssel-Modell, dem öffentlichen (public) und dem privaten (private) Schlüssel, die häufig durch ein Vorhängeschloss (öffentlicher Schlüssel) und den eigentlichen Schlüssel für den Zugang zum Vorhängeschloss (privater Schlüssel) repräsentiert werden (vgl. Abb. 2 auf Seite 17).

## 2 THEORETISCHER TEIL

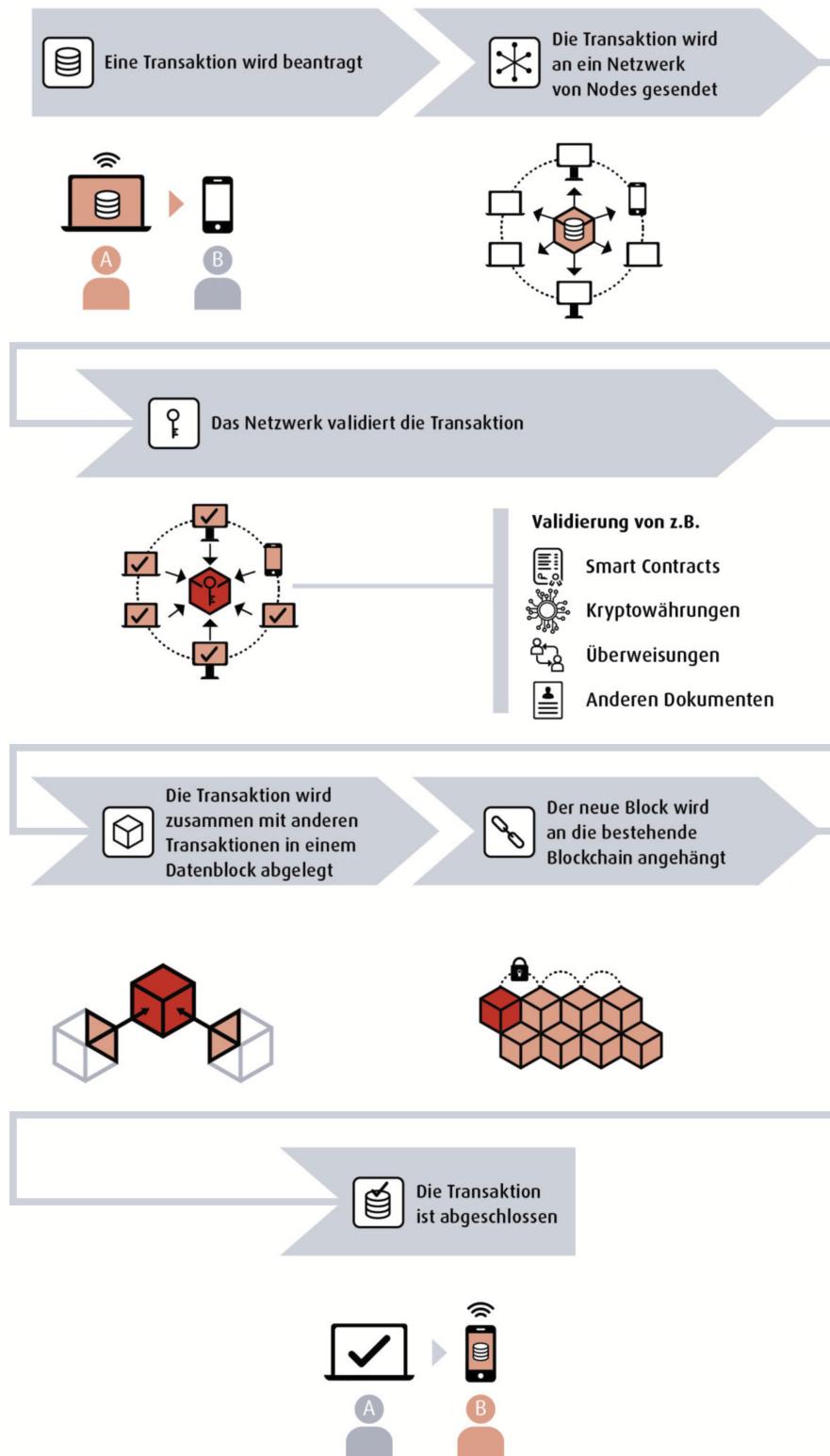


Abbildung 1: Funktionsweise der Blockchain schematisch erklärt [Schweizerischer Baumeisterverband 2020], bearbeitet.

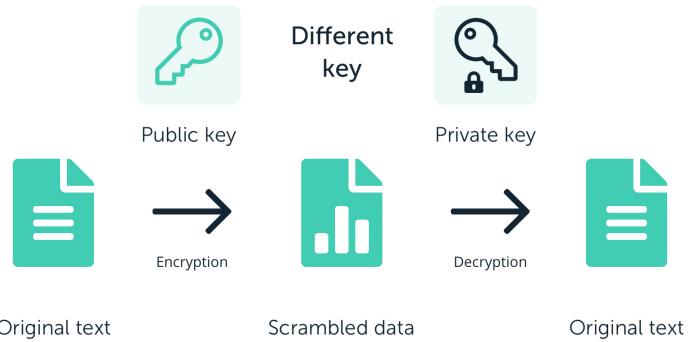


Abbildung 2: Asymmetrische Verschlüsselung schematisch erklärt  
[Ledger Academia 2019].

Das Ziel von öffentlichen und privaten Schlüsseln ist es, zu beweisen, dass eine getätigte Transaktion tatsächlich vom Eigentümer der Daten unterzeichnet wurde und nicht gefälscht ist. Wenn man einen Block aus Daten in einer Blockchain besitzt, ist das, was man wirklich besitzt, ein privater Schlüssel. Der private Schlüssel gewährt das Recht, über den zugehörigen Datenblock zu verfügen. Da er den Zugang zu eigenen Daten ermöglicht, sollte er privat bleiben. Es ist möglich, den öffentlichen Schlüssel wiederherzustellen, wenn man den privaten Schlüssel besitzt. Es ist jedoch unmöglich, den privaten Schlüssel nur mit Hilfe des öffentlichen Schlüssels zu eruieren (vgl. Abb. 3).



Abbildung 3: Trapdoor function von Schlüsseln bei asymmetrischer Verschlüsselung  
[Ledger Academia 2019].

Damit die kryptografisch gesicherte Angliederung von Blöcken für alle Nodes vertrauenswürdig ist, benötigt eine Blockchain weiter Regeln darüber, wie neue Blöcke an die bestehende Kette angehängt werden dürfen. Diese sogenannten *Konsensregeln* legen Prinzipien darüber fest, welche Node einen nächsten Block berechnen und erzeugen darf [Crosby et al. 2016, S. 11; Rauschenbach und Stucki 2020, S. 10]. Die heutzutage gängigsten Konsensregeln sind *Proof-of-Work* und *Proof-of-Stake*: Bei Proof-of-Work wird Konsens durch über grosse Rechenleistung zu lösende, komplexe mathematische Probleme hergestellt [Rauschenbach und Stucki 2020, S. 11 ff.; Pilkington 2016, S. 229]. Dieser Rechenprozess wird als *Mining* bezeichnet und kann von allen teilnehmenden Nodes durch die Zurverfügungstellung von Rechenleistung ausgeführt werden. Welche Node einen nächsten Block berechnen darf, hängt von diversen Faktoren ab, welche für diese Forschungsarbeit keine Relevanz besitzen.

Die Rechenprozesse des Minings gehen durch die Lösung der mathematischen Probleme mit erheblichen Kosten in Form von Energieverbrauch einher. Darin liegt auch die in der Öffentlichkeit häufig geäusserte Kritik begründet, nach derer Blockchain-Anwendungen ökologisch nicht vertretbar sein sollen. Doch genau dieser hohe Energieaufwand zur kryptografischen Absicherung der Blockchain-Einträge macht Proof-of-Work-Blockchains derart sicher. Eine Blockchain akzeptiert immer nur die längste Kette als die ‚wahre‘ Kette. Wenn ein Angreifer nun eine missbräuchliche Transaktion tätigen möchte, müsste dieser nicht nur den eigenen Block berechnen, sondern auch das mathematische Rennen gegenüber allen anderen Nodes und deren kumulierter Rechenleistung im Netzwerk gewinnen (eine sog. *51 %-Attacke*). Dies ist bei dezentral verteilten Blockchains mit tausenden von Nodes beinahe ausgeschlossen [Crosby et al. 2016, S. 13].

Proof-of-Work eignet sich hauptsächlich für Daten, welche nicht schützenswert sind und öffentlich einsehbar sein können. Proof-of-Stake eignet sich sowohl für schützenswerte als auch für nicht schützenswerte Daten, welche ebenfalls öffentlich einsehbar sein dürfen [Rauschenbach und Stucki 2020, S. 11 ff.; Pilkington 2016, S. 229]. ‚Schützenswert‘ ist in diesem Kontext als Daten- und Persönlichkeitsschutz zu verstehen. Im Gegensatz zu Proof-of-Work wird bei Proof-of-Stake von den Parteien, die einen neuen Block anlegen wollen, ein Vermögenswert als Garantie gegen Regelverstöße hinterlegt. Im Umkehrzug müssen von den Nodes weniger komplexe und rechenintensive Probleme gelöst werden. Der Prozess bei Proof-of-Stake hat im Vergleich zu Proof-of-Work zwar eine theoretisch mögliche Reduktion der Sicherheit zur Folge, mindert den Energieaufwand zur Berechnung eines neuen Blocks allerdings enorm.

Neben diesen beiden Konsensregeln existiert eine Vielzahl weiterer Regeln. Deren ausführliche Behandlung ist im Rahmen dieser Thesis nicht relevant. Erwähnenswert für schützenswerte Daten, welche nicht öffentlich einsehbar sein dürfen, ist die Konsensregel *Proof-of-Authority* [Rauschenbach und Stucki 2020, S. 11 ff.]. Bei dieser Konsensregel bestehen klare Berechtigungen und Kontrollmöglichkeiten darüber, wer einen neuen Block schürfen und an die Blockchain anhängen darf. Somit kann sich *Proof-of-Authority* beispielsweise auch für sensible Daten wie Identitätsdaten in einer Blockchain eignen.

Wie zuvor beschrieben, wird eine Blockchain häufig als dezentrale und öffentliche Datenbank verstanden. Der Bitcoin basiert beispielsweise auf einer Blockchain, welche das Öffentlichkeitsprinzip radikal umsetzt [Rauschenbach und Stucki 2020, S. 9]. Konsensregeln wie *Proof-of-Authority* zeigen allerdings, dass auch die Erstellung von vollständig privaten und zentralen Blockchains möglich ist. Blockchain sollte somit nicht als Synonym für einen rein dezentralen und öffentlich einsehbaren Kontext betrachtet werden. Neben öffentlichen Blockchains, welche öffentlich

einsehbar sind und allen zur Partizipation offen stehen, existieren auch private Blockchains, welche nicht öffentlich einsehbar sind und bei welchen teilnehmende Nodes selektiv ausgewählt werden [Bakre et al. 2017, S. 381; Pilkington 2016, S. 234; Prashanth Joshi et al. 2018, S. 130-131]. Transparenz in Form von Leserechten und Partizipation in Form von Schreibrechten können je nach Blockchain-Implementation und Kontext der Daten frei gewählt werden [Rauschenbach und Stucki 2020, S. 9]. Auch hybride Formen sind möglich [Pilkington 2016, S. 231].

Wie die technische Einordnung zeigt, bietet die Blockchain-Technologie durch ihre einzigartigen Eigenschaften das Potenzial für beinahe unbegrenzt scheinende Einsatzzwecke. Autor:in Underwood [2016, S. 15] spricht von revolutionären Möglichkeiten in den Bereichen Identität, Eigentum, finanzieller Inklusion und Krisenprävention, Gesundheitssystem, Supply Chain oder auch ethischem Geschäftsverhalten. Ammous [2016, S. 2-3] sieht Potenzial in den Bereichen digitale Zahlungsabwicklung, Verträge und Dokumentenverwaltung. Efanov und Roschin [2018, S. 120] beschreiben Anwendungszwecke in den Bereichen Kryptowährungen, Smart-Contracts, Smart Cities, digitale Patientenakten, digitale Identität, Reputationssysteme und dem *Internet of Things*. Auch Einsatzbereiche innerhalb der öffentlichen Verwaltung werden in der Literatur behandelt [Prashanth Joshi et al. 2018, S. 121-122; Rauschenbach und Stucki 2020]. Die derzeitige Aufteilung der globalen Anwendungsbereiche von Blockchains unterteilt sich in Zahlungsverkehr (15.9 %), Grundstücksverwaltung (10.7 %), Handel (10 %), Güterverwaltung (8.8 %), Identitätsmanagement (7.6 %) sowie einer Vielzahl weiterer Anwendungsbereiche (47 %) [Statista Inc. 2022]. Wie diese Statistik zeigt, machen Einsätze einer Blockchain im Kontext des Identitätsmanagements bereits einen grösseren Teil aller Anwendungsbereiche aus.

Ziel dieser kurzen Einführung zur Blockchain ist es, einen einfach verständlichen und dennoch der technischen Komplexität gerecht werdenden Einblick in die Blockchain-Technologie zu ermöglichen. Auch Leser:innen, welchen zuvor der Begriff *Blockchain* vollständig unbekannt war, sollten sich eine generelle Idee darüber verschaffen können, was die Blockchain-Technologie ist und wie sie grundlegend funktioniert. Eine perfekte Balance zwischen Verständlichkeit für Personen, welche sich zum ersten Mal mit der Blockchain befassen, und dem Abbilden der unterliegenden technologischen Komplexität zu finden, ist eine Herausforderung. Für Leser:innen, welche sich gerne tiefgreifender mit der Blockchain-Technologie befassen möchten, wird an dieser Stelle das ausgezeichnete Buch „*Bitcoin, Blockchain und Kryptoassets: Eine umfassende Einführung*“ von Berentsen und Schär [2017] empfohlen, welches u.a. im Universitätsverlag *MIT Press* veröffentlicht wurde und in deutscher und englischer Sprache verfügbar ist.

### 2.1.4 Digitale Demokratie & Krypto-Demokratie

Der Begriff der *digitalen Demokratie* ist ein nicht eindeutig definierter Dachbegriff und referenziert nach Poblet et al. [2020, S. 6] eine Form von Demokratie, in welcher digitale Instrumente verschiedenste demokratische Prozesse der Partizipation von Bürger:innen unterstützen. Im Fokus steht dabei der Einsatz von informations-technologischen Mitteln. Wie bereits bei der digitalen Identität können die Begriffe *digitale Demokratie* und *elektronische Demokratie* als Synonyme verstanden werden. Fivaz und Schwarz [2021, S. 76-77] beschreiben die digitale Demokratie als einen Bereich, welchem demokratische Prozesse und Institutionen im digitalen Raum zugeordnet werden können. Im spezifischen ordnen Fivaz und Schwarz [2021, S. 77] „*die Informationssuche, -verbreitung und -verarbeitung mit Blick auf politische Entscheidungen, die Meinungsbildung und Entscheidungsfindung sowie die politische Partizipation in der Form von Wahlen, Abstimmungen und anderen Möglichkeiten der Bürgerbeteiligung*“ dem Begriff zu. Mitschka und Unterberger [2018, S. 105] definieren die digitale Demokratie als „*eine Form der Öffentlichkeit, in der digitale Medien benutzt werden, um Demokratie zu praktizieren. Dies passiert durch demokratische Informierung, Kommunikation und Kooperation*“.

Die Mehrheit aller auffindbaren Definitionen zur digitalen Demokratie erwähnen drei zentrale Merkmale: Digitale Information (Webseiten, Open Data, digitale Behördengänge, etc.), digitaler Austausch (Diskussionsforen, digitale Meinungsbildung, etc.) sowie digitale Partizipation (Online-Petitionen, digitale Befragungen, andere digitale Formen von Bürger:innenbeteiligung) [Internetredaktion LpB BW 2022]. Es wird im Rahmen der Digitalisierung der Demokratie angestrebt, im digitalen Raum eine Ergänzung zur repräsentativen Demokratie der analogen Welt zu schaffen. Davon erhofft man sich neben einer Wiederbelebung der politischen Kommunikation auch eine Stärkung der Demokratie durch mehr Transparenz, Legitimation und Partizipation [Demokratiezentrums Wien 2022].

Die moderne Demokratie muss sich wie viele andere Bereiche einer Gesellschaft neuen Herausforderungen durch die Digitalisierung des Alltags stellen [Eixelsberger et al. 2019, S. 509]. Digitale Plattformen können im Kontext von digitaler Demokratie als sozio-technische Systeme verstanden werden, in welchen Menschen sich digitale Hilfsmittel für spezifische Zwecke innerhalb des demokratischen Zusammenlebens zu Nutze machen [Poblet et al. 2020, S. 6-7]. Bürger:innen müssen nicht mehr länger von Angesicht zu Angesicht oder über analoge Kommunikationsmittel wie Briefe mit Behörden und Institutionen des öffentlichen Sektors in Kontakt treten, sondern können theoretisch durch Informationstechnologie vollständig aus der Ferne mit diesen interagieren [Lips 2010, S. 273-274]. Nach Lips [S. 273-274] muss sich die moderne Demokratie deshalb wichtigen Fragen über das Verhältnis zwischen Staat und Bürger:innen stellen.

Wenn im Rahmen von allgemeinen digitalen Transaktionen von Vertrauen als Schlüsselement die Rede ist, so gilt dies für Transaktionen im Kontext der digitalen Demokratie im Besonderen. Digitale Demokratieprozesse unterliegen nach Cap und Maibaum [2001, S. 803] nicht nur Gefahren monetärer Natur, sondern es geht auch um persönliche Freiheits-, Bürger:innen- und Demokratierechte. Obwohl Vertrauen in den Bereichen Politik, Staatsführung und Demokratie zentral ist, hat das Vertrauen in demokratische Institutionen global neue Tiefststände erreicht [Crosby et al. 2016, S. 8; Poblet et al. 2020, S. 2]. Umso wichtiger scheint es, künftige digitale Lösungen im Bereich der digitalen Demokratie mit speziellem Fokus auf Privatsphäre, Integrität und Datenschutz zu entwerfen [Biswas und Muthukumarasamy 2016, S. 1392]. Gemäss Poblet et al. [2020, S. 2] ist ebenfalls evident, dass eine verstärkte Partizipation - auch in Form von digitalen Partizipationsmitteln - von Bürger:innen in Politik- und Entscheidungsprozessen die schlechende Erosion des Vertrauens in die Demokratie lindern kann.

Aus der Kombination von digitaler Demokratie und der (kryptografischen) Blockchain-Technologie ergibt sich der Kunstbegriff der *Krypto-Demokratie*. Wenn es um die Herstellung von Vertrauen in der digitalen Demokratie geht, bietet die Blockchain-Technologie ein Mittel, um im digitalen Raum neue Lösungen zur vertrauensvollen Information, Kommunikation und Partizipation zu entwickeln. Im Kontext der digitalen Demokratie ist es zukunftsweisend, dass Transaktionen durch eine neue Grundstruktur digital abgebildet, dokumentiert und authentifiziert werden und in der Folge das Internet zu einem Raum von werthaltigen Interaktionen weiterentwickelt wird [Eixelsberger et al. 2019, S. 506]. Obwohl der Einsatz von Blockchain-Technologie in öffentlichen Verwaltungen noch nicht die Regel ist, sollten sich künftig aus dem Vertrauensmechanismus ohne zentrale Autorität spannende Einsatzzwecke für den digitalen Staat und die digitale Demokratie ergeben [Pilkington 2016, S. 226; Rauschenbach und Stucki 2020, S. 15]. Nicht umsonst wird nach der ersten Generation von Blockchains für digitale Währungen (1.0), der zweiten Generation von Blockchains für die digitale Wirtschaft (2.0), bei der sich in Entwicklung befindenden dritten Generation von Blockchains für die digitale Gesellschaft (3.0) gesprochen [Efanov und Roschin 2018, S. 117].

Behördliche Einsatzgebiete von Blockchains der dritten Generationen umfassen nach Efanov und Roschin [2018, S. 118] Kunst, Gesundheit, Wissenschaft, Regierung, Bildung und weitere Aspekte der öffentlichen Kultur und Kommunikation. Eixelsberger et al. [2019, S. 509] ergänzen die Liste der Einsatzgebiete um die digitale Identität für Wahlsysteme, die Nachverfolgung öffentlicher Gelder und Eigentumsnachweise. In der Praxis entwickeln weltweit verschiedene Länder Blockchain-Anwendungen mit Pioniercharakter für die digitale Demokratie und die digitale öffentliche Verwaltung. Beispielsweise entwickeln Ghana und Schweden Blockchain-basierte Grundbücher, Dänemark Blockchain-basierte Dossiers für

Fahrzeuge oder die Niederlande Blockchain-basierte Abwicklungen für Pensions-Prozesse und Systeme zur Bestimmung von Zollwerten bei grenzüberschreitenden E-Commerce-Transaktionen [Rauschenbach und Stucki 2020, S. 19-20].

Auch in der Schweizerischen Eidgenossenschaft wird an einer gesetzlichen Grundlage für Praxiseinsätze der Blockchain gearbeitet, nachdem sich das Schweizer Parlament 2020 für bessere Rahmenbedingungen zum Einsatz der Blockchain-Technologie ausgesprochen hat [Eidgenössisches Finanzdepartement 2021a; Das Schweizer Parlament 2020]. Bereits heute bestehen in der Schweiz einige Pilotprojekte auf Basis der Blockchain-Technologie im öffentlichen Sektor. Im Bereich des Blockchain-basierten Identitätsnachweises existieren Projekte in Form von Pilotprojekten der Stadt Zug und des Kantons Schaffhausen [Stadt Zug 2017; Kanton Schaffhausen 2021]. Auf diese Projekte wird im Kapitel zum Blockchain-Identitätsnachweis in der Praxis in Abschnitt 2.7 auf Seite 55 detailliert eingegangen. Andere Blockchain-Projekte der öffentlichen Verwaltung umfassen unter anderem [Digitale Verwaltung für Bevölkerung, Wirtschaft und Behörden 2022a]:

- Blockchain-basiertes E-Voting der Stadt Zug.
- Die elektronische Bearbeitung und Archivierung von offiziellen Dokumenten auf der Basis von Blockchain des Kantons Genf.
- Eine ökologische private Blockchain für digitales Vertrauen in der Schweiz des Kantons Jura.
- Einen Blockchain-Betreibungsregisterauszug des Kantons Schaffhausen.

In der modernen und digitalen Demokratie legt die digitale Infrastruktur den Rahmen fest, innerhalb dessen sich eine digitale Demokratie entwickeln kann [Fivaz und Schwarz 2021, S. 77]. Als ein wichtiges Infrastruktur-Element einer digitale Demokratie spielt die digitale Identität eine entscheidende Rolle für künftige Entwicklungen. Gerade wenn (rechtlich relevante) Sachverhalte, Ansprüche und Forderungen - wie sie in behördlichen und demokratischen Transaktionen alltäglich sind - im digitalen Raum zwischen Parteien etabliert werden, müssen diese auch in der physischen Welt durchgesetzt werden können [Rauschenbach und Stucki 2020, S. 15]. Eine Grundvoraussetzung dafür ist die eindeutige Feststellbarkeit der vom Staat hoheitlich anerkannten Identität der beteiligten Rechtssubjekte. Für die digitale Demokratie und den digitalen Staat der Zukunft ist dadurch nach Pilkington [2016, S. 242-243] die Zentralisierung von digitalen Identitätsdaten der Bürger:innen von grösster politischer, rechtlicher und sozialer Bedeutung.

### 2.2 Fokussierung & Abgrenzung

Wie die theoretische Aufarbeitung der Blockchain-Technologie gezeigt hat, bietet diese diverse Einsatzmöglichkeiten. Diese Master-Thesis befasst sich im weiteren Verlauf exklusiv mit dem Anwendungszweck der Blockchain-Technologie für digitale Identitätsnachweislösungen. Weiter wird der Forschungsbereich dieser Thesis auf den öffentlichen Sektor und spezifisch auf digitale Identitätsnachweislösungen im Kontext der digitalen Demokratie der Schweizerischen Eidgenossenschaft eingegrenzt. Der privatwirtschaftliche Sektor wird abgegrenzt. Trotzdem sind viele theoretische Eigenschaften von allgemeinen digitalen Identitätslösungen und spezifisch auf der Blockchain basierenden Lösungen in gleichem Masse für den privaten Sektor und den öffentlichen Sektor gültig. Durch die Eingrenzung der Forschung auf die Schweizerische Eidgenossenschaft ergibt sich ein Rahmen, welcher durch die einzigartigen Eigenschaften des direktdemokratischen Regierungssystems (Direktorialsystem) geprägt ist [Sebaldt 2010; Vatter 2020]. Dadurch kann die Aussagekraft der Erkenntnisse dieser Arbeit im internationalen Kontext beeinflusst sein.

Der Identitätsnachweis in Form einer digitalen ID kann wie in Abschnitt 2.1.2 auf Seite 6 beschrieben als reine Authentifizierungsmethode im digitalen Raum (Log-in) oder auch als staatlich anerkanntes Identitätsdokument für jegliche digitalen Transaktionen verstanden werden. Mit Letzterem könnte auch auf digitale Weise die Identität im Rahmen einer Grenzüberschreitung, analog zu einem physischen Reisepass, geprüft werden. Eine klare Abgrenzung ist schwierig zu treffen, da die Grenzen zwischen Authentifizierungsmethode und Identitätsdokument mit Offizialcharakter oftmals flüssig sind. Im Rahmen dieser Arbeit wird deshalb festgelegt, dass der Begriff bewusst ambivalent zu verstehen ist. Wie die folgenden Kapitel dieser Thesis weiter erläutern werden, ist gerade im Kontext von digitaler Demokratie und behördlichen Dienstleistungen die Interpretation von Identität beinahe untrennbar mit einem staatlich anerkannten Identitätsnachweis verknüpft. Es bietet sich daher an, eine digitale ID als ein staatlichen Pässen und Identitätskarten äquivalentes Ausweismittel auszulegen.

### 2.3 Aktueller Identitätsnachweis in der Schweiz

Durch die Fokussierung auf die Schweizerische Eidgenossenschaft stellt sich die Frage, wie sich der aktuelle Identitätsnachweis von Bürger:innen der Schweiz gestaltet. In der Schweizerischen Eidgenossenschaft ist das Recht auf einen staatlichen Ausweis an das Staatsbürgerrecht gebunden. Dabei kennt die Schweiz drei Formen, nach welchen das schweizerische Bürgerrecht erworben werden kann [Staatssekretariat für Migration SEM 2022]:

- Durch väterliche oder mütterliche Abstammung (*ius sanguinis* = durch das Recht des Blutes).
- Durch Einbürgerung, also durch behördlichen Beschluss.
- Durch Adoption durch einen schweizerischen Elternteil.

Gesetzlich geregelt ist der Erwerb des Schweizer Bürgerrechts und das Erwerbsrecht von Ausweisen im *Bürgerrechtsgesetz* (BüG, SR 141.0) [Fedlex 2019a] sowie in der *Verordnung des EJPD über Ausweise für Schweizer Staatsangehörige* (SR 143.111) [Fedlex 2019b]. Wie aus den Gesetzestexten hervorgeht, erwerben Personen mit Schweizer Bürgerrecht ebenfalls Kantons- und Gemeindebürgerrecht [Fedlex 2019a, BüG Art. 2 Abs. 1-2; Fedlex 2019b, Verordnung des EJPD über Ausweise für Schweizer Staatsangehörige Art. 2 Abs. 1]. Das Staatsbürgerrecht beschreibt eine Rechtsbeziehung zwischen Mensch und Heimatstaat und beinhaltet Rechte und Pflichten wie politische Rechte, diplomatischen Schutz, Niederlassungsfreiheit, Ausweisungs- und Auslieferungsverbote oder auch eine Wehrpflicht [Schweizer und Müller 2021].

Die heutige gesetzliche Grundlage für staatliche Ausweise und der Grundauftrag sind im *Bundesgesetz über die Ausweise für Schweizer Staatsangehörige* (Ausweisgesetz, AwG, SR 143.1) [Fedlex 2018] sowie in der *Verordnung über die Ausweise für Schweizer Staatsangehörige* (Ausweisverordnung, VAWG, SR 143.11) [Fedlex 2022] festgehalten. AwG Art. 1 Abs. 1 definiert den rechtlichen Anspruch aller Schweizer Staatsangehörigen auf einen Ausweis je Ausweisart, während VAWG Art. 1 Abs. 1 die staatlichen Ausweisarten als Pass und Identitätskarte bestimmt.

Von zentraler Bedeutung im Kontext dieser Forschungsarbeit ist AwG Art. 1 Abs. 2: *Ausweise im Sinne dieses Gesetzes dienen der Inhaberin oder dem Inhaber zum Nachweis der Schweizer Staatsangehörigkeit und der eigenen Identität*. Hier zeigt sich, dass Ausweismittel im rechtlichen Sinne weniger als reine Authentifizierungsmittel, sondern als vollwertig identitätsstiftende Dokumente erachtet werden. Dies stützt die in Abschnitt 2.2 auf der vorherigen Seite zur Fokussierung und Abgrenzung getroffene Annahme, dass Identität beinahe untrennbar mit einem staatlich anerkannten Identitätsnachweis verknüpft ist. Wenn wir von einer digitalen ID sprechen,

ist in diesem Kontext die Interpretation der digitalen Lösung als offizielles und staatlich kontrolliertes Identitätsdokument beinahe unumgänglich. Es ist aufgrund der gesetzlichen und praktischen Handhabung von Ausweisen und Identität anzunehmen, dass im Verständnis der schweizerischen Bevölkerung die Begriffe von Identität und Ausweisdokumenten ebenfalls eng miteinander assoziiert werden.

Der Inhalt eines Ausweises wird in AwG Art. 2 Abs. 1 definiert. Jeder Ausweis muss die folgenden Daten enthalten: Amtlicher Name; Vornamen; Geschlecht; Geburtsdatum; Heimatort; Nationalität; Grösse; Unterschrift; Fotografie; ausstellende Behörde; Datum der Ausstellung; Datum des Ablaufs der Gültigkeit; Ausweisnummer und Ausweisart. Gewisse Personendaten werden aus dem staatlichen elektronischen Personenstandregister *Infostar* entnommen und in das *Informationssystem Ausweisschriften* (ISA) übertragen, um Ausweise ausstellen zu können [VAwG Art. 10, 28, 29]. Weiter halten AwG Art. 2 Abs. 2<sub>bis</sub> und VAwG Art. 14a Abs. 1 fest, dass der Ausweis mit einem Datenchip versehen werden kann, welcher ein Gesichtsbild und Fingerabdrücke der Inhaberin oder des Inhabers enthält. Digitale Inhalte in physischen Ausweisdokumenten haben durch europäische Gesetzgebung in Form von Verordnungen über Normen für Sicherheitsmerkmale und biometrische Daten in Pässen und Reisedokumenten auch in der Schweizerischen Eidgenossenschaft Einzug erhalten [EUR-Lex 2020; Rat der Europäischen Union 2004].

Die Beantragung, Ausstellung und behördliche Verantwortlichkeit wird in AwG Art. 4 und 5 sowie in VAwG Art. 12 geregelt. Gemäss Gesetzgebung sind sämtliche Stellen, welche Ausweise ausstellen dürfen, durch den Bundesrat und die Kantone der Schweizerischen Eidgenossenschaft definiert [AwG Art. 4]. Die Ausstellungen von Ausweisen ist eine Behördenaufgabe und -kompetenz. Ein zentrales Element der Beantragung und Ausstellung von Ausweisen ist die Pflicht von Staatsangehörigen, bei der zuständigen Behörde persönlich vorzusprechen und dadurch die geltend gemachte Identität durch die Behörde prüfen zu lassen [AwG Art. 5; VAwG Art. 12]. Staatlich ausgestellte Ausweise sind weiter in ihrer Gültigkeit befristet [AwG Art. 3] und können entzogen werden, wenn eine eindeutige Identifizierung der Inhaberin oder des Inhabers nicht mehr möglich ist [AwG Art. 7 Abs. 1 Ziff. b]. In diesen Punkten zeigt sich erneut die starke Verknüpfung von Ausweisdokumenten, Identität und analogen Prozessen.

Wie die Aufarbeitung der gesetzlichen Grundlagen von Identitätsdokumenten in der Schweizerischen Eidgenossenschaft zeigt, erlaubt das Gesetz derzeit nur analoge Ausweismittel in Form des physischen Passes und der physischen Identitätskarte. Diese Ausweismittel verkörpern sowohl ein amtliches Identitätspapier und stellen als gängige Authentifizierungsmethode gleichzeitig die Basis für diverse Transaktionen in der Privatwirtschaft und im öffentlichen Sektor dar. Abgesehen vom isoliert anmutenden Passus 2<sub>quarter</sub> in Art. 2 AwG, nach welchem Ausweise zudem elektronische

Merkmale für Authentisierungs-, Signatur- und Verschlüsselungsfunktionen enthalten können, gibt es keine gesetzlichen Grundlagen für eine vollwertige digitale ID.

Ein Beispiel für den Versuch, eine digitale ID für reine Authentifizierungszwecke innerhalb digitaler Transaktionen zu etablieren, geht von der *SwissSign AG* als Tochterunternehmen der Schweizerischen Post aus [SwissSign Group 2022]. Seit 2010 versuchte sich die damals noch *SuisseID* benannte digitale Identitätslösung am Markt zu etablieren, scheiterte allerdings [Müller und Windisch 2018, S. 11]. Eine neue Trägergesellschaft staatsnaher Unternehmen, Finanzdienstleistern und Versicherungen namens *SwissSign Group* hat die Markenrechte 2017 übernommen und bietet in Form der umbenannten *SwissID* eine an mehrere Anbieter:innen aus dem privaten und öffentlichen Sektor angebundene digitale ID-Lösung an [Müller und Windisch 2018, S. 12].

Die *SwissSign Group* hatte sich zum Ziel gesetzt, künftig als Privatanbieterin ebenfalls die Verwalterin einer offiziellen staatlichen E-ID mit Ausweis-Charakter im Auftrag des Bundes zu sein [Meyer 2020]. Dieses Vorhaben und auch die Zukunft von Identitätsnachweislösungen wie der *SwissID* sind seit der eidgenössischen Volksabstimmung vom 7. März 2021 über die gesetzliche Grundlage einer E-ID mit grossen Fragezeichen versehen. Das schweizerische Stimmvolk hat in dieser Abstimmung einer geplanten Lösung für die digitale ID basierend auf einem Konsortium von Behörden, Staatsbetrieben und Privatbetrieben eine deutliche Absage erteilt. Detailliert wird auf die *Eidgenössische Abstimmung E-ID 2020* in Abschnitt 2.5 auf Seite 37 eingegangen.

In der Schweizerischen Eidgenossenschaft existiert in der Folge bis zum jetzigen Zeitpunkt keine offiziell staatlich anerkannte digitale ID-Lösung. Auch die gesetzliche Grundlage konnte durch die abgelehnte Referendumsvorlage nicht geschaffen werden und der Bundesrat sowie das Parlament der Schweiz müssen neue Konzepte für eine digitale ID erarbeiten.

### 2.4 Digitale Demokratie & die Identität ihrer Bürger:innen

Die Art und Weise, wie Identitätsinformationen von Bürger:innen im Umfeld des öffentlichen Sektors demokratischer Länder erfasst und verwaltet werden, ist seit Jahrzehnten oder teilweise Jahrhunderten weitgehend unverändert [Lips 2010, S. 275]. Bürger:innen müssen Details über ihre Identität gegenüber ihrem Staat offenlegen, welcher diese in analoger Form in einem staatlich offiziell anerkannten Papierdokument festhält. Der Staat verfügt in diesem System über das Exklusivrecht zur Ausstellung und Verwaltung von offiziellen Identitätsdokumenten, wie beispielsweise Pässen, Identitätskarten oder auch dienstleistungsbezogenen Identitätsinformationen wie Sozialversicherungsnummern [Lips 2010, S. 275].

In einer hochgradig technologiebasierten und digitalen Umwelt ändern sich die Anforderungen an das Identitätsmanagement eines Staats. Die heutzutage noch immer gängigen Identitätslösungen mit starkem Fokus auf physische Identitätsdokumente, Prozesse und Methoden vermögen den neuen Anforderungen einer digitalen Gesellschaft nicht mehr gerecht zu werden. Dieser Umstand hat zur Folge, dass in digitalen Kontexten Identifizierungsprozesse mit Ineffizienzen wie hohen Kosten, Sicherheitsrisiken und beschwerlichen Zeitaufwänden für Unternehmen, Behörden und Bürger:innen einhergehen [Wolfond 2017, S. 35-36]. Für Lips [2010, S. 275-276] ergeben sich durch die Einführung digitaler Dienstleistungskanäle im öffentlichen Sektor neue Herausforderungen in der Art und Weise, wie Bürger:innen künftig Transaktionen mit Behörden vertrauensvoll und authentisch tätigen können. Auch Mir et al. [2020, S. 5] und Wolfond [2017, S. 35-36] sehen für den digitalen Staat Handlungsbedarf im Bereich der digitalen Identität. Als kritisches, bisher vernachlässigtes Element der digitalen Ära, ist die digitale Identität ein Grundstein für das Fortschreiten der digitalen Demokratie.

Der einwandfreie Nachweis einer Identität ist eine kritische und essenzielle Grundvoraussetzung für Bürger:innen, um Zugang zu öffentlichen Dienstleistungen zu erhalten: Praktisch jede Beziehung zwischen Bürger:innen und öffentlichen Einrichtungen wird durch Identitätsmanagement unterstützt und setzt den Nachweis von Identität voraus [Lips 2010, S. 275; Sullivan 2016, S. 481; Sullivan 2018, S. 724]. Digitale Bürger:innen werden nach Melin et al. [2016, S. 73] immer stärker von digitalen Lösungen zum Identitätsnachweis abhängig sein, um mit ihren Behörden im Rahmen digitaler Dienstleistungen interagieren zu können. Zentral ist bei diesen Transaktionen ein hoher Grad an Vertrauenswürdigkeit, Integrität und Nutzer:innenfreundlichkeit. In diesen Punkten sehen Stokkink und Pouwelse [2018, S. 1336] die Hauptprobleme der heutigen Identitätshandhabung im digitalen Raum. Viele unterschiedliche Lösungen und Prozesse zum Nachweis von Identität im privaten und öffentlichen Sektor haben in den letzten Jahren dazu geführt, dass Identitätsdaten von Bürger:innen stark fragmentiert verteilt und gespeichert wurden. Die Individuen haben über ihre Identitätsdaten nur wenig oder keine Kontrolle mehr.

Einer digitalen ID kommt in der Folge gerade im Kontext von Behördendienstleistungen und Demokratieprozessen eine grosse und neuartige Bedeutung zu. Wie kaum ein anderer Bereich ist die öffentliche Verwaltung darauf angewiesen, Identität für Dienstleistungen und demokratische Entscheidungsprozesse in verschiedenen Kontexten eindeutig nachweisen zu können [Lips 2010, S. 286; Wolfond 2017, S. 37-38]. Auf der Gegenseite wächst bei den Bürger:innen das Bewusstsein über den Wert und Schutzbedarf ihrer eigenen Identitätsdaten und damit die Verantwortungspflicht des Staats. Sullivan [2016, S. 478-479, 481; 2018, S. 729-730] sieht in der präzisen, funktionalen und einzigartigen Identität ein fundamentales Menschenrecht, welches jedem Menschen mit der Geburt zukommt. Sullivan argumentiert, es sei die Pflicht von demokratischen Staaten, diesem Grundrecht zum Besitz und Schutz von Identität im digitalen Raum in derselben Weise nachzukommen, wie dies in der analogen Welt der Fall ist. Dies stelle eine Grundvoraussetzung dar, um verantwortungsvoll und rechenschaftspflichtig digitale Staatsbürgerschaften zu ermöglichen. Da sich der Anwendungsbereich von digitalen Identitätsmitteln neben dem öffentlichen Sektor auch unausweichlich auf den privaten Sektor ausweiten wird, werden digitale Identitätslösungen als Hauptmittel für Transaktionen im digitalen Zeitalter betrachtet [Sullivan 2018, S. 726].

Die Gewichtigkeit einer digitalen Identitätslösung auf Staatsebene unterstreicht auch die *2030 Agenda for Sustainable Development*, eine von den United Nations (UN) veröffentlichte Agenda mit nachhaltigen Entwicklungszielen für Nationen [Treiblmaier und Beck 2019, S. 233-234]. Eines der wichtigsten Entwicklungsziele der Agenda ist die Existenz einer legalen Identität für alle Menschen. Es ist das erste Mal, dass die legale Identität für alle Menschen als offizielles globales Ziel definiert wurde. In einer Welt, in welcher Nationen ihre Strukturen hin zu digitalen Behörden weiterentwickeln, ist der Entwicklung einer legalen Identität für alle Menschen ebenfalls die Entwicklung einer legalen digitalen Identität für alle Menschen inhärent [Treiblmaier und Beck 2019, S. 234].

### 2.4.1 Demokratische Triebkräfte des digitalen Identitätsnachweises

Die Identitätsdaten von Bürger:innen verkörpern eine kritische Komponente des öffentlichen Dienstleistungsverhältnis zwischen Bürger:innen und Staat [Lips 2010, S. 273]. Die Digitalisierung von Identitätsdaten führt zu fundamentalen Umbrüchen im öffentlich-rechtlichen Dienstleistungsumfeld und verlangt nach breiten öffentlichen Debatten rund um die Transparenz im Management von digitalen Identitätsdaten [Lips 2010, S. 274, 287]. Weltweit versprechen sich Behörden enormes Potenzial für die Demokratie und behördliche Dienstleistungen durch die Einführung einer digitalen ID, wobei die Bevölkerung im Gegenzug den Entwicklungen je nach Land und Region unterschiedlich offen gegenübersteht.

Digitale Lösungen für den Identitätsnachweis können nach Irani und Kamal [2016, S. 2] das Angebot an staatlichen Dienstleistungen effizienter und effektiver machen. Gemäss Rüthi et al. [2020, S. 52] ermöglicht eine digitale ID zusätzlich die Weiterentwicklung von virtuellen Behördenschaltern. Effizienzsteigerungen sollen in diesem Kontext als Potenzial interpretiert werden und der digitale Identitätsnachweis als Weichensteller für neuartige, effizienzsteigernde Dienstleistungen. Die Ermöglichung von Zeit- und Kosteneinsparungen in Transaktionen, welche gleichzeitig sicher, bequem und vertrauensvoll sein müssen, ist eines der zentralen Versprechen des digitalen Identitätsnachweises.

Die Potenziale, welche dem digitalen Identitätsnachweis zugeschrieben werden, Formen starke Triebkräfte zur Einführung einer digitalen ID von Seiten der Staaten und deren Regierungen. Die digitale ID wird beispielsweise seit 2010 von der Europäischen Kommission als das Schlüsselement für vollständig digitale Behördenleistungen und die digitale Transformation der Verwaltung betrachtet [Melin et al. 2016, S. 92]. Die überragende Bedeutung und Relevanz einer digitalen ID kann nach Autor:innen wie Melin et al. [2016, S. 73], Rauschenbach und Stucki [2020, S. 34] und Fivaz und Schwarz [2021, S. 86] nicht überschätzt werden. Ohne digitale ID fehlt der öffentlichen Hand ein Grundbaustein, um Prozesse zwischen Staat und Bürger:innen vollständig digitalisieren zu können. Für die Digitalisierung der Verwaltung und der Demokratie ist eine digitale ID aus der Perspektive des digitalen Staats essenziell.

Auch im schweizerischen Staat wirken die genannten Triebkräfte. Die Etablierung der digitalen Verwaltung (E-Government) steht in der schweizerischen Politik bereits seit 20 Jahren auf der Agenda, wobei die Schweiz im Europäischen E-Government-Vergleich im Mittelfeld steht [Neuroni et al. 2019, S. 163, 170-173]. Für Bühler et al. [2022, S. 6] ist es im Kontext der Schweiz wichtig, den digitalen Staat oder die digitale Verwaltung richtig einzurordnen: In der Schweiz geht es dabei oftmals um die unmittelbare Interaktion zwischen Bürger:innen und dem Staat, also um digitale Behördenschalter und digitale Möglichkeiten zur (direkt-)demokratischen Beteiligung. Ladner et al. [2019, S. 184-185] unterstreichen ebenfalls die Einzigartigkeit des schweizerischen Systems, in welchem politischer Konsens und die Unterstützung der Bevölkerung für Digitalisierungsvorhaben zentral sind. Während breiter Konsens über geplante Entwicklungen diese auch durch Widerstände tragen kann, führen die komplexen Meinungsabstimmungsprozesse der Schweiz auch zu langsameren Adaptionen von neuen Technologien.

Um das eher langsame Vorankommen bei der Digitalisierung von Diensten und Demokratieprozessen der Verwaltung in der Schweiz zu beschleunigen, hat der schweizerische Bundesrat für die Jahre 2022 und 2023 Mittel von rund 15 Millionen Franken gesprochen [Digitale Verwaltung für Bevölkerung, Wirtschaft und Behörden

2022b; Geschäftsstelle Digitale Verwaltung Schweiz 2022]. Damit soll dem Aufbau von Infrastrukturen und Basisdiensten zur Abwicklung von elektronischen Prozessen Nachdruck gegeben werden. Die E-Government-Ziele entwickelten sich in den letzten Jahren unter anderem immer stärker in Richtung sicherer Datenumgang inklusive digitaler Identität [Neuroni et al. 2019, S. 164].

Auch Bühler et al. [2022, S. 3] und Fivaz und Schwarz [2021, S. 77-78] halten fest, dass es um den digitalen Staat in der Schweiz nicht zum Besten steht. Obwohl die technischen und rechtlichen Rahmenbedingungen zufriedenstellend bis hervorragend sind, haben Digitalisierungsprojekte in der Schweiz oft einen schweren Stand [Neuroni et al. 2019, S. 177; Fivaz und Schwarz 2021, S. 77-78, 86]. Die schweizerische Bevölkerung scheint die Potenziale und die Dringlichkeit der Einführung einer digitalen ID differenziert zu beurteilen. Dies hat einen direkten Einfluss auf die Triebkraft, welche von der Bevölkerung ausgeht. Allerdings ist gemäss den Studienautor:innen Bühler et al. [2022, S. 3] der Forschungsstelle *sotomo* über die allgemeinen Anforderungen der Bürger:innen der Schweiz an den digitalen Staat verhältnismässig wenig bekannt. Dies scheint zu überraschen, da die Bevölkerung gerade in der Schweiz durch die Möglichkeit der direktdemokratischen Einflussmöglichkeiten eine grosse Relevanz im Rahmen politischer Entscheidungen besitzt.

Aktuelle Forschungsbestrebungen haben versucht, die Erwartungen und Anforderungen der Bürger:innen in der Schweiz ein wenig genauer zu erfassen. Fivaz und Schwarz [2021, S. 79-82] konnten feststellen, dass zwischen der Einstellung gegenüber Digitalisierungsvorhaben von Kandidierenden für politische Ämter und den Wähler:innen signifikante Unterschiede erkennbar sind. Die Bevölkerung scheint insgesamt Digitalisierungsvorhaben weit weniger euphorisch zu begegnen, als dies von Seiten der Politik erwünscht und vertreten wird. Beim spezifischen Anwendungsfall zur beschleunigten Entwicklung einer digitalen ID haben Fivaz und Schwarz eine Differenz von 13 % zwischen den Parteien (Befürwortung 52 %) und der Basis (Befürwortung 39 %) beobachtet. Diese Ergebnisse decken sich mit den Resultaten der Untersuchungen im Rahmen des *Mobilier DigitalBarometer*, gemäss welchen die schweizerische Bevölkerung wenig bereit ist, einfach einmal etwas Neues auszuprobieren [Rüthi et al. 2020, S. 11]. Gemäss den Autor:innen steht dies im Widerspruch zur schnellen Dynamik der Digitalisierung selbst.

Rüthi et al. [2020, S. 15] haben im *Mobilier DigitalBarometer* in Bezug auf den digitalen Identitätsnachweis weiter herausgefunden, dass trotz einer zunehmenden Gefahrenwahrnehmung der Bevölkerung beim Thema „*meine Daten*“ eine Mehrheit der Menschen in der Thematik *E-ID* keine Notwendigkeit sieht, zu handeln. Über die Gründe dieser Diskrepanz kann an dieser Stelle lediglich spekuliert werden. Eine mögliche Erklärung könnte sein, dass die schweizerische Bevölkerung beim

Thema digitale ID mehr Risiken in Bezug auf die eigenen Daten sieht und das Schutz- und Kontrollpotenzial über die eigenen Identitätsdaten je nach gewählter technischer Implementationsweise unbekannt ist. Ebenfalls geringe Dringlichkeit seitens der Bevölkerung haben Bühler et al. [2022, S. 7-9] im Bereich digitale Demokratie, wozu beispielsweise das digitale Abstimmen (E-Voting) oder das digitale Unterschriftensammeln (E-Collecting) gehören, beobachtet. Die Bevölkerung scheint generell zufrieden mit dem derzeitigen Stand an digitalen Behördendienstleistungen zu sein.

Allerdings sehen trotz der im Vergleich zu anderen Digitalisierungsbereichen im öffentlichen Sektor eher geringen Relevanz der digitalen ID 41 % der schweizerischen Bevölkerung hohen Handlungsbedarf und nennen als wichtigste Akteure im Rahmen der digitalen ID Behörden (69 %) und Politik (64 %) [Rüthi et al. 2020, S. 54]. Dies stützt wiederum die Annahme, dass viele Bürger:innen der Schweiz die Identität und Identitätsnachweislösungen sehr stark mit der staatlichen Institution verbinden und eine digitale ID-Lösung als offizielles Ausweisdokument interpretieren. Zur Vollständigkeit sollte an dieser Stelle festgehalten werden, dass starke Triebkräfte zur Einführung einer digitalen ID natürlich auch aus der Privatwirtschaft stammen, welche ebenfalls enorm von einer digitalen ID profitieren würde. Allerdings zeigt der *Mobiliar DigitalBarometer* von Rüthi et al. [2020, S. 54], dass trotz starker Förderung einer digitalen ID von Seiten der Wirtschaft diese vergleichsweise nur von 31 % der Bevölkerung als wichtiger Akteur empfunden wird.

So kann festgehalten werden, dass sich die Wahrnehmung der Tragweite und Wichtigkeit einer digitalen Identitätslösung aus behördlicher, politischer, wirtschaftlicher und auch wissenschaftlicher Sicht stark von derjenigen der schweizerischen Bevölkerung zu unterscheiden scheint. Aus den verschiedenen Studien rund um die Einstellung der schweizerischen Bevölkerung gegenüber der Digitalisierung des Staats und der digitalen ID ist nicht zwingend ersichtlich, dass diese die Dringlichkeit einer digitalen ID ablehnt. Jedoch scheint es so, als würden Bürger:innen die Chancen und Risiken anders als die Politik bewerten und abweichende Ansprüche und Erwartungen an eine staatliche E-ID-Lösung stellen. Abschnitt 2.4.2 auf der nächsten Seite und Abschnitt 2.4.3 auf Seite 33 werden sich nochmals detaillierter mit den staatlichen Triebkräften auseinandersetzen, während in Abschnitt 2.5 auf Seite 37 durch die Analyse der Volksabstimmung zur E-ID von 2021 detailliertere Erkenntnisse über die Ablehnungsgründe seitens der Bevölkerung dargelegt werden.

### 2.4.2 E-Government-Strategie Schweiz 2020-2023 & Strategie Digitale Schweiz

Der Auftrag und interne Antrieb des Staats zur Digitalisierung der öffentlichen Verwaltung der Schweizerischen Eidgenossenschaft ist seit 2008 in einer E-Government-Strategie formuliert [Eidgenössisches Finanzdepartement 2021b]. Das übergeordnete Ziel ist eine verstärkte Zusammenarbeit von Bund, Kantonen, Gemeinden und Städten beim Aufbau und bei der Steuerung der digitalen Verwaltung. Auf den Behörden-Webseiten [www.egovernment.ch](http://www.egovernment.ch) und [www.digitale-verwaltung-schweiz.ch](http://www.digitale-verwaltung-schweiz.ch) sind die Bestrebungen, Ziele, Projekte und Fortschritte der Digitalisierung der Verwaltung einsehbar. Unter verschiedenen Umsetzungszielen wie elektronischen Adressänderungsplattformen, elektronischem Voting, elektronischer Signaturvalidation, elektronischer Partizipation, etc. findet sich auch das Ziel der Umsetzung einer elektronischen Identität [Digitale Verwaltung für Bevölkerung, Wirtschaft und Behörden 2022d; Digitale Verwaltung für Bevölkerung, Wirtschaft und Behörden 2022c].

Als übergeordnete Mission führt die Geschäftsstelle Digitale Verwaltung Schweiz [2022] an:

*„Die Digitale Verwaltung Schweiz verfolgt einen vernetzten, gesamtschweizerischen Ansatz. Sie koordiniert die Steuerung der digitalen Transformation zwischen und innerhalb der institutionellen Ebenen und ermöglicht Mitsprache und Mitgestaltung. Sie schafft einen Mehrwert für Bevölkerung, Wirtschaft und öffentliche Verwaltungen und fördert die Zusammenarbeit über Staatsebenen hinweg.“.*

Die Digitale Verwaltung für Bevölkerung, Wirtschaft und Behörden [2022] definiert die Ziele des strategischen Projekts der elektronischen Identität wie folgt:

*„Immer mehr Leute tätigen ganz unterschiedliche Geschäfte im Internet, bei denen sie sich identifizieren müssen. Die dafür eingesetzte elektronische Identität (E-ID) soll korrekt sein und vor Verwechslungen schützen. Um zu verhindern, dass falsche elektronische Identitäten ausgestellt werden, hat der Bundesrat die Kernaufgabe bei der Ausstellung einer E-ID, nämlich die amtliche Prüfung und Bestätigung der Existenz einer Person und ihrer Identitätsmerkmale wie Name, Geschlecht oder Geburtsdatum, als Staatsaufgabe definiert.“.*

Weiter wird beschrieben:

*„Die E-ID ist ein Schlüsselinfrastrukturelement, auf dem weitere digitale Dienste aufbauen, z. B. für ein durchgehend digitales E-Government, E-Voting, E-Banking, E-Health, E-Education oder E-Commerce. Dabei soll sie einen wichtigen Beitrag zur digitalen Transformation der Schweiz leisten.“.*

Die offizielle *E-Government-Strategie Schweiz 2020-2023* führt die digitale Identität unter dem Punkt *Basisdienste und Infrastruktur* für eine sichere, staatlich anerkannte Identifikation auf [Geschäftsstelle E-Government Schweiz 2020, S. 4, 14]:

*„Basisdienste sind im E-Government grundlegend für eine nutzerfreundliche und effiziente Abwicklung von elektronischen Prozessen. Zentral ist dabei die Bereitstellung von Diensten und Infrastrukturen für die Identitäts- und Zugriffsverwaltung sowie für die Nutzung und die Verwaltung von Daten. Die Schweiz liegt hier gemäss Studien hinter dem europäischen Durchschnitt zurück. Ziel der gemeinsamen Aktivitäten von Bund, Kantonen und Gemeinden soll es daher sein, die wichtigsten nationalen Basisdienste wie eine staatlich anerkannte elektronische Identität zu etablieren, eine Strategie für die gemeinsame Datenverwaltung zu erarbeiten und erste gemeinsame Register aufzubauen.“* [Geschäftsstelle E-Government Schweiz 2020, S. 15].

Eine weitere Triebkraft für die Digitalisierung der öffentlichen Verwaltung stellt die Strategie *Digitale Schweiz* dar, welche sich als Dachstrategie für die Digitalpolitik des Bundes versteht [GDS - Geschäftsstelle Digitale Schweiz 2021]. Damit die Vorteile der digitalen Transformation nutzbar gemacht werden können, müssen gemäss der Strategie die Behörden, Zivilgesellschaft, Wirtschaft, Wissenschaft und Politik gemeinsam agieren. Die Strategie definiert ebenfalls die Einführung einer elektronischen Identität als ein Basismodul der Infrastruktur der digitalen Verwaltung.

Eine erwähnenswerte Initiative mit Fokus auf die Digitalisierung der Schweiz im privaten und öffentlichen Sektor stellt die *Swiss Digital Initiative* dar [Eidgenössisches Finanzdepartement 2021c; Swiss Digital Initiative 2022]. Die Initiative zielt darauf ab, ethische Prinzipien und Werte im Umgang mit neuen Technologien zu etablieren. Im Umgang mit der Digitalisierung steht insbesondere die Stärkung des Vertrauens der beteiligten Akteure in neue digitale Technologien im Zentrum. Transparenz, Informationen und Kontrolle darüber, was mit den Daten der Nutzer:innen geschieht, ist eine Prämisse für neue technologische Entwicklungen. Gerade im Kontext von digitalen Identitätsdaten kommt dem Vertrauensaspekt eine grosse Bedeutung zu, um in der Bevölkerung auf Akzeptanz zu stossen.

### **2.4.3 Anwendungsbereiche einer digitalen ID für Dienstleistungen im öffentlichen Sektor und der Demokratie**

Die schweizerischen Behörden bieten ihren Bürger:innen diverse Dienstleistungen auf Bundes-, Kantons- und Gemeindeebene an. Im Folgenden soll eine Übersicht darüber geschaffen werden, welche behördlichen Dienstleistungen im Rahmen des öffentlichen Sektors von einer digitalen ID profitieren könnten. Dies betrifft sowohl

Dienstleistungen und Prozesse der öffentlichen Hand, welche bereits teilweise digital angeboten werden als auch Dienstleistungen, welche durch eine digitale ID erst in digitalisierter Form umsetzbar würden. Ebenfalls existieren Anwendungsbereiche innerhalb der digitalen (Direkt-)Demokratie der Schweizerischen Eidgenossenschaft, welche aus einer digitalen ID potenziell Nutzen ziehen könnten.

Aus Perspektive der digitalen Behördengänge (virtuelle Behördenshalter) auf Kantons- und Gemeindeebene existiert eine Vielzahl von Dienstleistungen, welche über digitale Kanäle angeboten werden. Die Angebote unterscheiden sich allerdings von Kanton zu Kanton und Gemeinde zu Gemeinde [Bühler et al. 2022, S. 40]. Nach Bühler et al. [2022, S. 40] sind digitale Behördengänge bei der schweizerischen Bevölkerung relativ gut etabliert. Im Vergleich zur digitalen ID werden diese digitalen Dienstleistungen von der Bevölkerung wichtiger eingeschätzt, obwohl Identitätsnachweise häufig Bestandteil davon sind. Eine breite Übersicht über mögliche Behördendienstleistungen in der Schweizerischen Eidgenossenschaft bietet das Bürger:innenportal *ch.ch* [chch - Das Bürgerportal 2022]. Viele dieser Angebote werden bereits digital zur Verfügung gestellt, erfordern jedoch oftmals parallel zur reinen Beantragung die postalische Einreichung von Dokumenten wie Kopien von Pass- oder Identitätskarten. Denkbare Behördendienstleistungen, deren Prozesse durch eine digitale ID von Effizienzsteigerungen und Erhöhungen der Nutzungsfreundlichkeit profitieren könnten, umfassen beispielsweise:

- Bestell- und Beantragungsprozesse von Dokumenten wie AHV-Ausweisen, Betreibungsregisterauszügen, Erbscheinen, Fahrzeugausweisen, IV-Leistungen, Strafregisterauszügen, Waffenerwerbsscheinen, Zivilstandsdokumenten, etc.
- Elektronische Eingaben bei Zivil- und Strafverfahren.
- Elektronische Eingaben von Betreibungsbegehren oder Privatkonkursen.
- Elektronisches Ausfüllen und Einreichen der Steuererklärung.
- Elektronisches Ab- und Anmelden bei der Wohngemeinde im Fall eines gemeindeübergreifenden Umzugs.

Diese digitalen Dienstleistungen werden generell von Kantonen oder Gemeinden angeboten. Einzelne Gemeinden oder Kantone bieten ihren Bürger:innen auch weiterführende, individuelle Dienstleistungen an. Ein aktuelles Beispiel eines digitalen Behördengangs auf Bundesebene ist die Ausstellung des COVID-19-Zertifikats, welches schweizweit online über eine Webseite des Bundes beantragt werden kann. Durch die digitale ID könnten auch neue, bisher unentdeckte Dienstleistungen seitens der Behörden möglich werden.

Für Anwendungen innerhalb der digitalen Demokratieprozesse in der Schweizerischen Eidgenossenschaft birgt die digitale Identität ebenfalls grosse Potenziale. Die elektronische Stimmabgabe bei Abstimmungen und Wahlen (E-Voting) ist ein Beispiel für einen Anwendungsfall, welcher erst durch die Existenz einer digitalen ID möglich würde [Bühler et al. 2022, S. 44]. Durch ihr direktdemokratisches Politiksystem können Bürger:innen in der Schweizerischen Eidgenossenschaft wie kaum eine andere Bevölkerung regelmässig ihre Meinung zu verschiedensten Volksinitiativen und Referenden abgeben. In diesem Demokratieprozess spielt der Identitätsnachweis eine Schlüsselrolle: Die Identität einer abstimmenden Person muss zweifelsfrei feststellbar sein, um sicherstellen zu können, dass diese Person stimmberechtigt ist [Cap und Maibaum 2001, S. 805]. Während dies im derzeitigen analogen Prozess mit individuell adressierten und auf postalischem Wege zugestellten Abstimmungsunterlagen umgesetzt wird, würden im digitalen Raum Identitätsnachweislösungen notwendig, um den Zugang zu elektronischen Abstimmungs- und Wahlinstrumenten gewähren und kontrollieren zu können.

Bisaz und Serdült [2017, S. 1] halten nicht das E-Voting, sondern das E-Collecting für die eigentliche Revolution der direkten Demokratie. E-Collecting beschreibt eine digitalisierte Unterschriftensammlung im Rahmen von Volksinitiativen und Referenden. Damit es bei Initiativen und den meisten Referenden zu einer Volksabstimmung kommt, müssen diese von einer bestimmten Anzahl an Bürger:innen unterstützt werden [Bisaz und Serdült 2017, S. 2]. Der Vorgang der Sammlung von Unterschriften wird derzeit analog auf Papier durchgeführt, wobei Bürger:innen einen Sammelbogen ausdrucken und mit ihren Identitätsdaten händisch ausfüllen und unterzeichnen müssen [Bisaz und Serdült 2017, S. 1-2]. Anschliessend müssen die ausgefüllten Sammelbögen wieder über die Briefpost zurückgesandt werden. Bei diesem Prozess ist die Identifizierung von stimmberechtigten Personen ebenso zentral wie bei der Abstimmung selbst.

Während bei Abstimmungen und Wahlen die brieflichen Unterlagen per Stimmregister an die stimmberechtigte Bevölkerung verteilt werden können, können die Sammelbögen zur Unterschriftensammlung grundsätzlich von jeder Person ausgefüllt und unterzeichnet werden. Eine händische Unterschrift ist generell nicht fälschungssicher und es ist möglich, dass sich Personen mit fremden Identitätsdaten als eine andere Person ausgeben. Aufgrund des Mangels an praxistauglichen Alternativen bietet die heutige Lösung keine Möglichkeit zur absolut sicheren Identifizierung einer unterzeichnenden Person [Bisaz und Serdült 2017, S. 3]. Im Rahmen des E-Collecting könnte die digitale ID als technisch zwingende Voraussetzung für die Digitalisierung des Unterschriftensammlns den gesamten demokratischen Prozess im Vergleich zur aktuellen Handhabung sogar sicherer und transparenter machen [Fivaz und Schwarz 2021, S. 91; Bisaz und Serdült 2017, S. 3]. Ebenfalls liessen sich gemäss den Autor:innen Fivaz und Schwarz [2021, S. 91] und Bisaz und Serdült [2017, S. 3]

die Senkung von Transaktionskosten für Behörden und Initiant:innen sowie die Vereinfachung der Teilnahme an direktdemokratischen Entscheidungsprozessen für Bürger:innen erreichen.

Ebenfalls profitieren könnte der Bereich der elektronischen Partizipation (E-Partizipation). Nach Lenz und Ruchlak [2001] ist politische Partizipation die Teilhabe und Beteiligung von Bürger:innen an politischen Willensbildungs- und Entscheidungsprozessen. Als Partizipationslevel gelten allgemein die behördliche Information (bspw. Informationen auf Webseiten, Informationsveranstaltungen), Konsultation (bspw. Vernehmlassungsverfahren, Befragungen) und die aktive Beteiligung (bspw. Workshops) von Bürger:innen in demokratischen Prozessen [Fischer et al. 2020, S. 131]. Von E-Partizipation wird gesprochen, wenn Bürger:innen sich mittels digitaler Hilfsmittel an diesen demokratischen Dialogen beteiligen [Bühler et al. 2022, S. 44]. Durch eine digitale ID könnten neue, die Demokratie stärkende Partizipationsformen realisierbar werden, welche in höherem Masse auf die Identifizierung von partizipierenden Bürger:innen angewiesen sind.

### 2.5 Eidgenössische Abstimmung zur E-ID 2020

Wie bereits in der Einleitung dieser Master-Thesis beschrieben, existiert in der Schweiz kein digitaler Identitätsnachweis. Dies ist weniger der schleppenden Adaption von technologischen Neuerungen innerhalb der Demokratie und des öffentlichen Sektors geschuldet, sondern vielmehr dem Ergebnis der erst kürzlich vollzogenen Volksabstimmung zum *Bundesgesetz über elektronische Identifizierungsdienste* (E-ID-Gesetz) [Eidgenössisches Justiz- und Polizeidepartement 2021b]. Die schweizerische Bevölkerung hat am 7. März 2021 im Rahmen einer eidgenössischen Volksabstimmung die zur Umsetzung einer digitalen ID notwendige Gesetzesgrundlage verhältnismässig deutlich abgelehnt. Der Anteil der Nein-stimmenden Bevölkerung betrug 64.4% und die Bürger:innen keines einzigen Kantons haben in der Mehrheit der Vorlage zugestimmt [Schweizer Radio und Fernsehen 2021].

Geplant gewesen wäre ein staatlich anerkannter, elektronischer Identifikationsnachweis (E-ID), der den Bürger:innen der Schweiz den digitalen Beweis ihrer Identität online ermöglichen sollte [Bundesamt für Justiz 2021]. Als Ziel galt die eindeutige Identifikation von Personen im digitalen Raum zur Unterstützung von Verwaltung und privatwirtschaftlichen Unternehmungen durch medienbruchfreie Prozesse sowie die Reduktion von unnötigen Aufwänden [Bundesamt für Justiz 2021]. Das Konzept sah vor, die technische Umsetzung der E-ID privaten Anbieter:innen zu überlassen, während der Staat als Prüfinstanz die Identität von antragsstellenden Bürger:innen und die Ausstellung einer E-ID durch Anbieter:innen kontrolliert [gfs.bern 2021, S. 25]. Die elektronische ID war als freiwillig zu beziehende Dienstleistung, angeboten von einer Kooperation aus Staat und privaten Unternehmen, geplant.

Gegen die geplante E-ID-Lösung und das ihr unterliegende E-ID-Gesetz wurde im Februar 2020 mit 64'933 gültigen Unterschriften das Referendum ergriffen [gfs.bern 2021, S. 25]. Das Hauptargument des Referendumskomitees war, dass die E-ID nicht von Anbieter:innen aus der Privatwirtschaft herausgegeben werden sollte. Wie das Abstimmungsresultat ein Jahr später zeigte, konnte das Referendumskomitee mit dieser Argumentation die Bevölkerung überzeugen und eine Mehrheit der stimmberechtigten Bürger:innen lehnte die Einführung der E-ID ab.

Das Markt- und Meinungsforschungsinstitut *gfs.bern* hat im Rahmen einer Abstimmungsanalyse die soziodemografischen und politischen Merkmale der Bürger:innen bei der E-ID-Abstimmung untersucht [gfs.bern 2021, S. 25-27]. Während bei den soziodemografischen Merkmalen keine nennenswerten Effekte feststellbar waren und alle gesellschaftlichen Gruppen letztlich mehrheitlich gegen die Vorlage votiert haben, zeigten sich die politischen Merkmale ausschlaggebender. Wähler:innen und Anhängerschaften aller politischen Parteien in der Schweiz haben die Vorlage mehrheitlich abgelehnt [gfs.bern 2021, S. 5].

Einzig die Wähler:innenschaft der Parteien der politischen Mitte (*FDP* und *Die Mitte*) votierten zu knapp 50 % für die E-ID-Vorlage. Allerdings verwiesen Personen, welche sich im politischen Spektrum linksaußen oder links einordnen, die Initiative deutlich stärker als Personen, welche sich der Mitte, rechts oder rechtsaußen zuordnen [gfs.bern 2021, S. 25-27].

Die Motive auf Seiten der Befürworter:innen der E-ID-Vorlage gliederten sich hauptsächlich in die Kategorien Digitalisierung, politökonomische Gründe und Bezüge zum Kompromisscharakter des Gesetzes [gfs.bern 2021, S. 29]. Die Befürworter:innen richteten nach den Autor:innen von gfs.bern [2021, S. 29] ihren Fokus mehrheitlich auf den Fortschritt, die Sinnhaftigkeit der digitalen Zukunft und sahen in der E-ID-Vorlage primär den logischen Schritt in die digitale Welt der Zukunft. Im Vergleich zur Orientierung in Richtung einer innovativen wirtschaftlichen Zukunft stand der praktische Nutzen als Einzelmotiv auf Individualebene eher im Hintergrund.

Auf der Gegenseite stellte gfs.bern [2021, S. 30] zwei Motive fest, welche bei der Bevölkerung Widerstand in Bezug auf die vorgeschlagene E-ID-Lösung auslösten. Der wichtigste Ablehnungsgrund waren Bedenken beim Datenschutz, dicht gefolgt von der Rolle des Staats im Rahmen von Identitätsausweisen. Letztlich wurde auch eine generelle Skepsis gegenüber privaten Unternehmen als Herausgeber:innen der E-ID von Nein-Stimmenden genannt. Insgesamt zeigte sich klar, dass Datenschutzbedenken, Rollen- und Vertrauensfragen sowie Ängste über mögliches Missbrauchspotenzial bei der Mehrheit der Bevölkerung eine ablehnende Haltung auslösten [gfs.bern 2021, S. 5, 25]. Fivaz und Schwarz [2021, S. 85] beschreiben den Widerstand zusätzlich als Resultat einer Dissonanz zwischen dem Anspruch der Bevölkerung an staatliche Identifikation analog zu einem Pass oder einer Identitätskarte und der Ausstellung einer Identifikationslösung durch private Unternehmen.

Welche Implikationen ergeben sich aus diesem Abstimmungsresultat für die Digitalisierung des Staats und der schweizerischen Demokratie? Es scheint angesichts der Analyseerkenntnisse offensichtlich, dass der Staat die Rollenerwartung seitens der Bürger:innen erfüllen muss. Umgekehrt muss eine technische Lösung für den digitalen Identitätsnachweis Vertrauen und Transparenz schaffen können. In Abschnitt 2.1.2 auf Seite 6 zur digitalen Identität sowie in Abschnitt 2.1.4 auf Seite 20 zur digitalen Demokratie und Krypto-Demokratie wurde die immense Wichtigkeit von Vertrauen bei Identifikationsprozessen bereits mehrfach erwähnt. Dass ein hoher Grad an Vertrauenswürdigkeit und Integrität im digitalen Raum ebenso zentral ist wie in der analogen Welt, haben nun ebenfalls die Hauptmotive der Ablehnung zum E-ID-Gesetz bestätigt.

Auch die Autor:innen von gfs.bern [2021, S. 5, 27, 30] führen an, es sei nicht gelungen, Vertrauen in die angedachte technische Lösung aus Datenschutzperspektive

und in die Rolle von privaten Anbieter:innen als Ausweisdienstleister:innen aufzubauen. Zu diesen Erkenntnissen kommt auch der *Mobiliar DigitalBarometer*. Rund 43 % der nachgängig zur Abstimmung befragten Bürger:innen gaben an, eine rein staatlich finanzierte und verwaltete E-ID zu bevorzugen, womit dieses Modell chancen- und gefahrenwahrnehmungsunabhängig das akzeptierteste Modell darstellt [Rüthi et al. 2020, S. 55]. Dabei sollen sich vor allem Bürger:innen der frankophonen Westschweiz für diese Form des digitalen Identitätsnachweis ausgesprochen haben.

Dass für die Bevölkerung die Ausstellung einer digitalen ID mehrheitlich in staatliche Hände gehört, haben die Analysen bestätigt. Ebenfalls hat sich herausgestellt, dass das Votum der Bevölkerung kein Ausdruck von Digitalisierungskritik oder Skepsis gegenüber Fortschritt allgemein ist [gfs.bern 2021, S. 5, 31-32]. Fast zwei Drittel der Bürger:innen assoziieren mit einer rein staatlichen E-ID-Lösung eine garantierter Einhaltung des Datenschutzes und würden einer E-ID-Lösung zustimmen, wenn deren Konzept ihr Vertrauen gewinnen kann. An diesem Punkt kommt die für diese Forschungsarbeit zentrale Technologie der Blockchain ins Spiel. Als postulierte Vertrauensmaschine scheint die Blockchain-Technologie prädestiniert für das Einsatzgebiet des digitalen Identitätsnachweises, in welchem absolute Vertrauenswürdigkeit für die Bürger:innen offensichtlich zentral ist.

Die Vertrauensprämissen im Umgang mit digitalen Identitätsdaten und Identitätsnachweisen bietet im Verbund mit der in der Praxis noch neuartigen Blockchain-Technologie die Grundlage für folgende Fragestellungen: Wie stehen Bürger:innen zur Blockchain-Technologie an sich? Haben Bürger:innen Bedenken vor dem Einsatz der Blockchain-Technologie im Allgemeinen? Würden sich allfällige Datenschutzbedenken in Bezug auf die Blockchain-Technologie auflösen lassen, wenn der Staat selbst diese Technologie vertrauenswürdig einsetzt? Wie stehen Bürger:innen einer Blockchain-Identitätsnachweislösung gegenüber, wenn diese die souveräne und sichere Selbstverwaltung von eigenen Identitätsdaten realisierbar machen würde? Könnten die Potenziale der Blockchain-Technologie - sofern sie Bürger:innen bekannt sind - eine Blockchain-E-ID im Vergleich zur abgelehnten E-ID-Lösung sogar vertrauenswürdiger und attraktiver machen? Fragestellungen dieser Art sollen im Rahmen der empirischen Untersuchung dieser Master-Thesis erforscht werden.

### 2.6 Blockchain-Technologie & Self-Sovereign Identity

Fragen nach der wahren Identität von Menschen und dem Vertrauen in Identitätsysteme stellen sich der Menschheit schon seit Jahrhunderten. Bereits in Texten der hebräischen Bibel Tora täuscht Jakob die Identität seines Bruders vor, um den Segen seines Vaters zu erhalten [Takemiya und Vanieiev 2018, S. 582]. Seither hat sich durch neue technische Entwicklungen, allen voran die Entwicklung des Internets, das Risikopotenzial im Rahmen von Identitätsdaten und -nachweisen stetig verschärft. Toth und Anderson-Priddy [2019, S. 17] sprechen gar von einer alarmierenden Krise der Identität im digitalen Raum, nachdem Identitätsdatenbanken von vielen global führenden Unternehmen mit Millionen von Datensätzen in den letzten Jahren Opfer von Datenlecks geworden sind. Die unautorisiert in fremde Hände gelangten Identitätsdaten haben durch die Vernetzung der Welt die Grundlage für Identitätsdiebstähle in globalem Ausmass geschaffen.

Theoretisch regeln die gebräuchlich vorhandenen Datenschutzgesetze der westlichen Welt den Schutz und die Nutzungsbestimmungen von persönlichen Daten [Toth und Anderson-Priddy 2019, S. 19]. Beim Management von Identitätsdaten schreiben Datenschutzgesetze in der Regel folgende Handlungsrichtlinien vor [Dunphy und Petitcolas 2018, S. 21-22]:

- Generelle Aufforderungen zum grösstmöglichen technischen Schutz von sensitiven Daten.
- Kontrollmöglichkeiten der Identitäts-besitzenden Personen über ihre eigenen Daten.
- Minimale Offenlegung der Identitätsdaten an berechtigte Parteien für eine eingeschränkte Nutzung.
- Offene und selbstbestimmte Teilmöglichkeit der eigenen Identitätsdaten.
- Grösstmögliche Nachvollziehbarkeit und Transparenz für Identitätsdatenteilende Personen darüber, welche Informationen geteilt werden und was mit diesen Informationen geschieht.
- Konsistente Nutzungserfahrungen in verschiedensten Sicherheitskontexten und über verschiedene Plattformen hinweg.

Die praktische Handhabung von Identitätsdaten gestaltet sich jedoch in den meisten Fällen anders, als das Gesetz dies im Optimalfall vorsehen würde. Identitätsdaten von Personen und Identitätsnachweissysteme sind trotz zentralisierter Identitätsdatenbanken oftmals stark fragmentiert. Unterschiedlichste Behörden und Unternehmen verwalten die Identitätsdaten ihrer Bürger:innen und Kund:innen getrennt und zentral in individuellen technischen Lösungen [Rivera et al. 2017, S.

2]. Gleichzeitig sind beispielsweise auch Identitätsdaten für Log-ins ausgesprochen fragmentiert. In den Vereinigten Staaten von Amerika geht man davon aus, dass eine einzelne E-Mail-Adresse durchschnittlich für 130 digitale Konten als Identifizierer dient, was das Missbrauchspotenzial für betrügerische Aktivitäten im Fall von Identitätsdiebstahl massiv erhöht [Zwitter et al. 2020, S. 7].

Während die Fragmentierung von Identitätsdaten über hunderte Identitätsmanagementsysteme hinweg die Wahrscheinlichkeit für Datenlecks steigert, ist auch die zentralisierte Handhabung der Identitätsdaten in den individuellen Systemen von Behörden und Unternehmen aus einer Vertrauensperspektive nicht unproblematisch [Takemiya und Vanieiev 2018, S. 582; Wolfond 2017, S. 36]. Zentralisierte Identitätsysteme bieten den Nutzer:innen zwar meistens eine einfache und bequeme Nutzungserfahrung, unterliegen aber dem technischen Konzept geschuldet Datensicherheits- und Privatsphäre-Limitationen. Sie sind nach Yang und Li [2020, S. 1] durch ihren zentralisierten Aufbau fragil, stellen einen *Single Point of Failure* dar, können vorsätzlicher und interner Manipulation unterliegen und sind durch die Ansammlung von hochsensiblen Daten ein beliebtes Ziel von Cyberangriffen. Ebenfalls bieten die verschiedensten Identitätssysteme ihren Nutzer:innen nur selten tatsächliche Transparenz und Kontrollmöglichkeiten über die eigenen Daten an.

Zentralisierte Identitätssysteme, wie sie heute zum Einsatz kommen, werden im Kontext der voranschreitenden Digitalisierung aller Lebensbereiche stetig unattraktiver. Da heutzutage vermehrt auch biometrische Daten von Menschen verarbeitet werden, entstehen immer grösser werdende Identitätssysteme mit sensibelsten Daten. Angesichts der Häufung von gross angelegten serverseitigen Angriffen, der Frustration der Nutzer:innen bei der Verwaltung von Log-in-Daten und der wachsenden Besorgnis über Datenschutz und Überwachung, ist es nicht überraschend, dass Server-zentrierte Lösungen immer stärker in die Kritik geraten [Stokkink und Pouwelse 2018, S. 1336; Toth und Anderson-Priddy 2019, S. 17].

### 2.6.1 Theoretische Konzepte zum Blockchain-Identitätsnachweis

Um im digitalen Raum ein sicheres, vertrauenswürdiges und technisch solides Identitätssystem etablieren zu können, sollten die derzeitigen Modelle zur digitalen Identität neu gedacht werden. Ein solider Ansatz für das Management digitaler Identitäten muss nach Zwitter et al. [2020, S. 12] verstärkt Fragen des Datenschutzes, der Verhältnismässigkeit von Identitätsdaten und des Dateneigentums berücksichtigen. Die Nutzer:innen von Identitätssystemen rücken dabei vermehrt in den Fokus. Bakre et al. [2017, S. 379-380] haben vier aufeinander aufbauende Stufen der Entwicklung von digitalen Identitätsmanagementsystemen definiert. Es handelt sich um die Stufen *Centralized Identity* (zentralisierte Identität), *Federated Iden-*

*tity* (förderierte Identität), *User-Centric Identity* (nutzer:innenzentrierte Identität) und *Self-Sovereign Identity* (selbstbestimmte Identität). Die meisten derzeitigen Identitätssysteme lassen sich aufgrund ihrer Zentralisation der untersten Entwicklungsstufe zuweisen [Dunphy und Petitcolas 2018, S. 21]. Die Konzepte der User-Centric Identity und der Self-Sovereign Identity gewinnen jedoch immer mehr an Relevanz [Toth und Anderson-Priddy 2019, S. 17]. Diese Konzepte stellen die Besitzenden einer Identität in den Vordergrund und sollen Individuen eine bessere, letztlich vollständig autonome Verwaltung und Kontrolle ihrer privaten Daten ermöglichen.



Abbildung 4: Die vier Entwicklungsstufen der digitalen Identität,  
eigene Darstellung in Anlehnung an Bakre et al. 2017, S. 379.

Auch das World Economic Forum (WEF) hat in einem Report von 2018 ähnliche Archetypen von digitalen Identitätssystemen beschrieben [World Economic Forum 2018]. Als zentralisierte Identitätssysteme ordnet das WEF Systeme ein, in welchen eine einzelne Organisation Identitäten ausstellt und verwaltet. Bei föderierten Systemen etablieren verschiedene öffentliche und private Institutionen ein einzelnes gemeinsames System. Diese Variante ist vergleichbar mit dem in der Volksabstimmung 2021 ursprünglich vorgesehenen Aufbau einer E-ID. Den dritten Archetyp bezeichnet das WEF als dezentralisierte Identitätssysteme. In diesen spielen Institutionen oder private Unternehmen nur noch eine Hilfsrolle, während die Nutzer:innen und deren Identität als Vermögenswert in Zentrum stehen.

Die wissenschaftliche Literatur scheint sich im Grundtenor einig darüber zu sein, dass neue Lösungen für den digitalen Identitätsnachweis bestrebt sein müssen, die rechtliche Identität wieder in die Hände der besitzenden Person zurück zu geben. Eine Weiterentwicklung von der stark zentralisierten Identitätshandhabung hin zu möglichst dezentralisierten, transparenten und eigenständig verwalt- und kontrollierbaren Identitätssystemen wird in praktisch sämtlichen Publikationen zu dieser Thematik empfohlen [Dunphy und Petitcolas 2018, S. 21]. Ähnlich argumentiert Lips [2010, S. 278-279]: Behörden könnten die Informationsbeziehungen zu Bürger:innen neu ausbalancieren, indem sie den Aspekt des Schutzes von Persönlichkeitsrechten in die Gestaltung von Identitätssystemen einbeziehen und dem Individuum die Kontrolle über die Verbreitung von Identitätsdaten ermöglichen. Wenn Identitäts-besitzende Personen wieder die vollständige Kontrolle über ihre Identitätsdaten erlangen sollen, kommt das Konzept der sogenannten *Self-Sovereign Identity* zum Zuge [Dunphy und Petitcolas 2018, S. 21; Stokkink und Pouwelse 2018, S. 1337].

Self-Sovereign Identity - zu Deutsch sinngemäss als vollständig selbstbestimmte Identität übersetzt - beschreibt das Konzept der Identitätsverwaltung auf der höchstmöglichen Entwicklungsstufe. Eine zentralisierte Vertrauenspartei wird in diesem Konzept nicht mehr benötigt. Derzeit existiert noch keine universelle und verbindliche Definition des Begriffs Self-Sovereign Identity [Zwitter et al. 2020, S. 2]. Ins Leben gerufen wurde der Begriff 2016 in einem Online-Beitrag mit dem Titel „*The Path to Self-Sovereign Identity*“ von Christopher Allen [Allen 2016]. Allen, Expert:in für Identitätsmanagement, erläutert darin, wie Identitäten online verwaltet und gespeichert werden sollten.

In diesem Modell werden digitale Identitätsnachweislösungen so konzipiert, dass sie den Besitzenden einer Identität die Schaffung, Verwaltung, Nutzung und Verteilung der Identität und Identitätsdaten vollständig autonom erlauben [Allen 2016; Stokkink und Pouwelse 2018, S. 1336; Takemiya und Vanieiev 2018, S. 582; Toth und Anderson-Priddy 2019, S. 18]. Davon verspricht man sich grosse Fortschritte bezüglich der Privatsphäre, dem Datenschutz und der Sicherheit von Identitätsdaten. Je vertrauensvoller, transparenter und selbstverwalteter ein Identitätssystem für die Nutzer:innen ist, desto breiter wird dieses eingesetzt werden können, was wiederum eine Reduktion der gespeicherten Datenmenge bei einzelnen Dienstleister:innen bedeutet [Toth und Anderson-Priddy 2019, S. 19, 27].



Abbildung 5: Die 10 Prinzipien der Self-Sovereign Identity nach Christopher Allen [Jolocom 2018], bearbeitet.

Damit das Konzept der Self-Sovereign Identity funktioniert, hat Allen [2016] zehn Prinzipien definiert (vgl. Abb. 5 auf der vorherigen Seite). Das Konzept der Self-Sovereign Identity wird möglich, wenn diese Prinzipien von einem Identitätssystem konsequent berücksichtigt werden [Bakre et al. 2017, S. 380-381; Stokkink und Pouwelse 2018, S. 1337; Toth und Anderson-Priddy 2019, S. 19-20]:

- Existenz. Die Nutzer:innen müssen eine unabhängige Existenz haben.
- Kontrolle. Die Nutzer:innen müssen ihre Identität selbst kontrollieren.
- Zugriff. Die Nutzer:innen müssen ständigen Zugriff auf ihre eigenen Daten haben.
- Transparenz. Systeme und Algorithmen müssen transparent sein.
- Beständigkeit. Identitäten müssen dauerhaft sein.
- Portabilität. Informationen und Dienste zur Identität müssen übertragbar sein.
- Interoperabilität. Identitäten sollten möglichst breit nutzbar sein.
- Einwilligung. Die Nutzer:innen müssen der Verwendung ihrer Identität zustimmen.
- Minimalisierung. Die Offenlegung von Informationen muss auf ein notwendiges Minimum reduziert werden.
- Schutz. Die Rechte der Nutzer:innen müssen geschützt werden.

Das Konzept der Self-Sovereign Identity verlangt also nach technischen Lösungen, die in der Lage sind, diesen prinzipiellen Anforderungen gerecht zu werden [Wolfond 2017, S. 36]. Die Architektur eines modernen Identitätssystems sollte die Abhängigkeit von einem einzelnen Vertrauenspunkt reduzieren und verhindern, dass eine einzelne Partei die Transaktionen von Nutzer:innen nachverfolgen kann. Gleichzeitig sollte ein vertrauliches, nicht manipulierbares Nachweisprotokoll über diese Transaktionen geführt werden können. Außerdem sollte die Identität der Teilnehmenden durch modernste kryptografische Technologien und Protokolle geschützt werden.

Eine Technologie, welche diesen hohen Ansprüchen gerecht werden kann, ist die Blockchain-Technologie. Identitätsnachweislösungen auf Basis von Blockchain-Technologie versprechen, einen direkten Sprung von zentralisierten Systemen zu Systemen, die eine Self-Sovereign Identity realisierbar machen. Wie in Abschnitt 2.1.3 auf Seite 13 zur Blockchain-Technologie beschrieben, wird die Blockchain-Technologie häufig mit Kryptowährungen wie Bitcoin in Verbindung gebracht. Allerdings ist es dieselbe Technologie, die jeder teilnehmenden Person in einem Blockchain-Netzwerk auch die Verifizierung anderer Daten, wie zum Beispiel nachprüfbar

Behauptungen über Identität, erlaubt [Takemiya und Vanieiev 2018]. Die Anwendung von Blockchain für digitale Identitätsnachweislösungen birgt folglich das Potenzial, die Transformation im Umgang mit Identitätsdaten fundamental zu beeinflussen [Treblmaier und Beck 2019, S. 234; Underwood 2016, S. 17]. Sie erlaubt die Konzeption von (dezentralen) Identitätssystemen, welche den Nutzer:innen die vollständige Kontrolle über ihre Identitätsdaten ermöglichen [Rivera et al. 2017, S. 1; Takemiya und Vanieiev 2018, S. 582]. Gewährleistet wird diese Kontrolle über die asymmetrische Verschlüsselung einer Blockchain, mithilfe derer Nutzer:innen durch den exklusiven Besitz des privaten Schlüssels alleinige Datenhoheit besitzen. Gleichzeitig stellt die Blockchain einen Rahmen zur Beseitigung von inhärenten Sicherheitsmängeln bei bestehenden Verfahren zur Authentifizierung, Überprüfung und Speicherung von Identitäten [Treblmaier und Beck 2019, S. 234].

Autor:innen wie Yang und Li [2020, S. 1-2] oder Takemiya und Vanieiev [2018, S. 582] führen an, dass die Blockchain als manipulationssichere, verteilte Ledger-Technologie jeder Person ermöglicht, verteilte Ledger zu hosten und Transaktionen dauerhaft aufzuzeichnen. Daher kann das dezentrale Register und der Konsens-Mechanismus zwischen den Nodes genutzt werden, um ein vertrauenswürdiges, verteiltes Digitales Identitätsmanagementsystem (DIMS) in einer nicht vertrauenswürdigen Umgebung zu schaffen. So kann der gesamte Lebenszyklus der Registrierung, Authentifizierung, Autorisierung und Widerrufung abgedeckt werden. Benutzer:innen können ihre Identitäten verwalten, ohne sich auf Dritte verlassen zu müssen. Auf diese Weise lassen sich die Probleme der Identitätsfragmentierung, des Identitätsdiebstahls und des Single Points of Failure in herkömmlichen zentralisierten DIMS lösen. Im Gegensatz zu den herkömmlichen DIMS soll die Blockchain ein vertrauensbasiertes System schaffen, in welchem das Vertrauen in das System und nicht in ein bestimmtes Unternehmen gesetzt wird [Treblmaier und Beck 2019, S. 243].

Generell muss festgehalten werden, dass es nicht ein einzelnes Standard-Modell für eine Blockchain-ID-Lösung gibt. Hunderte verschiedenste Implementationsarten sind je nach Anforderungsart denkbar. Aus diesem Grund werden in dieser Thesis keine technischen Details oder mögliche technische Umsetzungsvarianten diskutiert. Vielmehr wurde innerhalb dieses Kapitels die in der wissenschaftlichen und fachlichen Literatur beschriebene Einsatzmöglichkeit von Blockchain-Technologie für digitale Identitätssysteme auf einer Metaebene dargelegt. Für die geplante Forschung über die Einstellung der schweizerischen Bevölkerung gegenüber dem Einsatz der Blockchain-Technologie zum Zwecke eines digitalen Identitätsnachweises ist der konzeptionelle Machbarkeitsbeleg ausreichend. Ebenfalls beweisen bereits aktive Pilotprojekte in der Praxis, dass sich Blockchain-basierte Identitätsnachweislösungen umsetzen lassen (vgl. Abschnitt 2.7 auf Seite 55).

Rivera et al. [2017, S. 3-4] beschreiben ausserdem eine Limitierung der verfügbaren Arbeiten zum Blockchain-Einsatz im Rahmen von Identitätssystemen. Die Ergebnisse ihrer Untersuchungen zeigen, dass sich die Nutzung von Blockchain für die digitale Identität grösstenteils noch in der Konzeptionsphase befindet. Die Zahl hochwertiger Publikationen zu diesem kombinierten Technologieeinsatz ist gering, aber es ist deutlich zu erkennen, dass die Fachwelt ein grosses Interesse an diesem Thema hat. Die derzeitige Forschung im Bereich der digitalen Identität auf Grundlage von Blockchain konzentriert sich vorgängig darauf, Verbesserungen bezüglich Herausforderungen und Einschränkungen im Rahmen des Technologieeinsatzes zu finden und festzulegen. Ein Grossteil der aktuellen Arbeiten beschreibt weiter Vorteile der Nutzung von Blockchain zur Authentifizierung von Nutzer:innen. Ein weitaus geringerer Teil der Forschung konzentriert sich auf Sicherheitsfragen - gerade in Bezug auf Dezentralisierung und Öffentlichkeit von Daten in einer Blockchain.

Auch Zwitter et al. [2020, S. 12] äussern die Wichtigkeit einer kritischen Auseinandersetzung mit der Blockchain-Technologie für digitale Identitätssysteme. Obwohl Dezentralisierung derzeit sowohl in der Governance-Debatte als auch unter den Blockchain-Befürworter:innen *en vogue* ist, ist sie keineswegs ein Allheilmittel für alle bestehenden Probleme. Die Blockchain-Technologie kann ein Teil nützlicher Lösungen sein, allerdings nur, wenn sie die sozio-rechtlichen und philosophisch-ethischen Notwendigkeiten, welche die digitale Identität mit sich bringt, berücksichtigen kann.

Für die Schweiz ist seit der Abstimmung zur E-ID klar, dass das Vertrauen in neu konzipierte E-ID-Lösungen seitens der Bevölkerung gesteigert werden muss. Eine technische Basis wie die Blockchain-Technologie, welche Self-Sovereign Identity ermöglichen würde, könnte durch ihre positiven Eigenschaften dieses Vertrauen möglicherweise gewinnen. Allerdings ist die Blockchain trotz aktuellem Wirbel rund um die Technologie kein automatischer Heilsbringer. Die Risiken und Hürden einer solchen Umsetzungsvariante müssen ebenfalls sorgfältig evaluiert werden. Nachfolgend wird sich Abschnitt 2.6.2 zuerst spezifisch mit den Chancen und Vorteilen eines Blockchain-Identitätsnachweises befassen. Im Anschluss wird sich Abschnitt 2.6.3 auf Seite 49 mit den Hürden und Risiken auseinandersetzen, wobei - sofern sinnvoll - ein methodischer Relativierungsansatz der vorgängigen Chancen- und Vorteilsargumente verfolgt wird.

### 2.6.2 Chancen & Vorteile des Blockchain-Identitätsnachweises

In Abschnitt 2.1.2 auf Seite 6 zur Einordnung der digitalen Identität wurden allgemein gültige Chancen und Vorteile der Digitalisierung von Identitätsnachweislösungen bereits ausgeführt. Dazu gehören unter anderem Potenziale in der digitalen

Welt der Zukunft wie ökonomische Mehrwerte, neue Geschäftsmodelle, gesteigerte Benutzer:innenfreundlichkeit sowie erhöhte Transparenz und Inklusion. Für die öffentliche Verwaltung und Demokratie verspricht man sich von der Digitalisierung der Identität die Innovation oder Transformation öffentlicher Dienstleistungen, Effizienz- und Effektivitätssteigerungen sowie kundenorientierte, personalisierte und integrierte öffentliche Dienstleistungen [Lips 2010, S. 279]. Das Problem bei der herkömmlichen digitalen Identität besteht nach Treiblmaier und Beck [2019, S. 244] darin, dass das Datensubjekt darauf vertrauen muss, dass:

- Der Staat oder Bevollmächtigte (z. B. ein Unternehmen) die identifizierenden Informationen des Datensubjekts schützen,
- diese Informationen nur an Personen weitergegeben werden, die auf die Informationen zugreifen müssen,
- die Informationen nicht fälschlicherweise verändert werden oder verloren gehen und dass die Informationen bei Bedarf verfügbar sind.

Letztlich ist die digitale Identität Eigentum des Staats oder der Bevollmächtigten: Sie haben die volle Kontrolle über die Identität in vielen Konzepten des digitalen Identitätsnachweises. Hier kann die Blockchain-Technologie ansetzen, um einen dem Leitgedanken der Self-Sovereign Identity folgenden Lösungsansatz zu ermöglichen. Die Potenziale der kryptografisch verschlüsselten Datenbankstruktur von Blockchains gelten als revolutionär und können zur Verringerung der Informationsasymmetrien zwischen Bürger:innen und Staat beitragen [Prashanth Joshi et al. 2018, S. 143; Lips 2010, S. 279]. Identitätsnachweissysteme, welche auf der Blockchain-Technologie aufbauen, bieten neben den allen digitalen Ansätzen inhärenten Vorteilen zusätzliche Potenziale. Die spezifischen Chancen und Vorteile eines Blockchain-basierten Identitätssystems werden im Folgenden dargelegt.

*Schaffung von Vertrauen:* Die Essenz der Blockchain-Technologie liegt in ihrer Fähigkeit, vollständig vertrauensvolle Transaktionen in nicht vertrauenswürdigen Umgebungen zu ermöglichen [Efanov und Roschin 2018, S. 117; Prashanth Joshi et al. 2018, S. 142; Rivera et al. 2017, S. 4; Stokkink und Pouwelse 2018, S. 1342]. Die Herstellung von Vertrauen zählt zu den Grundpfeilern der Blockchain-Technologie und spielt im Umgang mit Identitäten eine kritische Rolle. Generell birgt die Eigenschaft der Vertrauensmaschine die Chance, auch das Vertrauen eher digitalisierungskritischer Personen für digitale Lösungen wie dem Identitätsnachweis und daran gekoppelte Dienstleistungen aus dem öffentlichen und privaten Sektor gewinnen zu können [Rauschenbach und Stucki 2020, S. 53-54; Prashanth Joshi et al. 2018, S. 143]. Das Vertrauenspotenzial eines Blockchain-Identitätsnachweises konstituiert sich aus vielen weiteren Vorteilen der Technologie wie Transparenz, Datenhoheit, Dezentralisierung, Sicherheit und Persistenz.

*Schaffung von Transparenz:* Transaktionen auf einer Blockchain sind automatisch in Form eines Transaktionsverlaufs für berechtigte Teilnehmende nachvollziehbar und somit verifizier- und validierbar [Hou 2017, S. 2; Prashanth Joshi et al. 2018, S. 143]. In Kombination mit dem Vorteil der Immutabilität von Einträgen auf einer Blockchain entsteht die Chance auf eine bisher unerreichte Transparenz und Nachvollziehbarkeit im Umgang mit Identitätsdaten [Rivera et al. 2017, S. 4]. Stokkink und Pouwelse [2018, S. 1337] sprechen von einen Art Prüfprotokoll, welches Identitätsdelikte sofort sichtbar machen kann und bei Notwendigkeit auch als rechtliche Grundlage zur Strafverfolgung bei Identitätsmissbrauch dienen könnte. Die Transparenz wirkt ebenfalls dem Blackbox-Charakter entgegen, welchem die Identitätsdaten verwaltenden Institutionen oder Unternehmen teilweise unterliegen [Rauschenbach und Stucki 2020, S. 53].

*Kontrolle und Datenhoheit:* Die Blockchain-Technologie ermöglicht durch asymmetrische Verschlüsselung die Umsetzung eines digitalen Identitätsnachweises, in welchem die Nutzer:innen erstmals in der Geschichte die vollständige Kontrolle über ihre eigenen Identitätsdaten erhalten [Stokkink und Pouwelse 2018, S. 1337, 1342]. Die eine Identität besitzende Person hat vollständigen, exklusiven Zugriff auf ihre Identitätsdaten und kann eigenständig entscheiden, welche Daten mit welchen Parteien geteilt werden [Stokkink und Pouwelse 2018, S. 1337; Takemiya und Vanieiev 2018, S. 583; Treiblmaier und Beck 2019, S. 251]. Ebenfalls ist ein Verlust der eigenen Identitätsdaten in einer Blockchain-Lösung nicht möglich, solange die Identität-besitzende Person über den privaten Schlüssel verfügt [Dunphy und Petitcolas 2018, S. 21].

*Dezentralisierung und Verfügbarkeit:* In dezentral aufgebauten Blockchain-Lösungen zum Identitätsnachweis werden Identitätsdaten nicht mehr von einer einzelnen, zentralisierten Autorität kontrolliert [Dunphy und Petitcolas 2018, S. 20]. Stattdessen sind die Informationen auf einem Ledger über alle am Netzwerk teilnehmenden Nodes verteilt verfügbar. Diese Eigenschaft von dezentralisierten Blockchains ist ebenfalls ein entscheidender Vorteil, wenn es um die Verfügbarkeit von Identitätsdaten geht [Prashanth Joshi et al. 2018, S. 142]. Es ist allerdings möglich, Blockchains in zentralisierter Form einzusetzen, womit dieser Vorteil entfallen würde.

*Sicherheit und Resilienz:* Blockchain-Netzwerke sind enorm resistent gegenüber Cyberangriffen [Bisaz und Serdült 2017, S. 1392; Hou 2017, S. 2; Wolfond 2017, S. 37]. Das wichtigste Merkmal der Blockchain ist für Prashanth Joshi et al. [2018, S. 142] die mit anderen technischen Lösungen unvergleichliche Sicherheit im Internet, wo Gefahren wie Phishing, Malware, *Distributed Denial-of-Service*-Attacken, Spam und Hacks global immer mehr zum Problem werden. Biswas und Muthukkumarasamy [2016, S. 1393] sehen in Resilienzaspekten von Blockchain-basierten Lösungen wie höherer Zuverlässigkeit und besserer Fehlertoleranz weitere Vorteile.

*Persistenz und Immutabilität:* Einmal in die Blockchain eingetragene Informationen können nachträglich nicht mehr verändert werden. Damit garantiert die Blockchain die absolute Immutabilität von vergangenen Transaktionen und die Persistenz derer Daten [Hou 2017, S. 2; Prashanth Joshi et al. 2018, S. 142; Stokkink und Pouwelse 2018, S. 1337]. Die Transaktionen bei der Handhabung von Identitätsdaten können so jederzeit im Nachhinein detailliert und zuverlässig nachvollzogen werden [Rauschenbach und Stucki 2020, S. 53]. Anpassungen an bestehenden Daten sind möglich, führen allerdings zu einem neuen Eintrag in der Blockchain. Die vorherigen Daten sind danach weiterhin einsehbar, da sämtliche getätigten Änderungen in der Transaktionshistorie transparent nachvollziehbar bleiben [Dunphy und Petitcolas 2018, S. 21].

*Effizienzsteigerungen und Kosteneinsparungen:* Obwohl die Potenziale von Kosten einsparungen und Effizienzsteigerungen allen digitalen Identitätsnachweislösungen gemein sind, bietet ein Blockchain-basierter Identitätsnachweis zusätzliche Chancen in diesem Bereich. Sowohl Dunphy und Petitcolas [2018, S. 2] als auch Rauschenbach und Stucki [2020, S. 54] sprechen von dem Blockchain-spezifischen Vorteil des effizienteren Mitteleinsatzes. Da Daten auf einer Blockchain für alle berechtigten Teilnehmenden gleichermaßen verfügbar sind, reduzieren sich die Kosten für den Datenzugang. Außerdem müssen Daten nur einmal gespeichert werden, was die Notwendigkeit zur Datenreplizierung in verschiedenen Datenbanken überflüssig macht. Dies erhöht letztlich auch die Datenkonsistenz und steigert die Effizienz im Zusammenhang mit der Datenverwaltung.

### 2.6.3 Hürden & Risiken des Blockchain-Identitätsnachweises

Hürden und Risiken der generellen Digitalisierung von Identitätssystemen und Identitätsdaten wurden in Abschnitt 2.1.2 auf Seite 6 zur digitalen Identität bereits behandelt. Risikobereiche umfassen die Sicherheit von sensiblen Daten als auch deren Transaktionen und Integrität. Weiter unterliegen digitale Identitätssysteme inhärentem Missbrauchspotenzial und Risiken durch Machtkonzentration. Auch Themen wie die Verfügbarkeit von Identitätsnachweislösungen gelten für sämtliche Ansätze der Digitalisierung von Identität. Als neuartige Technologie unterliegt die Blockchain-Technologie weiteren Ungewissheiten, Hürden und Risiken im Einsatz als Basisinfrastruktur für digitale Identitätssysteme.

Wie bei praktisch allen radikalen Innovationen bestehen bei deren Adaptionen erhebliche Risiken [Crosby et al. 2016, S. 16-17]. Trotz ihrer revolutionären und vielversprechenden Potenziale sollte die Blockchain-Technologie nicht als Patentlösung für technische Anwendungsbereiche wie Identitätsnachweislösungen betrachtet werden [Dunphy und Petitcolas 2018, S. 29]. Wie bei allen Technologien existieren

auch bei der Blockchain für jeden Einsatzbereich offene und ungeklärte Umsetzungsfragen und verschiedenste Implementationsmöglichkeiten der Blockchain müssen gegeneinander abgewogen werden [Efanov und Roschin 2018, S. 117]. Es besteht die Tendenz, die meisten neu entstehenden Technologien überzubewerten und übermäßig zu nutzen, ohne deren Limitationen und Misskonzeptionen ausreichend zu berücksichtigen [Yaga et al. 2018, S. 34].

Angesichts der Funktionsweise der Identifizierung im digitalen Raum sind die Auswirkungen eines Systemfehlers für eine ‚unschuldige‘ Person schwerwiegend [Sullivan 2016, S. 477]. Unabhängig davon, ob der Fehler zufällig ist oder durch den Missbrauch der Identität durch eine andere Person hervorgerufen wurde, gefährdet dieser die Integrität einer digitalen Identität. Dies kann schwerwiegende und langfristige Auswirkungen für die Identitäts-besitzende Person mit sich bringen. Aus diesem Grund ist Vertrauen in die hinter einer digitalen ID stehende Technologie von grösster Wichtigkeit. Für Hou [2017, S. 3] darf dies allerdings kein blindes Vertrauen sein.

Die grösste Gefahr geht derzeit nicht von den Schwachstellen des Systems aus, sondern von möglicherweise blinderem Vertrauen in die Blockchain seitens Blockchain-Entwickler:innen, Gesetzgeber:innen, Behörden und von Teilen der Öffentlichkeit im Allgemeinen. Dieses Vertrauen verlässt sich ausschliesslich auf die Versprechen der Technologie. Es kann jedoch nicht garantiert werden, dass die Technologie tatsächlich dauerhaft fehlerfrei funktioniert und bei einer Umsetzung deren Limitationen ausreichend berücksichtigt wurden. Folglich werden die wichtigsten Hürden und Risiken einer auf der Blockchain-Technologie basierenden Identitätsnachweislösung dargelegt. Hierzu werden ebenfalls einige der vorgängig in Abschnitt 2.6.2 auf Seite 46 angeführten Chancen und Vorteile einer Blockchain-ID relativiert und eingeordnet.

*Relativierung der Vertrauensmaschine:* Die Blockchain-Technologie verfügt über Eigenschaften, welche sie unter der Annahme perfekter Rahmenbedingungen zu einer absoluten Vertrauensmaschine machen können. Vertrauen basiert auf der Prämisse, dass die Blockchain die Sicherheit und Privatsphäre von in ihr gespeicherten Identitätsdaten durch Eigenschaften wie Kryptografie, Datenhoheit und Dezentralität schützt [Prashanth Joshi et al. 2018, S. 131-133, 140]. Je nach Umsetzungsart der Blockchain-ID sind die Daten - und damit auch Transaktionsdaten über beispielsweise das Vorzeichen der ID an einem bestimmten Ort - allerdings für sämtliche Netzwerke teilnehmende transparent einsehbar. Dies ist bei öffentlichen (public) und allen zugänglichen (non-permissioned) Blockchains der Fall. Werden anstelle von öffentlichen Blockchains private und zugangskontrollierte (permissioned) Blockchains verwendet, entstehen daraus wiederum sowohl Vor- als auch Nachteile. Es müssen für eine digitale ID auf Basis von Blockchain bei der Umsetzung folglich diverse Implementationsvarianten geprüft und deren Vor- und Nachteile sorgfältig abgewogen

werden. Eine weitere häufige Fehlinterpretation entsteht aus der Annahme, dass bei Blockchain-Systemen keine vertrauenswürdige dritte Partei existiert [Yaga et al. 2018, S. 38]. Zwar gibt es in öffentlich zugänglichen Blockchain-Systemen keine vertrauenswürdige Drittpartei, die Transaktionen zertifiziert (in zugangskontrollierten Systemen ist dies weniger eindeutig, da die Administrator:innen dieser Systeme als Vertrauensverwalter:innen fungieren, indem sie den Nutzer:innen Zutritt und Berechtigungen gewähren). Doch für die Nutzung eines Blockchain-Netzwerks ist immer noch ein hohes Mass an Vertrauen erforderlich: Es besteht Vertrauen in die verwendeten kryptografischen Technologien, in den korrekten und fehlerfreien Betrieb sowie in die Entwickler:innen der Software, eine möglichst fehlerfreie Software bereitzustellen. Das Vertrauensattribut der Blockchain ist in der Folge nicht absoluter, sondern relativer Natur. Werden berechtigte Bedenken hinsichtlich der Art und des Umfangs eines Identitätssystems nicht berücksichtigt, kann dies zu einer begrenzten Akzeptanz oder sogar zur Aufgabe des Systems führen [Whitley et al. 2014, S. 24]. Durch die relative Neuheit der Blockchain-Technologie an sich, der inhärenten Komplexität der Technologie als auch einer differenzierten Wahrnehmung der allgemeinen Bevölkerung von Bitcoin und Blockchain, ist von einer allgemeinen Skepsis gegenüber einer Blockchain-ID auszugehen. Es kann nicht davon ausgegangen werden, dass das Vertrauenspotenzial der Blockchain aus technologischer Sicht automatisch zu Vertrauen bei potenziellen Nutzer:innen, insbesondere im Kontext von Blockchain und hochsensiblen Identitätsdaten, führt.

*Relativierung der Kontrolle und des Netzwerkbesitzes:* Ein verbreiteter Trugschluss ist, dass Blockchain-Netzwerke Systeme vollständig ohne Kontrolle und Eigentum sind [Yaga et al. 2018, S. 35]. Dies ist nicht unbedingt richtig. Zugangskontrollierte Blockchain-Netzwerke werden in der Regel von Eigentümer:innen oder einem Konsortium eingerichtet, betrieben und kontrolliert. Offene und völlig dezentrale Blockchain-Netzwerke werden häufig von Nutzer:innen, Node-Betreiber:innen und Softwareentwickler:innen verwaltet. Jede Gruppe verfügt über ein gewisses Mass an Kontrolle über das Blockchain-Netzwerk. Umgekehrt stellen sich aus rechtlicher Sicht auch Fragen zur Verantwortlichkeit und Haftung bei Blockchain-Netzwerken im Falle von illegalen Praktiken oder Fehlfunktionen [Treiblmaier und Beck 2019, S. 252]. Je stärker ein Blockchain-Netzwerk zentralisiert und zugangskontrolliert wird, desto kleiner wird der Kreis an netzwerke teilnehmenden Nodes, was wiederum die relative Kontrollmöglichkeit und Verantwortlichkeit der beteiligten Nodes erhöht [Prashanth Joshi et al. 2018, S. 133].

*Relativierung der Dezentralisation:* Im Kontext von Identitätsdaten und der mutmasslich vorherrschenden Interpretation von Identität als Staatsaufgabe scheinen zentralisierte Blockchain-Lösungen naheliegend. Auch Dunphy und Petitcolas [2018, S. 26-28] haben festgestellt, dass bei Blockchain-Systemen für Identitätsnachweise in unterschiedlichem Ausmass Techniken der Dezentralisierung eingesetzt werden.

Diese dienen jedoch hauptsächlich dazu, die Rolle der Zentralisierung und der Vermittler:innen neu zu gestalten, anstatt sie zu beseitigen. Notwendig oder hilfreich kann die Zentralisierung für beispielsweise folgende Aufgaben sein: Die Erfassung zusätzlicher Authentifizierungsfaktoren von Endnutzer:innen, die Sicherung und Wiederherstellung kryptografischer Schlüssel oder die Wiederherstellung kompromittierter digitaler Identitäten. Die Verminderung der Dezentralität bringt jedoch unausweichlich Nachteile bezüglich der Vertrauensprämisse, Transparenz und Sicherheit vor Cyberangriffen der Blockchain-Technologie mit sich [Efanov und Roschin 2018, S. 119].

*Relativierung der inneren und äusseren Sicherheit:* Die enorme Sicherheit von Blockchain-Netzwerken stellt eines der Hauptargumente für den Einsatz dieser Technologie dar. Dennoch gilt auch die Sicherheit einer Blockchain nicht absolut [Ahram et al. 2017, S. 3; Prashanth Joshi et al. 2018, S. 140]. Blockchains werden als sicherer als bestehende Systeme angepriesen, und das scheint sich für die Anwendung Bitcoin auch zu bestätigen. Die Sicherheit einer breiteren Anwendung mit abweichenden Implementationsformen in Bezug auf Dezentralität und Öffentlichkeit, insbesondere für Identitätsnachweise und -daten, ist jedoch weitgehend ungetestet und unbekannt [Treiblmaier und Beck 2019, S. 252]. Eines der Hauptrisiken für Blockchain-Netzwerke besteht in der sogenannten *51 %-Attacke*. Wenn mehr als 51 % der Hash-Rate von einer einzigen Node oder einem Zusammenschluss von Nodes kontrolliert wird, kann die Blockchain böswillig manipuliert werden [Efanov und Roschin 2018, S. 119]. Angreifer:innen im Besitz von 51 % der Rechenleistung eines gesamten Blockchain-Netzwerks können beliebig die längste - und damit als „wahr“ geltende - Kette definieren. In diesem Fall ist auch die Immutabilität von Einträgen auf der Blockchain nicht mehr gewährleistet [Yaga et al. 2018, S. 34]. Im Allgemeinen ist es jedoch äusserst schwierig, die dazu erforderliche Rechenleistung zu erlangen. Hier besteht wiederum ein Bezug zur Relativität von Vertrauen: Die Nutzer:innen müssen in einem Blockchain-Netzwerk darauf vertrauen, dass andere Teilnehmende nicht im Geheimen zusammenarbeiten, um 51 % der Netzwerkleistung zu besitzen [Yaga et al. 2018, S. 38]. Der Einsatz der Blockchain-Technologie beseitigt ebenfalls nicht die inhärenten Cybersicherheitsrisiken, die ein umsichtiges und vorausschauendes Risikomanagement erfordern [Yaga et al. 2018, S. 36]. Künftige technologische Entwicklungen bergen weiter das Risiko, derzeit als sicher geltende und in Blockchain-Netzwerken eingesetzte Verschlüsselungsverfahren - und damit die Kernprämisse von Vertrauen - auszuhebeln [Crosby et al. 2016, S. 17]. Fortschritte im Bereich der Quantencomputer könnten durch enorm gestiegerte Rechenleistung die heutigen Verschlüsselungsmethoden umgehen. Allerdings kann davon ausgegangen werden, dass durch Quantencomputer ebenfalls neue, wiederum widerstandsfähige Verschlüsselungsmethoden entwickelt werden können, womit sich dieses Risiko aufheben würde.

*Relativierung des Kosteneinsparungspotenzials:* Die Potenziale im Bereich von Kosteneinsparungen durch den Einsatz von Blockchain-Technologie zum Identitätsnachweis müssen gegen diverse Kosten von Entwicklung und Betrieb eines Blockchain-Netzwerks abgewogen werden. Der Aufbau einer Blockchain-Plattform umfasst eine Reihe verschiedener Systeme und Organisationen und verursacht erhebliche Kosten. Für Behörden kann es umständlich sein, die Kosten für diese neue Plattform zu rechtfertigen, wenn bereits traditionelle Infrastruktur vorhanden ist. Bei Blockchain-Netzwerken, und insbesondere solchen, die Proof-of-Work verwenden, verursacht der Betrieb hohe Kosten in Form von Energieverbrauch [Yaga et al. 2018, S. 38]. Neben dem in der Öffentlichkeit in Kritik stehenden Energieverbrauch des Bitcoins verursachen auch andere Blockchain-Anwendungen erhebliche Energieaufwände [Gallersdörfer et al. 2020].

*Datenübertragbarkeit:* Blockchain-Systeme existieren nicht isoliert, sondern sind in einem komplexen Geflecht von Systemen mit unterschiedlichsten technologischen Basen eingebettet. Der Austausch von Identitätsdaten zwischen herkömmlichen Datenbanksystemen und Blockchain-Systemen ist mit Schwierigkeiten verbunden [Yaga et al. 2018, S. 36]. Das sogenannte *Oracle*-Problem umschreibt die Herausforderung, verlässliche Mechanismen zu schaffen, um externe und interne Daten vertrauenswürdig und genau auszutauschen. Darüber hinaus argumentieren Melin et al. [2016, S. 93], dass eine erweiterte, kontextbezogene Sichtweise gerade in Bezug auf Identitätsnachweise wahrscheinlich noch wichtiger werden wird, um die Anforderungen der *eIDAS*-Regulationen [Europäische Kommission 2022] im Zusammenhang mit grenzüberschreitenden ID-Interoperabilitäten bewältigen zu können.

*Skalierbarkeit:* Die Skalierung von Blockchain-basierten Diensten stellt eine Herausforderung dar. Breit genutzte Blockchains werden durch stetige Transaktionen immer umfangreicher und wachsen u.U. exponentiell [Crosby et al. 2016, S. 17]. Erstnutzer:innen müssen die gesamte Datenkette herunterladen und validieren, bevor Sie Ihre erste Transaktion ausführen können [Prashanth Joshi et al. 2018, S. 140]. Dies kann bei grossen Blockchains viel Zeit in Anspruch nehmen.

*Nutzer:innenfreundlichkeit:* Dunphy und Petitcolas [2018, S. 29] attestieren ein mangelndes Verständnis der Zusammenhänge in Bezug auf Elemente der Nutzer:innenerfahrung. Es scheint die weit verbreitete Annahme zu sein, dass Nutzer:innen eines Blockchain-Systems in der Lage sind, ein effektives kryptografisches Schlüsselmanagement durchzuführen und intuitiv die Wichtigkeit und Tragweite dessen zu verstehen. Die Sicherheit und Zugänglichkeit von Daten hängt von der (eigenständigen) Sicherung des privaten Schlüssels ab, der eine Form der digitalen Identität darstellt [Efanov und Roschin 2018, S. 119]. Wird die Verwaltung des privaten Schlüssels bei Self-Sovereign-Identitätssystemen auf

Blockchain-Basis (konsequenterweise) in die Hände der Nutzer:innen gegeben, so müssen diese auch die Verantwortung und Implikationen dieses Vorgehens verstehen können. Rauschenbach und Stucki 2020 [2020, S. 28] fassen die Problematik wie folgt zusammen: „*Wenn die alleinige Kontrolle über die kryptografischen Schlüssel bei den Benutzenden liegt - wie bei Blockchain-Lösungen üblich - gibt es allerdings diverse Herausforderungen bezüglich Benutzerfreundlichkeit und dementsprechend einen hohen Aufklärungsbedarf.*“ Es existieren in der Praxis allerdings bereits erste Ansätze, welche die verschlüsselte Verwaltung von Schlüsselpaaren durch eine zentralisierte Handhabung nutzer:innenfreundlicher zu gestalten versuchen, ohne die Sicherheit oder Datenhoheit zu beeinträchtigen (vgl. *Sora Identity System* und *Sovrin™* in Abschnitt 2.7 auf der nächsten Seite).

## 2.7 Blockchain-Identitätsnachweis in der Praxis

Im Gegensatz zu Projekten, welche die Digitalisierung der Identität mithilfe traditioneller technologischer Ansätze umzusetzen versuchen, existieren relativ wenig ID-Projekte auf Blockchain-Basis. Dennoch wird im Rahmen von Pilotprojekten und Konzepten global versucht, die Potenziale der Blockchain für Identitätsnachweislösungen auch in der Praxis nutzbar zu machen. Im Folgenden werden einige dieser Projekte und Konzepte vorgestellt, welche die Blockchain-Technologie zum Zwecke des Identitätsnachweises einsetzen.

Das *Sora Identity System* ist ein Konzept für ein Identitätssystem, welches über eine mobile Applikation auf Basis von Blockchain-Technologie ein sicheres Protokoll für die Abspeicherung verschlüsselter personenbezogener Daten sowie den Austausch derselben erstellt [Takemiya und Vanieiev 2018, S. 582]. Die Hauptkomponenten sind die Benutzer:innen, das mobile Gerät, ein zentraler Server und eine Blockchain-Plattform (*Hyperledger Iroha*). Die Besonderheit dieses Konzepts liegt in der Handhabung der Schlüssel von Benutzer:innen. Diese werden auf dem Server in verschlüsselter Form gespeichert und können vom Server nicht entschlüsselt werden [Shobanadevi et al. 2021, S. 2]. Nur die Besitzer:innen eines Schlüsselpaares können dieses entschlüsseln. Dadurch sollen die Problematiken der komplexen, eigenverantwortlichen Handhabung sowie des möglichen Verlusts von Schlüsselpaaren gelöst werden [Takemiya und Vanieiev 2018, S. 583-585]. Folglich kann durch diese Lösung die Nutzer:innenfreundlichkeit auch bei Self-Sovereign-Identity-Systemen erhöht werden.

Ein weiteres Konzept eines Blockchain-Identitätssystems nennt sich *Sovrin*<sup>TM</sup> [Sovrin Foundation 2018]. Das Protokoll *Sovrin*<sup>TM</sup> beschreibt eine Open-Source-Identität, die auf der Blockchain-Technologie aufbaut und Identitätsdaten speichert [Shobanadevi et al. 2021, S. 5]. *Sovrin*<sup>TM</sup> wurde streng nach dem Prinzip *Privacy by Design* entwickelt. Das Protokoll ermöglicht es den Benutzer:innen, verschiedene digitale Identitäten zu erstellen, welche sie eigenständig verwalten können. Die Benutzer:innen kommunizieren mit der *Sovrin*<sup>TM</sup>-Blockchain über eine mobile Applikation. Die mobile Anwendung hilft den Benutzer:innen - wie beim *Sora Identity System* - bei der Verwaltung ihrer kryptografischen Schlüssel. *Sovrin*<sup>TM</sup> bietet die volle Kontrolle über alle Aspekte der Identität und versucht damit, das Konzept der Self-Sovereign Identity nutzbar zu machen.

Eine Open-Source-Lösung, welche bereits innerhalb der Schweizerischen Eidgenossenschaft im Rahmen eines Pilotprojekts der Stadt Zug als technologische Basis zum Einsatz kam, ist *uPort* [uPort 2021]. Auf das Projekt der Stadt Zug wird nachfolgend detaillierter eingegangen. *uPort* ist ein System für die selbstverwaltete Identität und verwendet Smart-Contract-basierte Identitäten [Shobanadevi et al. 2021, S. 4-5]. Genauer gesagt ist eine *uPort*-Identität eine vollständige digitale

Repräsentation einer Person (oder einer App, einer Organisation, eines Geräts, etc.), die in der Lage ist, Aussagen darüber zu machen, wer sie ist, wenn sie mit Smart-Contracts und anderen *uPort*-Identitäten interagiert [Braendgaard 2017]. Die Fähigkeit, Aussagen über sich selbst zu machen, ohne sich auf zentralisierte Identitätsanbieter:innen zu verlassen, macht *uPort* zu einer Plattform für selbstverwaltete Identität. Das System wird von der *Ethereum Virtual Machine* ausgeführt und basiert somit auf der Ethereum-Blockchain. Die privaten Schlüssel der Nutzer:innen werden auf den mobilen Geräten der Benutzer:innen gespeichert. Im Gegensatz zu den zuvor beschriebenen Lösungen wie *Sora* oder *Sovrin*™ verfügt *uPort* nicht über einen zentralen Server zur Authentifizierung und Schlüsselverwaltung.

Blockchain-Einsätze für Identitätsnachweislösungen durch Behörden wurden auf Basis von Pilotprojekten in verschiedenen Ländern weltweit vorgenommen. Die finnische Migrationsbehörde führte ab 2015 ein Projekt zur beschleunigten Flüchtlingsintegration ein [Eixelsberger et al. 2019, S. 509; ReliefWeb 2018]. Die Regierung verteilte den Flüchtlingen Prepaid-Kreditkarten, wodurch diese automatisch auch in Besitz eines Bankkontos gelangten. Zur Identifikation der Menschen setzte die finnische Regierung auf einen Blockchain-Identitätsnachweis. Die Regierung von Moldawien versuchte im Rahmen der Bewältigung von Flüchtlingswellen ab 2018 ebenfalls eine Blockchain-Lösung für die fälschungssichere und dezentrale Verwaltung von Identitätsdaten zu entwickeln [Eixelsberger et al. 2019, S. 509]. Durch die Lösung können die Flüchtlinge über ein mit der Blockchain-ID verknüpftes Bankkonto via Fingerabdruck- oder Iris-Scan ihre Einkäufe bezahlen. Die biometrischen Daten werden auf der Blockchain gespeichert.

In Dubai, der Hauptstadt der Vereinigten Arabischen Emirate, wurde 2017 der Versuch für einen digitalen Pass zur weltweit ersten *Gate-Less*-Grenzüberschreitung am Flughafen von Dubai unternommen [Eixelsberger et al. 2019, S. 510; Cuen 2017]. Dubais digitale Pässe werden in diesem Konzept mit den physischen Pässen der Reisenden verbunden. In biometrischen Tunnels werden 3D-Scans von den Gesichtern der Reisenden gemacht und es wird Gesichtserkennungssoftware eingesetzt, um die Identität ohne langes Anstehen bei der Passkontrolle zu überprüfen. Dank der Blockchain-Technologie können die Reisenden selbst darüber entscheiden, welche Informationen in den digitalen Pass aufgenommen werden und wer diese einsehen kann. Dies macht die Lösung weniger invasiv, als es zunächst den Anschein hat.

Projekte zur Einführung von Identitätssystemen für den allgemeinen, staatlich anerkannten Identitätsnachweis auf Blockchain-Basis hat beispielsweise Estland entwickelt. Estland gilt als eines der Pionierländer, wenn es um die Entwicklung von Identitätsnachweislösungen unter Anwendung von Blockchain-Technologie und Self-Sovereign Identity geht [Takemiya und Vanieiev 2018, S. 582; Treiblmaier und Beck 2019, S. 249-250]. Sullivan [2018, S. 727-728] beschreibt das Projekt unter dem

Gesichtspunkt von *internationaler Identität* eingehend. Als *E-Residency-Programm* bezeichnet Estland das faktisch erste von einer Regierung genehmigte, betriebene, internationale und digitale Identitätsprogramm. Das Hauptziel des E-Residency-Programms ist die Erweiterung der wirtschaftlichen Basis Estlands. Personen, die weder estnische Staatsbürger sind noch ihren Wohnsitz in Estland haben oder sich dort physisch aufhalten, können virtuelle wirtschaftliche Einwohner:innen Estlands werden. Als E-Resident:in kann eine Person praktisch überall auf der Welt aus der Ferne eine ganze Reihe von Geschäftstätigkeiten mit Unternehmen und Behörden ausüben. Da Estland Mitglied der Europäischen Union ist, erleichtert die E-Residency auch den Zugang zu Europa.

Ein Beispiel eines unter dem Gesichtspunkt westlicher Demokratien streitbaren Einsatzes der Blockchain-Technologie zum Nachweis von Identitäten beschreibt Hou [2017]. Im Stadtbezirk Chancheng der chinesischen Provinz Guangdong wurde 2016 ein Pilotprojekt zum Einsatz der Blockchain-Technologie in E-Government-Systemen gestartet. Nach eigenen Angaben der Behörden von Chancheng sollte eine offene Plattform auf Basis von Blockchain-Technologie aufgebaut werden, um das gegenseitige Vertrauen zwischen Regierung, Unternehmen und Bürger:innen zu stärken. Eines der beiden Hauptziele der Einführung der Blockchain-Plattform war es, durch den Aufbau eines digitalen Identitätssystems das „*Problem des individuellen Kredits*“ von Personen zu lösen. Die beschriebene langfristige Vision, dass die Bürger:innen ihren individuellen Kredit dadurch vermehrt schätzen würden, ihr Bestes tun würden, um einen guten Kredit zu erhalten und dies der Regierung sowie der sozialen Harmonie zugute kommen würde, lassen die Vermutung zu, dass es sich dabei um das Sozialkredit-System Chinas handelt. Der Blockchain-Identitätsnachweis würde in diesem Kontext dazu dienen, die aus ethischer Sicht fragliche Überwachung und Kontrolle von Bürger:innen zu stärken.

In der Schweizerischen Eidgenossenschaft haben sowohl die Stadt Zug als auch der Kanton Schaffhausen Pilotprojekte für Behördendienstleistungen unter Anwendung von Blockchain-basierten Identitätsnachweisen durchgeführt [Stadt Zug 2017; Kanton Schaffhausen 2021]. Die Stadt Zug bot ihrem Bürger:innen bis zur Einstellung des Projekts im Sommer 2020 eine auf *uPort*-basierende, digitale ID an. 2017 war die Stadt damit die erste Behörde in der Schweiz, welche eine Blockchain-basierte Identität eingeführt und an rund 250 Personen ausgestellt hat [Rauschenbach und Stucki 2020, S. 27; Müller und Windisch 2018, S. 12]. Rauschenbach und Stucki [2020, S. 27-28] halten fest, dass das Projekt im Sinne eines *Proof-of-Concept* als Erfolg gewertet werden kann. Der provisorische Charakter des Vorhabens lässt jedoch nur beschränkt die Ableitung von Erkenntnissen bezüglich beispielsweise der Skalierbarkeit oder der datenschutzrechtlichen Perspektive der eingesetzten Lösung zu.

Der Kanton Schaffhausen hat 2018 ebenfalls ein *Schaffhauser eID+* benanntes Projekt zum digitalen Identitätsnachweis im Rahmen von Behördendienstleistungen des Kantons lanciert [Kanton Schaffhausen 2021; Müller und Windisch 2018, S. 12]. Stand Januar 2021 wurde die digitale Identität von rund 2'000 Bürger:innen verwendet. Die Basis dieser E-ID-Lösung bildete die *eID+* benannte Blockchain-Lösung der *Procivis AG*, eine Smart-Government-Lösung für digitale Behördendienstleistungen [Procivis 2022a]. Der Kanton Schaffhausen ermöglicht durch die selbstverwaltete, digitale ID ihren Bürger:innen sicheren und einfachen Zugriff auf verschiedene elektronische Behördendienstleistungen ohne zusätzliche Logins und Passwörter. Auch ein Einsatz der *eID+* im privatwirtschaftlichen Umfeld ist geplant. Die *Procivis AG* bietet mit der *SSI+* seit Januar 2022 ebenfalls eine Blockchain-Lösung an, welche die vollständig selbstverwaltete Identität ermöglicht [Procivis 2022b; Procivis 2022c].

Mit diesem Querschnitt durch verschiedene Praxisanwendungen des Blockchain-basierten Identitätsnachweises ist der theoretische Teil dieser Master-Thesis abgeschlossen und die Basis für das empirische Vorhaben gelegt. Im empirischen Teil werden die in Abschnitt 1.3 auf Seite 3 definierten Forschungsfragen sowie nachfolgend aufgestellte Hypothesen untersucht. Im Zentrum steht die Frage, ob ein Blockchain-basierter Identitätsnachweis auf nationaler Ebene in der Schweizerischen Eidgenossenschaft Akzeptanzpotenzial aufweist oder ob die Bürger:innen der Schweiz der Blockchain-Technologie und Blockchain-Identitätsnachweisen skeptisch gegenüberstehen.

## 3 Empirischer Teil

### 3.1 Ziele der Forschung

Wie bereits in Abschnitt 1.2 auf Seite 2 zu den Forschungszielen beschrieben, hat der empirische Forschungsteil dieser Master-Thesis zum Ziel, durch eine Umfrage die Einstellung von in der Schweiz stimmberechtigten Personen gegenüber diversen Fragestellungen rund um eine Blockchain-basierte Identitätsnachweislösung quantitativ zu erheben und zu analysieren. Es sollen Erkenntnisse darüber gewonnen werden, ob das Konzept einer Blockchain-Lösung zum Identitätsnachweis in der Schweizerischen Eidgenossenschaft bei einer erneuten Volksabstimmung Erfolgsschancen aufweisen könnte. Ebenfalls soll eine empirische Grundlage zur Beantwortung der in Abschnitt 1.3 auf Seite 3 aufgestellten Forschungsfragen und den nachfolgend in Abschnitt 3.1.1 auf der nächsten Seite beschrieben Hypothesen geschaffen werden.

Für die statistischen Grundtheorie wird die Methodenberatung der Universität Zürich konsultiert [Schwarz 2022]. Für die statistischen Auswertungen kommen Statistik-Programm und frei nutzbare GNU-Software *R* in Version 4.1.3 in Verbindung mit der integrierten Softwareumgebung (IDE) *RStudio*<sup>TM</sup> sowie *IBM SPSS Statistics*<sup>TM</sup> in Version 28 zum Einsatz [Gentleman und Ihaka 2022; RStudio Inc. 2022; IBM 2022]. Sämtliche Nachweise und Skripts für die innerhalb dieser Master-Thesis vollzogenen Berechnungen, Auswertungen, Analysen sowie den erstellten Visualisierungen sind auf einem *GitHub*<sup>TM</sup>-Repository<sup>1</sup> verfügbar.

Optimalerweise wird empirischen Untersuchungen zu Volksabstimmungen eine Repräsentativität der Gesamtbevölkerung zugrunde gelegt, um möglichst exakte Aussagen über die Einstellung und die Abstimmungsabsicht der Bevölkerung gegenüber einer Abstimmungsvorlage treffen zu können. Aus forschungsökonomischen Gründen ist eine für die schweizerische Bevölkerung repräsentative Stichprobe im Rahmen dieser Master-Thesis nicht erreichbar. Deshalb wird an dieser Stelle erstmals ausdrücklich festgehalten, dass die nachfolgenden Forschungsergebnisse keinen Anspruch auf Repräsentativität erheben. Eine empirische Forschung, welche sich rein auf die durch die Umfrage zufällig zusammengesetzte Stichprobe stützt, ist in ihrer Aussagekraft über die Mehrheitsfähigkeit einer potenziellen Abstimmungsvorlage stark begrenzt. Trotz Ausschluss eines Anspruchs auf Repräsentativität bietet es sich bei der Thematik und den Fragestellungen dieser Master-Thesis an, die empirische Forschung mit einer maximal möglichen Annäherung an die schweizerische Bevölkerungsstruktur durchzuführen. Um dies zu erreichen, sollen die erhobenen Daten der Zufallsstichprobe bestmöglich durch statistische Gewichtungsverfahren an die tatsächliche Bevölkerungsstruktur angeglichen werden.

---

<sup>1</sup>[https://github.com/wackt1/data\\_analysis\\_and\\_visualization\\_MATH](https://github.com/wackt1/data_analysis_and_visualization_MATH)

#### 3.1.1 Hypothesen

Hypothese 1: Je höher die Selbsteinschätzung der technologischen Kompetenz von Befragten in Bezug auf die Blockchain-Technologie ist, desto höher ist die Zustimmung gegenüber einer staatlichen, Blockchain-basierten E-ID.

$H_0$ : Es kann keine Korrelation zwischen der Selbsteinschätzung der technologischen Kompetenz der Befragten in Bezug auf die Blockchain-Technologie und der Zustimmung gegenüber einer staatlichen, Blockchain-basierten E-ID festgestellt werden.

$H_1$ : Es kann eine Korrelation zwischen der Selbsteinschätzung der technologischen Kompetenz der Befragten in Bezug auf die Blockchain-Technologie und der Zustimmung gegenüber einer staatlichen, Blockchain-basierten E-ID festgestellt werden.

---

Hypothese 2: Je wichtiger Anwendungsbereiche wie virtuelle Behördenshalter oder digitale demokratische Instrumente für Befragte sind, desto offener stehen diese einer staatlichen E-ID auf Blockchain-Basis gegenüber.

$H_0$ : Es kann keine Korrelation zwischen der Wichtigkeit von Anwendungsbereichen wie virtuellen Behördenschaltern oder digitalen demokratischen Instrumenten für Befragte und der Offenheit gegenüber einer staatlichen E-ID auf Blockchain-Basis festgestellt werden.

$H_1$ : Es kann eine Korrelation zwischen der Wichtigkeit von Anwendungsbereichen wie virtuellen Behördenschaltern oder digitalen demokratischen Instrumenten für Befragte und der Offenheit gegenüber einer staatlichen E-ID auf Blockchain-Basis festgestellt werden.

---

Hypothese 3: Es lassen sich Unterschiede bezüglich der Zustimmung gegenüber einer staatlichen, Blockchain-basierten E-ID bei Befragten der Kantone Zug und Schaffhausen im Vergleich zu den restlichen Befragten feststellen, da in diesen Kantonen bereits behördliche Angebote zur Nutzung von Blockchain-basierten Identitätsnachweisen den Bürger:innen zur Verfügung standen.

$H_0$ : Es lassen sich keine Unterschiede in der Zustimmung gegenüber einer staatlichen, Blockchain-basierten E-ID zwischen Befragten der Kantone Zug und Schaffhausen im Vergleich zu den restlichen Befragten feststellen.

$H_1$ : Es lassen sich signifikante Unterschiede in der Zustimmung gegenüber einer staatlichen, Blockchain-basierten E-ID zwischen Befragten der Kantone Zug und Schaffhausen im Vergleich zu den restlichen Befragten feststellen.

## 3.2 Datenerhebung

Um die aufgestellten Forschungsfragen und Hypothesen untersuchen zu können, wird mittels einer Online-Umfrage eine empirische Datengrundlage geschaffen. Der Fragebogen wird mithilfe der *Qualtrics™ XM-Plattform* [Qualtrics 2022] erstellt und ist in vollständiger Form im Anhang auf Seite 127 zur Einsicht verfügbar. Er umfasst diverse Fragestellungen rund um eine Blockchain-basierte Identitätsnachweislösung sowie Angaben zur eigenen Person in Form von Geschlecht, Alter, Bildung, Parteinähe und Wohnort. Trotz dieser personenbezogenen Angaben wird die Umfrage vollständig anonymisiert ausgewertet und Ergebnisse werden lediglich in aggregierter Form veröffentlicht.

Verteilt wird die Umfrage an Abonnent:innen des Newsletters der Online-Wahlhilfe oder Voting Advice Application (VAA) *smartvote* [Politools 2022b]. Das Tool *smartvote* soll stimm- und wahlberechtigte Personen in der Schweizerischen Eidgenossenschaft dabei unterstützen, durch die Bereitstellung einer transparenten Informationsbasis in einem (partei-)politisch komplexen Wahlumfeld den Überblick zu behalten [Politools 2022a]. Mithilfe der Online-Wahlhilfe können Bürger:innen zu diversen politischen Themen einen Fragebogen ausfüllen und danach ihre eigenen Antworten und Positionen mit den entsprechenden Ergebnissen von Kandidierenden, Parteien und Listen vergleichen. Seit 2003 hat der Verein bei mehr als 200 Wahlen auf sämtlichen Staatsebenen der Schweiz mitgewirkt und bei den Nationalratswahlen 2019 wurden über *smartvote* rund 2.1 Millionen Wahlempfehlungen ausgegeben [Politools 2022b]. Damit hat jede fünfte Wählerin bzw. jeder fünfte Wähler dieses Angebot genutzt.

Newsletter-Abonnent:innen von *smartvote* als die Empfänger:innen der Umfrage können als Personen beschrieben werden, bei welchen davon ausgegangen werden kann, dass sie sich für politische Entscheidungsfindungsprozesse stark interessieren und sich an diesen Prozessen auch aktiv beteiligen würden. Es wird deshalb davon ausgegangen, dass sich diese Bevölkerungsgruppe als die primäre Zielgruppe von Befragungen mit Bezug zu politischen Themen wie einer E-ID-Vorlage gut eignet. Zugleich macht die Wahl eines spezifischen Zielpublikums Verzerrungen bezüglich der Repräsentativität der Gesamtbevölkerung unvermeidbar.

### 3.2.1 Umfrageverlauf

Die Umfrage wurde in zwei Etappen über den *smartvote*-Newsletter verteilt. Im Rahmen des Newsletters wurde die Umfrage thematisch kurz beschrieben und forderte über einen integrierten Link zur Teilnahme auf. Am 31.03.2022 wurde die Umfrage innerhalb eines deutschsprachigen Newsletters an 42'859 Abonnent:innen verteilt, welche als deutschsprachige Nutzer:innen bei *smartvote* registriert sind.

Am 04.04.2022 folgte die Verteilung der Umfrage innerhalb eines französischsprachigen Newsletters an weitere 11'670 Abonnent:innen, welche als französischsprachige Nutzer:innen bei *smartvote* registriert sind. Insgesamt wurde die Umfrage somit 54'529 Newsletter-Abonnent:innen zugestellt, davon rund 79 % in deutscher Sprache und 21 % in französischer Sprache. Die Umfrage stand sämtlichen Teilnehmenden ungeachtet der Newsletter-Sprache in Deutsch und Französisch zur Verfügung.

Die Umfrage wurde am 09.04.2022 geschlossen. Insgesamt wurden 2'028 Antwort-Datensätze erfasst und aus der *Qualtrics*™ XM-Plattform exportiert. Dieser Rohdatensatz wurde für die geplanten statistischen Auswertungen gemäss den im Anhang auf Seite 144 beschriebenen Schritten aufbereitet und validiert. Total konnten nach der Aufbereitung 1'730 vollständig ausgefüllte und validierte Datensätze als Stichprobe erfasst werden. Die Rücklaufquote der Umfrage bezogen auf die vollständigen und verwertbaren Datensätze beträgt somit rund 3.17 %.

### 3.3 Analyse & Gewichtung der Stichprobe

Die Daten der gesammelten Stichprobe werden in einem ersten Schritt bezüglich den erfassten Personendaten analysiert. Damit sollen Aussagen über die Zusammensetzung der erlangten Stichprobe sowie Abweichungen zwischen der Stichprobe und der tatsächlichen Bevölkerungsstruktur getätigt werden können. Letzteres erlaubt in der Folge eine Analyse von möglicherweise notwendigen Schritten zur Erreichung der angestrebten maximal möglichen Annäherung der Stichprobe an die schweizerische Bevölkerungsstruktur.

Zum Abgleich der Stichprobe mit der tatsächlichen Bevölkerungsstruktur werden verschiedene Referenzdatensätze des Bundesamts für Statistik der Schweizerischen Eidgenossenschaft konsultiert [Bundesamt für Statistik 2022]. Sämtliche Bestrebungen zur maximal möglichen Annäherung der Stichprobe an die Bevölkerungsstruktur beschränken sich auf die folgenden Eigenschaftsmerkmale der schweizerischen Bevölkerung, ohne Anspruch auf Repräsentativität zu erheben:

- Geschlechterverteilung
- Sprachregion
- Altersgruppen
- Bildungsabschluss
- Parteinähe

Als erste Analyse wird eine Kontingenzanalyse nach *Pearson* für die nominalen Variablen sowie eine Rangkorrelation nach *Spearman* für die ordinalen Variablen der Stichprobe durchgeführt (vgl. Anhang auf Seite 145). Damit soll herausgefunden werden, ob zwischen Eigenschaftsmerkmalen der Umfrageteilnehmenden und thematischen Fragestellungen in der ungewichteten Stichprobe Korrelationen bestehen. Die Analyse hat Erkenntnisgewinne darüber zum Ziel, ob Referenzdaten in Form der Eigenschaftsmerkmale der Teilnehmenden überhaupt relevant für eine allfällige Gewichtung sind. Grundsätzlich wird eine möglichst geringe Anzahl zu gewichtender Variablen angestrebt.

Die Ergebnisse dieser Auswertung zeigen, dass mit der erlangten Stichprobe signifikante Effektstärken nachgewiesen werden können. Einige Fragestellungen der Umfrage weisen bei der Kontingenzanalyse resp. der Korrelationsanalyse je nach Eigenschaftsmerkmal signifikante Zusammenhänge auf. Bei der Kontingenzanalyse zeigen sich in rund der Hälfte der Fragestellung in Kombination mit einem Eigenschaftsmerkmal nach Cohen [1992] schwache ( $CC > .10$ ) bis mittlere Effektstärken ( $CC > .30$ ) signifikant. Eine starke Effektstärke ( $CC > .50$ ) wird von keiner Variablenkombination erreicht. Bei der Korrelationsanalyse zeigt sich ein ähnliches

Bild. Eine mittlere oder starke Effektstärke ( $r_s > 30$  resp.  $r_s > 50$ ) nach Cohen [1992] wird von keiner Variablenkombination signifikant erreicht. Auffällig ist zudem, dass in Kombination mit dem Eigenschaftsmerkmal der Partei keine einzige Fragestellung einen schwachen Effekt ( $r_s > .10$ ) nach Cohen [1992] signifikant erreichen kann.

Diese Ergebnisse sind in Anbetracht der repräsentativen Ergebnisse der Abstimmungsanalyse zur *E-ID 2020* des Markt- und Meinungsforschungsinstituts *gfs.bern* [2021, S. 26-27] vor allem unter dem Gesichtspunkt der politischen Merkmale der Teilnehmenden auffällig. Bei der vergangenen Referendumsabstimmung gingen von soziodemografischen Merkmalen eher schwache Effektstärken aus, während die politischen Merkmale deutlich ausschlaggebender waren (vgl. Abschnitt 2.5 auf Seite 37). In der erlangten Stichprobe konnte bei der Kontingenzanalyse unter dem Aspekt *Partei* ein mittlerer Zusammenhang bei Q4.1 (CC = .304, p = .000) signifikant nachgewiesen werden. Die Frage Q4.1 fragte die Teilnehmenden nach ihrem Abstimmungsverhalten bei der Vorlage *E-ID 2020*. Es zeigt sich hier eine deutliche Übereinstimmung mit den repräsentativen Ergebnissen von *gfs.bern*, wonach sich in dieser Kombination aus Eigenschaftsmerkmal (Partei) und Abstimmungsverhalten beim *E-ID-2020*-Gesetz eindeutige Effekte feststellen lassen.

Dieses Ergebnis gilt allerdings nicht für die Korrelationsanalyse unter dem Aspekt der politischen Merkmale (Partei) und der Frage Q11.2. Diese Frage erfasste die Abstimmungsintention der Teilnehmenden bei einer hypothetischen Volksabstimmung über eine staatliche und Blockchain-basierte E-ID-Lösung und ist folglich mit der Fragestellung der tatsächlichen *E-ID-2020*-Abstimmung vergleichbar. Es konnte allerdings entgegen der auf den Ergebnissen von *gfs.bern* basierenden Erwartung sowie den mittleren Effektstärken zwischen Partei und Q4.1 keine signifikante Effektstärke festgestellt werden. Generell konnte mittels Korrelationsanalyse zwischen politischen Merkmalen (Partei) und den Fragestellungen keine einzige Korrelation signifikant und mit zumindest schwacher Effektstärke berechnet werden. Vor dem Hintergrund der Ergebnisse von *gfs.bern*, gemäss derer politische Merkmale die relevantesten Effekte auf die Einstellung gegenüber einer E-ID und folglich des Abstimmungsverhaltens vorweisen, muss die erlangte Stichprobe in ihrer Aussagekraft über die Bevölkerung kritisch hinterfragt werden.

Weiter zeigt sich eine Abweichung zwischen der Stichprobe und der Gesamtbevölkerung von rund 5.51 Prozentpunkten im Kontext der Abstimmungsergebnisse zur *E-ID 2020*. Das Verhältnis von 64.4 % Nein-Stimmen zu 35.6 % Ja-Stimmen der Referendumsabstimmung (Soll-Wert) dient als weiterer Benchmark zur Beurteilung der Güte der Stichprobe. Während das vorgesehene E-ID-Gesetz an der Urne mit 64.4 % Nein-Stimmen abgelehnt wurde, liegt der Anteil an Nein-Stimmen der Teilnehmenden der Umfrage (Ist-Wert) lediglich bei 58.89 % (vgl. Tabelle 1 auf der nächsten Seite).

Die erlangte Stichprobe ist also im Vergleich zur Gesamtbevölkerung gegenüber der vergangenen E-ID-Vorlage zu positiv eingestellt, weshalb auch von einer Verzerrung in Bezug auf andere Fragestellungen der Umfrage im Vergleich zur tatsächlichen Bevölkerung ausgegangen werden muss. In der Summe aller bisher vorgenommenen Analysen scheint eine eingehende Betrachtung der einzelnen Persönlichkeitsmerkmale inklusive kritischer Evaluation der Gewichtungsnotwendigkeit und Gewichtungsfaktoren (GF) angebracht. Damit soll versucht werden, das Verhältnis zwischen Ja- und Nein-Stimmen näher an die Ergebnisse der Referendumsabstimmung zu rücken und so eine die schweizerische Bevölkerung besser abbildende Stichprobe zu erlangen. Es wird aufgrund dieser Ergebnisse davon ausgegangen, dass die erlangte Stichprobe in ausgewählten Variablen gewichtet werden muss, um zuverlässigere - wenn auch nicht repräsentative - Aussagen über die Bevölkerung treffen zu können.

Tabelle 1: Abstimmungsverhalten beim E-ID-Gesetz 2020 von Stichprobe und Bevölkerung.

Stimme	n	Ist-Wert in %	Soll-Wert in %	Δ in %
Ja	654	41.11	35.60	+5.51
Nein	937	58.89	64.40	-5.51
Total	1591	100	100	-

### 3.3.1 Analyse der persönlichen Merkmale

Als erstes Persönlichkeitsmerkmal wird die Geschlechterverteilung der Stichprobe (Ist-Wert) analysiert. Als Referenzdatensatz zur tatsächlichen Geschlechterverteilung der schweizerischen Bevölkerung (Soll-Wert) werden die Daten des Bundesamts für Statistik von 2020 verwendet [Bundesamt für Statistik 2021b]. Datensätze der Stichprobe, welche die Frage nach dem Geschlecht mit „Divers“ oder „Keine Antwort“ beantwortet hatten, werden in dieser Analyse aufgrund fehlender Referenzdaten des Bundesamts für Statistik nicht berücksichtigt. Davon betroffen sind 23 von 1'730 Datensätzen. Aufgrund der geringen Anzahl von betroffenen Datensätzen wird von einem vernachlässigbaren Effekt bezogen auf die Gesamtstichprobe ausgegangen und die statistische Unschärfe aus forschungsoökonomischen Gründen akzeptiert.

Tabelle 2: Vergleich von Stichprobe und Bevölkerungsstruktur nach Geschlecht.

Geschlecht	n	Ist-Wert in %	Soll-Wert in %	GF
Männlich	1'428	83.66	49.10	0.587
Weiblich	279	16.34	50.90	3.114
Total	1'707	100	100	-

Wie die Auswertung zeigt, ist der Anteil an männlichen Teilnehmenden mit rund 83.66 % deutlich höher als der Anteil an weiblichen Teilnehmenden mit rund 16.34 %. Im Vergleich zur Geschlechterverteilung in der Gesamtbevölkerung ergibt sich daraus die starke Notwendigkeit zur Gewichtung dieser Variable, um die Stichprobe näher an die Gesamtbevölkerung zu bringen. Dies wird ebenfalls durch die Erkenntnisse der Abstimmungsanalyse zur *E-ID 2020* von *gfs.bern* gestützt, gemäss derer das Geschlecht bei der E-ID-Vorlage einen signifikanten Einfluss hatte [gfs.bern 2021, S. 26]. Auf Basis dieser Analysen wird entschieden, die Variable *Geschlecht* innerhalb der Stichprobe entsprechend mithilfe der Gewichtungsfaktoren (GF) zu gewichten.

Als zweites Persönlichkeitsmerkmal werden die Sprachregionen der Stichprobe (Ist-Wert) analysiert. Als Referenzdatensatz zur tatsächlichen Sprachverteilung der schweizerischen Bevölkerung (Soll-Wert) werden die Daten des Bundesamts für Statistik von 2020 verwendet [Bundesamt für Statistik 2020]. Es wird dabei das Verhältnis der Sprachen Deutsch und Französisch unter der stimmberechtigten und damit volljährigen Bevölkerung betrachtet. Der *smartvote*-Newsletter wurde an ein deutschsprachiges und französischsprachiges Publikum verteilt. Die gesamtschweizerisch mit rund 6.1 % italienischsprachige und mit rund 0.6 % rätoromanischsprachige Bevölkerung wird innerhalb dieser Gewichtungsanalyse deshalb nicht berücksichtigt. Es wird von einem vernachlässigbaren Effekt bezogen auf die Gesamtstichprobe ausgegangen und die statistische Unschärfe aus forschungsökonomischen Gründen akzeptiert.

Tabelle 3: Vergleich von Stichprobe und Bevölkerungsstruktur nach Sprachregion.

Sprache	n	Ist-Wert in %	Soll-Wert in %	GF
DE	1'328	76.76	75.13	0.98
FR	402	23.24	24.87	1.07
Total	1'730	100	100	-

Die Analyse zeigt, dass die Stichprobe bei den Sprachanteilen nur sehr leicht von der Bevölkerungsstruktur abweicht. In der Schweizerischen Eidgenossenschaft sind Unterschiede im Wahl- und Abstimmungsverhalten zwischen der französisch- und der deutschsprachigen Schweiz bekannt (sog. *Röstigraben-Effekt*) [Eichenberger 31.12.2014]. Außerdem haben die repräsentativen Auswertungen innerhalb des *Mobiliar DigitalBarometer 2020/21* von Rüthi et al. [2020, S. 55] ergeben, dass die bevorzugte E-ID-Variante abhängig von der Sprachregion ist. Durch die geplante Gewichtung der Variable *Geschlecht* bietet es sich an, die Variable *Sprachregion* ebenfalls zu gewichten, um mögliche Verzerrungen durch die Geschlechtergewichtung auszugleichen. Eine Angleichung der deutschen und französischen Sprachanteile an die Bevölkerungsstruktur wird aus diesem Grund für sinnvoll erachtet, womit in der Folge die Variable *Sprachregion* innerhalb der Stichprobe entsprechend gewichtet wird.

Das nächste zu analysierende Persönlichkeitsmerkmal ist die Altersstruktur der Stichprobe (Ist-Wert). Um eine Vergleichbarkeit mit den Referenzdatensätzen des Bundesamts für Statistik zu ermöglichen, wurden die Teilnehmenden der Umfrage in drei Altersgruppen eingeteilt. Als Referenzdatensatz zur tatsächlichen Altersstruktur der schweizerischen Bevölkerung (Soll-Wert) werden die Daten des Bundesamts für Statistik von 2020 verwendet [Bundesamt für Statistik 2021c].

Tabelle 4: Vergleich von Stichprobe und Bevölkerungsstruktur nach Altersgruppen.

Altersgruppe	n	Ist-Wert in %	Soll-Wert in %	GF
18-39 Jahre	234	13.53	32.45	2.40
40-64 Jahre	943	54.51	40.30	0.74
65+ Jahre	553	31.96	27.25	0.85
Total	1'730	100	100	-

Während die Altersgruppe der 65+ Jahre alten Teilnehmenden relativ nahe am Bevölkerungsanteil liegt ( $\Delta = 4.71\%$ ), nehmen die Abweichungen mit abnehmendem Alter der Teilnehmenden stetig zu. Obwohl eine Gewichtung der Altersgruppen somit sinnvoll erscheint, wird im Rahmen dieser Forschungsarbeit davon abgesehen. Dieser Entscheid stützt sich wiederum auf die Ergebnisse der Abstimmungsanalyse zur *E-ID 2020* von *gfs.bern*. Die Studie kommt zum Schluss, dass altersbedingte Unterschiede im Abstimmungsverhalten zur *E-ID* möglicherweise aufgrund statistischer Unschärfen vollständig wegfallen [*gfs.bern* 2021, S. 26]. Aus diesem Grund wird entschieden, die Variable *Altersgruppe* nicht zu gewichten, wobei gestützt auf die Ergebnisse von *gfs.bern* ein vernachlässigbarer Effekt auf die geplanten Auswertungen erwartet wird.

Das vierte Persönlichkeitsmerkmal ist der derzeit höchste erreichte Bildungsabschluss (Ist-Wert) der Teilnehmenden der Umfrage. Die Teilnehmenden der Umfrage wurden wiederum in drei Bildungsstufen eingeteilt, um eine Vergleichbarkeit mit den Referenzdatensätzen des Bundesamts für Statistik zu ermöglichen. Als Referenzdatensatz zur tatsächlichen Bildungsstruktur der schweizerischen Bevölkerung (Soll-Wert) werden die Daten des Bundesamts für Statistik von 2020 verwendet [Bundesamt für Statistik 2021a]. Nicht berücksichtigt werden in dieser Auswertung 16 Datensätze von Teilnehmenden, bei welchen die über ein Textfeld angegebene Ausbildung keiner der Kategorien zugeordnet werden kann. Es wird von einem vernachlässigbaren Effekt bezogen auf die Gesamtstichprobe ausgegangen und die statistische Unschärfe aus forschungsoökonomischen Gründen akzeptiert.

Wie in Tabelle 5 auf der nächsten Seite ersichtlich ist, bestehen zwischen Stichprobe und tatsächlicher Bildungsstruktur erhebliche Differenzen. Teilnehmende auf *Tertiärstufe* sind stark überrepräsentiert, während Teilnehmende auf den Stufen *Sekundarstufe II* und *Obligatorische Schule* stark unterrepräsentiert sind.

Trotz dieser Abweichungen zwischen der Stichprobe und der Bevölkerung wird auf eine Gewichtung dieser Variable verzichtet. Einerseits wird der notwendige Gewichtungsfaktor ( $GF = 17.98$ ) als zu hoch sowie die Anzahl an Datensätzen ( $n = 12$ ) für die Stufe *Obligatorische Schule* als zu gering betrachtet, um bei einer Gewichtung keine anderweitigen Verzerrungen innerhalb der Stichprobe auszulösen. Andererseits wird dieser Entscheid ebenfalls durch die Abstimmungsanalyse zur *E-ID 2020* von *gfs.bern* gestützt. Die Studie kommt wie bereits bei den Altersgruppen zum Schluss, dass Unterschiede im Abstimmungsverhalten zur E-ID möglicherweise aufgrund statistischer Unschärfen beim Bildungshintergrund vollständig wegfallen [gfs.bern 2021, S. 26]. Aus diesem Grund wird entschieden, die Variable *Bildungsstufe* nicht zu gewichten, wobei gestützt auf die Ergebnisse von *gfs.bern* ein vernachlässigbarer Einfluss auf die geplanten Auswertungen erwartet wird.

Tabelle 5: Vergleich von Stichprobe und Bevölkerungsstruktur nach Bildungsabschluss.

Bildungsstufe	n	Ist-Wert in %	Soll-Wert in %	GF
Obligatorische Schule	12	0.70	12.59	17.98
Sekundarstufe II	380	22.17	51.73	2.33
Tertiärstufe	1'322	77.13	35.68	0.46
Total	1'714	100	100	-

Das letzte Persönlichkeitsmerkmal stellt die empfundene Parteinähe der Umfrageteilnehmenden (Ist-Wert) dar. Als Referenzdatensatz zu den tatsächlichen Parteistärken in der Schweizerischen Eidgenossenschaft (Soll-Wert) werden die Daten des Bundesamts für Statistik der Nationalratswahlen von 2019 verwendet [Bundesamt für Statistik 2019]. Die Parteilandschaft wird innerhalb dieser Forschungsarbeit mit den sechs stimmanteilmässig am stärksten im Nationalrat der Schweizerischen Eidgenossenschaft vertretenen Parteien abgebildet („Die Mitte“, „FDP“, „glp“, „Grüne“, „SP“, „SVP“). Zusätzlich existiert die Kategorie „Keine Partei“.

Datensätze der Stichprobe, welche auf die Frage nach der Parteinähe über die Texteingabe eine andere Partei nannten, wurden der Kategorie „Andere“ zugeordnet. Diese Zusammenfassung unterschiedlichster Parteien führt jedoch dazu, dass es sich bei der Kategorie „Andere“ um eine ideologisch höchst heterogene Gruppe handelt. Die Kategorie konstituiert sich aus unterschiedlichsten Parteien, welche im politischen Spektrum von stark linksorientiert bis stark rechtsorientiert sowie von stark liberal bis stark konservativ reichen können. Die Parteistärken gemessen am Wahlanteil in der Gesamtbevölkerung liegen bei dieser Gruppe zwischen 0.1 % und 2.4 %. Bei der Auswertung der empirischen Forschung muss diese Gegebenheit entsprechend berücksichtigt werden.

Tabelle 6: Vergleich von Stichprobe und Bevölkerungsstruktur nach Parteinähe.

Partei	n	Ist-Wert in %	Soll-Wert in %	GF
Andere	119	6.88	10.08	1.47
Die Mitte	149	8.61	11.38	1.32
FDP	226	13.07	15.11	1.16
glp	354	20.46	7.80	0.38
Grüne	209	12.08	13.20	1.09
Keine Partei	253	14.62	-	-
SP	319	18.44	16.84	0.91
SVP	101	5.84	25.59	4.38
Total	1'730	100	100	-

Die Analyse zeigt, dass die Vertretung der politischen Landschaft innerhalb der Schweizerischen Eidgenossenschaft in Form der Nationalratsparteien in der Stichprobe relativ gut abgebildet wird. Allerdings sind mit den Parteien „glp“ und „SVP“ zwei deutliche Ausreisser feststellbar. Während sich der Partei „glp“ zugehörig fühlende Teilnehmende in der erlangten Stichprobe deutlich überrepräsentiert sind, ist eine starke Unterrepräsentation von sich der Partei „SVP“ zugehörig fühlenden Teilnehmenden auszumachen.

Durch die Erkenntnisse der Abstimmungsanalyse von gfs.bern ist bekannt, dass politische Eigenschaftsmerkmale im Vergleich zu soziodemografischen Eigenschaftsmerkmalen bei der Thematik *E-ID* ausschlaggebender sind. Auf Basis dieser Analysen wird entschieden, die Variable *Partei* innerhalb der Stichprobe mithilfe der Gewichtungsfaktoren (GF) zu gewichten, um die Parteilandschaft der Schweizerischen Eidgenossenschaft adäquater abzubilden.

Insgesamt werden für die nachfolgenden Analysen somit die Faktoren *Geschlecht*, *Sprache* und *Partei* gewichtet. Die Gewichtung mehrerer Faktoren setzt geeignete statistische Verfahren voraus, um durch die Gewichtung eines einzelnen Faktors entstehende Verzerrungen bei den anderen Faktoren wieder auszugleichen. Um die beabsichtigte maximal mögliche Annäherung an die schweizerische Bevölkerungsstruktur zu erreichen, wird ein statistisches Gewichtungsverfahren namens *Raking* oder *Random Iterative Method Weighting* (Rim Weighting) eingesetzt [IBM 2020; Rodriguez 2020].

### 3.3.2 Güte der Gewichtung

Die Güte der vorgenommenen Gewichtung der Stichprobe wird am Benchmark der *E-ID-2020*-Abstimmung mit 64.4 % Nein-Stimmen und 35.6 % Ja-Stimmen im Vergleich zu Q4.1 der Umfrage gemessen. Q4.1 fragte die Teilnehmenden nach ihrem Abstimmungsverhalten bei der Vorlage *E-ID 2020*. Tabelle 7 zeigt die erneute Auswertung des Abstimmungsverhaltens beim *E-ID-Gesetz 2020* zwischen Stichprobe und Bevölkerung, nun jedoch nach Anwendung der Gewichtung.

Tabelle 7: Abstimmungsverhalten beim E-ID-Gesetz 2020 zwischen gewichteter Stichprobe und Bevölkerung.

Stimme	n	Ist-Wert in %	Soll-Wert in %	Δ in %
Ja	654	35.70	35.60	+0.10
Nein	937	64.30	64.40	-0.10
Total	1591	100	100	-

Die Gewichtung der Stichprobe nach Geschlechterverteilung, Sprachregion und Parteinähe hat eine deutliche Annäherung der Stichprobe an die Gesamtbevölkerung bezüglich des Abstimmungsverhaltens zur Folge. Die Abweichung der Nein-Stimmen zwischen Ist-Wert der gewichteten Stichprobe (64.30 %) und dem Soll-Wert der repräsentativen Referendumsabstimmung (64.40 %) reduziert sich um 5.41 Prozentpunkte. Die Gewichtung der Stichprobe kann die Repräsentation des Abstimmungsverhaltens folglich von einer Differenz von 5.51 Prozentpunkten auf lediglich 0.10 Prozentpunkte verbessern. Daraus lässt sich schliessen, dass die Gewichtung mit den relevantesten Faktoren und korrekten Referenzdaten durchgeführt wurde und die Studie von *gfs.bern* korrekt interpretiert wurde.

Aus statistischer Perspektive werden das Vorgehen und die Resultate der Gewichtung ebenfalls positiv bewertet. Die Annäherung der Stichprobe an den Benchmark in Form der Stimmverhältnisse der Referendumsabstimmung ist so konzipiert, dass die Gewichtung mit vertretbaren statistischen Auswirkungen einhergeht [Daza 2012]. Die Abweichung von 0.10 Prozentpunkten im Abstimmungsverhalten zwischen gewichteter Stichprobe und Bevölkerung wird mit einem maximalen Gewichtungsfaktor von 3.3 in 151 Iterationen erreicht. Damit können sog. *Design-Effekte* in einem akzeptablen Rahmen gehalten werden. Der durch die Gewichtung ausgelöste und errechnete Design-Effekt beträgt rund 1.50. Dies bedeutet, dass die Gewichtung zu einer Erhöhung der Varianz von rund 50 % führt [Collier 2018]. Damit erreichen Schlussfolgerungen auf Basis der Stichprobe zwar weniger wahrscheinlich eine Signifikanz, liegen aber potenziell näher an den tatsächlichen Gegebenheiten innerhalb der Grundgesamtheit.

Die positiven Ergebnisse der Gewichtung bestätigen sich auch bei einer erneuten Analyse der Zusammenhänge zwischen Eigenschaftsmerkmalen der Teilnehmenden und verschiedenen Fragestellungen (vgl. Anhang auf Seite 146). Nach der Gewichtung zeigt die Kontingenzanalyse nach *Pearson* bei der Frage Q4.1 nach dem vergangenen Abstimmungsverhalten zur Vorlage *E-ID 2020* bei sämtlichen Eigenschaftsmerkmalen gesteigerte Effektstärken. Der bereits mittelstarke Zusammenhang zwischen Partei und Abstimmungsverhalten wird durch die Gewichtung der Stichprobe um 0.035 erhöht ( $CC = .339$ ,  $p = .000$ ). Der durch *gfs.bern* festgestellte Effekt des Einflusses politischer Merkmale bestätigt sich auch in der gewichteten Stichprobe dieser Forschungsarbeit.

Die Rangkorrelation nach *Spearman* zeigt nach der Gewichtung ebenfalls Veränderungen in den Korrelationen zwischen Eigenschaftsmerkmalen und Fragestellungen. Gerade bei den politischen Merkmalen (Partei) sind nach Gewichtung insgesamt neun signifikante Effektstärken nach Cohen [1992] feststellbar, während vor Gewichtung noch keine Effekte nachgewiesen werden konnten. Frage Q11.2. über die Abstimmungsintention der Teilnehmenden bei einer hypothetischen Volksabstimmung über eine staatliche und Blockchain-basierte E-ID-Lösung weist nach der Gewichtung ebenfalls einen schwachen, signifikanten Zusammenhang ( $r_s = .130$ ,  $p = .000$ ) mit politischen Merkmalen (Partei) auf. Dies entspricht den auf der Studie von *gfs.bern* basierenden Erwartungen und bestätigt erneut die durch die Gewichtung erreichte Annäherung der Stichprobe an die tatsächliche Bevölkerungsstruktur.

Die durch die Gewichtung insgesamt in höherer Anzahl vorkommenden signifikanten Zusammenhänge zeigen, dass das Verfahren der Gewichtung trotz einem Design-Effekt von 1.50 offenbar kaum negativen Einfluss auf die Häufigkeit von signifikanten Zusammenhängen hat. Die Stichprobe deckt sich nach der Gewichtung deutlich genauer mit dem Abstimmungsverhalten und den erwarteten Effektstärken zwischen politischen Merkmalen der Bevölkerung. Das Ergebnis der Gewichtung verspricht, durch eine erwiesenermassen exaktere Abbildung der tatsächlichen Bevölkerungsstrukturen zuverlässigere Aussagen über die Bevölkerung im Kontext von Fragestellungen rund um eine digitale ID treffen zu können, als dies mit der ungewichteten Stichprobe möglich wäre.

### 3.4 Deskriptive Datenauswertungen

Die aus der Umfrage gewonnenen Daten werden innerhalb dieses Kapitels deskriptiv ausgewertet. Sämtliche Auswertungen werden mit 1'730 Datensätzen ( $n = 1'730$ ) vollzogen, auf welchen die vorgängig berechneten Gewichtungen angewandt sind. Grundsätzlich werden die Auswertungen zu den einzelnen Fragestellungen nach dem Parteizugehörigkeitsgefühl der Teilnehmenden dargestellt. Der Grossteil der Fragestellungen verlangt von den Teilnehmenden Angaben in Form von Zustimmungswerten gegenüber unterschiedlichsten Aussagen. Fragestellungen, deren Auswertungen nicht im Hauptteil dieser Arbeit dargestellt sind, sind im Anhang auf Seite 147 als zusätzliche Auswertungen einsehbar.

Die Zustimmungswerte werden für die deskriptiven Analysen und Visualisierungen mit dem arithmetischen Mittel berechnet, um eine adäquate Granularität der Ergebnisse zu ermöglichen. Zur richtigen Einordnung der durch das arithmetische Mittel erlangten Resultate gilt es festzuhalten, dass die Datenstrukturen der Fragestellungen mit Zustimmungswerten in den meisten Fällen eine starke Linksschiefe (*Skewness*) aufweisen (vgl. Abb. 6).

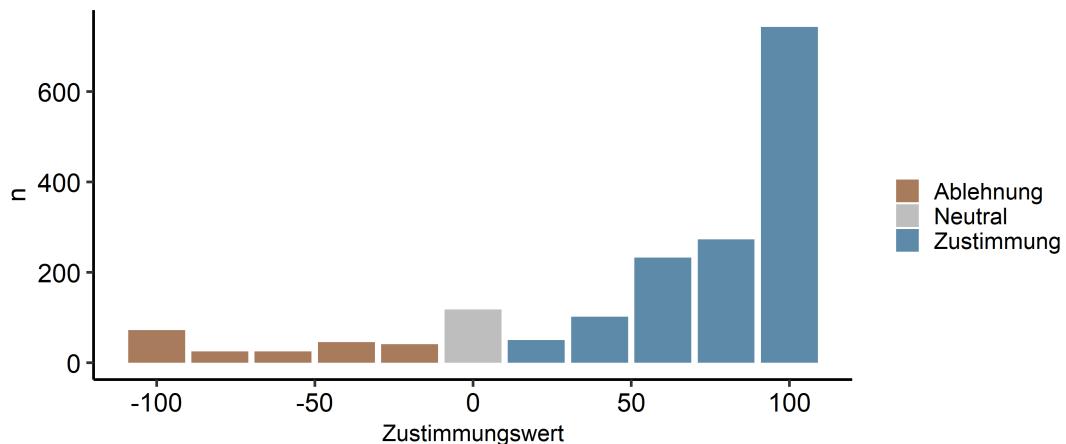


Abbildung 6: Schiefe der Stichprobe (Skewness) am Beispiel von Q5.2.

Über einen Schieberegler geben die Teilnehmenden an, in welchem Ausmass sie einer Aussage zustimmen. Im Fragebogen steht den Teilnehmenden eine Zustimmungsskala von 0 bis 100 zur Verfügung, wobei die Grundposition mittig bei einem Skalenwert von 50 liegt und beidseitig eine 10er-Abstufung bietet. Werte kleiner als 50 entsprechen einer Ablehnung und Werte grösser als 50 einer Zustimmung gegenüber einer als Aussage formulierten Fragestellung.

Zur erleichterten Interpretation und verbesserten Visualisierungsmöglichkeit wird diese Skala innerhalb der Auswertungen modifiziert. Die Grundposition des Schiebereglers wird mittig zu einem Skalenwert von 0 umkodiert (*Neutral*). Weiter werden die beidseitigen Extrempositionen auf -100 resp. +100 umkodiert. So entsteht eine Skala, welche ihren Neutralpunkt mittig bei 0 hat und beidseitig jeweils eine Ablehnung resp. Zustimmung über einen Bereich von 100 Skalenpunkten mit einer 20er-Abstufung abbildet.

Die Interpretation der Zustimmungswerte gegenüber einer Aussage gestaltet sich wie folgt:

- Werte  $> 0$  entsprechen einer Zustimmung gegenüber der Aussage. Je näher ein Wert am Maximum von 100 liegt (*Vollständige Zustimmung*), desto stärker ist die Zustimmung zur Aussage.
- Werte = 0 entsprechen einer Neutralität gegenüber der Aussage.
- Werte  $< 0$  entsprechen einer Ablehnung gegenüber der Aussage. Je näher ein Wert am Maximum von -100 liegt (*Vollständige Ablehnung*), desto stärker ist die Ablehnung zur Aussage.

Die vorgängig innerhalb der Merkmalsanalyse angeführte Besonderheit der Parteikategorie „Andere“ bedingt an dieser Stelle nochmals eine Spezifizierung, bevor mit der deskriptiven Analyse begonnen werden kann. Diese Gruppe setzt sich aufgrund der bewusst gewählten Einteilung der Parteigruppen aus bezüglich ihrem Parteizugehörigkeitsgefühl stark heterogenen Teilnehmenden zusammen. Da sich durch die hohe Heterogenität dieser Gruppe keine sinnvollen und stichhaltigen Aussagen über die Gruppe selbst formulieren lassen, wird die Gruppe im weiteren Verlauf lediglich auf deskriptiver Basis beschrieben. So soll die Vollständigkeit der Auswertung gewährleistet sein, während anerkannt wird, dass über diese Gruppe keine zuverlässigen Aussagen möglich sind. Wenn in der Folge von Bezügen zur Gruppe der ‚Kleinparteien‘ (Andere) die Rede ist, dienen die getätigten Aussagen lediglich informellen Zwecken ohne wissenschaftliche Aussagekraft.

#### 3.4.1 Vertrauen in den Staat

Die erste Gruppe von Fragestellungen behandelt das Vertrauen der Umfrageteilnehmenden in den Staat im Kontext einer E-ID. Abb. 7 auf der nächsten Seite zeigt, dass die exklusive Zuständigkeit des Staats für die Einführung, Ausstellung und den Betrieb einer E-ID einen hohen Zustimmungswert von durchschnittlich 58.9 erfährt. Trotz dieses eindeutigen Zuständigkeitsverständnisses nimmt die Zustimmung bezüglich des Vertrauens in die technologische Kompetenz des Staats ab.

Dennoch trauen es die Befragten dem Staat noch immer mit einem positiven Wert von 22.1 zu, eine passende Technologie für die E-ID zu wählen (vgl. Abb. 8). Ein Blick auf die Parteien zeigt, dass die stärkste Zustimmung zur exklusiv staatlichen Herausgabe einer E-ID von links-grün Parteibündeten stammt (Grüne und SP). Mitte bis rechts Parteibündene (Die Mitte, FDP und SVP) stimmen leicht schwächer zu.

Q5.2 Allein der Staat sollte für die Einführung, Ausstellung und den Betrieb einer E-ID verantwortlich sein.

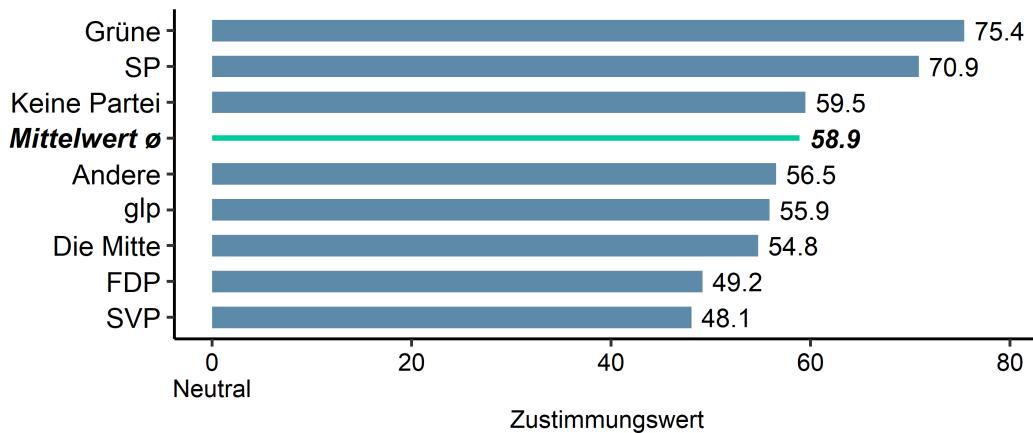


Abbildung 7: Auswertung der Fragestellung Q5.2.

Q5.3 Ich traue dem Staat zu, die passendste Technologie für die Umsetzung einer E-ID zu wählen.

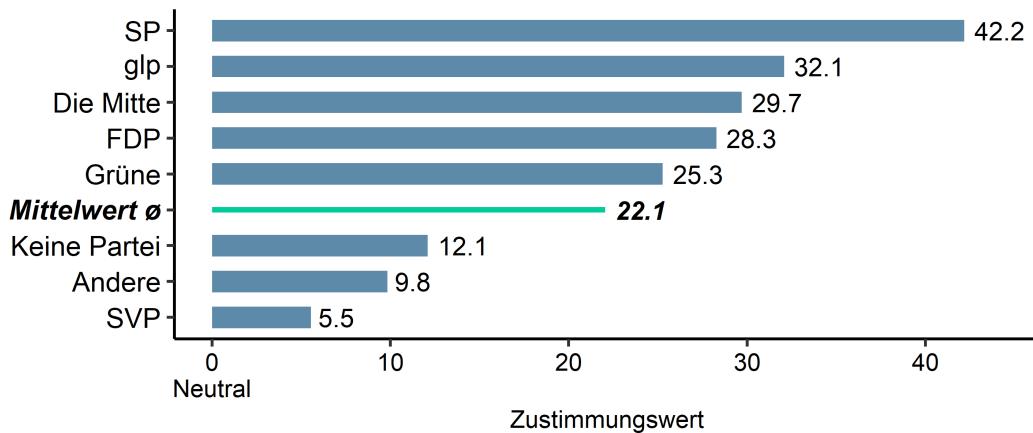


Abbildung 8: Auswertung der Fragestellung Q5.3.

Während Parteiverbundene der SVP auch beim Vertrauen in die staatliche Wahl einer passenden Technologie und der Bereitschaft zur Nutzung einer staatlichen E-ID-Lösung (vgl. Abb. 9) nur noch knapp positive Zustimmungswerte erreichen, sind Parteiverbundene von glp, Die Mitte oder FDP trotz relativ betrachtet unterdurchschnittlicher Zustimmung zur staatlichen Herausgabe einer E-ID überdurchschnittlich bereit, dem Staat die Wahl einer passenden Technologie zuzutrauen und eine solche Lösung zu nutzen. Mit einem Mittelwert von 41.3 liegt insgesamt eine relativ hohe Bereitschaft zur Nutzung einer rein staatlichen E-ID vor.

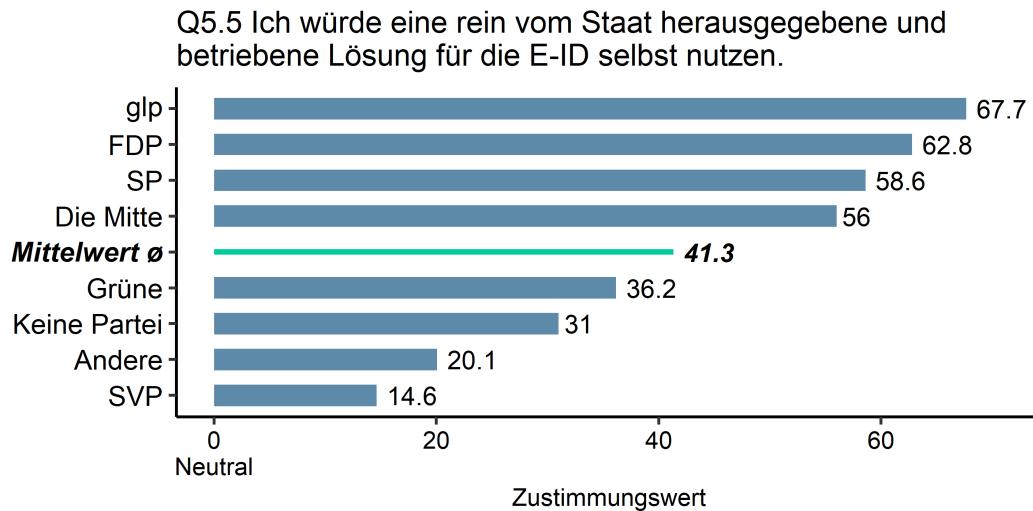


Abbildung 9: Auswertung der Fragestellung Q5.5.

#### 3.4.2 Wahrnehmung & Einordnung der digitalen ID

Die Wahrnehmung und Einordnung einer digitalen ID im Kontext von Log-in-Lösungen und offiziellen Ausweisdokumenten wird innerhalb dieser Fragegruppe analysiert. Mit einem hohen Zustimmungswert von 52.3 über sämtliche Teilnehmenden hinweg wird eine E-ID als offizielles und staatliches Ausweisdokument betrachtet (vgl. Abb. 10 auf der nächsten Seite).

Wird die Aussage durch die Definition einer E-ID als digitales Äquivalent zu einem Pass oder einer Identitätskarte spezifiziert, nimmt die Zustimmung insgesamt leicht ab, liegt jedoch noch immer bei einem Zustimmungswert von 34.9 (vgl. Abb. 11 auf der nächsten Seite). Die Auswertungen der Fragen Q6.2 und Q6.3 zeigen, dass die Mehrheit der Teilnehmenden eine E-ID als ein offizielles, staatliches sowie zu bestehenden Ausweisdokumenten gleichwertiges Identitätsnachweismittel versteht.

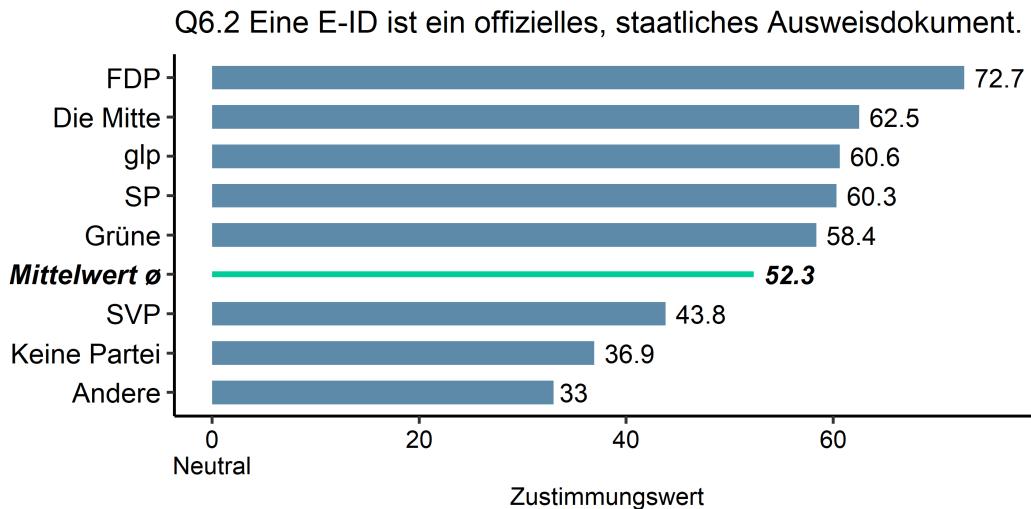


Abbildung 10: Auswertung der Fragestellung Q6.2.

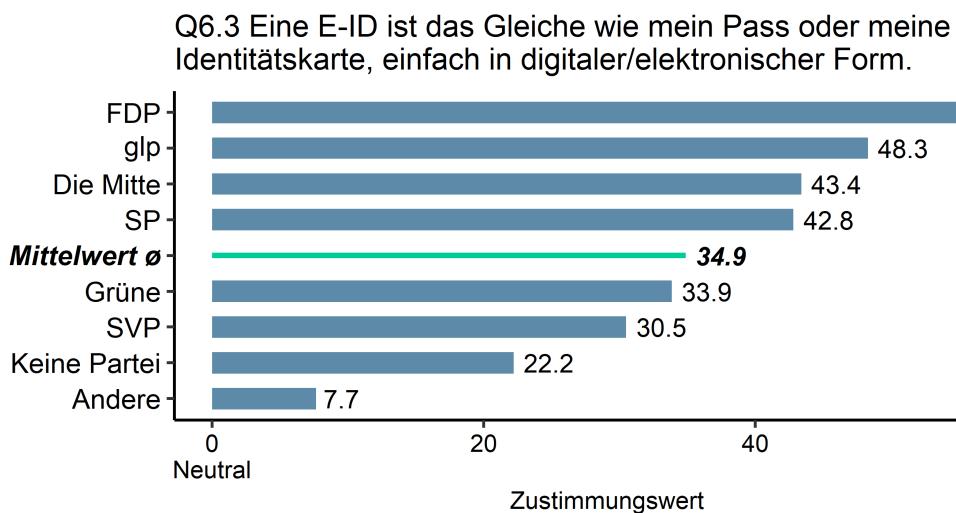


Abbildung 11: Auswertung der Fragestellung Q6.3.

Wird die E-ID in ein spezifisches Nutzungsszenario wie die Ausweiskontrolle im Rahmen eines Grenzübertritts eingebettet, sinkt die Zustimmung ein weiteres Mal leicht ab. Mit einem Mittelwert von 22.7 liegt jedoch auch bei diesem Szenario eine leichte Zustimmung vor und keine Parteigruppe der Teilnehmenden lehnt diese Aussage ab. Bei allen Fragestellungen dieser Gruppe stimmen Parteiverbundene von FDP, glp, Die Mitte und SP den Aussagen am stärksten zu, während Teilnehmende mit Bezug zu Kleinparteien (Andere) oder ohne Bezug zu einer Partei (Keine Partei) die relativ betrachtet tiefsten Zustimmungswerte erreichen.

Q6.4 Mit einer E-ID kann ich mich jederzeit und überall in digitaler Form wie mit meinem Pass oder meiner Identitätskarte ausweisen, bspw. bei einem Grenzübertritt.

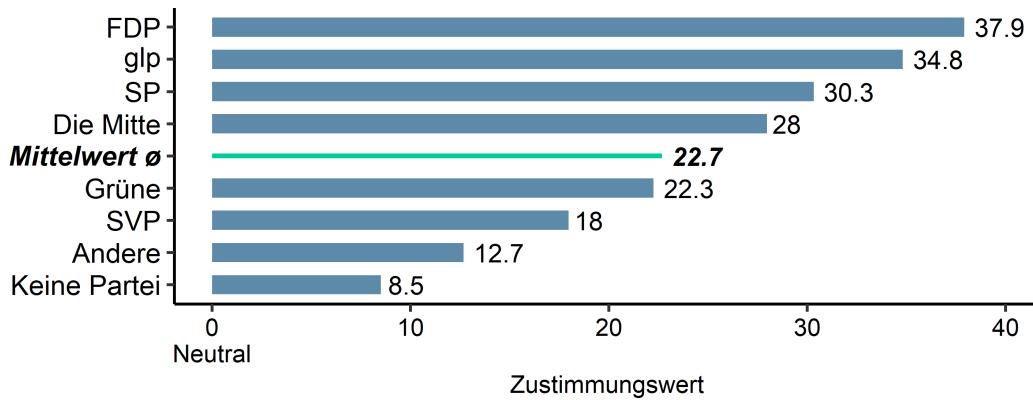


Abbildung 12: Auswertung der Fragestellung Q6.4.

### 3.4.3 Anwendungsbereiche der digitalen ID im öffentlichen Sektor & in der digitalen Demokratie

Der dritte Fragenblock befragt die Umfrageteilnehmenden mit vier Fragestellungen nach der subjektiv empfundenen Wichtigkeit von elektronischen Dienstleistungen des öffentlichen Sektors und der digitalen Demokratie (Visualisierungen im Anhang auf S. 147 ff.). Dienstleistungen über virtuelle Behördenshalter wird eine hohe Wichtigkeit attestiert (Mittelwert = 57.7). Die elektronische Partizipation (E-Partizipation) an politischen und demokratischen Prozessen erreicht noch eine mittelhohe Wichtigkeit (Mittelwert = 28.6).

Elektronisches Abstimmen und Wählen (E-Voting, Mittelwert = 21.7) und elektronisches Unterschriften sammeln für Initiativen und Referenden (E-Collecting, Mittelwert = 17.3) erreichen lediglich noch Werte, welche für eine moderate Wichtigkeit sprechen. Parteiverbundene der SVP sind jedoch die einzigen Teilnehmenden, welche sowohl beim E-Voting (-6.1) als auch beim E-Collecting (-1.5) die Wichtigkeitsfrage mit leicht ablehnenden Werten beurteilen.

Q7.3 (Abb. 13 auf der nächsten Seite) und Q7.4 (Abb. 14 auf der nächsten Seite) zielen darauf ab, die empfundene Notwendigkeit für eine E-ID als suggestive Voraussetzung für vollständig elektronische Behördendienstleistungen und elektronische Demokratie-Instrumente wie E-Voting und E-Collecting zu erfassen. Da vollständig digitale Verwaltungen und digitale Instrumente wie E-Voting oder E-Collecting aus technologischer Sicht ohne eine digitale ID nicht umsetzbar sind, deuten die lediglich mittelhohen Zustimmungswerte von durchschnittlich 24.7 resp. 31.4 auf informelles Aufklärungspotenzial hin.

Q7.3 Eine E-ID ist eine Voraussetzung, um elektronische Dienstleistungen von Behörden vollständig über das Internet beziehen zu können.

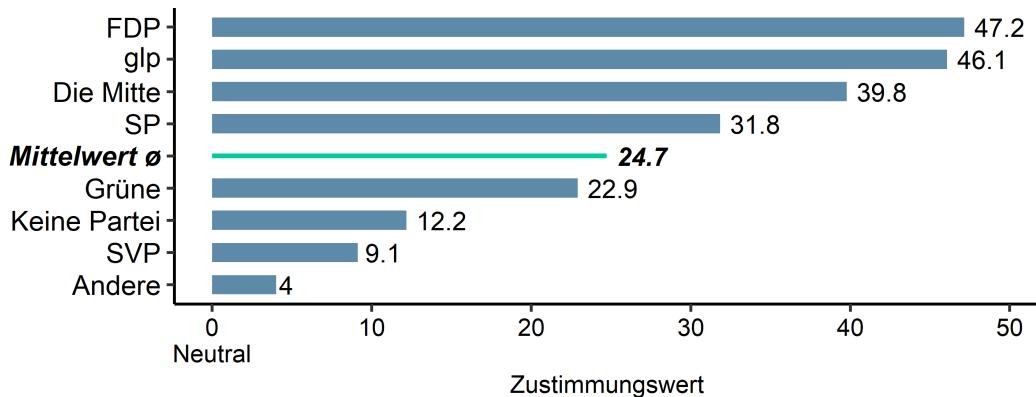


Abbildung 13: Auswertung der Fragestellung Q7.3.

Q7.4 Eine E-ID ist eine Voraussetzung, um elektronische Demokratie-Instrumente wie E-Voting oder E-Collecting nutzen zu können.

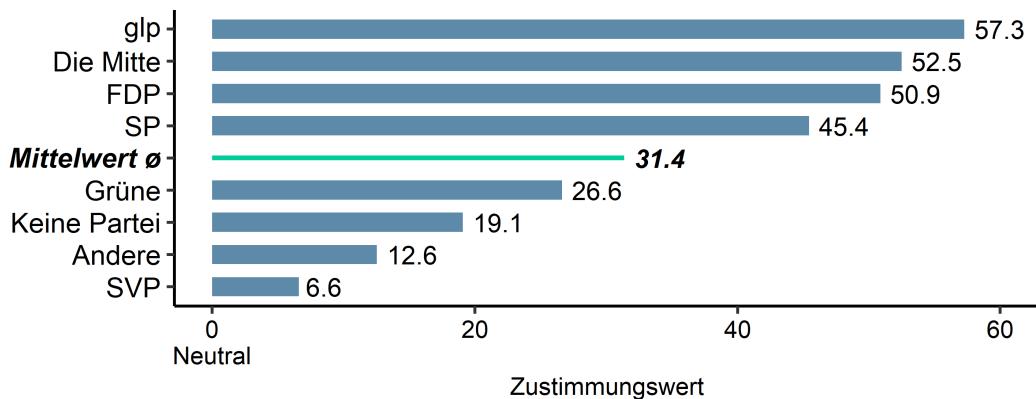


Abbildung 14: Auswertung der Fragestellung Q7.4.

#### 3.4.4 Vorkenntnisse & Einstellung gegenüber der Blockchain-Technologie

Ein Ziel dieser Forschungsarbeit ist es, Erkenntnisse über die Einstellung der schweizerischen Bevölkerung gegenüber der Blockchain-Technologie zu gewinnen. Mit Fragestellungen rund um die Blockchain-Technologie im Allgemeinen befasst sich aus diesem Grund der Fragenblock Q8. Wenn es um bereits bestehende praktische Erfahrungswerte und Berührungs punkte mit der Blockchain-Technologie geht, deuten die erhobenen Daten auf relativ geringe Vorkenntnisse der Umfrageteilnehmenden hin.

Wie in Abb. 15 ersichtlich ist, geben lediglich rund 21% der Befragten an, bereits einmal bewusst mit der Blockchain-Technologie in Kontakt gekommen zu sein. Eine grosse Mehrheit von 67.8% hatte nach eigenen Kenntnissen bisher noch keine Berührungspunkte mit Anwendungen oder Systemen, welche auf der Blockchain-Technologie basieren. Mit 9.76% existiert ebenfalls eine Gruppe von Teilnehmenden, welche diese Frage nicht eindeutig beantworten kann.

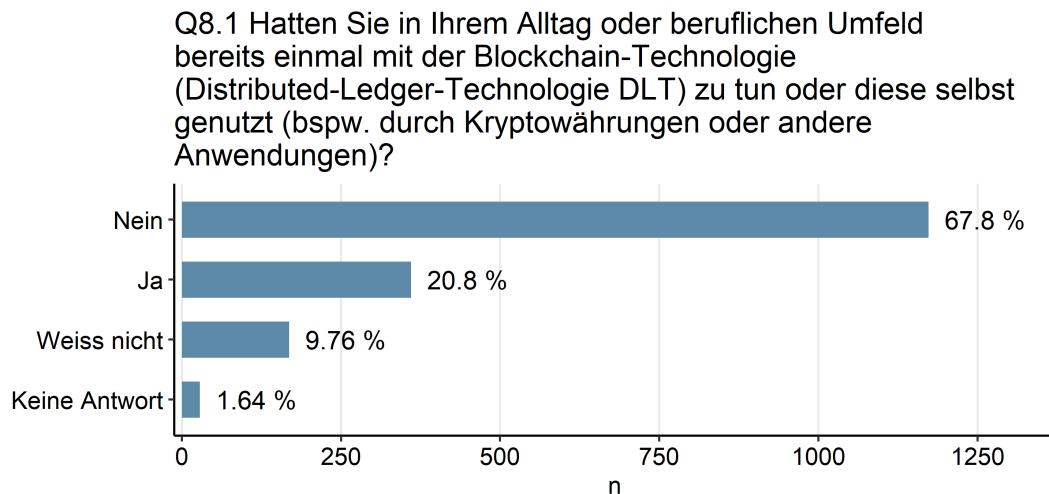


Abbildung 15: Auswertung der Fragestellung Q8.1.

Die zusätzliche Auswertung von Fragestellung Q8.1 im Anhang auf Seite 149 visualisiert diese Daten auf Parteiebene. Parteiverbundene von FDP, glp, SVP sowie Parteilose haben gemäss dieser Auswertung im Verhältnis deutlich mehr Erfahrungen im Umgang mit Blockchain-Anwendungen als Parteiverbundene anderer Parteien. Bei den Parteiverbundenen von SP, Grüne und Die Mitte geben anteilmässig deutlich weniger Teilnehmende an, bereits einmal mit der Blockchain-Technologie in Kontakt gekommen zu sein.

Dieses Bild bestätigt sich ebenfalls in der Auswertung der Fragestellung Q8.3 (vgl. Abb. 16 auf der nächsten Seite). Die Frage, ob die Teilnehmenden mit dem Begriff „Blockchain“ vertraut sind, wird mit einem Mittelwert von 4.1 neutral bewertet, womit dieser Aussage weder zugestimmt noch diese abgelehnt wird. Die relativ betrachtet höchsten Zustimmungswerte erreichen wie bei Frage Q8.1 Parteiverbundene von FDP, glp, SVP sowie Parteilose, während die restlichen Teilnehmenden diese Aussage mit Ausnahme der Grünen leicht ablehnen. Die Ergebnisse decken sich damit mit den Angaben bezüglich praktischen Erfahrungen mit der Blockchain-Technologie. Wird die Frage nach der Vertrautheit mit dem Begriff „Blockchain“ auf die Vertrautheit mit deren technischer Funktionsweise angepasst, wird erstmals innerhalb dieser empirischen Auswertungen eine Aussage durchschnittlich abgelehnt (vgl. Abb. 17 auf der nächsten Seite).

Mit einem Mittelwert von -15.5 ist diese Ablehnung insgesamt relativ schwach. Mit Ausnahme der Parteiverbundenen der SVP geben allerdings sämtliche anderen Parteigruppen durchschnittlich an, mit der technischen Funktionsweise eher mässig vertraut zu sein. Dennoch scheinen sich die Umfrageteilnehmenden insgesamt trotz einem Anteil von 67.8 % der Befragten ohne bisherige Berührungs punkte ein durchschnittlich moderates Wissen über die Technologie zu attestieren.

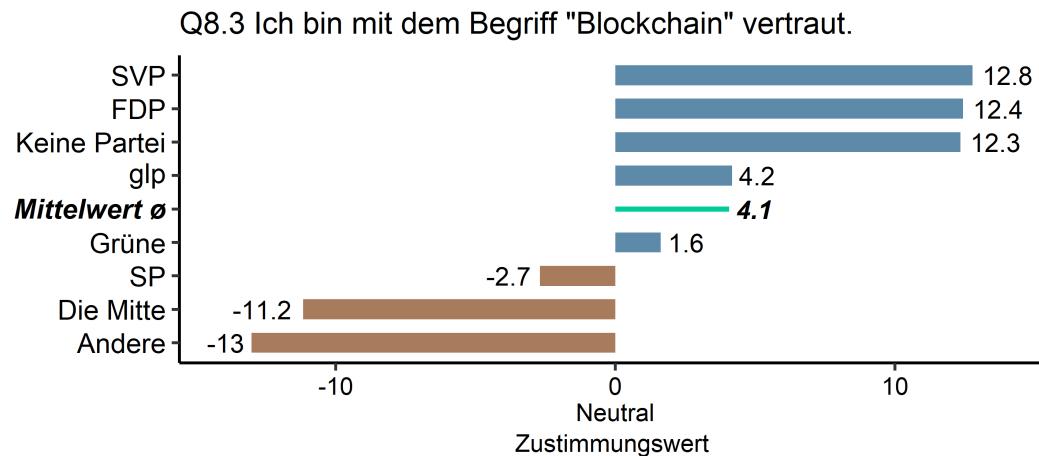


Abbildung 16: Auswertung der Fragestellung Q8.3.

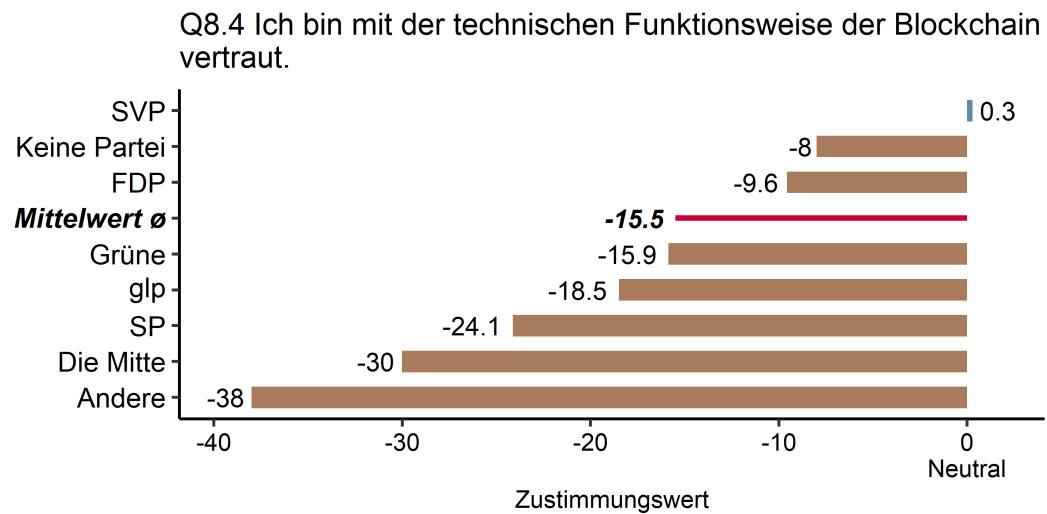


Abbildung 17: Auswertung der Fragestellung Q8.4.

Um einer durchgehenden Gleichförmigkeit der Antwortmuster vorzubeugen und damit die Aufmerksamkeit der Umfrageteilnehmenden im Verlauf der Umfrage punktuell erneut anzuregen, wurde Q8.5 in Abb. 18 invers zu den restlichen Fragestellungen in Form einer Negativformulierung gestellt. Mit einem Durchschnittswert von -7.7 lehnen die Befragten die Aussage, dass sie den Begriff „Blockchain“ mit etwas Negativem verbinden, insgesamt leicht ab.

Der Begriff „Blockchain“ scheint damit im Mittel relativ neutral oder leicht positiv beurteilt zu werden, was sich auf die Einstellung der Befragten gegenüber der Blockchain-Technologie übertragen lässt. Parteiverbundene von Kleinparteien (Andere) stellen die einzige Gruppe dar, welche den Begriff leicht negativ interpretieren. Während die Werte von Parteiverbundenen der SVP, SP und Grüne im Durchschnitt dem Begriff neutral gegenüberstehen, interpretieren Parteiverbundene von Die Mitte, FDP, glp sowie Parteilose den Begriff tendenziell positiv.

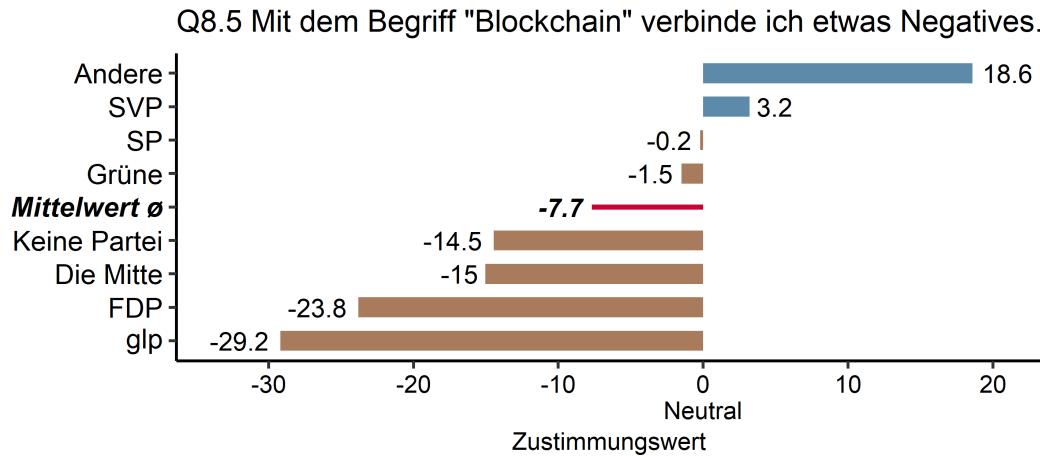


Abbildung 18: Auswertung der Fragestellung Q8.5.

Die Bereitschaft, auf Blockchain-Technologie basierende Anwendungen zu nutzen, deckt sich mit der Einstellung gegenüber dem Begriff „Blockchain“. Die Visualisierung dieser Fragestellung befindet sich in Abb. 19 auf der nächsten Seite. Der Mittelwert von 14.4 offenbart eine leichte Zustimmung gegenüber der Aussage, welche insgesamt von allen Parteigruppen mit Ausnahme der Kleinparteien (Andere) unterstützt wird. Mit Zustimmungswerten von 36.7 (glp) und 31.4 (FDP) existieren auch zwei Gruppen von Parteiverbundenen, welche eine mittelhohe bis hohe Bereitschaft zur grundsätzlichen Nutzung von Blockchain-Anwendungen unterschiedlichster Art aufweisen. Insgesamt scheint die Bereitschaft der Befragten, Blockchain-Anwendungen verschiedenster Art zu nutzen oder deren Nutzung zumindest anwendungsspezifisch in Erwägung zu ziehen somit im Durchschnitt durchaus vorhanden zu sein.

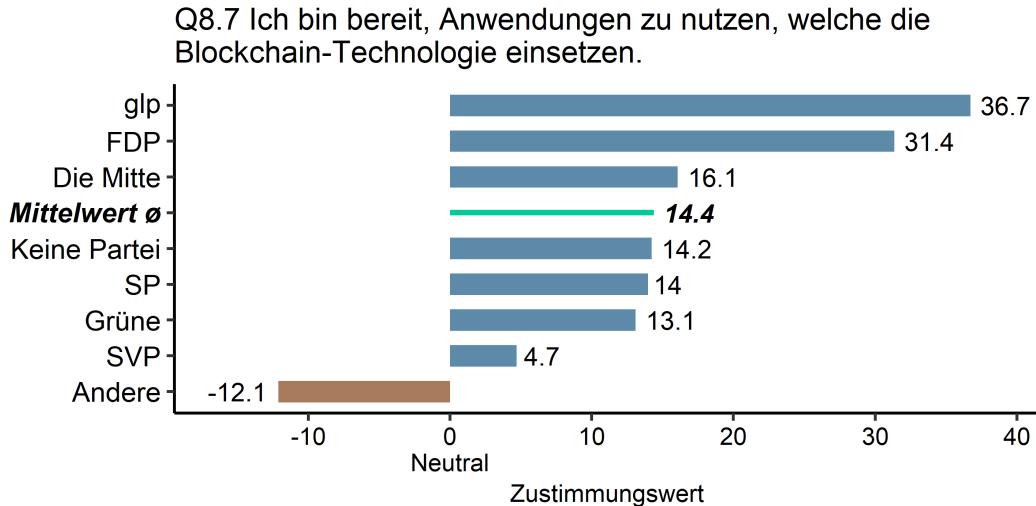


Abbildung 19: Auswertung der Fragestellung Q8.7.

#### 3.4.5 Einstellung gegenüber der Self-Sovereign Identity

Das innerhalb des theoretischen Teils dieser Master-Thesis beschriebene Konzept der Self-Sovereign Identity - also die vollständig selbstbestimmte Identität - ist Bestandteil der Fragestellungen des Fragenblocks Q9. Innerhalb dieses Fragenblocks geht es um die Einstellung der Umfrageteilnehmenden bezüglich der Wichtigkeit von Datenhoheit, Datenkontrolle und Transparenz im Umgang mit den eigenen Identitätsdaten.

Die Auswertungen der einzelnen Fragestellungen zur Wichtigkeit von Datenhoheit, Datenkontrolle und Transparenz sind im Anhang auf Seite 151 einsehbar. Die Analyse der Daten macht deutlich, dass die Teilnehmenden der Umfrage die Kernaspekte von Self-Sovereign Identity unabhängig der Parteiverbundheit mit sehr hoher Zustimmung bewerten. Die Teilnehmenden erwarten mit einem sehr hohen Zustimmungswert von durchschnittlich 85.4, dass ihnen eine E-ID-Lösung bei der Verwendung digitaler Dienstleistungen eine selbstbestimmte Teilung oder Kontrolle der Identitätsdaten erlaubt (Q9.3). Weiter ist mit einem Spitzenwert von 92.2 die Zustimmung zur vollständigen Transparenz über die Verwendung der eigenen Identitätsdaten beinahe absolut (Q9.4). Die Befragten erachten es folglich als unabdingbar, dass eine E-ID-Lösung die Möglichkeit zur transparenten Nachvollziehbarkeit anbietet.

Ein wenig tiefer liegt die Zustimmung und folglich die Erwartung bezüglich der alleinigen Datenhoheit des Datensubjekts im digitalen Raum (vgl. Q9.5 im Anhang auf Seite 151). Der Mittelwert von 73 deutet jedoch auch bei dieser Fragestellung auf eine sehr hohe Zustimmung hin.

Dass sich bei der Frage um die von den Umfrageteilnehmenden erwartete Datenhoheit bezüglich den eigenen Identitätsdaten die Betrachtung ein wenig stärker differenziert, zeigt sich ebenfalls bei der Auswertung von Q9.1 (vgl. Abb. 20). Die Fragestellung erlaubte es den Befragten, „Der Staat“, „Ich selbst“ oder „Private Unternehmen“ zu wählen. Auch mehrere Parteien konnten angegeben und so kombiniert werden.

Rund 59.6 % der Teilnehmenden erwarten, dass die Datenhoheit und Möglichkeit zur Datenkontrolle sowohl beim Datensubjekt selbst sowie beim Staat liegt. Von der Mehrheit wird damit eine E-ID-Lösung erwartet, welche optimalerweise die Datenhoheit zwischen Bund und Datensubjekt teilt. Rund 32 % der Befragten wünschen sich, im digitalen Raum durch entsprechende technologische Lösungen die vollständig autonome und exklusive Datenhoheit und Kontrolle zu besitzen. Diese Gruppe von Befragten spricht sich somit auch indirekt für Lösungen aus, welche das Konzept der Self-Sovereign Identity konsequent umsetzen.

Mit knapp 5 % existiert ebenfalls eine Minderheit, welche sich für eine exklusiv beim Staat liegende Datenhoheit ausspricht. Bemerkenswert ist, dass Kombinationen, welche private Unternehmen in die Datenhoheit miteinbeziehen, mit rund 2,9 % kaum Anklang finden. Eine exklusiv bei privaten Anbieter:innen liegende Datenhoheit und Datenkontrolle wird von praktisch sämtlichen Befragten abgelehnt.

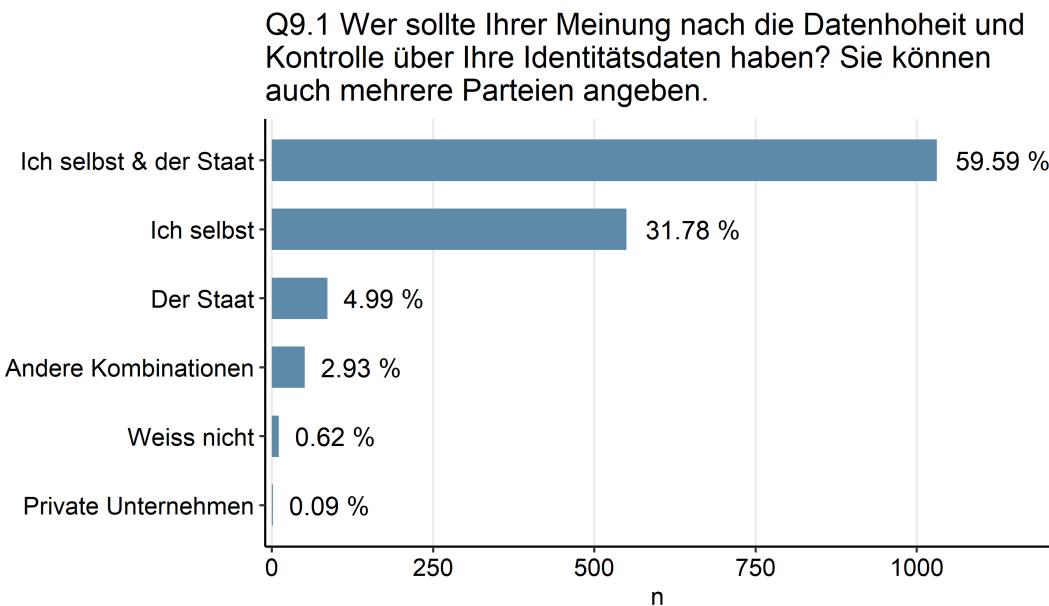


Abbildung 20: Auswertung der Fragestellung Q9.1.

### 3.4.6 Einstellung gegenüber einer digitalen ID auf Basis von Blockchain-Technologie

Nach den Fragestellungen rund um die Thematik der Self-Sovereign Identity werden in diesem Fragenblock spezifische Fragen zur Einstellung der Teilnehmenden gegenüber einer digitalen ID auf Basis von Blockchain-Technologie analysiert. Durch die erste Fragestellung Q10.2 in Abb. 21 wird die Einstellung der Teilnehmenden gegenüber einer E-ID auf Basis von Blockchain-Technologie - ungeachtet den Fragen nach Datenhoheit, Ausstellungsinstanz, etc. - erfasst.

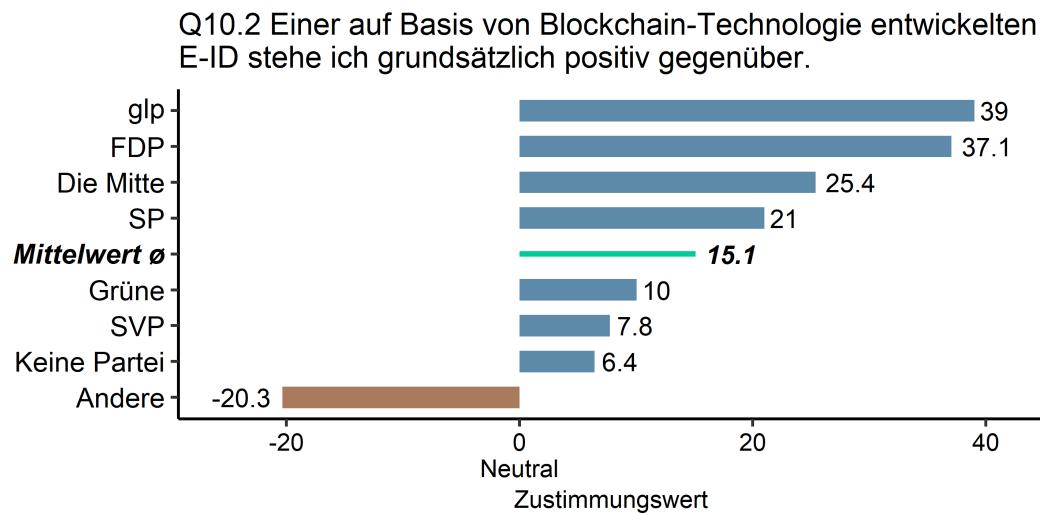


Abbildung 21: Auswertung der Fragestellung Q10.2.

Der Mittelwert von 15.1 deutet darauf hin, dass die Befragten eine E-ID auf Basis von Blockchain-Technologie mit aktuellem Wissensstand leicht positiv beurteilen. Parteiverbundene von glp (39) und FDP (37.1) stehen einer Blockchain-basierten E-ID sogar deutlich positiv gegenüber. Die einzige Gruppe, welche eine Blockchain-basierte E-ID tendenziell leicht ablehnt, sind Parteiverbundene von Kleinparteien (-20.3). Allerdings besitzt dieser Wert aufgrund der Heterogenität der Gruppe kaum Aussagekraft, womit insgesamt von einer parteiübergreifend positiven Wahrnehmung gesprochen werden kann.

Um die Umfrageteilnehmenden auf einen gemeinsamen Wissensstand über die technologischen Potenziale zu bringen, wurde innerhalb der Umfrage nach Q10.2 sämtlichen Befragten folgender Informationstext vorgelegt:

*Expertinnen und Experten gehen davon aus, dass die Blockchain-Technologie eine E-ID-Lösung möglich macht, welche die vollständig selbstbestimmte Verwaltung von Identitätsdaten (Self-Sovereign Identity) erlaubt. Dies würde Ihnen erlauben:*

- *Die alleinige Datenhoheit über Ihre Identitätsdaten zu besitzen.*
  - *Selbst zu entscheiden, ob und wie lange Identitätsdaten jemand anderem zur Verfügung stehen.*
  - *Sämtliche Verwendungen Ihrer Identitätsdaten jederzeit transparent nachvollziehen zu können.*
  - *Ihre Identitätsdaten manipulationssicher und kryptografisch geschützt speichern zu können.*

Dieser Informationstext könnte beispielsweise als Text innerhalb von offiziellen Abstimmungsunterlagen zu Initiativen oder Referenden abgedruckt werden. Durch die Vorlage dieses Informationstexts soll untersucht werden, inwiefern bereits eine kurze Aufklärung über die Potenziale einer Blockchain-basierten E-ID die Einstellung der Befragten beeinflussen kann. Die zusätzliche, im Anhang auf Seite 152 in Q10.5 dargestellte Auswertung bestätigt, dass der vorgelegte Informationstext über die vollständig selbstbestimmte Verwaltung von Identitätsdaten dieses Konzept für die Befragten verständlich erläutert hat (Mittelwert = 50). Ebenfalls beurteilen die Umfrageteilnehmenden das erklärte Konzept mit einem Mittelwert von 39.2 als interessant.

Um den Effekt einer kurzen, textuellen Aufklärung über das Self-Sovereign-Identity-Potenzial erfassen zu können, wurde die Fragestellung Q10.7 in Abb. 22 als Äquivalenzfrage zu Q10.2 nochmals gestellt.

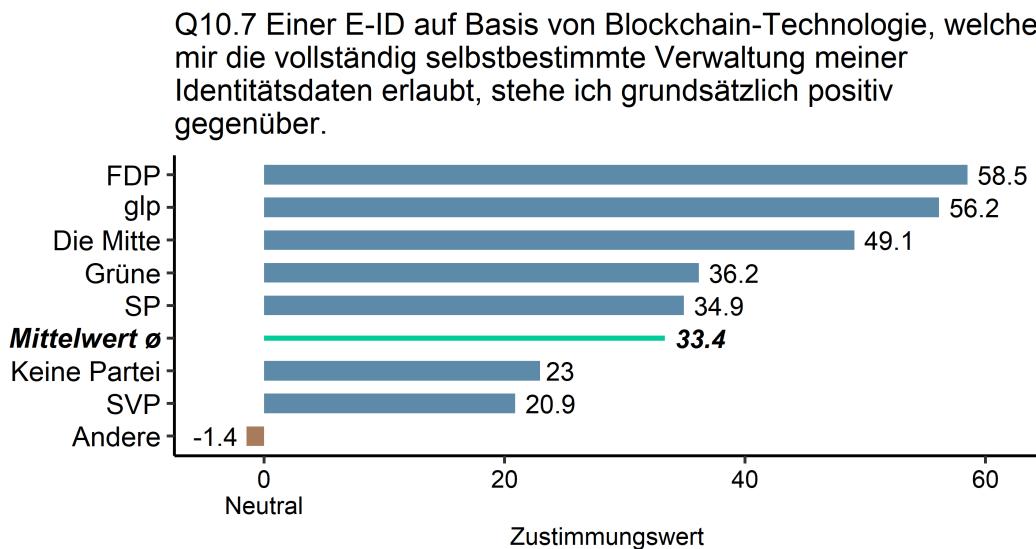


Abbildung 22: Auswertung der Fragestellung Q10.7.

Wie die Auswertung zeigt, steigert bereits eine kurze Aufklärung über das technologische Potenzial der Blockchain-Technologie zur Lösungsentwicklung einer E-ID zum Zwecke der vollständig selbstbestimmten Verwaltung der Identitätsdaten die Zustimmung nochmals deutlich. Mit einem Mittelwert von 33.4 kann nun von einer durchschnittlich mittelhohen Zustimmung gesprochen werden, wobei Parteiverbundene von FDP, glp und Die Mitte nach dem Informationstext einer derartigen Blockchain-Lösung sogar stark zustimmen. Ebenfalls steigert sich die Zustimmung der Parteiverbundenen von Kleinparteien deutlich von vormals -20.3 auf einen neutralen Wert von -1.4. Diese Ergebnisse deuten darauf hin, dass eine Blockchain-basierte E-ID unter den Teilnehmenden der Umfrage im Mittel eine Zustimmung an der Urne erreichen könnte.

#### 3.4.7 Abstimmungsabsicht bezüglich einer staatlichen & Blockchain-basierten ID-Lösung

Zentrales Ziel der Umfrage ist es, Aussagen über die Einstellung der Bevölkerung gegenüber einer Blockchain-basierten E-ID fassen zu können. Damit sollen ebenfalls Aussagen über eine potenzielle Mehrheitsfähigkeit einer derartigen Lösung gemacht werden können. Die Umfrageteilnehmenden werden deshalb in Q11.2 nach ihrer Abstimmungsabsicht bei einer hypothetischen Volksabstimmung über eine rein staatliche und Blockchain-basierte E-ID-Lösung befragt (vgl. Abb. 23). Die Datenanalyse wird für diese Fragestellung ausführlicher vorgenommen, wobei neben den bereits bekannten Auswertungen nach Partei auch Auswertungen bezüglich Geschlecht und Sprachregion vorgenommen werden. Im Gegensatz zum Fragenblock Q10 wird in diesem Fragenblock der Staat exklusiv als die eine E-ID herausgebende Instanz definiert.

Q11.2 Angenommen, am nächsten Wochenende würde eine Volksabstimmung über eine rein staatliche und Blockchain-basierte E-ID-Lösung stattfinden. Würden Sie einer solchen Vorlage zustimmen?

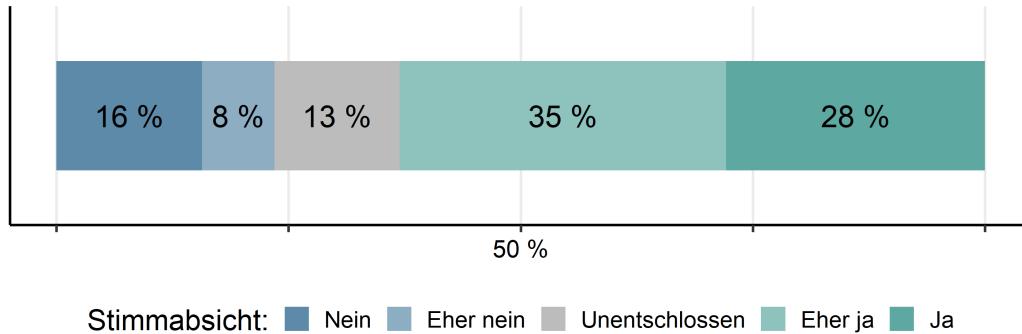


Abbildung 23: Auswertung der Fragestellung Q11.2 - Total.

Die Gesamtauswertung von Q11.2 (vgl. Abb. 23 auf der vorherigen Seite) zeigt die Stimmabsicht sämtlicher Teilnehmenden der Umfrage ( $n = 1'730$ ). Mit einem ‚Ja‘-Anteil von 28 % und einem ‚Eher ja‘-Anteil von 35 % erreicht die hypothetische Volksabstimmung über eine staatliche, Blockchain-basierte E-ID eine potenzielle Zustimmung von 63 % an der Urne. Der Anteil an unentschlossenen Teilnehmenden beläuft sich auf 13 %. Mit einem Anteil von 16 % und einen Anteil 8 % machen die Teilnehmenden, welche eine derartige Vorlage mit ‚Nein‘ oder ‚Eher nein‘ ablehnen würden, 24 % aus. Unter den Befragten Personen scheint eine staatliche und Blockchain-basierte E-ID folglich realistische Chancen für eine Mehrheit an der Urne vorweisen zu können. Selbst wenn man davon ausgeht, dass sich der Anteil an Unentschlossenen (13 %) noch vollständig gegen eine derartige E-ID-Lösung entscheidet, läge das Verhältnis von ‚Ja‘-Stimmen und ‚Nein‘-Stimmen bei 63 % zu 37 %. Dies entspräche einer deutlichen Annahme der hypothetischen Vorlage.

Da aufgrund der Erkenntnisse der Studien zur *E-ID 2020* von *gfs.bern* [gfs.bern 2021] und des *Mobiliar DigitalBarometer 2020/21* [Rüthi et al. 2020] die Eigenschaftsmerkmale Geschlecht, Sprachregion und Partei relevant sind, wird die Fragestellung Q11.2 zusätzlich nach diesen Merkmalen analysiert. Abb. 24 wertet die Fragestellung nach Geschlecht aus. Insgesamt sind die Unterschiede zwischen männlichen und weiblichen Umfrageteilnehmenden relativ gering, wobei die Zustimmung (‚Ja‘ und ‚Eher ja‘) bei den männlichen Befragten mit 67 % im Vergleich zu den weiblichen Befragten mit 59 % höher ist.

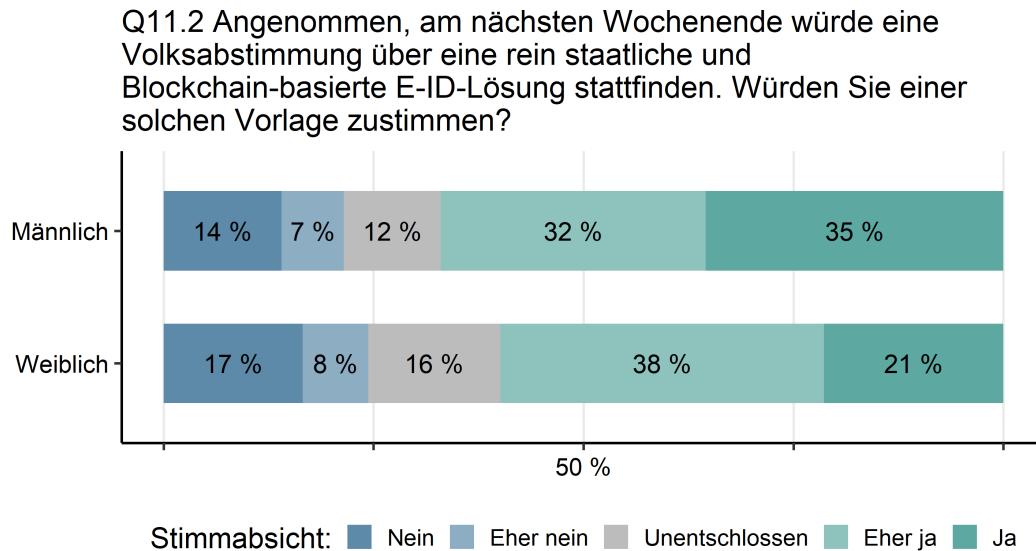


Abbildung 24: Auswertung der Fragestellung Q11.2 nach Geschlecht.

Der deutlichste Unterschied zeigt sich bei den ‚Ja‘-Anteilen. Mit 21 % stehen die weiblichen Teilnehmenden einer hypothetischen Volksabstimmung deutlich weniger entschlossen gegenüber, als die männlichen Teilnehmenden mit 35 %. Diese Tendenz zeigt sich ebenfalls bei den Anteilen an Unentschlossenen.

Bei der Auswertung nach Sprachregion fallen die Unterschiede zwischen deutschsprachigen und französischsprachigen Teilnehmenden ebenfalls eher gering aus (vgl. Abb. 25). Bei den deutschsprachigen Teilnehmenden sind die Anteile in den Kontrapositionen ‚Ja‘ und ‚Nein‘ jeweils stärker vertreten, als bei den französischsprachigen Teilnehmenden. Als logische Folge dessen ist die Unentschlossenheit bei den französischsprachigen Teilnehmenden höher. Teilnehmende beider Sprachregionen würden insgesamt der hypothetischen Vorlage mit 64 % (DE) resp. 59 % (FR) zustimmen.

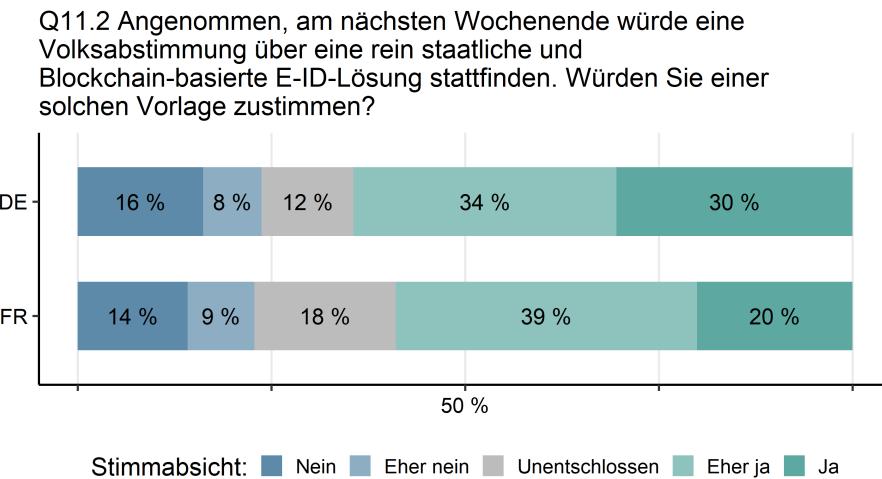


Abbildung 25: Auswertung der Fragestellung Q11.2 nach Sprache.

Als letzte Auswertung von Q11.2 folgt eine Aufgliederung der Resultate nach Parteiverbundenheit (vgl. Abb. 26 auf der nächsten Seite). Sehr hohe Zustimmungswerte von über 75 % (‚Ja‘ und ‚Eher ja‘) erreicht die hypothetische Vorlage bei Parteiverbundenen von glp, FDP und Die Mitte. Vor allem bei den Parteiverbundenen der glp und der FDP ist der Anteil an Personen, welche ein ‚Ja‘ an der Urne einlegen würden, mit 46 % und 41 % verhältnismässig hoch. Den vier der hypothetischen Volksvorlage am stärksten zustimmenden Parteien (glp, FDP, Die Mitte, SP) ist gemein, dass die Anteile an Befragten, welche die Vorlage bestimmt oder eher ablehnen würden, jeweils lediglich im einstelligen Prozentbereich liegen. Nach diesen vier Parteien verdoppelt sich der ‚Nein‘-Anteil von 7 % bei Parteiverbundenen der SP auf 14 % bei Parteiverbundenen der Grünen. Letztere weisen ebenfalls einen relativ geringen Anteil an ‚Ja‘-Stimmenden (19 %) auf, was für eine vergleichsweise hohe Unentschlossenheit oder Unsicherheit sprechen kann.

Parteilose sowie Parteiverbundene der SVP weisen ein ausgeglichenes Verhältnis zwischen ‚Ja‘-Stimmenden und ‚Nein‘-Stimmenden auf. Jeweils rund ein Viertel der sich diesen Gruppen zugehörig fühlenden Teilnehmenden lehnen die hypothetische Vorlage definitiv ab oder stimmen ihr definitiv zu. Während bei den Parteilosen durch einen Anteil von 32 % ‚Eher ja‘-Stimmenden insgesamt noch eine knappe Zustimmungsmehrheit von 57 % vorliegt, kann bei den Parteiverbundenen der SVP mit 48 % erstmals die 50 %-Grenze an ‚Ja‘- und ‚Eher ja‘-Stimmen nicht erreicht werden. In der Gesamtbetrachtung der SVP ist die Zustimmung mit 48 % allerdings noch immer höher, als die Ablehnung mit 37 %. Die stärkste Ablehnung erfährt die vorgeschlagene E-ID-Lösung durch Parteiverbundene von Kleinparteien. Die Heterogenität der Gruppe ‚Andere‘ schliesst eine wissenschaftliche Relevanz dieses Resultats allerdings erneut aus.

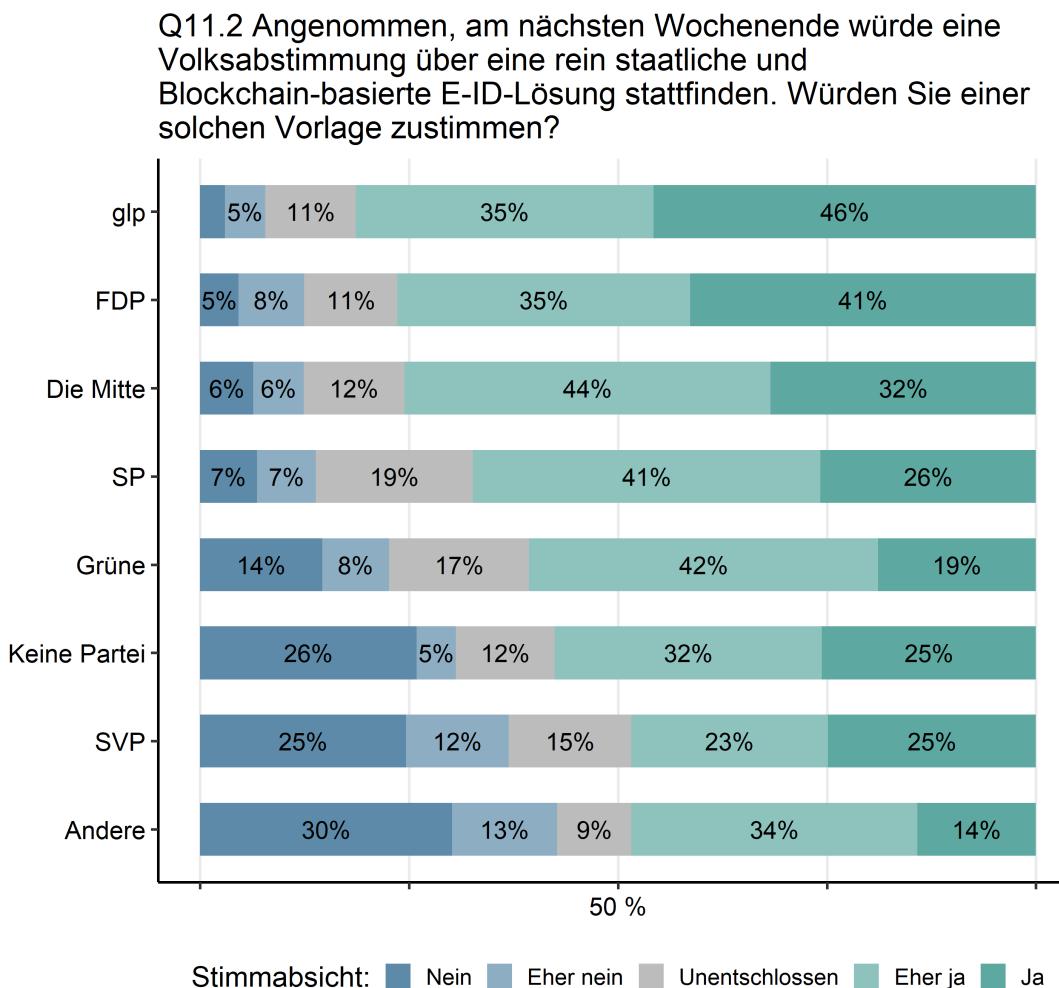


Abbildung 26: Auswertung der Fragestellung Q11.2 nach Partei.

Zusammenfassend scheint im Gegensatz zur vergangenen Volksabstimmung *E-ID 2020* die vorgeschlagene, rein staatliche und Blockchain-basierte E-ID-Lösung insgesamt auf Zustimmung zu stossen. Sofern diese Ergebnisse korrekt sind, müsste sich ein positiver Trend auch bei der Fragestellung Q11.3 feststellen lassen (Abb. 27). Diese Frage erfasst die Veränderung der Zustimmung oder Ablehnung von Teilnehmenden zwischen der Volksabstimmung *E-ID 2020* und der zuvor dargelegten, hypothetischen E-ID-Lösung.

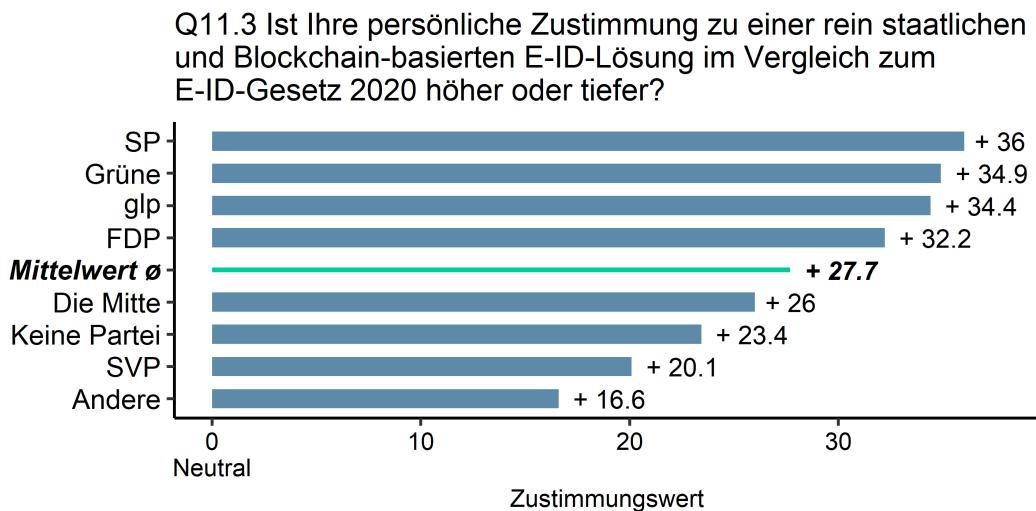


Abbildung 27: Auswertung der Fragestellung Q11.3.

Wie die Auswertung zeigt, bestätigt sich das Ergebnis der Abstimmungsabsicht. Mit einem Mittelwert von + 27.7 ist die Zustimmung für die vorgeschlagene und hypothetische E-ID-Lösung im Vergleich zur Volksabstimmung *E-ID 2020* insgesamt höher. Bemerkenswert ist ausserdem, dass bei sämtlichen Parteigruppen eine erhöhte Zustimmung feststellbar ist. Diese Ergebnisse stützen die in Q11.2 evaluierten Ergebnisse zur Stimmabsicht der Umfrageteilnehmenden.

### **3.4.8 Gründe für und gegen eine staatliche & Blockchain-basierte ID-Lösung**

Nach Angabe der Stimmabsicht geben die Umfrageteilnehmenden Gründe für und gegen eine staatliche und Blockchain-basierte ID-Lösung an. Unabhängig von der Antwort zur Stimmabsicht werden die Befragten nach Gründen für eine Zustimmung oder Ablehnung befragt. Somit geben auch Teilnehmende, welche die Vorlage annehmen oder ablehnen würden, denkbare Gründe an, welche aus ihrer Sicht für eine gegenteilige Stimmabgabe sprechen könnten. Die Fragestellung erlaubt jeweils die gleichzeitige Auswahl von mehreren Gründen.

### Zustimmungsgründe staatliche Blockchain-ID Q11.4, Q11.7, Q11.8

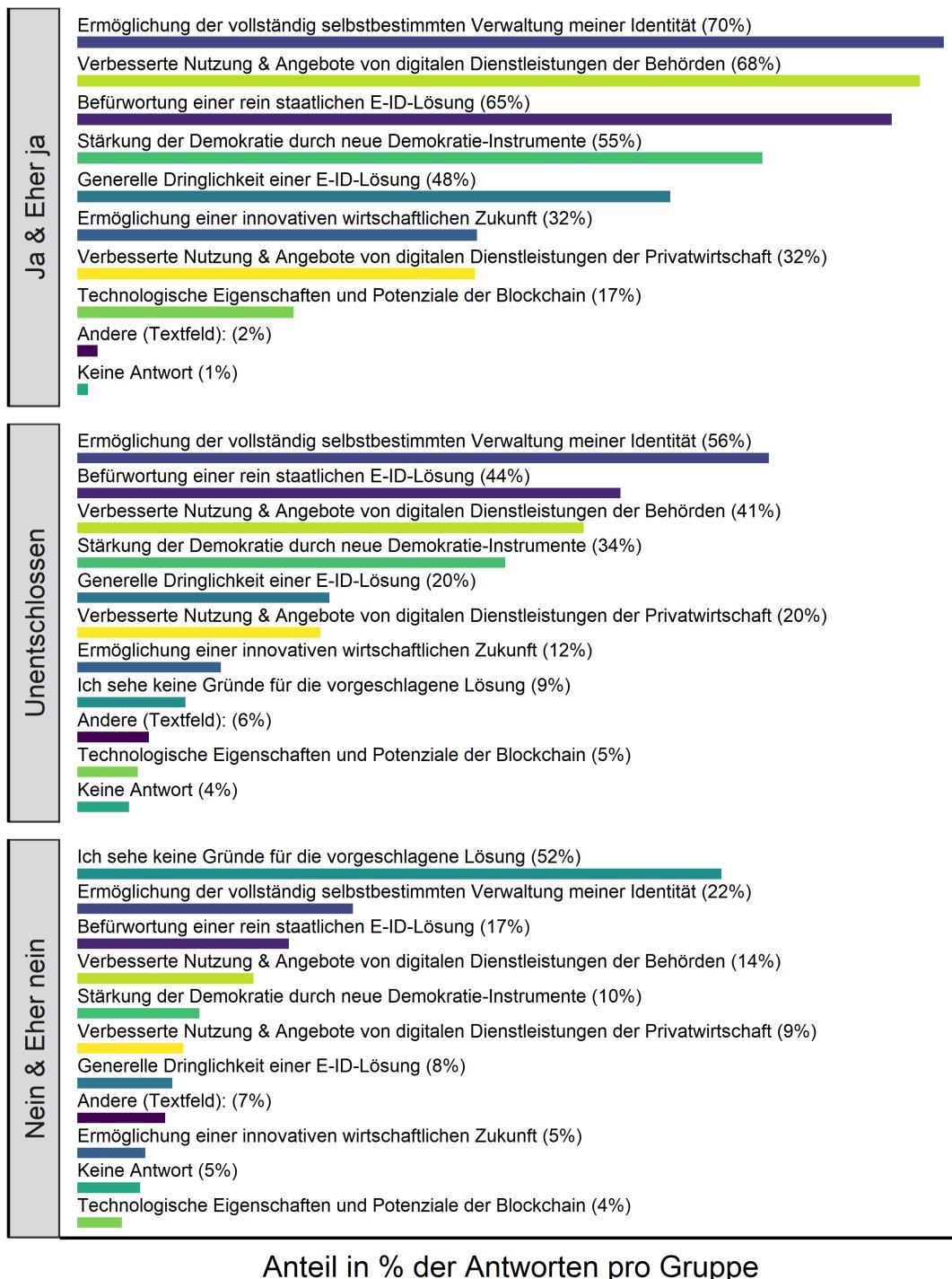


Abbildung 28: Auswertung der Fragestellungen Q11.4, Q11.7 und Q11.8 nach Stimmabsicht.

In einem ersten Schritt werden die Zustimmungsgründe sämtlicher Antwortgruppen (*Ja & Eher ja*, *Unentschlossen*, *Nein & Eher nein*) in Abb. 28 auf der vorherigen Seite ausgewertet. 70 % der Teilnehmenden, welche bei einer Volksabstimmung (eher) beabsichtigen, mit ‚Ja‘ abzustimmen, nennen als wichtigsten Grund für die Zustimmung die Ermöglichung der vollständig selbstbestimmten Verwaltung der eigenen Identität. Dieser Grund wird von 56 % der unentschlossenen Teilnehmenden ebenfalls als Hauptgrund für eine potenzielle Zustimmung betrachtet.

Weiter wird bei Teilnehmenden, welche mit (eher) ‚Nein‘ abstimmen würden, dieser Grund noch immer von 22 % als potenziell wichtigster Zustimmungsgrund erachtet. Die Ermöglichung der vollständig selbstbestimmten Verwaltung der eigenen Identität stellt damit das Hauptargument für eine staatliche Blockchain-ID über sämtliche Teilnehmende hinweg dar.

Mit 68 % in der Gruppe *Ja & Eher ja*, 41 % in der Gruppe *Unentschlossen* sowie 14 % in der Gruppe *Nein & Eher nein* sehen die Teilnehmenden einen weiteren wichtigen Zustimmungsgrund in der Verbesserung von digitalen Behördendienstleistungen. Ebenfalls als Hauptargument für die vorgeschlagene Blockchain-ID wird die rein staatliche Verantwortlichkeit von den Umfrageteilnehmenden angeführt. Dieses Argument erreicht ebenfalls hohe Anteilswerte und wurde von den Gruppen *Ja & Eher ja* und *Unentschlossen* von jeweils 65 % resp. 44 % der Befragten genannt. Auch die Stärkung der Demokratie durch neue, mithilfe einer Blockchain-ID realisierbare Instrumente wie beispielsweise E-Voting oder E-Collecting, wird von diesen beiden Gruppen noch mit 55 % resp. 34 % der Teilnehmenden angeführt.

(Privat-)Wirtschaftliche Aspekte scheinen für die Befragten in sämtlichen Gruppen eine eher untergeordnete Rolle zu spielen. Mit Werten von maximal 32 % kommt der Verbesserung von digitalen Dienstleistungen in der Privatwirtschaft sowie der Ermöglichung einer innovativen wirtschaftlichen Zukunft durch eine Blockchain-ID eine sekundäre Rolle zu. Ebenfalls scheint den technologischen Potenzialen der Blockchain-Technologie an sich keine bedeutende Stellung für die Zustimmung zu einer staatlichen und Blockchain-basierten ID zuzukommen. Dies scheint auf den ersten Blick in einem möglichen Widerspruch zum meistgenannten Zustimmungsgrund zu stehen. Die Ermöglichung der vollständig selbstbestimmten Verwaltung der eigenen Identität stellt eines der technologischen Haupteigenschaften der Blockchain-Technologie dar.

Bemerkenswert ist ausserdem, dass rund die Hälfte der Teilnehmenden (52 %), welche mit (eher) ‚Nein‘ abstimmen würden, überhaupt keine Gründe für die vorgeschlagene E-ID-Lösung sieht. Mit den Ablehnungsgründen wird sich die Auswertung in Abb. 29 auf der nächsten Seite befassen.

### Ablehnungsgründe staatliche Blockchain-ID Q11.5, Q11.6, Q11.9

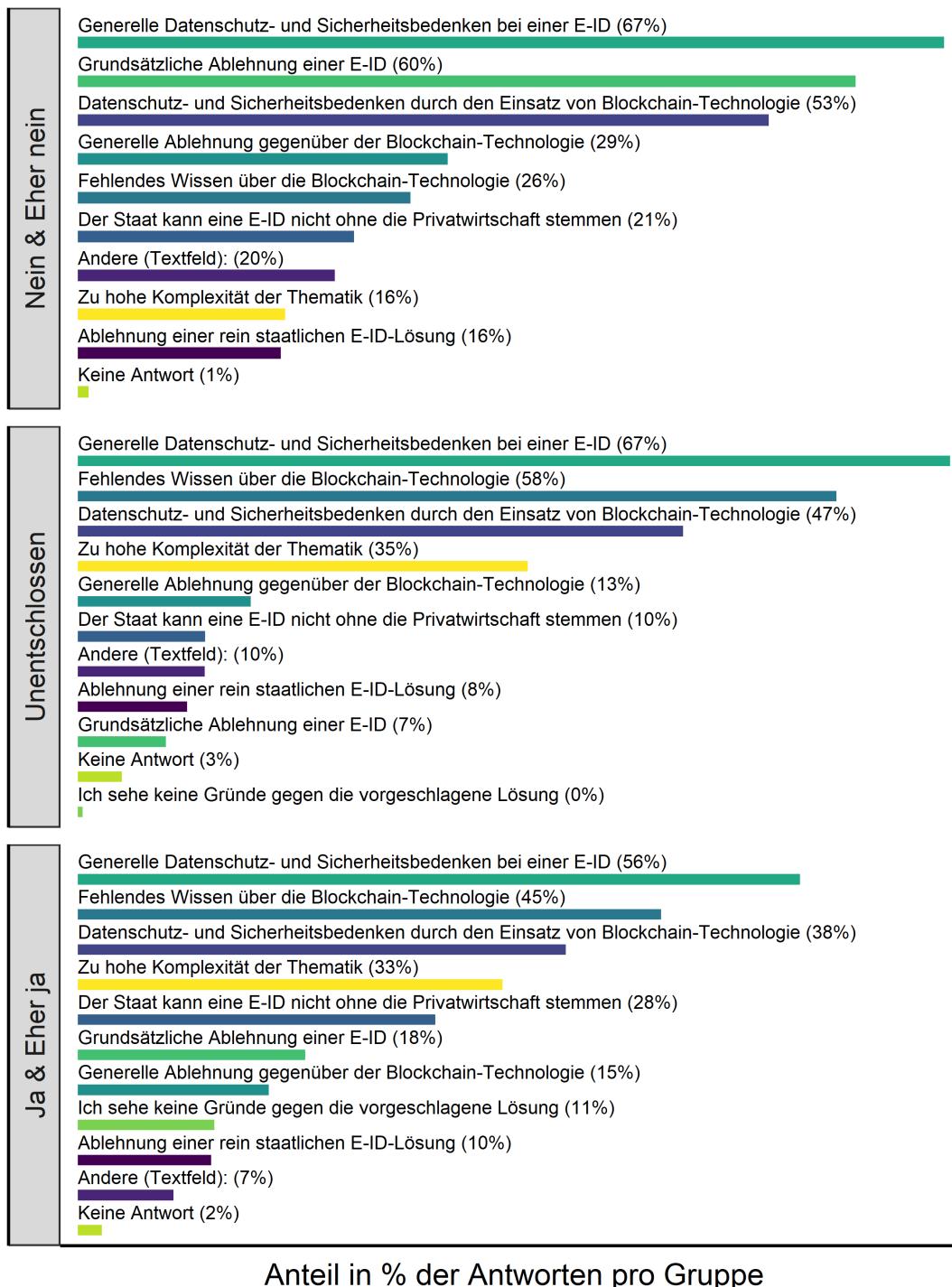


Abbildung 29: Auswertung der Fragestellungen Q11.5, Q11.6 und Q11.9 nach Stimmabsicht.

67% der Teilnehmenden, welche bei einer Volksabstimmung (eher)beabsichtigen, mit ‚Nein‘ abzustimmen, nennen als wichtigsten Grund für die Ablehnung generelle Datenschutz- und Sicherheitsbedenken bei einer E-ID, unabhängig der technologischen Basis. Dieser Grund wird ebenfalls von 67% der unentschlossenen Teilnehmenden als Hauptgrund für eine potenzielle Ablehnung betrachtet. Auch Teilnehmende, welche der vorgeschlagenen E-ID-Lösung zustimmen, nennen mit immerhin noch 56% generelle Datenschutzbedenken als denkbaren Ablehnungsgrund. Für 60% der Gruppe *Nein & Eher nein* ist weiter die grundsätzliche Ablehnung einer E-ID ausschlaggebend. Dieser Ablehnungsgrund findet sich zwischen den bereits erwähnten generellen Datenschutz- und Sicherheitsbedenken (67%) und Datenschutz- und Sicherheitsbedenken durch den Einsatz von Blockchain-Technologie (53%) wieder. Für die die vorgeschlagene E-ID-Lösung ablehnenden Teilnehmenden stellen diese drei Gründe damit die Hauptargumente gegen eine staatliche Blockchain-ID sowie gegen eine E-ID im Allgemeinen dar.

Dass der angedachte Einsatz von Blockchain-Technologie zur Umsetzung einer E-ID nicht umstritten ist, zeigen auch die Auswertungen der Gruppen *Ja & Eher ja* und *Unentschlossen*. Diese Gruppen führen mit relativ hohen Werten von 45% resp. 58% ein fehlendes Wissen über die Blockchain-Technologie als denkbare Ablehnungsgründe an. Auch Datenschutz- und Sicherheitsbedenken durch den Einsatz von Blockchain-Technologie sind für die beiden Gruppen relevant (38% resp. 47%). Auffällig ist, dass für die ablehnende Gruppe *Nein & Eher nein* das Argument des fehlenden Wissens im Gegensatz zu den anderen Gruppen eine eher untergeordnete Rolle spielt (26%). Für keine der drei Gruppen stellt die generelle Ablehnung der Blockchain-Technologie eine der Haupthürden zur Akzeptanz der vorgeschlagenen E-ID-Lösung dar. Mit 29% geben zwar knapp ein Drittel der Teilnehmenden der Gruppe *Nein & Eher nein* an, die Blockchain-Technologie per se abzulehnen. Damit platziert sich das Argument jedoch lediglich auf Rang vier der Ablehnungsgründe für diese Gruppe und liegt prozentual deutlich hinter den drei darüber liegenden Hauptargumenten. Dass die 29% starke Ablehnung der Blockchain-Technologie dieser Gruppe nicht auf eine zu hohe Komplexität der Thematik zurückzuführen ist, zeigt der relativ geringe Anteil von 16%. Dieser Wert ist im Gegensatz zu den Angaben der Gruppen *Ja & Eher ja* (33%) und *Unentschlossen* (35%) bemerkenswert tief.

Kaum zur Ablehnung tragen Gründe wie die Notwendigkeit privatwirtschaftlicher Beteiligung oder die Ablehnung einer rein staatlichen E-ID-Lösung bei. Hier bestätigt sich nochmals, dass die Umfrageteilnehmenden mehrheitlich eine rein staatliche E-ID fordern. Im Gegensatz zu den Zustimmungsgründen wird bei den Ablehnungsgründen die Möglichkeit zur Angabe eigener Gründe über ein Textfeld (Andere) von 20% der Teilnehmenden genutzt. Die manuell ausgewerteten Texteingaben führen mehrheitlich Gründe mit Bezügen zur Ökobilanz und dem Energieverbrauch der Blockchain-Technologie als Ablehnungsgründe an.

## 3.5 Inferenzstatistische Datenauswertungen

Um die in Abschnitt 3.1.1 auf Seite 60 aufgestellten Hypothesen untersuchen zu können, werden verschiedene inferenzstatistische Methoden und Instrumente angewandt. Die Hypothesen werden jeweils statistisch ausgewertet und die Resultate anschliessend visualisiert. Die Visualisierungen der inferenzstatistischen Auswertungen setzen sich aus *Box-Whisker-Plots* in Kombination mit *Violin-Diagrammen* sowie jeweils einer Regressionskurve zusammen. Für Leser:innen, welche mit der Interpretation dieser Diagramme nicht vertraut sind, steht im Anhang auf Seite 154 eine Hilfestellung zur Verfügung. Vollendet wird die inferenzstatistische Datenauswertung mit einer multivariaten Datenanalyse in Form eines Entscheidungsbaums (vgl. Abschnitt 3.5.4 auf Seite 103). Mit der multivariaten Datenanalyse wird ebenfalls der empirische Teil dieser Master-Thesis insgesamt abgeschlossen.

### 3.5.1 Hypothese 1: Blockchain-Kompetenz & Stimmabsicht

*Je höher die Selbsteinschätzung der technologischen Kompetenz von Befragten in Bezug auf die Blockchain-Technologie ist, desto höher ist die Zustimmung gegenüber einer staatlichen, Blockchain-basierten E-ID.*

Als erster Schritt zur Auswertung von Hypothese 1 wird ein Index *Selbsteinschätzung Kompetenz* in Bezug auf die Blockchain-Technologie geschaffen. Zu diesem Zweck wird beabsichtigt, die Fragestellungen oder Items Q8.3 und Q8.4 zusammenzufassen. In diesen Fragestellungen geben die Umfrageteilnehmenden eine Selbsteinschätzung zur Vertrautheit mit dem Begriff „Blockchain“ und der Funktionsweise der Blockchain-Technologie an. Um festzustellen, ob diese beiden Fragestellungen sich für die Indexbildung eignen, wird die Reliabilität mittels Cronbach Alpha-Koeffizient geprüft. Der Cronbach Alpha-Koeffizient ( $\alpha = .919$ ) erreicht für die untersuchten Items Q8.3 und Q8.4 einen exzellenten Wert. Damit kann davon ausgegangen werden, dass die beiden Items sich gleich verhalten resp. das gleiche messen und diese im Index *Selbsteinschätzung Kompetenz* als arithmetischer Mittelwert zusammengefasst werden können. Zur Untersuchung des Zusammenhangs zwischen Selbsteinschätzung der Kompetenz und der Stimmabsicht bei einer hypothetischen Volksabstimmung wird eine Rangkorrelation nach *Spearman* durchgeführt. Die Auswertung ergibt, dass die Selbsteinschätzung der Umfrageteilnehmenden bezüglich ihrer Blockchain-Kompetenz signifikant positiv mit der Stimmabsicht bei einer hypothetischen Volksabstimmung korreliert ( $r_s = .127$ ,  $p = < .001$ ,  $n = 1'629$ ). Dabei handelt es sich nach Cohen [1992] lediglich um einen schwachen Effekt.

Ein Blick auf die Visualisierung des Zusammenhangs zwischen Selbsteinschätzung der Kompetenz und der Stimmabsicht bei einer hypothetischen Volksabstimmung offenbart eine interessante Korrelationstendenz (vgl. Abb. 30). Die rötlich

gekennzeichnete Regressionskurve zeigt, dass sich in der Tendenz die Stimmabsicht stärker auf die beiden Polpositionen ‚Nein‘ und ‚Ja‘ verteilt, je höher die Teilnehmenden ihre eigene Kompetenz in Bezug auf die Blockchain-Technologie einschätzen. Teilnehmende, welche bezüglich ihrer Stimmabsicht noch unentschlossen sind, attribuieren sich selbst tendenziell die tiefste Kompetenz. Über das Zustandekommen dieser speziellen Verteilung kann im Rahmen dieser Arbeit lediglich spekuliert werden. Eine mögliche Interpretation dieser Korrelation kann sein, dass die Blockchain-Technologie über derart polarisierende positive wie auch negative Eigenschaften und Potenziale verfügt, sodass sich gut informierte Personen entweder klar für oder gegen den Einsatz der Technologie im Rahmen einer E-ID stellen.

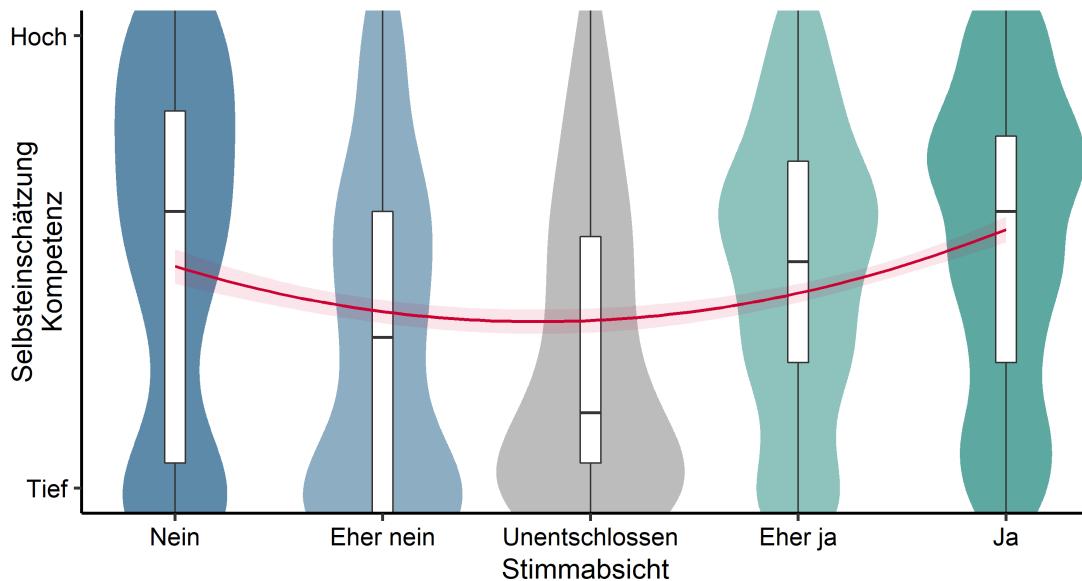


Abbildung 30: Visualisierung Hypothese 1 - Rangkorrelation nach Spearman von Kompetenz und Zustimmung.

Die relativ symmetrisch anmutende Regressionskurve erschwert die Einordnung der Stimmabsichtstendenz der drei verbleibenden und noch nicht vollständig entschlossenen Positionen. Einen möglichen Anhaltspunkt könnte die deskriptive Auswertung von Q10.8 in Abb. 31 auf der nächsten Seite liefern. Der Mittelwert von 24.3 deutet als mittelhoher Zustimmungswert darauf hin, dass die Parteiverbundenen fast aller Parteien bezogen auf die verwendete Technologie tendenziell offen sind. Unentschlossene oder teilweise unentschlossene Teilnehmende könnten bei einer Volksabstimmung auf Basis dieser Auswertung in der Gesamttendenz und ungeachtet ihrer Kompetenz eine eher zustimmende Haltung gegenüber einer staatlichen, Blockchain-basierten E-ID entwickeln.

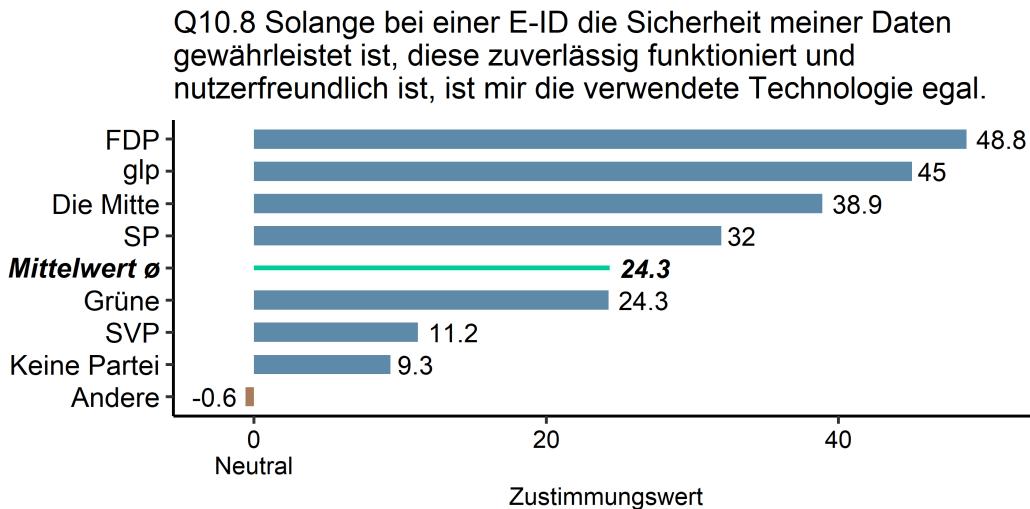


Abbildung 31: Auswertung der Fragestellung Q10.8.

Basierend auf den Ergebnissen der Rangkorrelation nach *Spearman* ( $r_s = .127$ ,  $p = < .001$ ,  $n = 1'629$ ) in Verbindung mit den deskriptiven Analysen kann die Nullhypothese  $H_0$  verworfen und die Alternativhypothese  $H_1$  angenommen werden. Somit kann eine nach Cohen [1992] schwache Korrelation zwischen der Selbsteinschätzung der technologischen Kompetenz in Bezug auf die Blockchain-Technologie und der Zustimmung gegenüber einer staatlichen, Blockchain-basierten E-ID festgestellt werden. Allerdings ist die Korrelation zwischen Selbsteinschätzung der Kompetenz und der Stimmabsicht nicht eindeutig positiv, sondern von einer Dualität der beiden Polpositionen geprägt. Ebenfalls muss festgehalten werden, dass die Kompetenzeinschätzung lediglich auf einer Selbsteinschätzung der Umfrageteilnehmenden basiert. Unterschiedliche Massstäbe in der Einschätzung der eigenen Kompetenz einzelner Umfrageteilnehmenden in Relation zu anderen Teilnehmenden können nicht ausgeschlossen werden.

### 3.5.2 Hypothese 2: Wichtigkeit von öffentlichen Dienstleistungen & Stimmabsicht

*Je wichtiger Anwendungsbereiche wie virtuelle Behördenschalter oder digitale demokratische Instrumente für Befragte sind, desto offener stehen diese einer staatlichen E-ID auf Blockchain-Basis gegenüber.*

Zur Auswertung von Hypothese 2 wird wiederum ein Index *Wichtigkeit* in Bezug auf die Wichtigkeit von öffentlichen Dienstleistungen wie virtuellen Behördenschaltern und digitalen demokratischen Instrumenten geschaffen. Dazu sollen die vier Unterfragen der Fragestellung Q7.2 (Q7.2\_1, Q7.2\_2, Q7.2\_3, Q7.2\_4) zu einem Index zusammengefasst werden. In diesen Fragestellungen geben

die Umfrageteilnehmenden die subjektiv empfundene Wichtigkeit von digitalen Behördendienstleistungen wie virtuellen Behördenschaltern, E-Voting, E-Collecting und E-Partizipation an. Um festzustellen, ob diese beiden Fragestellungen sich für die Indexbildung eignen, wird zuerst ein *KMO*- und *Bartlett*-Test durchgeführt, um die Eignung der Variablen für eine Faktorenanalyse zu prüfen. Sowohl der *Bartlett*-Test (Chi-Quadrat(6) = 3'081.608,  $p = .000$ ) als auch das *Kaiser-Meyer-Olkin Measure of Sampling Adequacy* ( $KMO = .781$ ) weisen darauf hin, dass sich die Variablen für eine Faktorenanalyse eignen.

Die Eigenwertanalyse (Eigenwert  $> 1$ ) weist auf eine Lösung mit einem Faktor hin. Die Auswertung der Komponentenmatrix zeigt, dass die Unterfragestellungen Q7.2\_1, Q7.2\_2, Q7.2\_3 und Q7.2\_4 alle mit Werten von  $> 0.8$  auf den Faktor 1 laden. Nachfolgend wird erneut eine Reliabilitätsprüfung mittels *Cronbach Alpha*-Koeffizient durchgeführt. Der *Cronbach Alpha*-Koeffizient ( $\alpha = .844$ ) erreicht für die vier Items Q7.2\_1, Q7.2\_2, Q7.2\_3 und Q7.2\_4 einen sehr guten Wert.

Ebenfalls verdeutlicht die Item-Skala der Reliabilitätsprüfung, dass der Wegfall keines der Items eine Verbesserung des *Cronbach Alpha*-Koeffizienten mit sich bringen würde. Die Items verfügen über eine gute Trennschärfe (Korrigierte Item-Skala-Korrelation  $> .3$ ). Es kann folglich davon ausgegangen werden, dass alle vier Items sich mit ausreichender Trennschärfe gleich verhalten, womit diese im Index *Wichtigkeit* als arithmetischer Mittelwert zusammengefasst werden können.

Zur Untersuchung des Zusammenhangs zwischen Wichtigkeit von digitalen Dienstleistungen im öffentlichen Sektor sowie der Demokratie und der Stimmabsicht bei einer hypothetischen Volksabstimmung wird eine Rangkorrelation nach *Spearman* durchgeführt. Die Auswertung ergibt, dass die von den Umfrageteilnehmenden empfundene Wichtigkeit dieser Angebote signifikant positiv mit der Stimmabsicht bei einer hypothetischen Volksabstimmung korreliert ( $r_s = .581$ ,  $p = < .001$ ,  $n = 1'629$ ). Dabei handelt es sich nach Cohen [1992] um einen starken Effekt.

Dass die Wichtigkeit von digitalen Dienstleistungen im öffentlichen Sektor und der Demokratie stark mit der Stimmabsicht korreliert, zeigt auch die Visualisierung des Zusammenhangs (vgl. Abb. 32 auf der nächsten Seite). Die rötlich gekennzeichnete Regressionskurve zeigt, dass sich Umfrageteilnehmende mit steigendem Wichtigkeitsempfinden immer stärker für eine staatliche und Blockchain-basierte E-ID aussprechen. Teilnehmende, welche eine solche Lösung mit ‚Nein‘ ablehnen würden, weisen umgekehrt das tiefste Wichtigkeitsempfinden für digitale Dienstleistungen im öffentlichen Sektor und der Demokratie aus. Die Auswertung zeigt einen stark positiven Zusammenhang zwischen Wichtigkeitsempfinden und Stimmabsicht der Umfrageteilnehmenden.

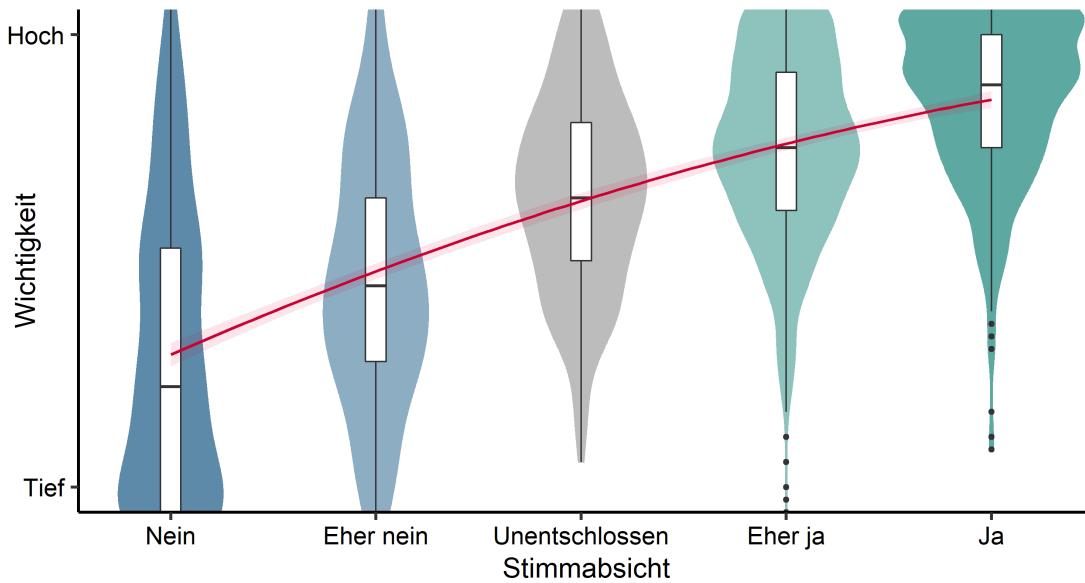


Abbildung 32: Visualisierung Hypothese 2 - Rangkorrelation nach Spearman von Wichtigkeit und Zustimmung.

Es stellt sich in der Folge die Frage, ob dieser Zusammenhang rein mit der individuell empfundenen Wichtigkeit und Nutzungspräferenz der Umfrageteilnehmenden einhergeht. Wie der theoretische Teil dieser Master-Thesis aufzeigt, ist für die Einführung von vollständig digitalen Behördendienstleistungen und Demokratie-Instrumenten eine E-ID unabdingbar. Individuell empfundene Wichtigkeit von vollständig digitalen Dienstleistungen und die tatsächliche Notwendigkeit einer E-ID zu deren Umsetzung sind dabei getrennt zu betrachten. Inwiefern dieses Bewusstsein und die gedankliche Trennung auch bei den Befragten vorhanden ist, soll deshalb mit einer weiteren statistischen Auswertung überprüft werden. Durch die Kombination der Fragestellungen Q7.3 und Q7.4 wird ein Index *Voraussetzungsbewusstsein* in Bezug auf das Bewusstsein der Voraussetzung einer E-ID für vollständig digitale Behördenschalter und Demokratie-Instrumente geschaffen. In diesen Fragestellungen geben die Umfrageteilnehmenden ihre Zustimmung oder Ablehnung gegenüber der Aussage an, dass eine E-ID die Voraussetzung für vollständig digitale Behördenschalter und Demokratie-Instrumente sei. Mit einem sehr guten *Cronbach Alpha*-Koeffizienten ( $\alpha = .858$ ) eignen sich die Items für die Indexbildung.

Zur Untersuchung des Zusammenhangs zwischen Voraussetzungsbewusstsein einer E-ID und der Stimmabsicht bei einer hypothetischen Volksabstimmung wird eine Rangkorrelation nach *Spearman* durchgeführt. Die Auswertung ergibt, dass das Voraussetzungsbewusstsein von Umfrageteilnehmenden signifikant mit der Stimmabsicht bei einer hypothetischen Volksabstimmung positiv korreliert ( $r_s = .521$ ,  $p = < .001$ ,  $n = 1'629$ ).

Dabei handelt es sich nach Cohen [1992] um einen starken Effekt. Die Visualisierung des Zusammenhangs in Abb. 33 macht den Zusammenhang grafisch deutlich und offenbart eine deutliche Ähnlichkeit zur Korrelation zwischen Wichtigkeit und Stimmabsicht.

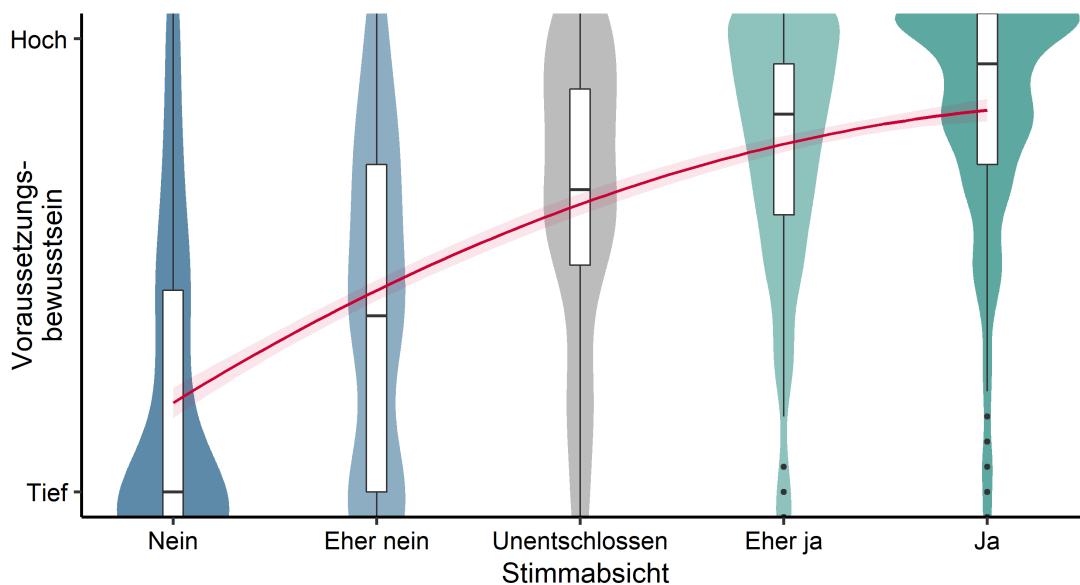


Abbildung 33: Visualisierung Hypothese 2 - Rangkorrelation nach Spearman von Voraussetzungsbewusstsein und Zustimmung.

Die Kombination der Auswertungen wird so interpretiert, dass sich Befragte mit ablehnender Stimmabsicht und tiefem Wichtigkeitsempfinden augenscheinlich deutlich weniger über die Voraussetzung einer E-ID für vollständig digitale Dienstleistungen im öffentlichen Sektor sowie der Demokratie bewusst sind. Umgekehrt scheint bei den Befürwortern einer staatlichen und Blockchain-basierten E-ID neben einem hohen subjektiven Wichtigkeitsempfinden dieses Bewusstsein stark vertreten zu sein. Diese Auswertung deutet - unabhängig von der subjektiven Wichtigkeit und damit Nutzungsabsicht solcher Dienstleistungen - auf eine starke Diskrepanz im Wissens- und Aufklärungsstand zwischen ablehnenden und befürwortenden Personen in Bezug auf die gegenseitige Abhängigkeit von E-ID und digitaler Demokratie hin.

Aufgrund der Ergebnisse der Rangkorrelation nach *Spearman* ( $r_s = .581$ ,  $p = .001$ ,  $n = 1'629$ ) in Verbindung mit den deskriptiven Analysen kann die Nullhypothese  $H_0$  verworfen und die Alternativhypothese  $H_1$  angenommen werden. Somit kann eine nach Cohen [1992] starke Korrelation zwischen der subjektiv empfundenen Wichtigkeit von digitalen Dienstleistungen im öffentlichen Sektor sowie der Demokratie und der Zustimmung gegenüber einer staatlichen, Blockchain-basierten E-ID festgestellt werden.

### 3.5.3 Hypothese 3: Kantonale Unterschiede bezüglich Stimmabsicht

*Es lassen sich Unterschiede bezüglich der Zustimmung gegenüber einer staatlichen, Blockchain-basierten E-ID bei Befragten der Kantone Zug und Schaffhausen im Vergleich zu den restlichen Befragten feststellen, da in diesen Kantonen bereits behördliche Angebote zur Nutzung von Blockchain-basierten Identitätsnachweisen den Bürger:innen zur Verfügung standen.*

In den Kantonen Zug und Schaffhausen stehen der Bevölkerung auf Stadt- bzw. Kantonsebene bereits seit einigen Jahren Angebote zur Nutzung von Blockchain-basierten Identitätssystemen zur Verfügung. Es kann somit davon ausgegangen werden, dass Teile der Bevölkerung in diesen Kantonen auf informeller Ebene mit einem Blockchain-basierten Identitätsnachweis in Kontakt gekommen sind oder diesen auch bereits selbst in der Praxis einsetzen. Aufgrund dieser Tatsache soll mittels Hypothese 3 untersucht werden, ob sich bei Umfrageteilnehmenden der beiden Kantone Zug und Schaffhausen Unterschiede in der Stimmabsicht im Vergleich zu den restlichen Umfrageteilnehmenden feststellen lassen. Wichtig ist an dieser Stelle zu erwähnen, dass lediglich 27 der insgesamt 1'730 Datensätze aus den Kantonen Zug und Schaffhausen stammen. Diese relativ geringe Zahl kann die Genauigkeit und Aussagekraft der statistischen Auswertungen beeinflussen.

Mithilfe des *Mann-Whitney-U*-Test wird getestet, ob die zentralen Tendenzen zweier unabhängiger Stichproben verschieden sind. Der Vergleich der beiden mittleren Ränge zeigt, dass die beiden Gruppen (Gruppe 1 = ZG und SH, Gruppe 2 = Restliche Kantone) mit mittleren Rangwerten von 1'023.14 resp. 797.91 eine unterschiedliche zentrale Tendenz aufweisen könnten. Aufgrund der hinreichend grossen Stichprobengrösse ( $N = 1'601$ ) wird die asymptotische Signifikanz berichtet. Der *Mann-Whitney-U*-Test ergibt, dass sich die beiden zentralen Tendenzen signifikant unterscheiden ( $U = 12'482.000$ ,  $z = -2.355$ ,  $p = .019$ ,  $n = 1'601$ ).

Um die Effektstärke des signifikanten Unterschieds zwischen den beiden Gruppen zu berechnen, wird ein *t*-Test durchgeführt. Die berechnete Effektgrösse (*Cohen's d* = .437) deutet erstmal auf einen mittleren Effekt nach Cohen [1992] hin. Allerdings wird bei genauerer Betrachtung der 95 %-Konfidenzintervalle klar, dass sich die Punktschätzung des *Cohen's d* auf einen sehr grossen Konfidenz-Wertbereich zwischen 0.018 und 0.855 bezieht. Der ausgeführte *t*-Test eignet sich somit in dieser Fragestellung nur begrenzt zur Berechnung einer Effektstärke. Die Effektstärke des *Mann-Whitney-U*-Tests kann alternativ manuell mittels folgender Formel berechnet werden:

$$r = \left| \frac{z}{\sqrt{n}} \right|$$

Als Resultat dieser Berechnung ergibt sich lediglich eine sehr schwache Effektstärke Cohen [1992] ( $r = .059$ ). Damit ist eine eindeutige Interpretation der Unterschiede in der Stimmabsicht zwischen Befragten aus Zug oder Schaffhausen und Befragten der restlichen Schweiz nur schwer möglich. Die visuelle Auswertung in Abb. 34 verdeutlicht, dass die Unterschiede der beiden Gruppen relativ gering ausfallen. Allerdings lassen sich visuell dennoch eindeutige Tendenzen feststellen. Während in der Dichtekurve der restlichen Kantone die ablehnenden Stimmen deutlich ersichtlich sind, stellen diese in der Dichtekurve der Kantone Zug und Schaffhausen lediglich Ausreisser dar.

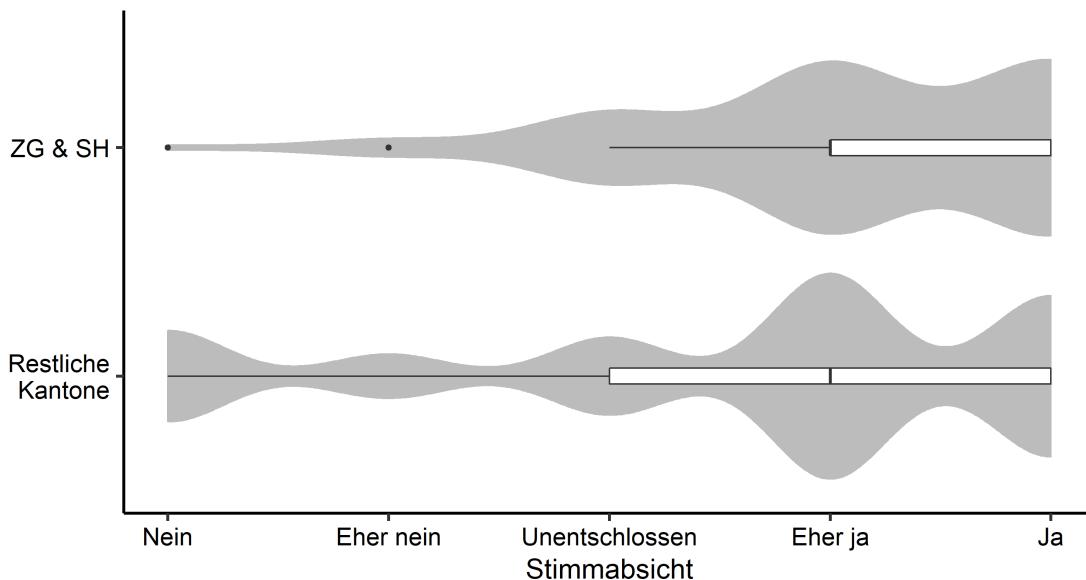


Abbildung 34: Visualisierung Hypothese 3 - Unterschiede in der Zustimmung zwischen ZG und SH im Vergleich zu den restlichen Kantonen.

Auf Basis der Ergebnisse des *Mann-Whitney-U*-Tests ( $U = 12'482.000$ ,  $z = -2.355$ ,  $p = .019$ ,  $n = 1'601$ ) in Verbindung mit den deskriptiven Analysen kann die Nullhypothese  $H_0$  verworfen und die Alternativhypothese  $H_1$  angenommen werden. Nach Cohen [1992] kann allerdings lediglich ein sehr schwacher Unterschied in der Stimmabsicht zwischen Teilnehmenden der Kantone Zug und Schaffhausen im Vergleich zu den restlichen Teilnehmenden festgestellt werden. Aufgrund der visuellen Auswertung in Kombination mit dem *t*-Test, der manuell berechneten Effektstärke sowie mit dem als signifikant berechneten Unterschied der beiden Gruppen kann jedoch von einer zumindest schwachen Tendenz ausgegangen werden. Ob allerdings tatsächlich die Existenz des Blockchain-ID-Angebots der beiden Kantone für den Unterschied ausschlaggebend ist, kann mit dieser Auswertung nicht abschliessend beurteilt werden.

#### 3.5.4 Multivariate Datenanalyse - Entscheidungsbaum

Als letzter Teil der inferenzstatistischen Datenauswertungen wird eine Datenanalyse vorgenommen, welche multiple Variablen gleichzeitig in einem Modell berücksichtigt. Diese zusätzliche Auswertung ist experimenteller Natur und soll versuchsweise ermöglichen, Personen innerhalb der Schweizerischen Eidgenossenschaft im Kontext der hypothetischen Vorlage zur staatlichen Blockchain-ID anhand ihrer Stimmabsicht in Gruppen - sogenannte *Cluster* - einteilen zu können. Damit sollen grobe Tendenzen in der Stimmabsicht von Personen mit unterschiedlichen Eigenschaftsmerkmalen sichtbar gemacht werden.

Um einen Entscheidungsbaum in *R* berechnen und visualisieren zu lassen, kommen die *R*-Pakete *rpart* und *rpart.plot* zum Einsatz [Carchedi 2022a; Carchedi 2022b]. Über den *complexity parameter* kann die Tiefe des Entscheidungsbaums festgelegt werden. Durch experimentelles Ausprobieren wird ein neunstufiger Entscheidungsbaum als die sinnvollste Baumtiefe eruiert, da diese Tiefe einen guten Kompromiss zwischen Detailgrad und Übersichtlichkeit liefert.

Dem Algorithmus zur Verfügung gestellt werden als Zielwert die Antworten zu Q11.2 (Stimmabsicht bei hypothetischer Vorlage) und als Entscheidungsmerkmale sämtliche persönlichen Eigenschaftsmerkmale der Teilnehmenden (Geschlecht, Sprachregion, Altersgruppe, Bildungsabschluss und Parteiverbundenheitsgefühl). Der Algorithmus entscheidet aufgrund der Datengrundlage autonom, welche relevantesten Gruppen oder Cluster sich innerhalb der Daten auf Basis der Eigenschaftsmerkmale in Abhängigkeit der Fragestellung Q11.2 finden lassen.

Interpretiert werden kann der Entscheidungsbaum wie folgt: Die Skala der Abstimmungsabsicht bei der hypothetischen Vorlage wurde in die numerischen Werte 1 bis 5 umkodiert. 1 steht dabei für die Stimmabsicht ‚Nein‘, 2 für ‚Eher nein‘, 3 für ‚Unentschlossen‘, 4 für ‚Eher ja‘ und 5 für ‚Ja‘. Je höher der Wert ist, desto höher ist die jeweilige Zustimmung zur hypothetischen Vorlage. Für jede Stufe des Entscheidungsbaums wurde der jeweils gewichtete Mittelwert der Zustimmung (Werte zwischen 1 und 5) sowie der gewichtete Stichprobenanteil in Prozent berechnet.

Die Visualisierung des errechneten Entscheidungsbaums ist in Abb. 35 auf der nächsten Seite einsehbar. Der Ursprung oder Startpunkt des Entscheidungsbaums liegt bei einem Wert von 3.5 über sämtliche Befragten hinweg. Dies entspricht den vorgängig erhobenen hypothetischen Zustimmungsanteilen von 63 % bestehend aus *Ja & Eher ja*, 13 % bestehend aus *Unentschlossen* und 24 % bestehend aus *Nein & Eher nein*.

#### ZUSTIMMUNGSWERTE ZUR FRAGESTELLUNG Q11.2

Skala mit Werten zwischen 1 und 5  
**1 = Nein** ← **3 = Unentschlossen** → **5 = Ja**

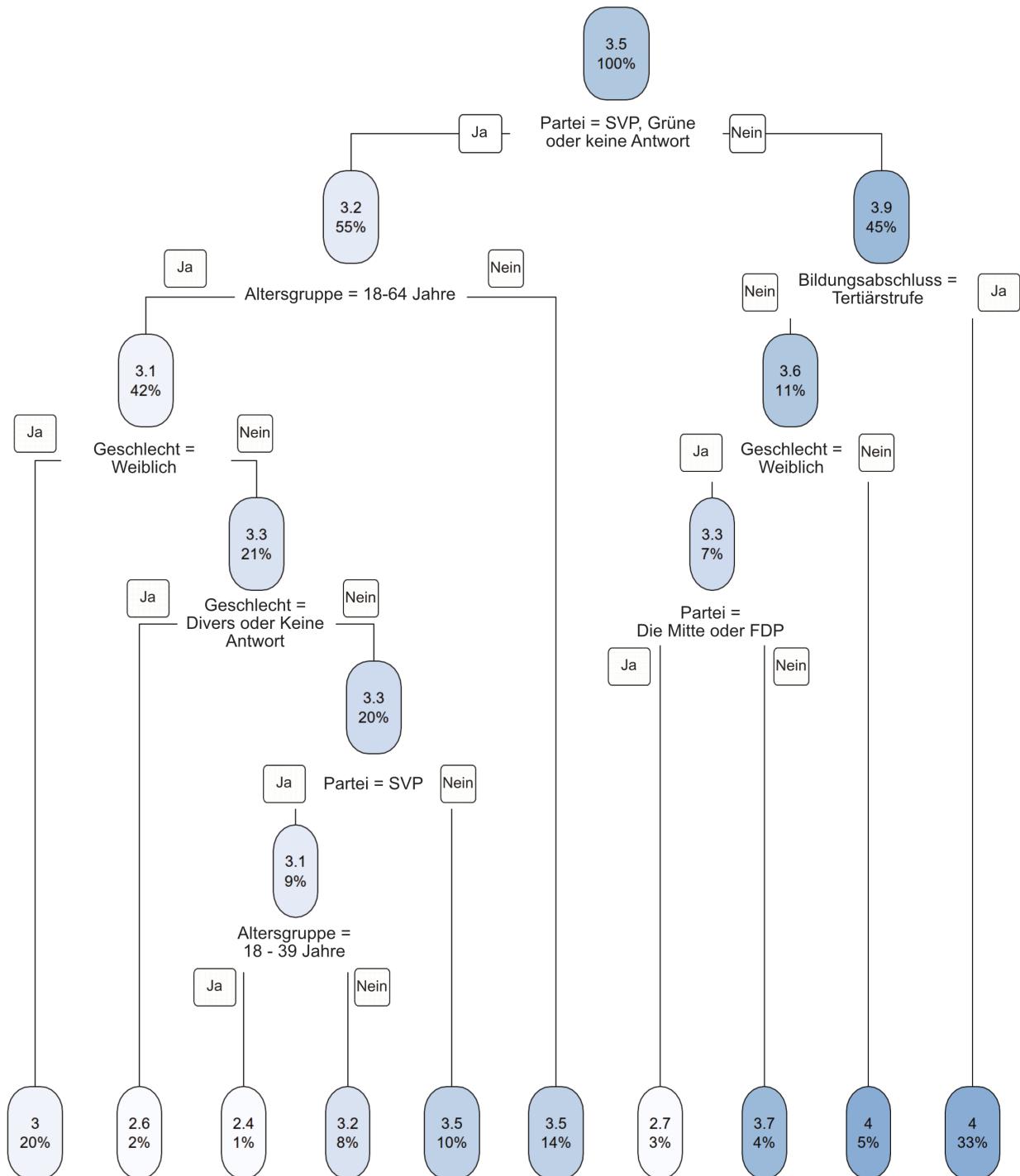


Abbildung 35: Multivariate Datenanalyse - Entscheidungsbaum.

Um den Informationsgehalt dieser Auswertung und Visualisierung greifbar zu machen, ohne den gesamten Entscheidungsbaum vollständig deskriptiv zu beschreiben, wird ein beispielhafter Interpretationsvorgang durchgeführt: Die Betrachtung des Entscheidungsbaums beginnt zuoberst beim Startpunkt mit den Werten 3.5 und 100 %. Gehören Personen nach ihrem Parteizugehörigkeitsgefühl den Parteien SVP, Grüne oder keiner Partei an, so bilden diese Personen ein gemeinsames Cluster und stimmen mit einem Anteil von 55 % der Stichprobe tendenziell mit einem Wert von 3.2 weniger stark für die vorgeschlagene E-ID-Lösung. Die restlichen 45 % der gewichteten Stichprobe bilden ein weiteres Cluster, welches mit einem Wert von 3.9 deutlich stärker zustimmt. Ausgehend von diesen beiden Clustern kann wiederum nach dem gleichen Prinzip eine weitere Stufe analysiert und interpretiert werden, womit sich die gebildeten Cluster Stufe für Stufe um eine Informationsebene erweitern.

An dieser Stelle wird auf die letzte Stufe des Entscheidungsbaums eingegangen. Der Algorithmus gliedert die stimmberechtigten Personen in insgesamt zehn Cluster von unterschiedlicher Grösse (Prozentangaben). Die wichtigste Gruppe von abstimmenden Personen stellen zum einen Personen dar, welche den Parteien Die Mitte, FDP, glp, SP oder Kleinparteien angehören und über einen Bildungsabschluss auf Tertiärstufe verfügen. Die Personen machen rund 33 % der Stichprobe aus und nehmen die hypothetische Vorlage mit einem Wert von 4 an. Die Gruppe mit dem zweithöchsten Gewicht (20 %) setzt sich aus weiblichen Personen im Alter zwischen 18 und 64 Jahren zusammen, welche sich den Parteien SVP, Grüne oder keiner Partei verbunden fühlen. Diese Gruppe steht der hypothetischen Vorlage mit einem Wert von 3 insgesamt unentschlossen gegenüber. Danach folgt eine Gruppe mit einem Gewicht von 14 % aus Personen mit einem Alter höher als 65 Jahre und einer Parteiverbundenheit zu SVP, Grüne oder keiner Partei. Diese Gruppe steht der vorgeschlagenen E-ID-Lösung mit einem Wert von 3.5 positiver gegenüber. Ebenfalls einen Wert von 3.5 erreicht die Gruppe von 18 bis 64 Jahre alten, männlichen, sich mit den Grünen oder keiner Partei assoziierenden Personen mit einem Gewicht von 10 %. Am stärksten abgelehnt wird die hypothetische Vorlage von der Gruppe aus männlichen, 18 bis 39 Jahre alten SVP-Parteverbundenen. Der Wert von 2.4 weist jedoch lediglich ein Gewicht von 1 % auf.

Die Ergebnisse eines Entscheidungsbaums können dabei helfen, eine Wahrscheinlichkeitsaussage über den antizipierten, ungefähren Zustimmungswert einer Person zu tätigen. Allerdings ist eine Übertragbarkeit und Generalisierbarkeit bezogen auf das Abstimmungsverhalten einer Einzelperson auf Basis des experimentellen Entscheidungsbaums dieser Forschungsarbeit stark eingeschränkt. Ein empirischer Gültigkeitsanspruch der Cluster bezogen auf die Gesamtpopulation wird an dieser Stelle explizit ausgeschlossen. Der Entscheidungsbaum erlaubt lediglich grobe und breit gefasste Interpretationen und Prognosen von Abstimmungstendenzen auf Basis von verschiedenen Eigenschaftsmerkmalen von Personen.

## 4 Konklusion

### 4.1 Diskussion der Resultate

Im ersten Teil der Konklusion werden die empirischen Resultate und Erkenntnisse diskutiert. Bevor die empirischen Erkenntnisse inhaltlich evaluiert werden, wird deren Relevanz und das Ausmass deren Gültigkeit behandelt. Dass die empirischen Ergebnisse keinen Anspruch auf Repräsentativität erheben, wurde bereits in Abschnitt 3.1 auf Seite 59 festgehalten.

Dank der hohen Rücklaufquote der Umfrage konnte eine breite Datenbasis bestehend aus Antwort-Datensätzen von 1'730 Teilnehmenden gewonnen werden. Wie die Analyse der Stichprobe zeigte, verfügt die Stichprobe trotz hoher Rücklaufquote über erhebliche Abweichungen bezüglich diversen soziodemografischen und politischen Merkmalen im Vergleich zur tatsächlichen Bevölkerung. Trotz Ausschluss der Repräsentativität aus forschungsökonomischen Gründen bot es sich aufgrund der Thematik und den Fragestellungen dieser Master-Thesis an, die empirische Forschung mit einer maximal möglichen Annäherung an die schweizerische Bevölkerungsstruktur durchzuführen. Um dies zu erreichen, wurden die erhobenen Daten der Zufallsstichprobe bestmöglich durch statistische Gewichtungsverfahren an die tatsächliche Bevölkerungsstruktur angeglichen.

Die auf Basis der Ergebnisse der Abstimmungsanalyse zur *E-ID 2020* von *gfs.bern* gewonnenen Erkenntnisse über die Relevanz einzelner soziodemografischer und politischer Merkmale erwiesen sich dabei als ausserordentlich zutreffend. Mithilfe der Gewichtung der Stichprobe über die drei relevantesten Merkmale liess sich eine den Abstimmungsergebnissen zur *E-ID 2020* auf 0.10 Prozentpunkte nahe kommende gewichtete Stichprobe erreichen. Diese Annäherung der Stichprobe an die tatsächliche Bevölkerungsstruktur erlaubt allerdings nach wie vor keinen Anspruch auf Repräsentativität der schweizerischen Bevölkerung. Dennoch lassen diese Ergebnisse die Vermutung zu, dass sich die gewichtete Stichprobe zumindest im Kontext der E-ID nahe an der tatsächlichen Bevölkerungsstruktur einordnet.

Aus diesem Grund scheint es zulässig, die empirischen Resultate im weiteren Verlauf als Erkenntnisse zu betrachten, welche der tatsächlichen Realität im Kontext einer E-ID zumindest nahe kommen dürften. Damit dürften sich ebenfalls relativ zuverlässige Aussagen über die Bevölkerung im Kontext von Fragestellungen rund um eine digitale ID tätigen lassen, wenngleich der Vorbehalt eines möglicherweise substanziellen Fehlerbereichs gegenüber repräsentativen Umfragen bestehen bleibt. Die erfolgreiche Gewichtung der Stichprobe wird folglich als Begründung angeführt, um im weiteren Verlauf der Diskussion die empirischen Resultate bezogen auf die schweizerische Bevölkerung anstelle der Umfrageteilnehmenden zu beziehen.

Einschränkend zu beachten ist, dass bei den Teilnehmenden der Umfrage von einem stark überdurchschnittlichen Interesse an politischen Themen als auch an spezifischen Fragestellungen rund um die Thematiken E-ID sowie Blockchain aus gegangen werden muss. Dies ist der Tatsache geschuldet, dass an der freiwilligen Umfrage mutmasslich eher Personen aktiv teilnahmen, welche sich überhaupt für diese Thematiken als auch die Politik im Allgemeinen interessieren. Die Haltung von an den Thematiken eher weniger stark interessierten Personen, welche aber dennoch an einer nächsten Volksabstimmung zur E-ID teilnehmen würden, kann trotz Gewichtung nicht exakt prognostiziert werden. Dennoch wird davon ausgegangen, dass sich durch die Gewichtung - unter stetigem Vorbehalt der erwähnten Einschränkungen - zumindest in der Tendenz zutreffende Aussagen über die Bevölkerung tätigen lassen.

Vor dem Hintergrund dieser Relevanz- und Evidenzeinschätzung der Resultate werden die empirischen Erkenntnisse inhaltlich evaluiert. Wie die empirischen Auswertungen zeigen, ist für die schweizerische Bevölkerung die exklusiv staatliche Datenhoheit, Kontrolle, Herausgabe sowie ein rein staatlicher Betrieb einer digitalen ID weitgehend unbestritten und wird von einem Grossteil der Bevölkerung vorausgesetzt. Diese Ergebnisse decken sich mit den Erkenntnissen aus den repräsentativen Studien rund um die Abstimmung zur *E-ID 2020*. Eine E-ID-Lösung innerhalb der Schweizerischen Eidgenossenschaft sollte vor diesem Hintergrund keine weiteren partizipierenden Akteure außer dem Staat selbst berücksichtigen. Einzig Konzepte, welche neben vollständig staatlichen Lösungen in puncto Datenkontrolle die Identitätsdaten in die Hände des Datensubjekts geben, könnten in einer Kombinationslösung aus Staat (Verantwortung und Betrieb) und Individuum (Datenhoheit) eine Volksmehrheit finden.

Als mögliche Begründung dieser Präferenz lässt sich eine enge Assoziation der E-ID mit dem Offizialcharakter eines staatlichen Ausweisdokuments anführen. Die getätigten Auswertungen rund um die Wahrnehmung und Einordnung einer digitalen ID zeigen, dass die schweizerische Bevölkerung eine E-ID tendenziell als eine dem Pass oder der Identitätskarte äquivalentes Ausweisdokument interpretiert. Schwach diskrepanz dazu steht die leicht sinkende Zustimmung, wenn vom Einsatz einer E-ID zum Zwecke einer Grenzüberschreitung gesprochen wird. Dies legt die Vermutung nahe, dass die Wahrnehmung der E-ID trotz genereller Äquivalenzauslegung zu einem Pass oder einer Identitätskarte je nach konkretem Anwendungsfall differenziert ausfallen kann. Dies wiederum spricht für eine noch nicht vollständig gefestigte Wahrnehmung und Einordnung der E-ID seitens der Bevölkerung im Allgemeinen.

Ein Fokuspunkt dieser Master-Thesis ist es, einen Bezug zur Digitalisierung des öffentlichen Sektors und der schweizerischen Demokratie zu schaffen. Während digitalen Dienstleistungen über virtuelle Behördenschalter eine hohe Wichtigkeit zukommt, scheinen demokratische Instrumente wie E-Voting, E-Collecting oder

E-Partizipation für die schweizerische Bevölkerung in der Tendenz noch eine untergeordnete Rolle zu spielen. Dieser Effekt kann bezogen auf die gesamte Bevölkerung als noch gewichtiger interpretiert werden, wenn man von der vorgängig antizipierten Verzerrung der Umfrageteilnehmenden in Richtung hohem Politik-, E-ID- und Digitalisierungsinteresse der öffentlichen Hand ausgeht. Insgesamt scheint das Bewusstsein zur Notwendigkeit einer E-ID für vollständig digitale Behördendienstleistungen seitens der Bevölkerung eher niedrig.

Da vollständig digitale Verwaltungen und digitale Instrumente wie E-Voting oder E-Collecting aus technologischer Sicht ohne eine digitale ID nicht umsetzbar sind, deuten die Ergebnisse auf ein Informations- und Aufklärungsdefizit seitens der schweizerischen Bevölkerung bezogen auf die behördlichen E-ID-Abhängigkeiten hin. Die überragende Bedeutung und Relevanz einer digitalen ID nach Autor:innen wie Melin et al. [2016, S. 73], Rauschenbach und Stucki [2020, S. 34] und Fivaz und Schwarz [2021, S. 86] als Grundbaustein zur vollständigen Digitalisierung von Prozessen zwischen Staat und Bürger:innen scheint der Bevölkerung gemäss den eigenen Auswertungen relativ schwach bewusst zu sein. Dass ein erhöhtes Voraussetzungsbewusstsein weiter positiv mit der Stimmabsicht von Personen korreliert, konnte im Rahmen dieser Forschungsarbeit ebenfalls bewiesen werden, womit sich ein weiteres Argument zur (staatlichen) Informationsförderung rund um die Thematik einer E-ID ergibt.

Aufklärungspotenzial scheint ebenfalls bezogen auf die Blockchain-Technologie zu bestehen. Weder der Begriff ‚Blockchain‘ noch die technische Funktionsweise scheinen der Bevölkerung in hohem Masse vertraut zu sein, was angesichts der relativen Neuheit und Komplexität der Materie wenig überraschend ist. Die Wahrnehmung des Begriffs ‚Blockchain‘ innerhalb der Bevölkerung ist im Mittel relativ neutral bis leicht positiv. Dies zeigt sich ebenfalls in einer relativen Offenheit zur grundsätzlichen persönlichen Nutzung von Blockchain-basierten Anwendungen unterschiedlichster Art. Vor dem Hintergrund der relativen Neuheit und Komplexität der Blockchain-Technologie sowie der im theoretischen Teil dieser Arbeit beschriebenen Digitalisierungskepsis seitens der schweizerischen Bevölkerung scheint die durchschnittlich eigens attribuierte Kompetenz der Befragten allerdings wiederum überraschend hoch. Die erlangten Ergebnisse würden in dieser Form einen durchschnittlich moderaten Wissensstand sämtlicher Bürger:innen über die Blockchain-Technologie beschreiben.

Bezogen auf die Gesamtbevölkerung scheint es aufgrund der Neuheit und Komplexität der Blockchain-Technologie kaum realistisch, dass in einer tendenziell digitalisierungsskeptischen Bevölkerung bereits jede Person durchschnittlich über objektiv moderates technologisches Blockchain-Wissen verfügen soll, während die Technologie selbst in der Fachwelt noch kaum grossflächig zum Einsatz kommt.

Eine mögliche Erklärung für diese Auffälligkeit könnte die bereits festgehaltene Verzerrungstendenz der erhobenen Stichprobe in Richtung überdurchschnittlicher Technikaffinität der Befragten im Vergleich zur schweizerischen Bevölkerung sein. Das vorgängig als Prämisse definierte und antizipierte überdurchschnittliche Interesse an Themen wie der Blockchain dürfte an dieser Stelle einen Einfluss auf die Übertragbarkeit der Ergebnisse auf die Gesamtbevölkerung haben.

Dass sich die erhobene Stichprobe - die antizipierten Verzerrungen leicht relativierend - ebenfalls nicht rein aus bereits hochgradig informierten Blockchain-Expert:innen zusammensetzt, beweisen die Auswertungen zur Einstellung gegenüber einer digitalen ID auf Basis von Blockchain-Technologie. Durch die Aufklärung der Befragten über die Potenziale eines Blockchain-basierten Identitätsnachweises mithilfe eines kurzen Informationstexts konnte auch bei der Stichprobe die Zustimmung gegenüber einer Blockchain-ID deutlich gesteigert werden. Dies lässt folgende Schlussfolgerungen zu: Entweder konnten sämtliche Befragten trotz antizipierter hoher Technikaffinität und hohem Grundinteresse von einem Informationsgewinn profitieren, oder die Gruppe der Blockchain-Unerfahreneren innerhalb der Stichprobe profitierte durch den kurzen Informationstext überdurchschnittlich stark.

In beiden Fällen scheint damit bewiesen, dass innerhalb der schweizerischen Bevölkerung bereits ein sehr kurzer Informationstext über die Blockchain-Potenziale in Bezug auf eine E-ID die Zustimmung von Personen gegenüber einer solchen Lösung stark steigern kann - ungeachtet der vorgängig bestehenden Wissensbasis. Ebenfalls wurde durch den Befragten vorgelegten Informationstext evident, dass die Bevölkerung das Konzept rund um die Self-Sovereign Identity als erstrebenswert erachtet, womit sich mutmasslich auch die Offenheit gegenüber Technologien verstärkt, welche die vollständig selbstverwaltete Identität ermöglichen.

Der Hauptfokus der empirischen Untersuchungen dieser Master-Thesis lag neben den bereits vollzogenen Analysen darin, die Zustimmung oder Ablehnung von Bürger:innen der Schweizerischen Eidgenossenschaft gegenüber einer staatlichen und Blockchain-basierten ID-Lösung zu evaluieren. Dabei zeigte sich, dass die schweizerische Bevölkerung einer derartigen E-ID-Lösung im Vergleich zur abgelehnten *E-ID 2020* verhältnismässig positiv gegenübersteht. Sowohl geschlechter-, sprach- als auch beinahe parteiübergreifend scheint eine vergleichsweise hohe Offenheit und Zustimmung gegenüber einer staatlichen und Blockchain-basierten E-ID im Rahmen einer Volksabstimmung möglich.

Der wichtigste Grund für diese Zustimmung gegenüber der Blockchain-ID stellt für die schweizerische Bevölkerung die Ermöglichung der vollständig selbstbestimmten Verwaltung der eigenen Identität dar. Ebenfalls wichtig sind die Verbesserungen von digitalen Behördendienstleistungen sowie die rein staatliche Verantwortlichkeit über

die Herausgabe und den Betrieb der E-ID. Auf der Gegenseite stehen hauptsächlich Datenschutz- und Sicherheitsbedenken gegenüber einer E-ID im Allgemeinen als auch gegenüber dem Einsatz von Blockchain-Technologie im Zentrum.

Hervorzuheben ist insbesondere das Ergebnis, dass ablehnende Personen zu 52 % absolut keine Zustimmungsgründe sehen, während unter den befürwortenden Personen lediglich 11 % absolut keine Gründe gegen die vorgeschlagene Lösung sehen. Dies deutet darauf hin, dass die Gegner:innen der hypothetischen Vorlage in ihrer ablehnenden Haltung tendenziell gefestigter sind, als die Befürworter:innen in ihrer positiven Haltung. Ebenfalls spannend zu sehen ist, dass Wirtschaftsaspekte wie schon bei der *E-ID-2020*-Abstimmung für die Bürger:innen eine stark untergeordnete Rolle spielen. Die grossen, im Theorienteil dieser Forschungsarbeit dargelegten ökonomischen Potenziale, scheinen primär keine grosse Relevanz für die Bevölkerung zu besitzen. Hier besteht augenscheinlich ein weiteres Mal eine erhebliche Informationslücke seitens der breiten Bevölkerung, woraus sich folglich ein starkes Aufklärungspotenzial seitens Behörden und insbesondere auch des privatwirtschaftlichen Sektors als Profiteure einer E-ID ergibt.

Die hypothetische Volksabstimmung über eine staatliche, Blockchain-basierte E-ID erreicht gemäss der empirischen Erhebung eine potenzielle Zustimmung von 63 % an der Urne. Der erhobene Anteil an ablehnenden Stimmen beläuft sich auf 24 %. Basierend auf diesen Ergebnissen würde eine staatliche und Blockchain-basierte E-ID folglich durch das Erreichen von mindestens 50 % „Ja“-Anteil realistische Chancen für eine Mehrheit an der Urne vorweisen können. Selbst wenn man davon ausgeht, dass sich der Anteil an Unentschlossenen (13 %) noch vollständig gegen eine derartige E-ID-Lösung entscheidet, läge das Verhältnis von „Ja“-Stimmen und „Nein“-Stimmen bei 63 % zu 37 %. Dies entspräche einer deutlichen Annahme der hypothetischen Vorlage durch die schweizerische Bevölkerung.

Aufgrund der beschriebenen Zurückhaltung bezüglich Digitalisierung und technischen Innovationen der schweizerischen Bevölkerung ist dies ein Resultat, welches nicht unbedingt erwartet werden konnte. Wie bereits mehrfach erwähnt, kann die verhältnismässig stark positive Einstellung der Bevölkerung gegenüber einer staatlichen Blockchain-ID teilweise durch Faktoren wie überdurchschnittliches Themeninteresse oder überdurchschnittliche Technikkompetenz der Stichprobe zu stande kommen. Wie verschiedenste Analysen gezeigt haben, unterliegen die Ergebnisse dieser Forschungsarbeit trotz einer beinahe perfekten Annäherung der Stichprobe an das Abstimmungsverhalten bei der *E-ID-2020*-Abstimmung mutmasslich diesen verzerrnden Einflüssen. Deshalb stellt sich an dieser Stelle die Frage nach dem Ausmass und der Einflussstärke dieser antizipierten und nicht kompensierten Verzerrungstendenzen. Eine quantitative Analyse der trotz Gewichtung verbleibenden Verzerrungstendenzen ist im Rahmen dieser Master-Thesis nicht möglich.

Die Einschätzung der Auswirkung dieser Effekte lässt sich lediglich abschätzen und in einen hypothetischen Kontext einordnen. Trotz der verbleibenden antizipierten Verzerrungen der Stichprobe wird davon ausgegangen, dass sich die Ergebnisse dieser Forschungsarbeit in der Tendenz auf die schweizerische Gesamtbevölkerung übertragen lassen. Dies wird zum einen mit der beinahe perfekten Annäherung der Stichprobe an das Abstimmungsverhalten bei der *E-ID-2020*-Abstimmung und zum anderen mit dem grossen Spielraum innerhalb der erlangten Ergebnisse zur hypothetischen Abstimmungsabsicht begründet. Die Verteilung der prozentualen Anteile an potenziellen ‚Ja‘- und ‚Nein‘-Stimmen gestaltet sich derart positiv, dass auch bei einem Wechsel der Stimmabsicht von grösseren Teilen der Stichprobe noch immer mehr als 50 % der potenziell Abstimmenden für die vorgeschlagene E-ID-Lösung stimmen würden. Damit die vorgeschlagene E-ID-Lösung bei einer Volksabstimmung abgelehnt würde, müssten sämtliche der 13 % der unentschlossenen Personen sowie zusätzlich nochmals 13 % der befürwortenden Personen ihre Stimmabsicht wechseln.

Auch wenn ein Wechsel der Stimmabsicht von 26 % der Abstimmenden im Verlauf eines Abstimmungskampfs durchaus möglich ist, liefern die Ergebnisse dieser Forschungsarbeit einen unter empirischen Aspekten ausreichenden Anhaltspunkt, um von zumindest realistischen Chancen zur Annahme einer staatlichen und Blockchain-basierten E-ID durch die schweizerische Bevölkerung sprechen zu können. Über genauere mögliche Verteilungen der prozentualen Stimmverhältnisse kann jedoch aufgrund der fehlenden Repräsentativität der Gesamtbevölkerung keine Prognose getätigter werden. Geht man davon aus, dass die tatsächliche Bevölkerung sich auf Basis des derzeitig durchschnittlichen Informationsstands tendenziell kritischer als die erlangte, mutmasslich eher techniknahe Stichprobe verhalten würde, so zeigen die positiven Effekte einer informellen Aufklärung über die Chancen und Potenziale der Blockchain-Technologie im Rahmen einer E-ID, dass sich auch ablehnende Haltungen innerhalb der Bevölkerung zumindest teilweise aufweichen oder zustimmende Haltungen der Bevölkerung stärken lassen.

Somit erscheint es insgesamt betrachtet zulässig, davon auszugehen, dass sich verbleibende Abweichungen zwischen den empirischen Ergebnissen dieser Arbeit und der tatsächlichen Bevölkerung sowohl auf Zustimmungs- als auch auf Ablehnungsseite teilweise kompensieren lassen. Damit kann - eine die Bevölkerung erreichende Kommunikationsstrategie vorausgesetzt - trotz antizipierter Verringerung der totalen Zustimmung im Vergleich zu den erlangten 63 % Zustimmung insgesamt von einer zumindest realistischen Möglichkeit zur Erreichung einer 50 %-Mehrheit im Rahmen einer Volksabstimmung für eine staatliche und Blockchain-basierte E-ID ausgegangen werden.

### 4.1.1 Bezug zu den Forschungsfragen

- *Welche Chancen und Herausforderungen ergeben sich im Hinblick auf die Verwendung der Blockchain-Technologie im Bereich der digitalen Demokratie und insbesondere im Bereich eines digitalen Identitätsnachweises?*

Im theoretischen Teil dieser Master-Thesis wurden verschiedenste Chancen und Herausforderungen erarbeitet. Zu den Chancen der Blockchain-Technologie innerhalb der digitalen Demokratie und insbesondere für den Anwendungszweck einer digitalen ID zählen unter anderem die Potenziale zur unter heutigen technologischen Voraussetzungen ausserordentlich sicheren und resilienten Schaffung von Vertrauen, Transparenz, autonomer Datenkontrolle sowie einzigartiger Datenpersistenz im Verbund mit erheblichen ökonomischen Effizienzsteigerungs- und Kosteneinsparungspotenzialen. Allerdings gehen mit dem Einsatz von Blockchain-Technologie zum Zwecke eines Identitätsnachweises ebenfalls Herausforderungen einher, welche die Chancen des Technologieeinsatzes teilweise relativieren. Viele der Vorteile der Blockchain im Kontext einer digitalen ID sind in der Folge nicht absoluter, sondern relativer Natur und müssen sorgfältig gegen der Technologie inhärente Risiken und Nutzungshürden abgewogen werden.

- *Wie ist die Einstellung der schweizerischen Bevölkerung gegenüber der Blockchain-Technologie und insbesondere gegenüber dem Einsatz von Blockchain-Technologie zum Zwecke eines digitalen Identitätsnachweises?*

Die Wahrnehmung des Begriffs ‚Blockchain‘ innerhalb der Bevölkerung offenbarte sich im Mittel als relativ neutral bis leicht positiv, was in Anbetracht der Neuartigkeit und dem in der Öffentlichkeit nicht immer unumstrittenen Image der Technologie nicht unbedingt zu erwarten war. Dies zeigt sich ebenfalls in einer relativen Offenheit zur persönlichen Nutzung von Blockchain-basierten Anwendungen unterschiedlichster Art. Limitierend festzuhalten ist allerdings, dass die erlangte Stichprobe durch eine hohe Technikaffinität geprägt sein kann, womit die tatsächliche Einstellung und Offenheit gegenüber der Blockchain-Technologie an sich sowie deren Anwendung innerhalb einer E-ID tiefer liegen kann. Trotz dem festgestellten grossen Vertrauen in den Staat als die eine E-ID ausstellende und betreibende Instanz seitens der Bevölkerung stellt dieses keinen Blankoscheck bezüglich der eingesetzten Technologie dar. Dem Einsatz der Blockchain-Technologie zum Zwecke einer E-ID steht die Bevölkerung dennoch grundsätzlich offen gegenüber, wobei vor allem die Umsetzbarkeit des Konzepts der Self-Sovereign Identity ein starkes Pro-Argument für die Bevölkerung darstellt.

- *Ist eine auf der Blockchain-Technologie basierende E-ID-Lösung in der Schweizerischen Eidgenossenschaft mehrheitsfähiger als die in der Volksabstimmung zur E-ID 2020 vorgeschlagene und von der Bevölkerung abgelehnte Lösung?*

Die empirische Erhebung dieser Master-Thesis zeigt, dass die schweizerische Bevölkerung einer staatlichen und Blockchain-basierten E-ID-Lösung im Vergleich zur abgelehnten *E-ID 2020* positiver gegenübersteht. Sowohl geschlechter-, sprach- als auch weitgehend parteiübergreifend zeigt sich eine vergleichsweise hohe Offenheit und Zustimmung gegenüber einer staatlichen und Blockchain-basierten ID. Da sich verbleibende Abweichungen zwischen den empirischen Ergebnissen dieser Arbeit und der tatsächlichen Bevölkerung sowohl auf Zustimmungs- als auf Ablehnungsseite teilweise kompensieren lassen, kann von einer realistischen Möglichkeit zur Erreichung einer 50 %-Mehrheit im Rahmen einer Volksabstimmung für eine staatliche und Blockchain-basierte E-ID ausgegangen werden. Dies setzt jedoch voraus, dass der Staat die Potenziale einer E-ID-Lösung auf Basis von Blockchain-Technologie durch eine transparente und offensive Informationspolitik der Bevölkerung im Abstimmungsvorfeld näher bringen kann.

### 4.1.2 Handlungsempfehlungen

Trotz fehlender repräsentativer Grundlage ergibt sich aus dieser Forschungsarbeit eine solide Basis für eine Handlungsempfehlung an die in die Ausarbeitung der neuen E-ID-Lösung involvierten behördlichen Instanzen. Die vom Bundesamt für Justiz [2021] für Mitte 2022 geplante Vernehmlassung zum neuen E-ID-Gesetz, gefolgt von einer Botschaft und der parlamentarischen Beratung zum neuen E-ID-Gesetz im Verlauf des Jahres 2023 bietet theoretisch die Möglichkeit, die Erkenntnisse dieser Master-Thesis in den Entscheidungsfindungs- und Evaluationsprozess einfließen zu lassen. Gestützt auf die Ergebnisse dieser Master-Thesis könnte bei der Planung der E-ID das Konzept einer staatlichen und Blockchain-basierten E-ID wohl als eine mehrheitsfähige Option unter verschiedenen anderen Umsetzungsmöglichkeiten zumindest in Erwägung gezogen werden. Insbesondere die Erkenntnis, dass die Bevölkerung das Konzept der selbstbestimmten Verwaltung der eigenen Identitätsdaten als wichtigstes Argument für die Zustimmung zu einer E-ID erachtet, dürfte für die behördliche Ausarbeitung von technologischen Lösungsvarianten interessant sein. Denkbar für eine mehrheitsfähige E-ID-Lösung innerhalb der Schweizerischen Eidgenossenschaft könnte beispielsweise eine Orientierung an bestehenden schweizerischen Blockchain-Lösungen zum digitalen Identitätsnachweis sein.

## 4.2 Ausblick & künftige Forschung

Die generelle Einführung einer digitalen ID birgt sowohl für die Demokratie und den öffentlichen Sektor als auch für den privaten Wirtschaftssektor grosses Potenzial. Grundsätzlich scheint die Einführung einer digitalen ID im Kontext einer fortwährenden Digitalisierung und Technologisierung des alltäglichen Lebens unumgänglich, um neben einer Vielzahl von Potenzialen auch die durch das McKinsey Global Institute [2019, S. 51] für möglich befundene Steigerung des Bruttoinlandsprodukts von rund 6 % bis 2030 zu realisieren. Die genaue Art und Weise der Umsetzung einer digitalen ID ist jedoch Teil von aufwändigen und komplexen Evaluations- und Entscheidungsfindungsprozessen. Dabei müssen unterschiedliche Bedürfnisse, Interessen und Vorbehalte von diversen Parteien im Verbund mit verschiedenen technologischen Ansätzen zur Umsetzung einer digitalen ID vereint werden.

Die innerhalb dieser Master-Thesis vollzogene empirische Untersuchung bietet einen Anhaltspunkt über verschiedene Wahrnehmungs- und Einstellungsaspekte der schweizerischen Bevölkerung bezogen auf die Einführung einer digitalen ID. Ebenfalls erlauben die Ergebnisse dieser Forschungsarbeit eine erste Einschätzung der Einstellung der schweizerischen Bevölkerung gegenüber der Blockchain-Technologie und deren Einsatz im Kontext einer digitalen ID. Damit schafft die getätigte Forschung eine Basis für potenziell weiterführende Forschungsvorhaben innerhalb der aktuell laufenden Evaluations- und Entscheidungsfindungsprozesse im Rahmen des behördlichen Rechtsetzungsprojekts für eine staatliche E-ID. Anbieten würde sich beispielsweise eine weiterführende, repräsentative Studie über die Mehrheitsfähigkeit einer staatlichen und Blockchain-basierten E-ID, um die innerhalb dieser Forschungsarbeit verbleibenden Unschärfen besser quantifizieren und folglich die tatsächliche Mehrheitsfähigkeit und Popularität einer derartigen E-ID-Lösung innerhalb der Schweizerischen Eidgenossenschaft abschliessend beurteilen zu können.

---

# Literaturverzeichnis

- [Ahram et al. 2017] AHRAM, Tareq ; SARGOLZAEI, Arman ; SARGOLZAEI, Saman ; DANIELS, Jeff ; AMABA, Ben: Blockchain technology innovations. In: *2017 IEEE Technology & Engineering Management Conference (TEMSCON)*, IEEE, 2017, S. 137–141. – ISBN 978-1-5090-1114-8
- [Allen 2016] ALLEN, Christopher: The Path to Self-Sovereign Identity. In: *CoinDesk* (2016). – URL <https://www.coindesk.com/markets/2016/04/27/the-path-to-self-sovereign-identity/>. – Zugriffsdatum: 31.05.2022
- [Ammous 2016] AMMOUS, Saifedean H.: Blockchain Technology: What is it Good for? In: *SSRN Electronic Journal* (2016). – DOI: 10.2139/ssrn.2832751
- [Bakre et al. 2017] BAKRE, Akshay ; NIKITA PATIL ; SAKSHUM GUPTA: Implementing Decentralized Digital Identity using Blockchain. In: *International Journal of Engineering Technology Science and Research* (2017), Nr. Volume 4, Issue 10, S. 379–385. – URL [https://www.researchgate.net/profile/Nikita-Patil-5/publication/320487423\\_Implementing-Decentralized\\_Digital\\_Identity\\_using\\_Blockchain/links/59e844230f7e9bc89b50bb96/Implementing-Decentralized-Digital-Identity-using-Blockchain.pdf](https://www.researchgate.net/profile/Nikita-Patil-5/publication/320487423_Implementing-Decentralized_Digital_Identity_using_Blockchain/links/59e844230f7e9bc89b50bb96/Implementing-Decentralized-Digital-Identity-using-Blockchain.pdf). – Zugriffsdatum: 31.05.2022
- [Berentsen und Schär 2017] BERENTSEN, Aleksander ; SCHÄR, Fabian: *Bitcoin, Blockchain und Kryptoassets: Dissertation*. Erste Auflage. 2017. – ISBN 978-3-73865-392-2
- [Bisaz und Serdült 2017] BISAZ, Corsin ; SERDÜLT, Uwe: E-Collecting als Herausforderung für die direkte Demokratie der Schweiz. In: *LeGes: Gesetzgebung Evaluation:531-545* (2017). – DOI: 10.5167/uzh-150203
- [Biswas und Muthukumarasamy 2016] BISWAS, Kamanashis ; MUTHUKUMARASAMY, Vallipuram: Securing Smart Cities Using Blockchain Technology. In: *2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, IEEE, 2016, S. 1392–1393. – ISBN 978-1-5090-4297-5
- [Braendgaard 2017] BRAENDGAARD, Pelle: What is a uPort identity? In: *Medium* 2017 (2017). – URL <https://medium.com/uport/what-is-a-uport-identity-b790b065809c>. – Zugriffsdatum: 31.05.2022
- [Bühler et al. 2022] BÜHLER, Gordon ; HERMANN, Michael ; KRÄHENBÜHL, David: Digitaler Staat in der Schweiz: Einschätzungen und Bedürfnisse der Bevölkerung. (2022). – URL [https://www.swico.ch/media/filer\\_public/99/19/9919fe71-b4c7-4024-bc6a-e1aa9743c06f/sotomo\\_swico\\_digitaler\\_staat.pdf?vgo\\_ee=FQkJhwU4Mu1Ew7y14DU8sE5I2jKxc%2Bu7z1tNMUbXOLI%3D](https://www.swico.ch/media/filer_public/99/19/9919fe71-b4c7-4024-bc6a-e1aa9743c06f/sotomo_swico_digitaler_staat.pdf?vgo_ee=FQkJhwU4Mu1Ew7y14DU8sE5I2jKxc%2Bu7z1tNMUbXOLI%3D). – Zugriffsdatum: 31.05.2022
- [Bundesamt für Justiz 2021] BUNDESAMT FÜR JUSTIZ: *Staatliche E-ID*. 2021. – URL <https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/staatliche-e-id.html>. – Zugriffsdatum: 31.05.2022
- [Bundesamt für Statistik 2019] BUNDESAMT FÜR STATISTIK: *Nationalratswahlen: Stärke der Parteien*. 2019. – URL <https://www.bfs.admin.ch/asset/de/je-d-17.02.02.03.01>. – Zugriffsdatum: 31.05.2022

- 
- [Bundesamt für Statistik 2020] BUNDESAMT FÜR STATISTIK: *Hauptsprachen seit 1910 - 1910-2020*. 2020. – URL <https://www.bfs.admin.ch/bfs/de/home/statistiken/bevoelkerung/sprachen-religionen/sprachen.assetdetail.20964034.html>. – Zugriffsdatum: 31.05.2022
- [Bundesamt für Statistik 2021a] BUNDESAMT FÜR STATISTIK: *Höchste abgeschlossene Ausbildung, nach Migrationsstatus, verschiedenen soziodemografischen Merkmalen und Grossregion*. 2021. – URL <https://www.bfs.admin.ch/asset/de/su-d-01.05.07.03.01.01>. – Zugriffsdatum: 31.05.2022
- [Bundesamt für Statistik 2021b] BUNDESAMT FÜR STATISTIK: *Ständige Wohnbevölkerung ab 15 Jahren nach Migrationsstatus und verschiedenen soziodemografischen Merkmalen*. 2021. – URL <https://www.bfs.admin.ch/asset/de/su-d-01.05.03.01.01>. – Zugriffsdatum: 31.05.2022
- [Bundesamt für Statistik 2021c] BUNDESAMT FÜR STATISTIK: *Ständige Wohnbevölkerung nach Alter, Geschlecht und Staatsangehörigkeitskategorie, 2010-2020*. 2021. – URL <https://www.bfs.admin.ch/asset/de/je-d-01.02.03.02>. – Zugriffsdatum: 31.05.2022
- [Bundesamt für Statistik 2022] BUNDESAMT FÜR STATISTIK: *Bundesamt für Statistik*. 2022. – URL <https://www.bfs.admin.ch/bfs/de/home.html>. – Zugriffsdatum: 31.05.2022
- [Camp 2004] CAMP, L. J.: Digital identity. In: *IEEE Technology and Society Magazine* 23 (2004), Nr. 3, S. 34–41. – DOI: 10.1109/MTAS.2004.1337889. – ISSN 0278-0097
- [Cap und Maibaum 2001] CAP, Clemens H. ; MAIBAUM, Nico: Digital Identity and its Implication for Electronic Government. In: SCHMID, Beat (Hrsg.) ; STANOEVSKA-SLABEVA, Katarina (Hrsg.) ; TSCHAMMER, Volker (Hrsg.): *Towards the e-society* Bd. 74. Boston, Mass. : Kluwer Acad. Publ, 2001, S. 803–816. – ISBN 0-7923-7529-7
- [Carchedi 2022a] CARCHEDI, Nick: *rpart: Recursive Partitioning and Regression Trees*. 2022. – URL <https://www.rdocumentation.org/packages/rpart/versions/4.1.16/topics/rpart>. – Zugriffsdatum: 31.05.2022
- [Carchedi 2022b] CARCHEDI, Nick: *rpart.plot: Plot an rpart model. A simplified interface to the prp function*. 2022. – URL <https://www.rdocumentation.org/packages/rpart.plot/versions/3.1.0/topics/rpart.plot>. – Zugriffsdatum: 31.05.2022
- [chch - Das Bürgerportal 2022] CHCH - DAS BÜRGERPORTAL: *ch.ch, das Portal der Schweizer Behörden*. 2022. – URL <https://www.ch.ch/de/>. – Zugriffsdatum: 31.05.2022
- [Cohen 1992] COHEN, J.: A power primer. In: *Psychological bulletin* 112 (1992), Nr. 1, S. 155–159. – DOI: 10.1037//0033-2909.112.1.155. – ISSN 0033-2909
- [Collier 2018] COLLIER, Andrew B. ; DATAWOKIE.DEV (Hrsg.): *Survey Raking: An Illustration*. 2018. – URL <https://datawookie.dev/blog/2018/12/survey-raking-an-illustration/>. – Zugriffsdatum: 31.05.2022
- [Crosby et al. 2016] CROSBY, M. ; PATTANAYAK, P. ; VERMA, S. ; KALYANARAMAN, V.: Blockchain technology: Beyond bitcoin. In: *AIR Applied Innovation Review* (2016), Nr. Issue No. 2. – URL <https://j2-capital.com/wp-content/uploads/2017/11/AIR-2016-Blockchain.pdf>. – Zugriffsdatum: 31.05.2022

- 
- [Cuen 2017] CUEN, Leigh ; INTERNATIONAL BUSINESS TIMES (Hrsg.): *Dubai Airport To Use Blockchain To Create The First 'Gate-Less Border'*. 2017. – URL <https://www.ibtimes.com/dubai-airport-use-blockchain-create-first-gate-less-border-2551566>. – Zugriffssdatum: 31.05.2022
- [Das Schweizer Parlament 2020] DAS SCHWEIZER PARLAMENT ; KEYSTONE-SDA-ATS AG (Hrsg.): *Parlament setzt bessere Rahmenbedingungen für Blockchain*. 2020. – URL [https://www.parlament.ch/de/services/news/Seiten/2020/20200910092808664194158159041\\_bs039.aspx](https://www.parlament.ch/de/services/news/Seiten/2020/20200910092808664194158159041_bs039.aspx). – Zugriffssdatum: 31.05.2022
- [Daza 2012] DAZA, Sebastian: *Raking weights with R*. 2012. – URL <https://sdaza.com/blog/2012/raking/>. – Zugriffssdatum: 31.05.2022
- [Deloitte 2022] DELOITTE: *The Future of Digital Identity: What does it mean to you?* 2022. – URL <https://www2.deloitte.com/global/en/pages/risk/articles/the-future-of-digital-identity.html>. – Zugriffssdatum: 31.05.2022
- [Demokratiezentrums Wien 2022] DEMOKRATIEZENTRUM WIEN: *Demokratiemodelle - E-Democracy*. 2022. – URL <https://www.demokratiezentrum.org/bildung/ressourcen/themenmodule/demokratiemodelle/e-democracy-liquid-democracy/>. – Zugriffssdatum: 31.05.2022
- [Digitale Verwaltung für Bevölkerung, Wirtschaft und Behörden 2022a] DIGITALE VERWALTUNG FÜR BEVÖLKERUNG, WIRTSCHAFT UND BEHÖRDEN: *Blockchain*. 2022. – URL <https://www.egovernment.ch/de/dokumentation/trends-in-der-digitalisierung/blockchain/>. – Zugriffssdatum: 31.05.2022
- [Digitale Verwaltung für Bevölkerung, Wirtschaft und Behörden 2022b] DIGITALE VERWALTUNG FÜR BEVÖLKERUNG, WIRTSCHAFT UND BEHÖRDEN: *E-Government Schweiz*. 2022. – URL <https://www.egovernment.ch/de>. – Zugriffssdatum: 31.05.2022
- [Digitale Verwaltung für Bevölkerung, Wirtschaft und Behörden 2022c] DIGITALE VERWALTUNG FÜR BEVÖLKERUNG, WIRTSCHAFT UND BEHÖRDEN: *E-ID umsetzen*. 2022. – URL <https://www.egovernment.ch/de/umsetzung/umsetzungsziele/elektronische-identitat/>. – Zugriffssdatum: 31.05.2022
- [Digitale Verwaltung für Bevölkerung, Wirtschaft und Behörden 2022d] DIGITALE VERWALTUNG FÜR BEVÖLKERUNG, WIRTSCHAFT UND BEHÖRDEN: *Umsetzungsziele*. 2022. – URL <https://www.egovernment.ch/de/umsetzung/umsetzungsziele/>. – Zugriffssdatum: 31.05.2022
- [Duden 2022] DUDEK ; DUDEKREDAKTION (Hrsg.): *Identität*. 2022. – URL <https://www.duden.de/rechtschreibung/Identitaet>. – Zugriffssdatum: 31.05.2022
- [Dunphy und Petitcolas 2018] DUNPHY, Paul ; PETITCOLAS, Fabien A.: A First Look at Identity Management Schemes on the Blockchain. In: *IEEE Security & Privacy Magazine* 16 (2018), Nr. 4, S. 20–29. – DOI: 10.1109/msp.2018.3111247. – ISSN 1540-7993
- [Efanov und Roschin 2018] EFANOV, Dmitry ; ROSCHIN, Pavel: The All-Pervasiveness of the Blockchain Technology. In: *Procedia Computer Science* 123 (2018), S. 116–121. – DOI: 10.1016/j.procs.2018.01.019. – ISSN 18770509

- 
- [Eichenberger 31.12.2014] EICHENBERGER, Isabelle: Der "Röstigraben", die verbindende Kluft der Helvetier. In: *swissinfo.ch* (31.12.2014). – URL [https://www.swissinfo.ch/ger/gesellschaft/deutsch-vs--franzoesisch\\_der--roestigraben---die-verbindende-kluft-der-helvetier/41177160](https://www.swissinfo.ch/ger/gesellschaft/deutsch-vs--franzoesisch_der--roestigraben---die-verbindende-kluft-der-helvetier/41177160). – Zugriffssdatum: 31.05.2022
- [Eidgenössisches Finanzdepartement 2021a] EIDGENÖSSISCHES FINANZDEPARTEMENT: *Blockchain*. 2021. – URL <https://www.efd.admin.ch/efd/de/home/digitalisierung/blockchain.html>. – Zugriffssdatum: 31.05.2022
- [Eidgenössisches Finanzdepartement 2021b] EIDGENÖSSISCHES FINANZDEPARTEMENT: *Digitale Verwaltung*. 2021. – URL <https://www.efd.admin.ch/efd/de/home/digitalisierung/e-government-schweiz.html>. – Zugriffssdatum: 31.05.2022
- [Eidgenössisches Finanzdepartement 2021c] EIDGENÖSSISCHES FINANZDEPARTEMENT: *Swiss Digital Initiative*. 2021. – URL <https://www.efd.admin.ch/efd/de/home/digitalisierung/swiss-digital-initiative.html>. – Zugriffssdatum: 31.05.2022
- [Eidgenössisches Justiz- und Polizeidepartement 2021a] EIDGENÖSSISCHES JUSTIZ- UND POLIZEIDEPARTEMENT: *E-ID: Bundesrat will vorwärts machen*. 2021. – URL <https://www.ejpd.admin.ch/ejpd/de/home/aktuell/mm.msg-id-83679.html>. – Zugriffssdatum: 31.05.2022
- [Eidgenössisches Justiz- und Polizeidepartement 2021b] EIDGENÖSSISCHES JUSTIZ- UND POLIZEIDEPARTEMENT: *Elektronische Identität: das E-ID-Gesetz*. 2021. – URL <https://www.ejpd.admin.ch/ejpd/de/home/themen/abstimmungen/bgeid.html>. – Zugriffssdatum: 31.05.2022
- [Eidgenössisches Justiz- und Polizeidepartement 2021c] EIDGENÖSSISCHES JUSTIZ- UND POLIZEIDEPARTEMENT: *Staatliche digitale Identität: Bundesrätin Keller-Sutter startet öffentliche Konsultation*. 2021. – URL <https://www.ejpd.admin.ch/ejpd/de/home/aktuell/mm.msg-id-84966.html>. – Zugriffssdatum: 31.05.2022
- [Eixelsberger et al. 2019] EIXELSBERGER, Wolfgang ; WUNDARA, Manfred ; HUEMER, Walter: *Blockchain in der Verwaltung*. In: STEMBER, Jürgen (Hrsg.) ; EIXELSBERGER, Wolfgang (Hrsg.) ; SPICHTIGER, Andreas (Hrsg.) ; NEURONI, Alessia (Hrsg.) ; HABELL, Franz-Reinhard (Hrsg.) ; WUNDARA, Manfred (Hrsg.): *Handbuch E-Government*. Wiesbaden : Springer Fachmedien Wiesbaden, 2019, S. 505–517. – ISBN 978-3-658-21401-2
- [EUR-Lex 2020] EUR-LEX: *Aufnahme von biometrischen Daten in Pässe und Reisedokumente: Zusammenfassungen der EU-Gesetzgebung*. 2020. – URL <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=LEGISSUM:114154>. – Zugriffssdatum: 31.05.2022
- [Europäische Kommission 2022] EUROPÄISCHE KOMMISSION: *eIDAS Regulation: eIDAS is a key enabler for secure cross-border transactions*. 2022. – URL <https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation>. – Zugriffssdatum: 31.05.2022
- [Fedlex 2018] FEDLEX ; SCHWEIZERISCHE EIDGENOSSENSCHAFT (Hrsg.): *SR 143.1 - Bundesgesetz vom 22. Juni 2001 über die Ausweise für Schweizer Staatsangehörige: Ausweisgesetz, AwG - Stand am 1. Januar 2018*. 2018. – URL <https://www.fedlex.admin.ch/eli/cc/2002/441/de>. – Zugriffssdatum: 31.05.2022
- [Fedlex 2019a] FEDLEX ; SCHWEIZERISCHE EIDGENOSSENSCHAFT (Hrsg.): *SR 141.0 - Bundesgesetz vom 20. Juni 2014 über das Schweizer Bürgerrecht: Bürgerrechtsgesetz, BüG - (Bürgerrechtsgezetz, BüG)*. 2019. – URL <https://www.fedlex.admin.ch/eli/cc/2016/404/de>. – Zugriffssdatum: 31.05.2022

- 
- [Fedlex 2019b] FEDLEX ; SCHWEIZERISCHE EIDGENOSSENSCHAFT (Hrsg.): *SR 143.111 - Verordnung des EJPD vom 16. Februar 2010 über die Ausweise für Schweizer Staatsangehörige: Stand am 1. Januar 2019*. 2019. – URL <https://www.fedlex.admin.ch/eli/cc/2010/96/de>. – Zugriffsdatum: 31.05.2022
- [Fedlex 2022] FEDLEX ; SCHWEIZERISCHE EIDGENOSSENSCHAFT (Hrsg.): *SR 143.11 - Verordnung vom 20. September 2002 über die Ausweise für Schweizer Staatsangehörige: Ausweisverordnung, VAwG - Stand am 1. Januar 2022*. 2022. – URL <https://www.fedlex.admin.ch/eli/cc/2002/468/de>. – Zugriffsdatum: 31.05.2022
- [Fischer et al. 2020] FISCHER, Damaris ; BRÄNDLE, Fabio ; MERTES, Alexander ; PLEGER, Lyn E. ; RHYNER, Alexander ; WULF, Bettina: Partizipation im digitalen Staat : Möglichkeiten und Bedeutung digitaler und analoger Partizipationsinstrumente im Vergleich. (2020). – DOI: 10.21256/ZHAW-20974
- [Fivaz und Schwarz 2021] FIVAZ, Jan ; SCHWARZ, Daniel: Die digitale Demokratie in der Schweiz. In: STEMBER, Jürgen (Hrsg.) ; EIXELSBERGER, Wolfgang (Hrsg.) ; SPICHIGER, Andreas (Hrsg.) ; NEURONI, Alessia (Hrsg.) ; HABELL, Franz-Reinhard (Hrsg.) ; WUNDARA, Manfred (Hrsg.): *Aktuelle Entwicklungen zum E-Government*. Wiesbaden : Springer Fachmedien Wiesbaden, 2021 (Edition Innovative Verwaltung), S. 75–96. – ISBN 978-3-658-33585-4
- [Fleishman 2000] FLEISHMAN, Glenn: Cartoon Captures Spirit of the Internet. In: *The New York Times* (2000). – URL <https://www.nytimes.com/2000/12/14/technology/cartoon-captures-spirit-of-the-internet.html>. – Zugriffsdatum: 31.05.2022. – ISSN 1553-8095
- [Gallersdörfer et al. 2020] GALLERSDÖRFER, Ulrich ; KLAASSEN, Lena ; STOLL, Christian: Energy Consumption of Cryptocurrencies Beyond Bitcoin. In: *Joule* 4 (2020), Nr. 9, S. 1843–1846. – DOI: 10.1016/j.joule.2020.07.013
- [GDS - Geschäftsstelle Digitale Schweiz 2021] GDS - GESCHÄFTSSTELLE DIGITALE SCHWEIZ: *Strategie Digitale Schweiz - Strategie*. 2021. – URL <https://www.digitaldialog.swiss/de/>. – Zugriffsdatum: 31.05.2022
- [Gentleman und Ihaka 2022] GENTLEMAN, Robert ; IHAKA, Ross: *The R Project for Statistical Computing*. 2022. – URL <https://www.r-project.org/contributors.html>. – Zugriffsdatum: 31.05.2022
- [Geschäftsstelle Digitale Verwaltung Schweiz 2022] GESCHÄFTSSTELLE DIGITALE VERWALTUNG SCHWEIZ: *Digitale Verwaltung Schweiz*. 2022. – URL <https://www.digitale-verwaltung-schweiz.ch/>. – Zugriffsdatum: 31.05.2022
- [Geschäftsstelle E-Government Schweiz 2020] GESCHÄFTSSTELLE E-GOVERNMENT SCHWEIZ: *E-Government Strategie Schweiz 2020-2023*. 2020. – URL [https://www.digitale-verwaltung-schweiz.ch/application/files/3016/3636/7600/E-Government-Strategie-Schweiz-2020-2023\\_D\\_def.pdf](https://www.digitale-verwaltung-schweiz.ch/application/files/3016/3636/7600/E-Government-Strategie-Schweiz-2020-2023_D_def.pdf). – Zugriffsdatum: 31.05.2022
- [gfs.bern 2021] GFS.BERN: VOX-Analyse März 2021: Nachbefragung und Analyse zur eidgenössischen Volksabstimmung vom 7. März 2021. (2021). – URL [https://vox.gfsbern.ch/wp-content/uploads/2021/04/d\\_vox\\_schlussbericht\\_def.pdf](https://vox.gfsbern.ch/wp-content/uploads/2021/04/d_vox_schlussbericht_def.pdf). – Zugriffsdatum: 31.05.2022
- [Goode 2019] GOODE, Alan: Digital identity: solving the problem of trust. In: *Biometric Technology Today* 2019 (2019), Nr. 10, S. 5–8. – DOI: 10.1016/S0969-4765(19)30142-0. – ISSN 09694765

- 
- [Grassi et al. 2017] GRASSI, Paul A. ; GARCIA, Michael E. ; FENTON, James L.: Digital identity guidelines: revision 3. (2017). – DOI: 10.6028/NIST.SP.800-63-3
- [Heinzer und Reichenbach 2013] HEINZER, Sarah ; REICHENBACH, Roland: Schlussbericht zum Forschungsprojekt "Die Entwicklung der beruflichen Identität": Z.H. des Leitungsausschusses des Bundesamtes für Berufsbildung und Technologie (BBT). (2013). – URL [https://www.ife.uzh.ch/dam/jcr:00000000-272b-1a72-0000-00002d44d5b6/Schlussbericht\\_zum\\_BBT-Projekt\\_Beruflische\\_Identitaet.pdf](https://www.ife.uzh.ch/dam/jcr:00000000-272b-1a72-0000-00002d44d5b6/Schlussbericht_zum_BBT-Projekt_Beruflische_Identitaet.pdf). – Zugriffsdatum: 31.05.2022
- [Ho 2021] HO, Frederic: How National Digital IDs Benefit Both Citizens And Businesses. In: *Forbes* (2021). – URL <https://www.forbes.com/sites/jumio/2021/05/03/how-national-digital-ids-benefit-both-citizens-and-businesses/?sh=106c64876fc6>. – Zugriffsdatum: 31.05.2022
- [Hou 2017] HOU, Heng: The Application of Blockchain Technology in E-Government in China. In: *2017 26th International Conference on Computer Communication and Networks (ICCCN)*, IEEE, 2017, S. 1–4. – ISBN 978-1-5090-2991-4
- [IBM 2020] IBM ; INTERNATIONAL BUSINESS MACHINES CORPORATION (Hrsg.): *Raking or Rim Weighting in SPSS Statistics*. 2020. – URL <https://www.ibm.com/support/pages/raking-or-rim-weighting-spss-statistics>. – Zugriffsdatum: 31.05.2022
- [IBM 2022] IBM ; INTERNATIONAL BUSINESS MACHINES CORPORATION (Hrsg.): *SPSS Statistics*. 2022. – URL <https://www.ibm.com/ch-de/products/spss-statistics>. – Zugriffsdatum: 31.05.2022
- [Identity2020 Systems 2022a] IDENTITY2020 SYSTEMS: *ID2020 / Digital Identity Alliance: Homepage*. 2022. – URL <https://id2020.org/>. – Zugriffsdatum: 31.05.2022
- [Identity2020 Systems 2022b] IDENTITY2020 SYSTEMS: *ID2020 / Digital Identity: The Need for Good Digital ID is Universal*. 2022. – URL <https://id2020.org/digital-identity>. – Zugriffsdatum: 31.05.2022
- [Internetredaktion LpB BW 2022] INTERNETREDAKTION LPB BW ; LANDESZENTRALE FÜR POLITISCHE BILDUNG BADEN-WÜRTTEMBERG (Hrsg.): *Digitale Demokratie: E-Partizipation, Open Government und Online-Wahlen*. 2022. – URL <https://www.lpb-bw.de/demokratie-digital#c61526>. – Zugriffsdatum: 31.05.2022
- [Irani und Kamal 2016] IRANI, Zahir ; KAMAL, Muhammad: Transforming Government: People, Process, and Policy. In: *Transforming Government: People, Process and Policy* 10 (2016), Nr. 2, S. 190–195. – DOI: 10.1108/TG-03-2016-0016. – ISSN 1750-6166
- [Jolocom 2018] JOLOCOM ; JOLOCOM GMBH (Hrsg.): *The 10 principles of self-sovereign identity according to Christopher Allen*. 2018. – URL <https://jolocom.io/blog/a-universal-identity-layer-we-can-only-build-together/>. – Zugriffsdatum: 31.05.2022
- [Kanton Schaffhausen 2021] KANTON SCHAFFHAUSEN: *Schaffhauser eID+*. 2021. – URL <https://sh.ch/CMS/Webseite/Kanton-Schaffhausen/Beh-rde/Services/Schaffhauser-eID--2077281-DE.html>. – Zugriffsdatum: 31.05.2022
- [Klenk 2022] KLENK, Mathias: The Next Evolution Of Digital Identity In 2022. In: *Forbes* (2022). – URL <https://www.forbes.com/sites/forbestechcouncil/2022/01/07/the-next-evolution-of-digital-identity-in-2022/?sh=181f952158d1>. – Zugriffsdatum: 31.05.2022

- 
- [Ladner et al. 2019] LADNER, Andreas (Hrsg.) ; SOGUEL, Nils (Hrsg.) ; EMERY, Yves (Hrsg.) ; WEERTS, Sophie (Hrsg.) ; NAHRATH, Stéphane (Hrsg.): *Swiss public administration: Making the state work successfully*. Cham : Springer International Publishing, 2019 (SpringerLink Bücher). – ISBN 978-3-319-92380-2
- [Ledger Academia 2019] LEDGER ACADEMIA: *What Are Public Keys and Private Keys?* 2019. – URL <https://www.ledger.com/academy/blockchain/what-are-public-keys-and-private-keys>. – Zugriffsdatum: 31.05.2022
- [Lenz und Ruchlak 2001] LENZ, Carsten ; RUCHLAK, Nicole: *Kleines Politik-Lexikon*. Reprint 2018. Berlin and Boston : Oldenbourg Wissenschaftsverlag, 2001 (Lehr- und Handbücher der Politikwissenschaft). – ISBN 978-3-486-80054-8
- [Lips 2010] LIPS, Miriam: Rethinking citizen – government relationships in the age of digital identity: Insights from research. In: *Information Polity* 15 (2010), Nr. 4, S. 273–289. – DOI: 10.3233/IP-2010-0216. – ISSN 15701255
- [McKinsey Global Institute 2019] MCKINSEY GLOBAL INSTITUTE: Digital identification: A key to inclusive growth. (2019). – URL [https://www.swisssign-group.com/dam/jcr:65b7324b-392b-4c2d-9737-ed9574eb1c0c/McKinsey\\_Digital\\_Identification\\_2019.pdf](https://www.swisssign-group.com/dam/jcr:65b7324b-392b-4c2d-9737-ed9574eb1c0c/McKinsey_Digital_Identification_2019.pdf). – Zugriffsdatum: 31.05.2022
- [Melin et al. 2016] MELIN, Ulf ; AXELSSON, Karin ; SÖDERSTRÖM, Fredrik: Managing the development of e-ID in a public e-service context. In: *Transforming Government: People, Process and Policy* 10 (2016), Nr. 1, S. 72–98. – DOI: 10.1108/TG-11-2013-0046. – ISSN 1750-6166
- [Meyer 2020] MEYER, Philip ; SCHWEIZER RADIO UND FERNSEHEN (Hrsg.): *SwissSignGroup wünscht Lizenz - Privatfirma will Verwalterin der elektronischen ID sein*. 2020
- [Mir et al. 2020] MIR, Umar B. ; KAR, Arpan K. ; DWIVEDI, Yogesh K. ; GUPTA, M. P. ; SHARMA, R. S.: Realizing digital identity in government: Prioritizing design and implementation objectives for Aadhaar in India. In: *Government Information Quarterly* 37 (2020), Nr. 2, S. 101442. – DOI: 10.1016/j.giq.2019.101442. – ISSN 0740624X
- [Mitschka und Unterberger 2018] MITSCHKA, Konrad ; UNTERBERGER, Klaus ; ORF GENE-RALDIREKTION PUBLIC VALUE (Hrsg.): *Studie »Der Auftrag: Demokratie«: Die Public Value-Jahreststudie 2017/18 in Kooperation mit dem Bayerischen Rundfunk und der EBU*. 2018. – URL [https://zukunft.orf.at/show\\_content.php?sid=147&pvi\\_id=1986&pvi\\_medientyp=t&oti\\_tag=studie](https://zukunft.orf.at/show_content.php?sid=147&pvi_id=1986&pvi_medientyp=t&oti_tag=studie). – Zugriffsdatum: 31.05.2022
- [Müller und Windisch 2018] MÜLLER, Andrea ; WINDISCH, Andreas: E-Identity-Lösungen in Europa: Ein europäischer Vergleich. (2018), Nr. asquared Blog Post № 3/2018. – URL [https://www.swisssign-group.com/dam/jcr:4b056c65-3b0c-47e4-a9ce-80cf404588e4/2018\\_Asquared-blog\\_post\\_de\\_2018-02-13\\_e-identity-loesungen-in-europa\\_v1.pdf](https://www.swisssign-group.com/dam/jcr:4b056c65-3b0c-47e4-a9ce-80cf404588e4/2018_Asquared-blog_post_de_2018-02-13_e-identity-loesungen-in-europa_v1.pdf). – Zugriffsdatum: 31.05.2022
- [Nakamoto 2008] NAKAMOTO, Satoshi: Bitcoin: A Peer-to-Peer Electronic Cash System. In: *SSRN Electronic Journal* (2008). – URL <https://bitcoin.org/bitcoin.pdf>. – Zugriffsdatum: 31.05.2022. – DOI: 10.2139/ssrn.3440802
- [Neuroni et al. 2019] NEURONI, Alessia ; KISSLING-NÄF, Ingrid ; RIEDL, Reinhard: E-Government und smarter Staat: Die Schweiz auf halbem Weg. In: STEMBER, Jürgen (Hrsg.) ; EIXELSBERGER,

---

Wolfgang (Hrsg.) ; SPICHIGER, Andreas (Hrsg.) ; NEURONI, Alessia (Hrsg.) ; HABEL, Franz-Reinhard (Hrsg.) ; WUNDARA, Manfred (Hrsg.): *Handbuch E-Government*. Wiesbaden : Springer Fachmedien Wiesbaden, 2019, S. 163–180. – ISBN 978-3-658-21401-2

[Nicke 2018] NICKE, Sascha: Der Begriff der Identität. In: *Bundeszentrale für politische Bildung* (2018). – URL <https://www.bpb.de/themen/parteien/rechtspopulismus/241035/der-begriff-der-identitaet/>. – Zugriffsdatum: 31.05.2022

[OECD 2022] OECD: *Digital Identity Management and Electronic Authentication*. 2022. – URL <https://www.oecd.org/sti/ieconomy/digitalidentitymanagementandelectronicauthentication.htm>. – Zugriffsdatum: 31.05.2022

[Pilkington 2016] PILKINGTON, Marc: Blockchain technology: principles and applications. In: OLLEROS, F. (Hrsg.) ; ZHEGU, Majlinda (Hrsg.): *Research Handbook on Digital Transformations*. Edward Elgar Publishing, 2016, S. 225–253. – ISBN 978-1-78471-776-6

[Poblet et al. 2020] POBLET, Marta ; ALLEN, Darcy W. E. ; KONASHEVYCH, Oleksii ; LANE, Aaron M. ; DIAZ VALDIVIA, Carlos A.: From Athens to the Blockchain: Oracles for Digital Democracy. In: *Frontiers in Blockchain* 3 (2020). – DOI: 10.3389/fbloc.2020.575662

[Politools 2022a] POLITICOOLS ; POLITICOOLS (Hrsg.): *Politools – Home of Smartvote*. 2022. – URL <https://politools.net/>. – Zugriffsdatum: 31.05.2022

[Politools 2022b] POLITICOOLS ; POLITICOOLS (Hrsg.): *smartvote - Online-Wahlhilfe*. 2022. – URL <https://smartvote.ch/de/home>. – Zugriffsdatum: 31.05.2022

[Prashanth Joshi et al. 2018] PRASHANTH JOSHI, Archana ; HAN, Meng ; WANG, Yan: A survey on security and privacy issues of blockchain technology. In: *Mathematical Foundations of Computing* 1 (2018), Nr. 2, S. 121–147. – DOI: 10.3934/mfc.2018007. – ISSN 2577-8838

[PricewaterhouseCoopers 2022] PRICEWATERHOUSECOOPERS: *Digital identity - Your key to unlock the digital transformation*. 2022. – URL <https://www.pwc.ch/en/insights/fs/digital-identity.html>. – Zugriffsdatum: 31.05.2022

[Procivis 2022a] PROCIVIS: *eID+: Die Smart-Government-Lösung für digitale Behördendienstleistungen*. 2022. – URL <https://www.procivis.ch/eid>. – Zugriffsdatum: 31.05.2022

[Procivis 2022b] PROCIVIS: *Procivis SSI+: Die selbstverwaltete Identitätslösung, die Bürger\*innen die Kontrolle über ihre Daten gibt*. 2022. – URL <https://www.procivis.ch/procivis-ssi>. – Zugriffsdatum: 31.05.2022

[Procivis 2022c] PROCIVIS: *Ein Schritt näher zur selbstverwalteten Identität - Procivis lanciert SSI+*. 2022. – URL <https://www.procivis.ch/post/ein-schritt-nahe-zur-selbstverwalteten-identitat-procivis-lanciert-ssi>. – Zugriffsdatum: 31.05.2022

[Qualtrics 2022] QUALTRICS: *Marktforschung, Umfrage & Erlebnismanagement Software*. 2022. – URL <https://www.qualtrics.com>. – Zugriffsdatum: 31.05.2022

[Rat der Europäischen Union 2004] RAT DER EUROPÄISCHEN UNION: *VERORDNUNG (EG) Nr. 2252/2004 DES RATES vom 13. Dezember 2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten*. 2004. – URL <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R2252:DE:HTML>. – Zugriffsdatum: 31.05.2022

- 
- [Rauschenbach und Stucki 2020] RAUSCHENBACH, Rolf ; STUCKI, Sven: Studie zum Einsatz der Blockchain-Technologie in der kantonalen Verwaltung: Staatskanzlei Kanton Zürich - Digitale Verwaltung und E-Government. (2020). – URL [https://www.zh.ch/content/dam/zhweb/bilder-dokumente/organisation/staatskanzlei/digitale-verwaltung-und-e-government/studie\\_blockchain.pdf](https://www.zh.ch/content/dam/zhweb/bilder-dokumente/organisation/staatskanzlei/digitale-verwaltung-und-e-government/studie_blockchain.pdf). – Zugriffsdatum: 31.05.2022
- [ReliefWeb 2018] RELIEFWEB: *How Finland is Using the Blockchain to Revolutionise Financial Services for Refugees*. 2018. – URL <https://reliefweb.int/report/finland/how-finland-using-blockchain-revolutionise-financial-services-refugees>. – Zugriffsdatum: 31.05.2022
- [Rivera et al. 2017] RIVERA, Rogelio ; ROBLEDO, Jose G. ; LARIOS, Victor M. ; AVALOS, Juan M.: How digital identity on blockchain can contribute in a smart city environment. In: *2017 International Smart Cities Conference (ISC2)*, IEEE, 2017, S. 1–4. – ISBN 978-1-5386-2524-8
- [Rodriguez 2020] RODRIGUEZ, Tony: *iterake: Create weights with iterative raking*. 2020. – URL <https://github.com/ttrodigz/iterake>. – Zugriffsdatum: 31.05.2022
- [RStudio Inc. 2022] RSTUDIO INC.: *RStudio / Open Source & Professional Software for Data Science Teams*. 2022. – URL <https://www.rstudio.com/>. – Zugriffsdatum: 31.05.2022
- [Rüthi et al. 2020] RÜTHI, Timothy ; HOLENSTEIN, Matthias ; STÜBI, Nathalie ; KÖNG, Anna-Lena ; STIFTUNG RISIKO-DIALOG (Hrsg.): *Mobilair #Digital Barometer 2020/21: Die Stimme der Schweizer Bevölkerung*. 2020. – URL <https://www.digitalbarometer.ch/de/digitalbarometer#downloads>. – Zugriffsdatum: 31.05.2022
- [Schwarz 2022] SCHWARZ, Jürg: *Methodenberatung*. 2022. – URL <https://www.methodenberatung.uzh.ch/de.html>. – Zugriffsdatum: 31.05.2022
- [Schweizer und Müller 2021] SCHWEIZER, Rainer J. ; MÜLLER, Christina: *Bürgerrecht: Version vom 11.01.2021*. 2021. – URL <https://hls-dhs-dss.ch/de/articles/008969/2021-01-11/>. – Zugriffsdatum: 31.05.2022
- [Schweizer Radio und Fernsehen 2021] SCHWEIZER RADIO UND FERNSEHEN: *Eidgenössische Abstimmung - Das E-ID-Gesetz wird deutlich abgelehnt*. 2021. – URL <https://www.srf.ch/news/abstimmungen/elektronische-identitaet/eidgenoessische-abstimmung-das-e-id-gesetz-wird-deutlich-abgelehnt>. – Zugriffsdatum: 31.05.2022
- [Schweizerischer Baumeisterverband 2020] SCHWEIZERISCHER BAUMEISTERVERBAND: *Blockchain im Bauhauptgewerbe*. 2020. – URL <https://baumeister.swiss/blockchain-im-bauhauptgewerbe/>. – Zugriffsdatum: 31.05.2022
- [Sebaldt 2010] SEBALDT, Martin: *Politische Führung in westlichen Regierungssystemen: Theorie und Praxis im internationalen Vergleich*. Wiesbaden : VS Verl. für Sozialwiss, 2010. – ISBN 978-3-531-91929-4
- [Shobanadevi et al. 2021] SHOBANADEVI, A. ; THAREWAL, Sumegh ; SONI, Mukesh ; KUMAR, D. D. ; KHAN, Ihtiram R. ; KUMAR, Pankaj: Novel identity management system using smart-blockchain technology. In: *International Journal of System Assurance Engineering and Management* (2021). – DOI: 10.1007/s13198-021-01494-0. – ISSN 0975-6809

- 
- [Sovrin Foundation 2018] SOVRIN FOUNDATION: Sovrin: A protocol and token for self-sovereign identity and decentralized trust: A White Paper from the Sovrin Foundation. (2018). – URL <https://sovrin.org/wp-content/uploads/2018/03/Sovrin-Protocol-and-Token-White-Paper.pdf>. – Zugriffsdatum: 31.05.2022
- [Staatssekretariat für Migration SEM 2022] STAATSSEKRETARIAT FÜR MIGRATION SEM: *Wie werde ich Schweizerin oder Schweizer*. 2022. – URL <https://www.sem.admin.ch/sem/de/home/integration-einbuergerung/schweizer-werden.html>. – Zugriffsdatum: 31.05.2022
- [Stadt Zug 2017] STADT ZUG: *Blockchain-basierte digitale ID für alle Einwohner jetzt erhältlich*. 2017. – URL <https://www.stadtzug.ch/newsarchiv/431448>. – Zugriffsdatum: 31.05.2022
- [Statista Inc. 2022] STATISTA INC.: *Top blockchain use cases 2021*. 2022. – URL <https://www.statista.com/statistics/982566/worldwide-top-use-cases-blockchain-technology-by-market-share/>. – Zugriffsdatum: 31.05.2022
- [Stokkink und Pouwelse 2018] STOKKINK, Quinten ; POUWELSE, Johan: Deployment of a Blockchain-Based Self-Sovereign Identity. In: *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, IEEE, 2018, S. 1336–1342. – ISBN 978-1-5386-7975-3
- [Sullivan 2016] SULLIVAN, Clare: Digital citizenship and the right to digital identity under international law. In: *Computer Law & Security Review* 32 (2016), Nr. 3, S. 474–481. – DOI: 10.1016/j.clsr.2016.02.001. – ISSN 02673649
- [Sullivan 2018] SULLIVAN, Clare: Digital identity – From emergent legal concept to new reality. In: *Computer Law & Security Review* 34 (2018), Nr. 4, S. 723–731. – DOI: 10.1016/j.clsr.2018.05.015. – ISSN 02673649
- [Swiss Digital Initiative 2022] SWISS DIGITAL INITIATIVE: *Ethics & Fairness in the Age of Digital Transformation*. 2022. – URL <https://www.swiss-digital-initiative.org/>. – Zugriffsdatum: 31.05.2022
- [SwissSign Group 2022] SWISSSIGN GROUP: *SwissSign loves to keep you safe*. 2022. – URL <https://www.swisssign-group.com/>. – Zugriffsdatum: 31.05.2022
- [Takemiya und Vanieiev 2018] TAKEMIYA, Makoto ; VANIEIEV, Bohdan: Sora Identity: Secure, Digital Identity on the Blockchain. In: *2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)*, IEEE, 2018, S. 582–587. – ISBN 978-1-5386-2666-5
- [Toth und Anderson-Priddy 2019] TOTH, Kalman C. ; ANDERSON-PRIDDY, Alan: Self-Sovereign Digital Identity: A Paradigm Shift for Identity. In: *IEEE Security & Privacy Magazine* 17 (2019), Nr. 3, S. 17–27. – DOI: 10.1109/MSEC.2018.2888782. – ISSN 1540-7993
- [Treiblmaier und Beck 2019] TREIBLMAIER, Horst (Hrsg.) ; BECK, Roman (Hrsg.): *Business transformation through Blockchain*. Cham, Switzerland : Palgrave Macmillan, 2019. – ISBN 978-3-319-99057-6
- [Underwood 2016] UNDERWOOD, Sarah: Blockchain beyond bitcoin. In: *Communications of the ACM* 59 (2016), Nr. 11, S. 15–17. – DOI: 10.1145/2994581. – ISSN 0001-0782

- 
- [uPort 2021] uPORT: Veramo: uPort's Open Source Evolution. In: *Medium* 2021 (2021). – URL <https://medium.com/uport/veramo-uports-open-source-evolution-d85fa463db1f>. – Zugriffsdatum: 31.05.2022
- [Vatter 2020] VATTER, Adrian: *Das politische System der Schweiz*. 4th ed. Baden-Baden : Nomos Verlagsgesellschaft, 2020 (Studienkurs Politikwissenschaft). – URL <https://ebookcentral.proquest.com/lib/kxp/detail.action?docID=6405378>. – ISBN 978-3-74890-681-0
- [Whitley et al. 2014] WHITLEY, Edgar A. ; GAL, Uri ; KJAERGAARD, Annemette: Who do you think you are? A review of the complex interplay between information systems, identification and identity. In: *European Journal of Information Systems* 23 (2014), Nr. 1, S. 17–35. – DOI: 10.1057/ejis.2013.34. – ISSN 0960-085X
- [Wikipedia - Diverse Autor:innen 2021] WIKIPEDIA - DIVERSE AUTOR:INNEN ; WIKIPEDIA - DIE FREIE ENZYKLOPÄDIE (Hrsg.): *Box-Plot*. 2021. – URL <https://de.wikipedia.org/w/index.php?title=Box-Plot&oldid=213627175>. – Zugriffsdatum: 31.05.2022
- [Wikipedia - Diverse Autor:innen 2022] WIKIPEDIA - DIVERSE AUTOR:INNEN ; WIKIPEDIA - DIE FREIE ENZYKLOPÄDIE (Hrsg.): *Violin plot*. 2022. – URL [https://en.wikipedia.org/w/index.php?title=Violin\\_plot&oldid=1082809795](https://en.wikipedia.org/w/index.php?title=Violin_plot&oldid=1082809795). – Zugriffsdatum: 31.05.2022
- [Wolfond 2017] WOLFOND, Greg: A Blockchain Ecosystem for Digital Identity: Improving Service Delivery in Canada's Public and Private Sectors. In: *Technology Innovation Management Review* 7 (2017), Nr. 10, S. 35–40. – DOI: 10.22215/timreview/1112
- [World Economic Forum 2018] WORLD ECONOMIC FORUM: Identity in a Digital World - A New Chapter in the Social Contract. Insight Report. (2018). – URL [https://www3.weforum.org/docs/WEF\\_INSIGHT\\_REPORT\\_Digital%20Identity.pdf](https://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf). – Zugriffsdatum: 31.05.2022
- [Yaga et al. 2018] YAGA, Dylan ; MELL, Peter ; ROBY, Nik ; SCARFONE, Karen: Blockchain technology overview. (2018). – DOI: 10.6028/NIST.IR.8202
- [Yang und Li 2020] YANG, Xiaohui ; LI, Wenjie: A zero-knowledge-proof-based digital identity management scheme in blockchain. In: *Computers & Security* 99 (2020), S. 102050. – DOI: 10.1016/j.cose.2020.102050. – ISSN 01674048
- [Zwitter et al. 2020] ZWITTER, Andrej J. ; GSTREIN, Oskar J. ; YAP, Evan: Digital Identity and the Blockchain: Universal Identity Management and the Concept of the “Self-Sovereign” Individual. In: *Frontiers in Blockchain* 3 (2020). – DOI: 10.3389/fbloc.2020.00026

---

## **Anhang**

---

**Anhang I: Export *Qualtrics*<sup>TM</sup> Online-Fragebogen**

## Umfrage - Blockchain-ID - Master-Thesis

Deutsch ▾

### Begrüssung zur Umfrage

#### Q1.1.

*Cette enquête est aussi disponible en français. Vous pouvez changer de langue dans le champ ci-dessus.*

#### Geschätzte Umfrageteilnehmende

Herzlichen Dank, dass Sie sich **10 Minuten** Zeit nehmen, einige Fragen zu Ihrer **Einstellung gegenüber dem Einsatz von Blockchain-Technologie für eine elektronischen Identität (E-ID)** zu beantworten.

Das **E-ID-Gesetz 2020** für eine elektronische Identität wurde anlässlich der Referendumsabstimmung am 7. März 2021 **mit 64.4% Nein-Stimmen** vom schweizerischen Stimmvolk **abgelehnt**. Diese Umfrage hat deshalb zum Ziel, Erkenntnisse über die Einstellung der Bevölkerung gegenüber alternativen Lösungsansätzen für eine elektronische ID zu gewinnen.

- Die Auswertung der Daten dient **rein wissenschaftlichen Zwecken**. Es erfolgt lediglich eine aggregierte und anonymisierte Publikation der Ergebnisse, die **keine Rückschlüsse auf einzelne Umfrageteilnehmer:innen** zulässt.
- Die Umfrage findet im Rahmen der Master-Thesis des Masterstudiengangs Business Administration der Berner Fachhochschule BFH statt. Betreut wird die Master-Thesis von **Dr. Daniel Schwarz Badertscher** (Politikwissenschaftler)

- und Mitbegründer des Vereins *Politoos* und der Online-Wahlhilfe *smartvote*).
- Bei Fragen oder Problemen mit der Umfrage können Sie sich jederzeit an Tim Wackernagel ([wackt1@bfh.ch](mailto:wackt1@bfh.ch)) wenden.

Besten Dank für Ihre Teilnahme!

### **Soziodemografische Merkmale**

Q2.1. Bitte geben Sie Ihr Geschlecht an.

Weiblich

Männlich

Divers

Keine Antwort

Q2.2. Bitte geben Sie Ihr Geburtsjahr an (Format JJJJ, z.B. 1980).

Q2.3. Bitte geben Sie die Postleitzahl Ihrer aktuellen Wohngemeinde an.

Q2.4. Besitzen Sie die schweizerische Staatsbürgerschaft?

Ja

Nein

Keine Antwort

## Q2.5. Was ist Ihr derzeit höchster Bildungsabschluss?

(Noch) kein Abschluss

Obligatorische Schule (Primarschule, Sekundarschule)

Allgemeinbildende Schulen (Gymnasiale Maturität, Maturitätsschule, Berufsmatura, FMS, DMS, etc.)

Berufliche Grundausbildung (Berufslehre, Berufsschule, Handelsschule, etc.)

Höhere Fach- und Berufsausbildung (HF, HFP, HTL, etc.)

Fachhochschule, PH

Universität, ETH

Anderer Abschluss (Textfeld):

Keine Antwort

## Politische Merkmale

### Q3.1. Welcher der folgenden Parteien fühlen Sie sich am stärksten verbunden?

Die Mitte

EDU

EVP

FDP

Grüne

glp

Lega

PdA

SVP

solidaritéS

SP

Andere (Textfeld):

Keine Partei

## **Abstimmung "E-ID-Gesetz 2020"**

**Q4.1. Wie haben Sie bei der vergangenen Referendumsabstimmung vom 7. März 2021 zum E-ID-Gesetz 2020 abgestimmt?**

Mit 'Ja', Gesetz angenommen

Mit 'Nein', Gesetz abgelehnt

Ich habe nicht abgestimmt

Keine Antwort

## **Vertrauen in Staat im Umgang mit Identitätsdaten**

**Q5.1. Bitte geben Sie an, inwieweit Sie den folgenden Aussagen zustimmen.**

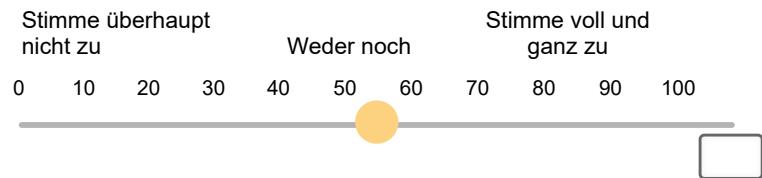
**Q5.2. Allein der Staat sollte für die Einführung, Ausstellung und den Betrieb einer E-ID verantwortlich sein.**



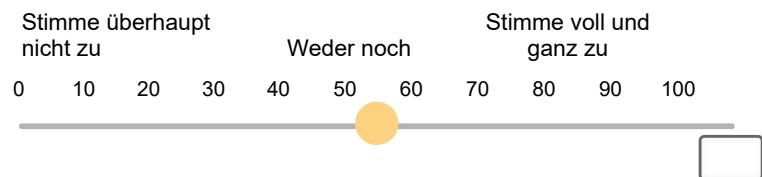
**Q5.3. Ich traue dem Staat zu, die passendste Technologie für die Umsetzung einer E-ID zu wählen.**



Q5.4. Ich glaube, dass meine Identitätsdaten beim Gebrauch einer rein staatlichen E-ID im Internet sicher sind.



Q5.5. Ich würde eine rein vom Staat herausgegebene und betriebene Lösung für die E-ID selbst nutzen.



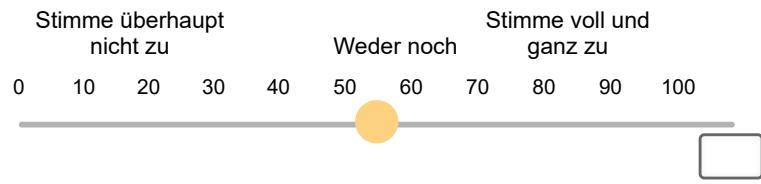
### Einordnung E-ID und offizielle Ausweisdokumente

Q6.1. **Bitte geben Sie an, inwieweit Sie den folgenden Aussagen zustimmen.**

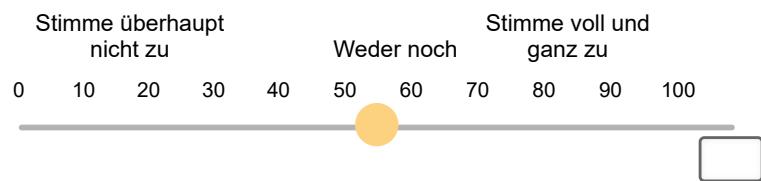
Q6.2. Eine E-ID ist ein offizielles, staatliches Ausweisdokument.



Q6.3. Eine E-ID ist das Gleiche wie mein Pass oder meine Identitätskarte, einfach in digitaler/elektronischer Form.



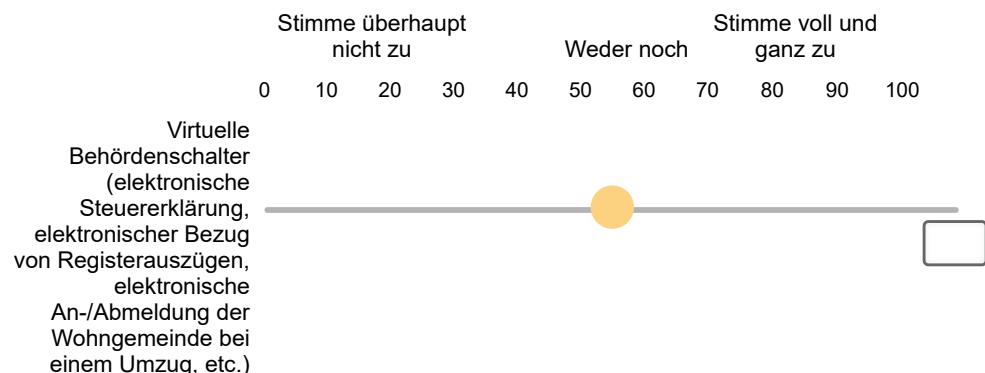
**Q6.4.** Mit einer E-ID kann ich mich jederzeit und überall in digitaler Form wie mit meinem Pass oder meiner Identitätskarte ausweisen, bspw. bei einem Grenzübertritt.

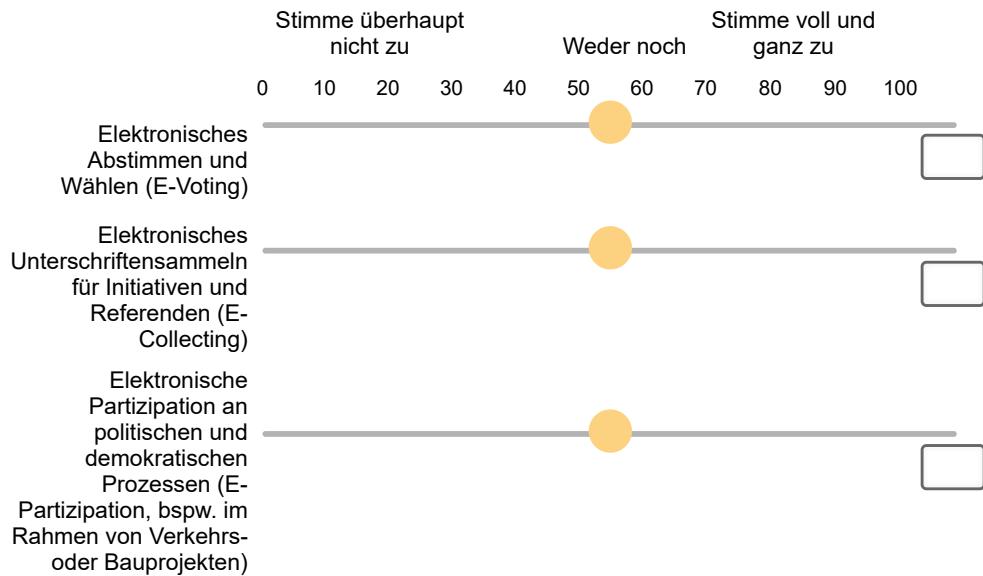


### Betroffenheit & Anwendungsbereiche E-ID im öff. Sektor & digitaler Demokratie

**Q7.1. Bitte geben Sie an, inwieweit Sie den folgenden Aussagen zustimmen.**

**Q7.2. Folgende elektronischen Dienstleistungen des öffentlichen Sektors und der Demokratie sind mir wichtig.**





Q7.3. Eine E-ID ist eine Voraussetzung, um elektronische Dienstleistungen von Behörden vollständig über das Internet beziehen zu können.



Q7.4. Eine E-ID ist eine Voraussetzung, um elektronische Demokratie-Instrumente wie E-Voting oder E-Collecting nutzen zu können.



## **Vorkenntnisse & Einstellung gegenüber Blockchain-Technologie generell**

**Q8.1. Hatten Sie in Ihrem Alltag oder beruflichen Umfeld bereits einmal mit der Blockchain-Technologie (Distributed-Ledger-Technologie DLT) zu tun oder diese selbst genutzt (bspw. durch Kryptowährungen oder andere Anwendungen)?**

- Ja
- Nein
- Weiss nicht
- Keine Antwort

**Q8.2. Bitte geben Sie an, inwieweit Sie den folgenden Aussagen zustimmen.**

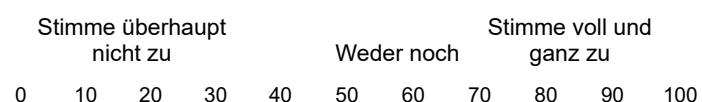
**Q8.3. Ich bin mit dem Begriff "Blockchain" vertraut.**

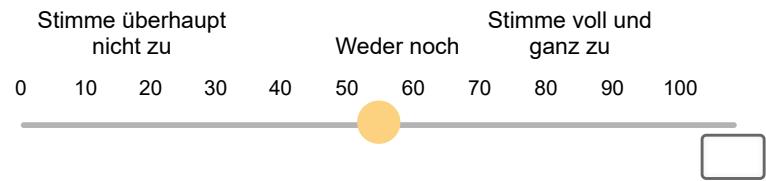


**Q8.4. Ich bin mit der technischen Funktionsweise der Blockchain vertraut.**



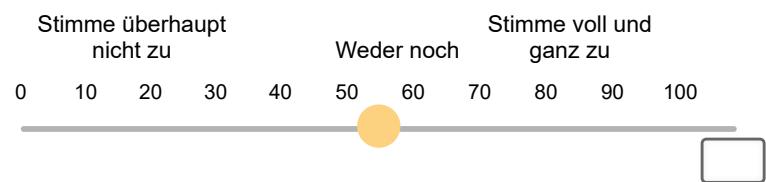
**Q8.5. Mit dem Begriff "Blockchain" verbinde ich etwas Negatives.**



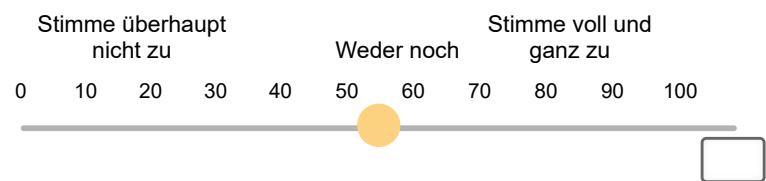


Q8.6.

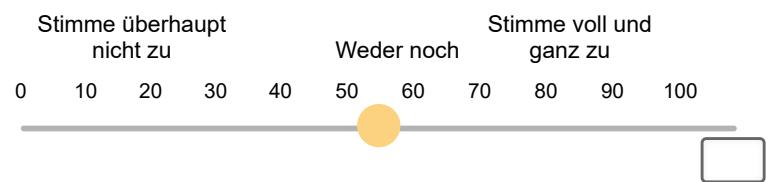
Ich vertraue Anwendungen grundsätzlich, wenn diese Blockchain-Technologie in kompetenter Weise nutzen.



Q8.7. Ich bin bereit, Anwendungen zu nutzen, welche die Blockchain-Technologie einsetzen.



Q8.8. Der Staat sollte innovative Technologien wie die Blockchain-Technologie vermehrt einsetzen.



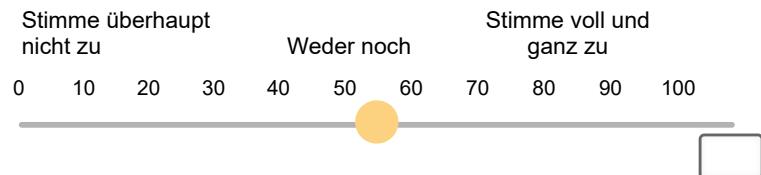
## **Self-Sovereign-Identity**

**Q9.1.** Wer sollte Ihrer Meinung nach die Datenhoheit und Kontrolle über Ihre Identitätsdaten haben? Sie können auch mehrere Parteien angeben.

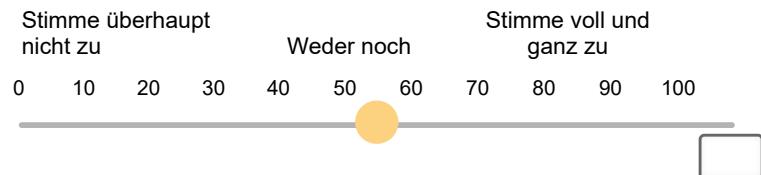
- Ich selbst
- Der Staat
- Private Anbieter/Unternehmen
- Weiss nicht

**Q9.2. Bitte geben Sie an, inwieweit Sie den folgenden Aussagen zustimmen.**

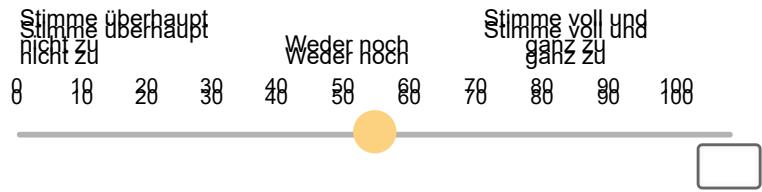
**Q9.3.** Bei der Verwendung von digitalen Anwendungen sollte ich selbst bestimmen können, mit wem meine Identitätsdaten geteilt werden.



**Q9.4.** Bei der Verwendung von digitalen Anwendungen sollte ich transparent nachvollziehen können, wie meine Identitätsdaten verwendet werden.



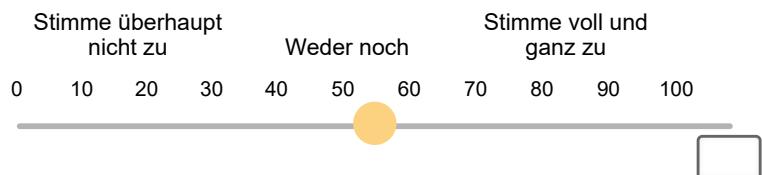
**Q9.5.** Ich sollte im digitalen Raum die alleinige Datenhoheit und Kontrolle über meine Identitätsdaten besitzen.



### **Blockchain-Technologie für digitale ID**

**Q10.1. Bitte geben Sie an, inwieweit Sie den folgenden Aussagen zustimmen.**

Q10.2. Einer auf Basis von Blockchain-Technologie entwickelten E-ID stehe ich grundsätzlich positiv gegenüber.



**Q10.3. Bitte lesen Sie den folgenden Text genau durch:**

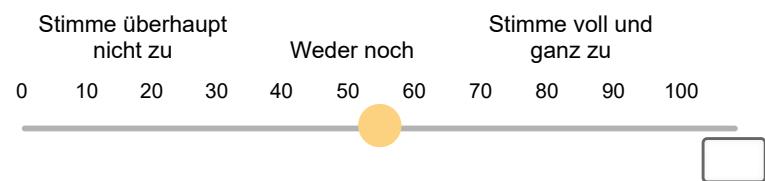
Expertinnen und Experten gehen davon aus, dass die Blockchain-Technologie eine E-ID-Lösung möglich macht, welche die vollständig selbstbestimmte Verwaltung von Identitätsdaten (*Self-Sovereign Identity*) erlaubt.

Dies würde Ihnen erlauben:

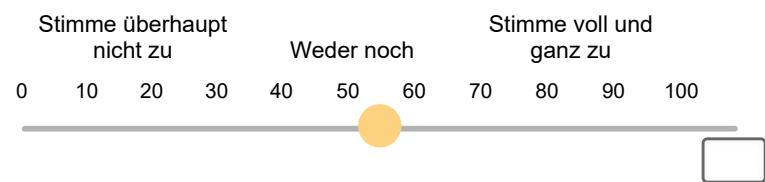
- Die alleinige Datenhoheit über Ihre Identitätsdaten zu besitzen.
- Selbst zu entscheiden, ob und wie lange Identitätsdaten jemand anderem zur Verfügung stehen.
- Sämtliche Verwendungen Ihrer Identitätsdaten jederzeit transparent nachvollziehen zu können.
- Ihre Identitätsdaten manipulationssicher und kryptografisch geschützt speichern zu können.

**Q10.4. Bitte geben Sie an, inwieweit Sie den folgenden Aussagen zustimmen.**

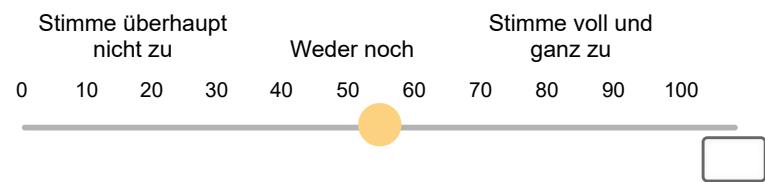
Q10.5. Das Konzept der *vollständig selbstbestimmten Verwaltung von Identitätsdaten* ist für mich verständlich.



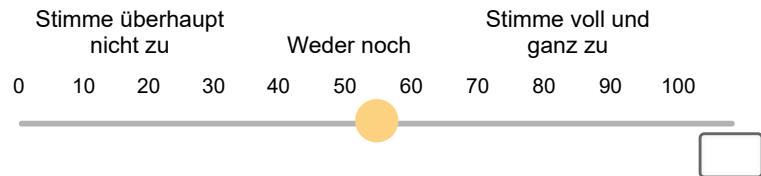
Q10.6. Das Konzept der *vollständig selbstbestimmten Verwaltung von Identitätsdaten* durch Blockchain-Technologie finde ich interessant.



Q10.7. Einer E-ID auf Basis von Blockchain-Technologie, welche mir die vollständig selbstbestimmte Verwaltung meiner Identitätsdaten erlaubt, stehe ich grundsätzlich positiv gegenüber.



Q10.8. Solange bei einer E-ID die Sicherheit meiner Daten gewährleistet ist, diese zuverlässig funktioniert und nutzerfreundlich ist, ist mir die verwendete Technologie egal.



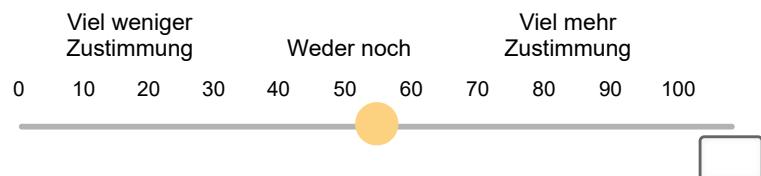
### Blockchain-ID vs E-ID 2020

Q11.1. Bitte lesen Sie die folgenden Fragen genau durch:

Q11.2. Angenommen, am nächsten Wochenende würde eine Volksabstimmung über eine **rein staatliche** und **Blockchain-basierte** E-ID-Lösung stattfinden. Würden Sie einer solchen Vorlage zustimmen?

- Ja
- Eher ja
- Unentschlossen / Weiss nicht
- Eher nein
- Nein

Q11.3. Ist Ihre persönliche Zustimmung zu einer **rein staatlichen** und **Blockchain-basierten** E-ID-Lösung im Vergleich zum *E-ID-Gesetz 2020* höher oder tiefer?



Q11.4. Bitte geben Sie an, weshalb Sie einer **rein staatlichen** und **Blockchain-basierten E-ID-Lösung** (eher) **zustimmen** würden. Sie können mehrere Gründe angeben.

Generelle Dringlichkeit einer E-ID-Lösung

Befürwortung einer rein staatlichen E-ID-Lösung

Ermöglichung der vollständig selbstbestimmten Verwaltung meiner Identität

Ermöglichung einer innovativen wirtschaftlichen Zukunft

Technologische Eigenschaften und Potenziale der Blockchain

Verbesserte Nutzung & Angebote von digitalen Dienstleistungen der Privatwirtschaft

Verbesserte Nutzung & Angebote von digitalen Dienstleistungen der Behörden

Stärkung der Demokratie durch neue Demokratie-Instrumente (E-Voting, E-Collecting, etc.)

Andere (Textfeld):

Keine Antwort

Q11.5. Welche der folgenden Gründe könnten Ihrer Meinung nach **dennnoch** (eher) **gegen** eine **rein staatliche** und **Blockchain-basierte E-ID-Lösung** sprechen? Sie können mehrere Gründe angeben.

Grundsätzliche Ablehnung einer E-ID

Generelle Datenschutz- und Sicherheitsbedenken bei einer E-ID

Ablehnung einer rein staatlichen E-ID-Lösung

Der Staat kann eine E-ID nicht ohne die Privatwirtschaft stemmen

Generelle Ablehnung gegenüber der Blockchain-Technologie

Fehlendes Wissen über die Blockchain-Technologie

Datenschutz- und Sicherheitsbedenken durch den Einsatz von Blockchain-Technologie

Zu hohe Komplexität der Thematik

Andere (Textfeld):

Ich sehe keine Gründe gegen die vorgeschlagene Lösung

Keine Antwort

**Q11.6. Bitte geben Sie an, weshalb Sie eine **rein staatliche** und **Blockchain-basierte** E-ID-Lösung (eher) **ablehnen** würden. Sie können mehrere Gründe angeben.**

- Grundsätzliche Ablehnung einer E-ID
- Generelle Datenschutz- und Sicherheitsbedenken bei einer E-ID
- Ablehnung einer rein staatlichen E-ID-Lösung
- Der Staat kann eine E-ID nicht ohne die Privatwirtschaft stemmen
- Generelle Ablehnung gegenüber der Blockchain-Technologie
- Fehlendes Wissen über die Blockchain-Technologie
- Datenschutz- und Sicherheitsbedenken durch den Einsatz von Blockchain-Technologie
- Zu hohe Komplexität der Thematik
- Andere (Textfeld):

Keine Antwort

**Q11.7. Welche der folgenden Gründe könnten Ihrer Meinung nach **dennoch** (eher) **für** eine **rein staatliche** und **Blockchain-basierte** E-ID-Lösung sprechen? Sie können mehrere Gründe angeben.**

- Generelle Dringlichkeit einer E-ID-Lösung
- Befürwortung einer rein staatlichen E-ID-Lösung
- Ermöglichung der vollständig selbstbestimmten Verwaltung meiner Identität
- Ermöglichung einer innovativen wirtschaftlichen Zukunft
- Technologische Eigenschaften und Potenziale der Blockchain
- Verbesserte Nutzung & Angebote von digitalen Dienstleistungen der Privatwirtschaft
- Verbesserte Nutzung & Angebote von digitalen Dienstleistungen der Behörden
- Stärkung der Demokratie durch neue Demokratie-Instrumente (E-Voting, E-Collecting, etc.)
- Andere (Textfeld):

Ich sehe keine Gründe für die vorgeschlagene Lösung

Keine Antwort

**Q11.8.** Welche der folgenden Gründe könnten Ihrer Meinung nach **trotz Unentschlossenheit** (eher) **für** eine **rein staatliche** und **Blockchain-basierte** E-ID-Lösung sprechen? Sie können mehrere Gründe angeben.

- Generelle Dringlichkeit einer E-ID-Lösung
- Befürwortung einer rein staatlichen E-ID-Lösung
- Ermöglichung der vollständig selbstbestimmten Verwaltung meiner Identität
- Ermöglichung einer innovativen wirtschaftlichen Zukunft
- Technologische Eigenschaften und Potenziale der Blockchain
- Verbesserte Nutzung & Angebote von digitalen Dienstleistungen der Privatwirtschaft
- Verbesserte Nutzung & Angebote von digitalen Dienstleistungen der Behörden
- Stärkung der Demokratie durch neue Demokratie-Instrumente (E-Voting, E-Collecting, etc.)
- Andere (Textfeld):

Ich sehe keine Gründe für die vorgeschlagene Lösung

Keine Antwort

**Q11.9.** Welche der folgenden Gründe könnten Ihrer Meinung nach **trotz Unentschlossenheit** (eher) **gegen** eine **rein staatliche** und **Blockchain-basierte** E-ID-Lösung sprechen? Sie können mehrere Gründe angeben.

- Grundsätzliche Ablehnung einer E-ID
- Generelle Datenschutz- und Sicherheitsbedenken bei einer E-ID
- Ablehnung einer rein staatlichen E-ID-Lösung
- Der Staat kann eine E-ID nicht ohne die Privatwirtschaft stemmen
- Generelle Ablehnung gegenüber der Blockchain-Technologie
- Fehlendes Wissen über die Blockchain-Technologie
- Datenschutz- und Sicherheitsbedenken durch den Einsatz von Blockchain-Technologie
- Zu hohe Komplexität der Thematik
- Andere (Textfeld):

Ich sehe keine Gründe gegen die vorgeschlagene Lösung

Keine Antwort

---

## Anhang II: Protokoll Datenaufbereitung & Datenvalidierung

Der aus der *Qualtrics*<sup>TM</sup> XM-Plattform am 09.04.2022 exportierte Rohdatensatz mit 2'028 Datensätzen wurde wie folgt aufbereitet und validiert:

- Nicht benötigte Datenspalten mit automatisch durch die *Qualtrics*<sup>TM</sup> XM-Plattform erfassten Metadaten wurden entfernt.
- 268 nicht vollständig ausgefüllte Datensätze (Attribute *Progress*  $\neq 100$  und *Finished*  $\neq True$ ) wurden entfernt. Im Datensatz verbleiben 1'760 vollständig ausgefüllte Datensätze.
- 4 durch die *Qualtrics*<sup>TM</sup> XM-Plattform als *doppelte Teilnehmer* oder *mögliche Bots* angezeigte Datensätze wurden manuell überprüft und entfernt. Im Datensatz verbleiben 1'756 vollständig ausgefüllte Datensätze.
- 11 Datensätze wurde aufgrund von inkonsistenten Angaben entfernt. Im Datensatz verbleiben 1'745 vollständig ausgefüllte Datensätze.
- 1 am 30.03.2022 zur finalen Validierung und Freigabe der Umfrage erstellter Testdatensatz wurde entfernt. Es verbleiben 1'744 vollständig ausgefüllte Datensätze.
- 14 Datensätze von Teilnehmenden, welche die schweizerische Staatsbürgerschaft nicht besitzen und somit zum jetzigen Zeitpunkt bei einer erneuten E-ID-Vorlage nicht abstimmen könnten, wurden entfernt. Im Datensatz verbleiben 1'730 vollständig ausgefüllte Datensätze.
- Die Frage Q2.5 „Was ist Ihr derzeit höchster Bildungsabschluss?“ erlaubte neben einer vorgefertigten Auswahl an Bildungskategorien die manuelle Eingabe von Bildungsabschlüssen über ein Textfeld „Anderer Abschluss“. Diese Eingabe wurde von 28 Teilnehmenden genutzt. Manuelle Texteingaben, welche eindeutig einer der vorgefertigten Bildungskategorien zuzuordnen waren, wurden entsprechend angepasst. Manuelle Texteingaben, welche keiner Kategorie zuzuordnen waren, wurden der Bildungskategorie „Andere“ zugeordnet.
- Die Frage Q3.1 „Welcher der folgenden Parteien fühlen Sie sich am stärksten verbunden?“ erlaubte neben einer vorgefertigten Auswahl an Parteien die manuelle Eingabe von Parteien über ein Textfeld „Andere“. Diese Eingabe wurde von 51 Teilnehmenden genutzt. Manuelle Texteingaben, welche eindeutig einer der vorgefertigten Parteien zuzuordnen waren, wurden entsprechend angepasst. Manuelle Texteingaben, welche keiner Partei zuzuordnen waren, wurden der Kategorie „Andere“ zugeordnet.

---

### Anhang III: Ungewichtete & gewichtete Kontingenzanalysen nach Pearson und Korrelationsanalysen nach Spearman

Kontingenzanalyse der ungewichteten Stichprobe nach *Pearson*.

	Geschlecht		Sprache		Alter		Bildung		Partei	
	CC	p-Val	CC	p-Val	CC	p-Val	CC	p-Val	CC	p-Val
Q4.1	0.160	0.000	0.109	0.000	0.143	0.000	0.109	0.051	0.304	0.000
Q8.1	0.184	0.000	0.093	0.002	0.273	0.000	0.160	0.000	0.186	0.000
Q9.1	0.076	0.980	0.088	0.062	0.091	0.411	0.154	0.045	0.283	0.000
	n = 1'730		n = 1'730		n = 1'730		n = 1'730		n = 1'730	

Korrelationsanalyse der ungewichteten Stichprobe nach *Spearman*.

	Geschlecht		Sprache		Alter		Bildung		Partei	
	r <sub>s</sub>	p-Val								
Q5.2_1	-0.084	0.000	0.023	0.341	0.014	0.571	0.004	0.873	0.098	0.000
Q5.3_1	-0.078	0.001	-0.077	0.001	0.115	0.000	-0.040	0.093	-0.008	0.727
Q5.4_1	-0.084	0.000	-0.139	0.000	0.165	0.000	-0.048	0.048	-0.052	0.029
Q5.5_1	-0.125	0.000	-0.153	0.000	0.099	0.000	0.040	0.100	-0.047	0.052
Q6.2_1	-0.106	0.000	-0.023	0.341	0.083	0.001	0.037	0.127	-0.042	0.080
Q6.3_1	-0.070	0.003	-0.038	0.117	0.086	0.000	-0.021	0.384	-0.021	0.374
Q6.4_1	-0.040	0.099	0.042	0.082	0.120	0.000	-0.044	0.069	-0.047	0.052
Q7.2_1	-0.089	0.000	-0.093	0.000	-0.044	0.065	0.118	0.000	-0.091	0.000
Q7.2_2	-0.026	0.275	-0.019	0.432	0.131	0.000	-0.018	0.455	-0.075	0.002
Q7.2_3	-0.001	0.978	-0.035	0.140	-0.023	0.334	-0.003	0.915	0.079	0.001
Q7.2_4	-0.087	0.000	-0.047	0.051	0.021	0.378	0.036	0.138	-0.012	0.609
Q7.3_1	-0.077	0.001	-0.089	0.000	0.196	0.000	-0.025	0.303	-0.087	0.000
Q7.4_1	-0.089	0.000	-0.077	0.001	0.134	0.000	0.014	0.567	-0.077	0.001
Q8.3_1	-0.205	0.000	-0.105	0.000	-0.202	0.000	0.144	0.000	-0.021	0.386
Q8.4_1	-0.214	0.000	-0.046	0.056	-0.167	0.000	0.121	0.000	0.001	0.968
Q8.5_1	0.149	0.000	-0.009	0.704	0.075	0.002	-0.121	0.000	0.054	0.026
Q8.6_1	-0.106	0.000	0.008	0.730	0.003	0.916	0.013	0.580	-0.032	0.184
Q8.7_1	-0.175	0.000	-0.061	0.011	-0.110	0.000	0.103	0.000	-0.050	0.038
Q8.8_1	-0.126	0.000	-0.025	0.303	-0.008	0.725	0.050	0.037	-0.039	0.108
Q9.3_1	-0.043	0.072	-0.002	0.940	-0.030	0.214	0.010	0.690	0.060	0.013
Q9.4_1	0.037	0.125	-0.073	0.002	-0.038	0.114	0.000	0.991	0.097	0.000
Q9.5_1	-0.013	0.576	0.047	0.048	0.061	0.011	-0.055	0.023	0.077	0.001
Q10.2_1	-0.119	0.000	-0.006	0.815	0.041	0.087	0.055	0.021	-0.045	0.063
Q10.5_1	-0.071	0.003	-0.093	0.000	0.028	0.239	0.021	0.374	-0.003	0.891
Q10.6_1	-0.107	0.000	-0.075	0.002	0.050	0.039	0.056	0.020	-0.032	0.178
Q10.7_1	-0.098	0.000	-0.069	0.004	0.074	0.002	0.001	0.955	-0.054	0.024
Q10.8_1	-0.098	0.000	-0.085	0.000	0.050	0.037	0.020	0.411	-0.087	0.000
Q11.2_1	-0.119	0.000	-0.062	0.010	0.023	0.329	0.049	0.043	-0.069	0.004
Q11.3_1	-0.128	0.000	-0.044	0.067	-0.022	0.352	0.024	0.318	0.050	0.037
	n = 1'730		n = 1'730		n = 1'730		n = 1'730		n = 1'730	

Kontingenzanalyse der gewichteten Stichprobe nach *Pearson*.

	Geschlecht		Sprache		Alter		Bildung		Partei	
	CC	p-Val	CC	p-Val	CC	p-Val	CC	p-Val	CC	p-Val
Q4.1	0.195	0.000	0.135	0.000	0.189	0.000	0.137	0.001	0.339	0.000
Q8.1	0.281	0.000	0.095	0.001	0.221	0.000	0.240	0.000	0.206	0.000
Q9.1	0.139	0.034	0.097	0.022	0.085	0.559	0.210	0.000	0.323	0.000
	n = 1'730		n = 1'730		n = 1'730		n = 1'730		n = 1'730	

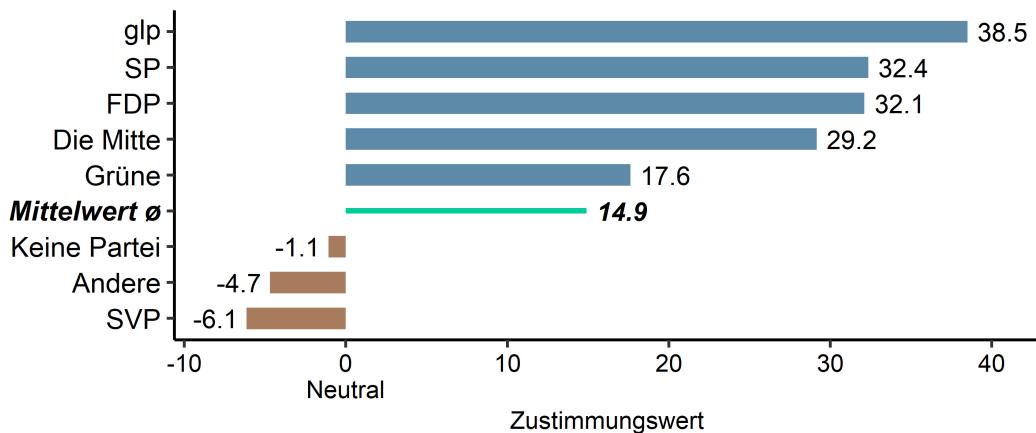
Korrelationsanalyse der gewichteten Stichprobe nach *Spearman*.

	Geschlecht		Sprache		Alter		Bildung		Partei	
	r <sub>s</sub>	p-Val								
Q5.2_1	-0.043	0.085	0.022	0.381	0.024	0.331	0.056	0.025	0.051	0.038
Q5.3_1	-0.025	0.319	-0.091	0.000	0.138	0.000	-0.030	0.227	-0.061	0.014
Q5.4_1	-0.015	0.552	-0.129	0.000	0.161	0.000	-0.026	0.287	-0.119	0.000
Q5.5_1	-0.064	0.010	-0.069	0.006	0.121	0.000	0.045	0.068	-0.115	0.000
Q6.2_1	-0.081	0.001	-0.023	0.364	0.123	0.000	0.053	0.034	0.049	0.050
Q6.3_1	-0.056	0.024	-0.037	0.137	0.089	0.000	-0.004	0.875	-0.022	0.367
Q6.4_1	-0.005	0.854	0.018	0.465	0.110	0.000	-0.067	0.007	-0.050	0.043
Q7.2_1	-0.019	0.436	-0.077	0.002	0.019	0.432	0.104	0.000	-0.111	0.000
Q7.2_2	0.036	0.151	-0.024	0.323	0.150	0.000	0.013	0.588	-0.118	0.000
Q7.2_3	0.139	0.000	-0.058	0.019	-0.025	0.323	-0.046	0.066	-0.010	0.700
Q7.2_4	-0.001	0.976	-0.081	0.001	0.036	0.148	0.058	0.020	-0.083	0.001
Q7.3_1	-0.050	0.045	-0.093	0.000	0.220	0.000	-0.039	0.117	-0.094	0.000
Q7.4_1	-0.025	0.305	-0.122	0.000	0.139	0.000	-0.017	0.487	-0.125	0.000
Q8.3_1	-0.246	0.000	-0.126	0.000	-0.135	0.000	0.129	0.000	0.087	0.000
Q8.4_1	-0.272	0.000	-0.061	0.014	-0.113	0.000	0.099	0.000	-0.118	0.000
Q8.5_1	0.170	0.000	-0.027	0.271	0.082	0.001	-0.106	0.000	0.077	0.002
Q8.6_1	-0.112	0.000	-0.015	0.534	-0.024	0.328	0.027	0.269	-0.036	0.141
Q8.7_1	-0.181	0.000	-0.061	0.014	0.079	0.001	0.094	0.000	-0.052	0.036
Q8.8_1	-0.137	0.000	-0.056	0.025	-0.014	0.586	0.062	0.012	-0.044	0.075
Q9.3_1	-0.023	0.363	-0.007	0.792	0.023	0.363	-0.032	0.199	0.078	0.002
Q9.4_1	0.062	0.012	-0.037	0.138	-0.007	0.777	-0.006	0.807	0.101	0.000
Q9.5_1	-0.044	0.074	0.056	0.024	0.058	0.020	-0.046	0.066	0.156	0.000
Q10.2_1	-0.130	0.000	-0.042	0.086	0.046	0.066	0.054	0.029	-0.055	0.028
Q10.5_1	-0.046	0.065	-0.102	0.000	0.002	0.923	0.025	0.321	0.001	0.953
Q10.6_1	-0.074	0.003	-0.077	0.002	0.064	0.010	0.069	0.005	-0.075	0.002
Q10.7_1	-0.075	0.002	-0.060	0.015	0.092	0.000	0.004	0.868	-0.097	0.000
Q10.8_1	-0.062	0.012	-0.046	0.063	0.140	0.000	0.017	0.505	-0.089	0.000
Q11.2_1	-0.073	0.003	-0.063	0.011	0.061	0.014	0.051	0.041	0.130	0.000
Q11.3_1	-0.105	0.000	-0.071	0.004	0.045	0.072	0.018	0.470	0.021	0.388
	n = 1'730		n = 1'730		n = 1'730		n = 1'730		n = 1'730	

---

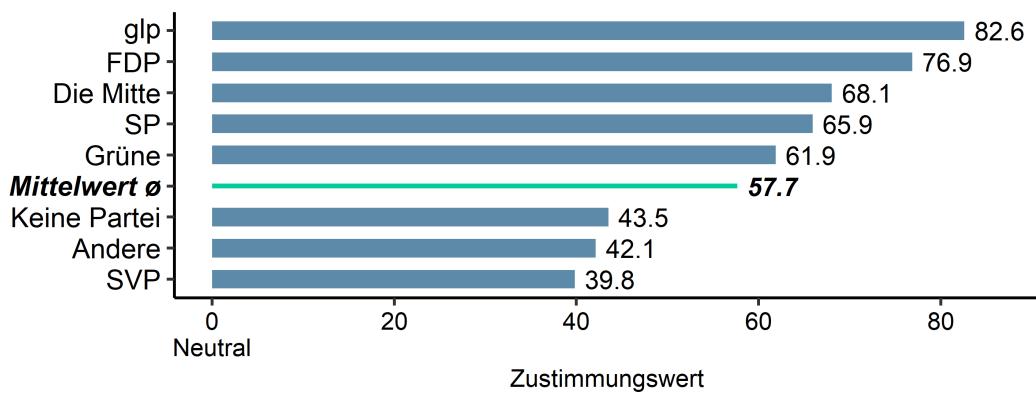
## Anhang IV: Zusätzliche statistische Auswertungen - Deskriptive Datenauswertungen

Q5.4 Ich glaube, dass meine Identitätsdaten beim Gebrauch einer rein staatlichen E-ID im Internet sicher sind.



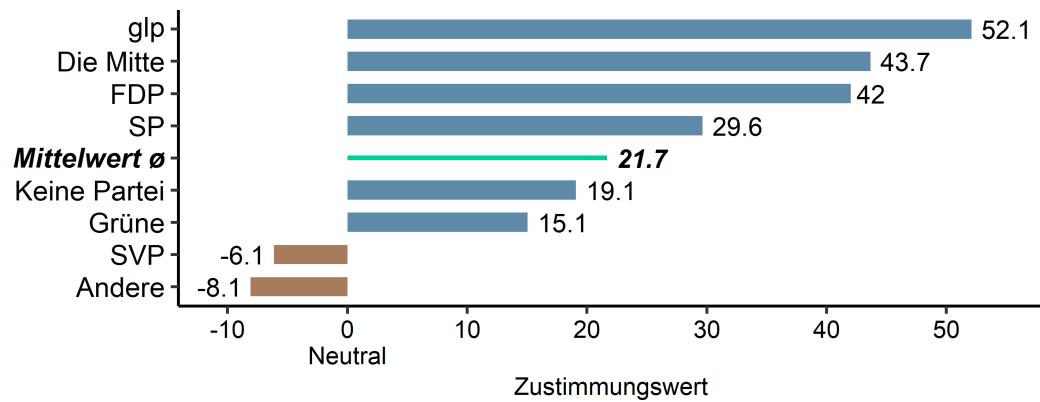
Auswertung der Fragestellung Q5.4.

Q7.2 Folgende elektronischen Dienstleistungen des öffentlichen Sektors und der Demokratie sind mir wichtig. - Virtuelle Behördenshalter (elektronische Steuererklärung, elektronischer Bezug von Registerauszügen, elektronische An-/Abmeldung der Wohngemeinde bei einem Umzug, etc.)



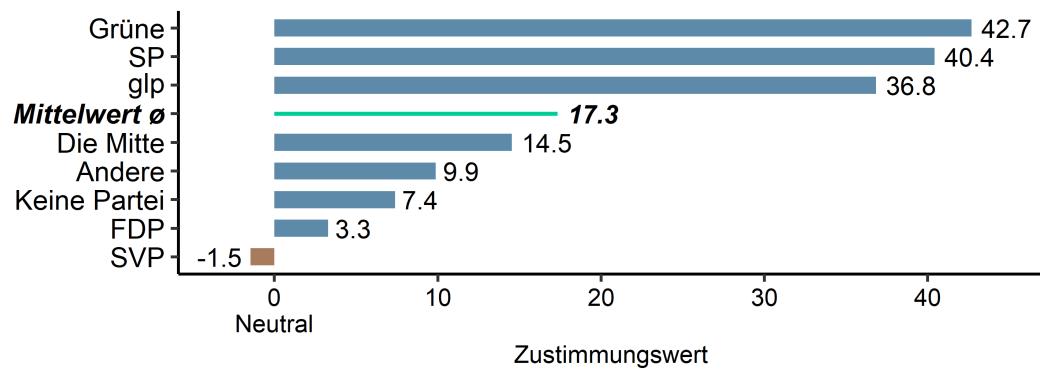
Auswertung der Fragestellung Q7.2 - Virtuelle Behördenshalter.

Q7.2 Folgende elektronischen Dienstleistungen des öffentlichen Sektors und der Demokratie sind mir wichtig. - Elektronisches Abstimmen und Wählen (E-Voting)



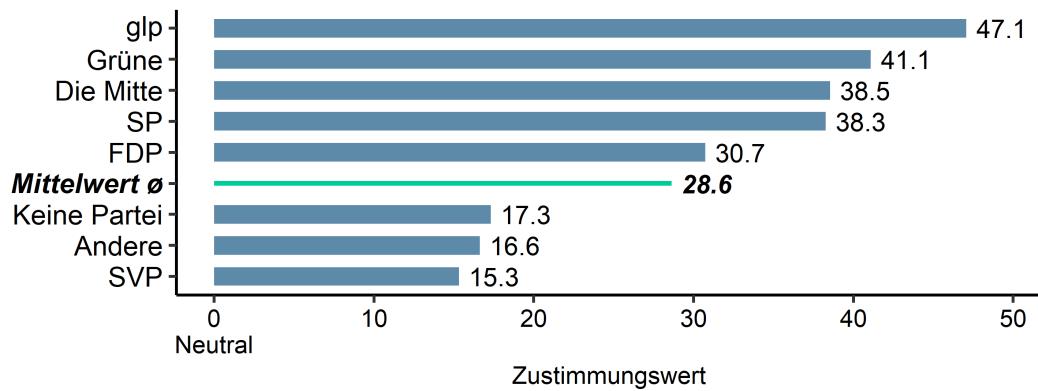
Auswertung der Fragestellung Q7.2 - E-Voting.

Q7.2 Folgende elektronischen Dienstleistungen des öffentlichen Sektors und der Demokratie sind mir wichtig. - Elektronisches Unterschriften sammeln für Initiativen und Referenden (E-Collecting)



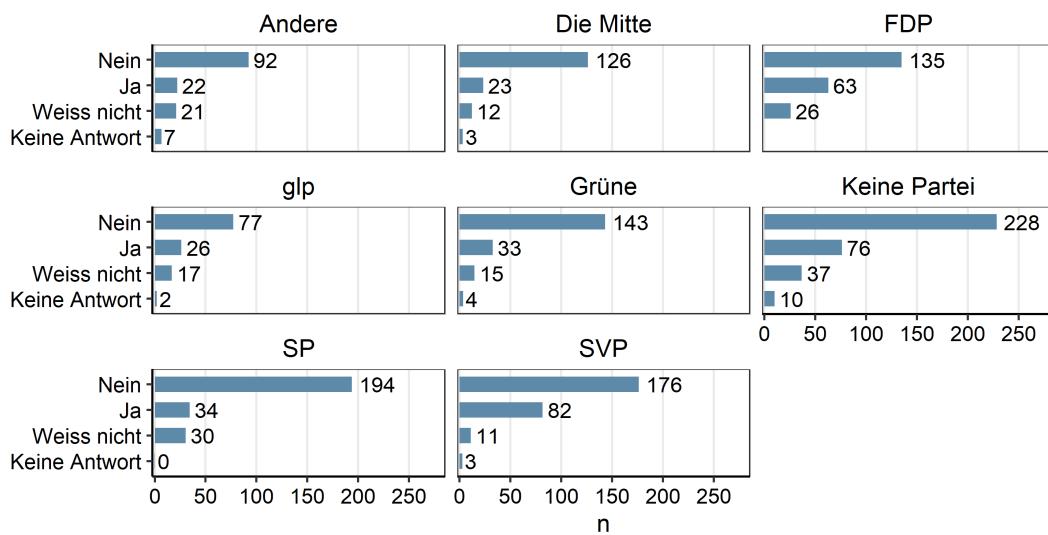
Auswertung der Fragestellung Q7.2 - E-Collecting.

Q7.2 Folgende elektronischen Dienstleistungen des öffentlichen Sektors und der Demokratie sind mir wichtig. - Elektronische Partizipation an politischen und demokratischen Prozessen (E-Partizipation, bspw. im Rahmen von Verkehrs- oder Bauprojekten)



Auswertung der Fragestellung Q7.2 - E-Partizipation.

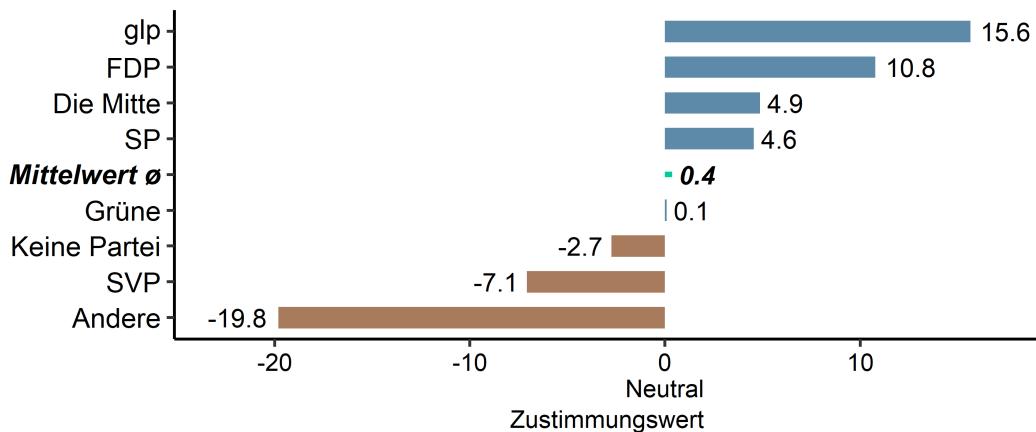
Q8.1 Hatten Sie in Ihrem Alltag oder beruflichen Umfeld bereits einmal mit der Blockchain-Technologie (Distributed-Ledger-Technologie DLT) zu tun oder diese selbst genutzt (bspw. durch Kryptowährungen oder andere Anwendungen)?



Auswertung der Fragestellung Q8.1 nach Partei.

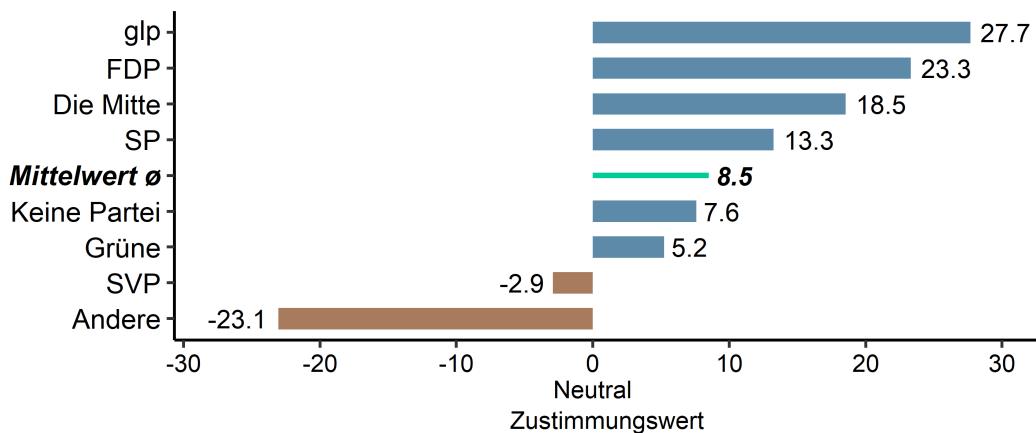
---

Q8.6 Ich vertraue Anwendungen grundsätzlich, wenn diese Blockchain-Technologie in kompetenter Weise nutzen.



Auswertung der Fragestellung Q8.6.

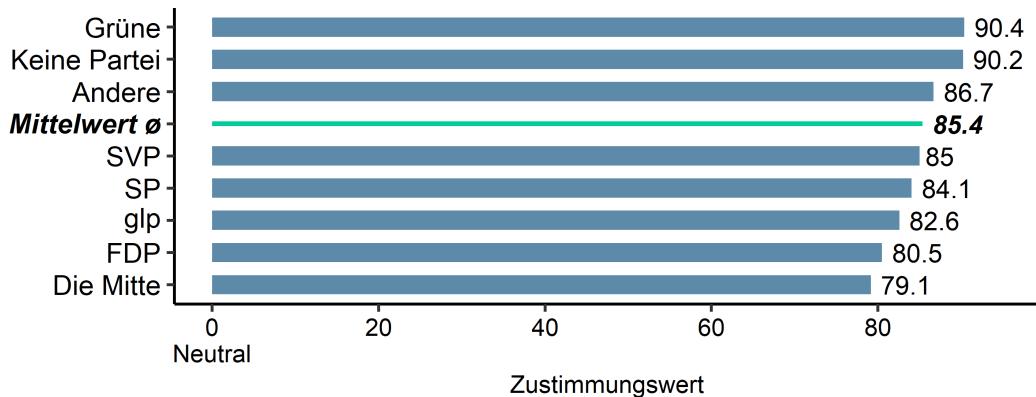
Q8.8 Der Staat sollte innovative Technologien wie die Blockchain-Technologie vermehrt einsetzen.



Auswertung der Fragestellung Q8.8.

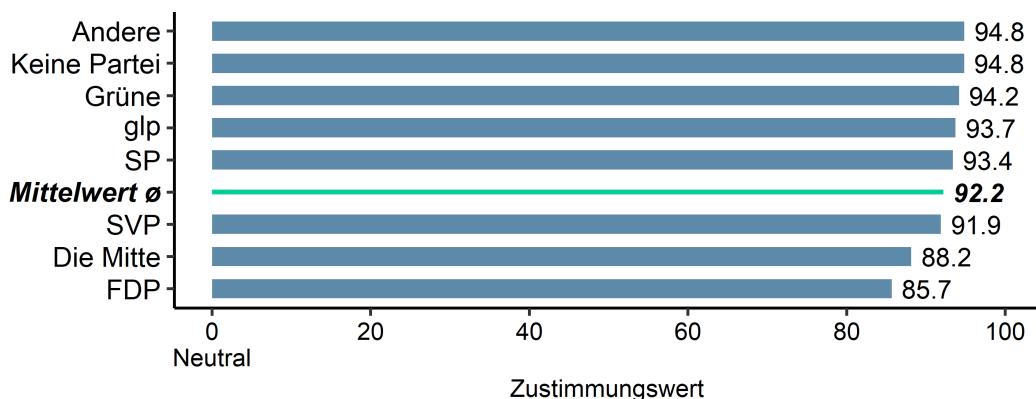
---

Q9.3 Bei der Verwendung von digitalen Anwendungen sollte ich selbst bestimmen können, mit wem meine Identitätsdaten geteilt werden.



Auswertung der Fragestellung Q9.3.

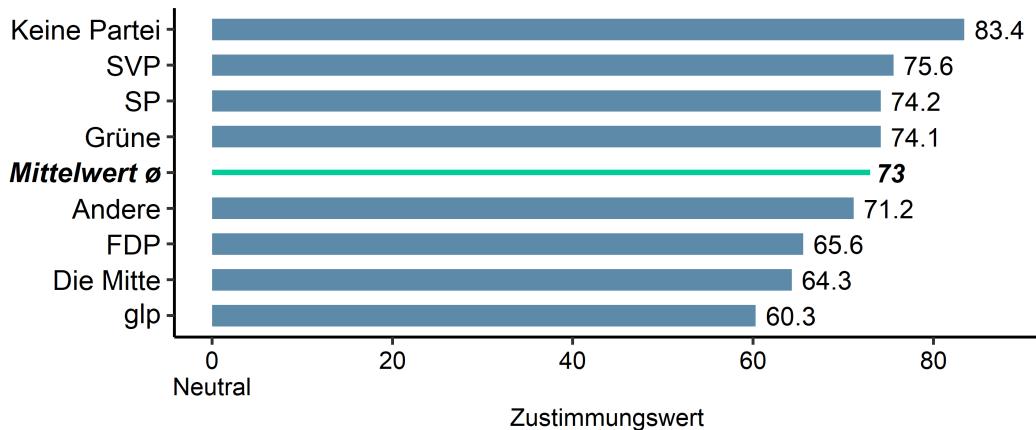
Q9.4 Bei der Verwendung von digitalen Anwendungen sollte ich transparent nachvollziehen können, wie meine Identitätsdaten verwendet werden.



Auswertung der Fragestellung Q9.4.

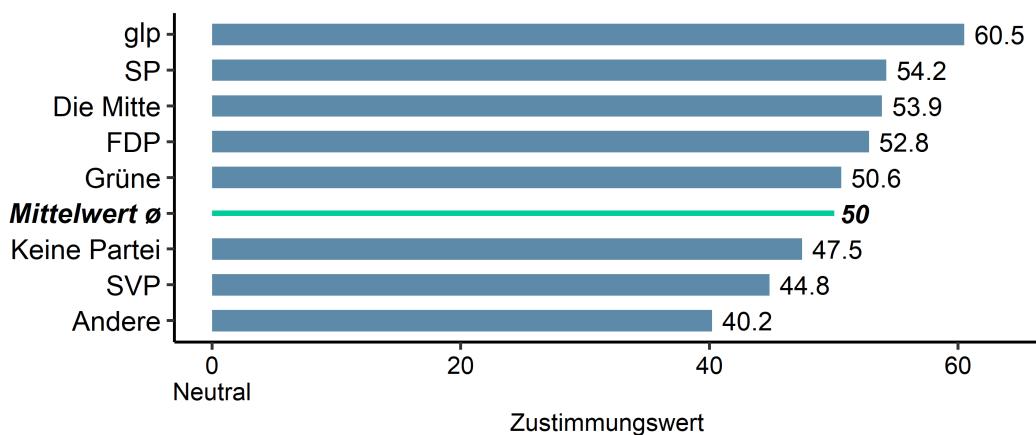
---

Q9.5 Ich sollte im digitalen Raum die alleinige Datenhoheit und Kontrolle über meine Identitätsdaten besitzen.



Auswertung der Fragestellung Q9.5.

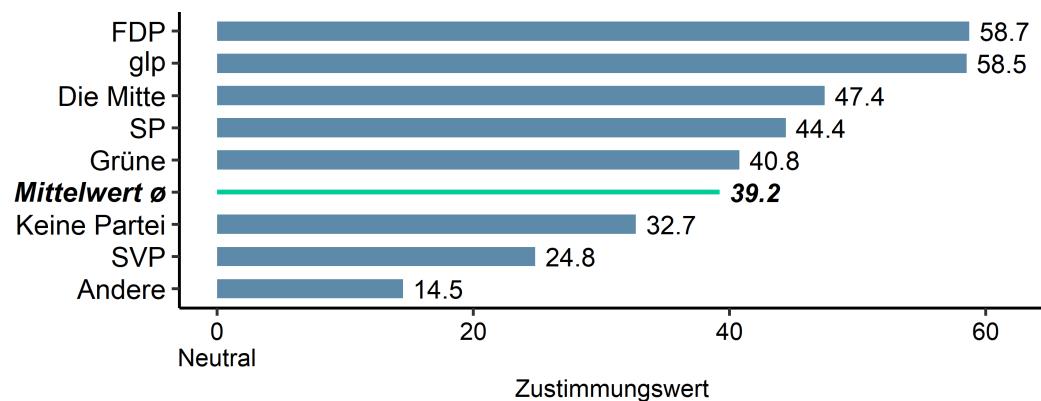
Q10.5 Das Konzept der vollständig selbstbestimmten Verwaltung von Identitätsdaten ist für mich verständlich.



Auswertung der Fragestellung Q10.5.

---

Q10.6 Das Konzept der vollständig selbstbestimmten Verwaltung von Identitätsdaten durch Blockchain-Technologie finde ich interessant.



Auswertung der Fragestellung Q10.6.

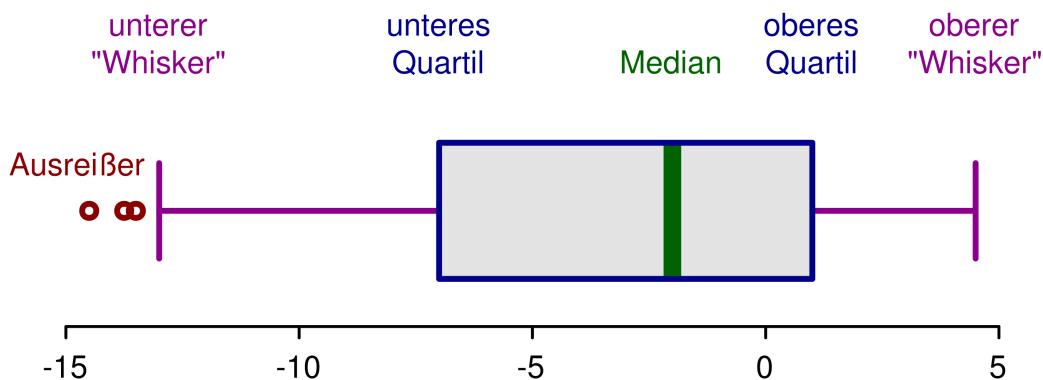
---

## Anhang V: Hilfestellung Interpretation Box-Whisker-Plot & Violin-Diagramm

### Box-Whisker-Plot

Die Hilfestellung zur Interpretation des *Box-Whisker-Plots* wird als Direktzitat aus der freien Enzyklopädie *Wikipedia* zitiert [Wikipedia - Diverse Autor:innen 2021]:

„Der *Box-Plot* (auch *Box-Whisker-Plot* oder deutsch *Kastengrafik*) ist ein Diagramm, das zur grafischen Darstellung der Verteilung eines mindestens ordinal-skalierten Merkmals verwendet wird. Es fasst dabei verschiedene robuste Streuungs- und Lagemasse in einer Darstellung zusammen. Ein *Box-Plot* soll schnell einen Eindruck darüber vermitteln, in welchem Bereich die Daten liegen und wie sie sich über diesen Bereich verteilen. Deshalb werden alle Werte der sogenannten Fünf-Punkte-Zusammenfassung, also der Median, die zwei Quartile und die beiden Extremwerte, dargestellt.“



Generisches Beispiel eines Box-Plots [Wikipedia - Diverse Autor:innen 2021].

In der Tabelle auf der nächsten Seite ist eine Zusammenfassung der Kennwerte eines Box-Plots einsehbar.

---

Zusammenfassung der Kennwerte Box-Plot [Wikipedia - Diverse Autor:innen 2021].

Kennwert	Beschreibung	Lage im Box-Plot
Minimum	Kleinster Datenwert des Datensatzes	Ende eines Whiskers oder entferntester Ausreisser
Unteres Quartil	Die kleinsten 25 % der Datenwerte sind kleiner als dieser oder gleich diesem Kennwert	Beginn der Box
Median	Die kleinsten 50 % der Datenwerte sind kleiner als dieser oder gleich diesem Kennwert	Strich innerhalb der Box
Oberes Quartil	Die kleinsten 75 % der Datenwerte sind kleiner als dieser oder gleich diesem Kennwert	Ende der Box
Maximum	Grösster Datenwert des Datensatzes	Ende eines Whiskers oder entferntester Ausreisser
Spannweite	Gesamter Wertebereich des Datensatzes	Länge des gesamten Box-Plots (inklusive Ausreisser)
Interquartilsabstand	Wertebereich, in dem sich die mittleren 50 % der Daten befinden. (Liegt zwischen dem 0,25- und dem 0,75-Quartil.)	Ausdehnung der Box

---

## **Violin-Diagramm**

Die Hilfestellung zur Interpretation des Violin-Diagramms wird als in Deutsch übersetztes Direktzitat aus der freien Enzyklopädie *Wikipedia* zitiert [Wikipedia - Diverse Autor:innen 2022]:

*„Ein Violindiagramm ist eine Methode zur Darstellung von numerischen Daten. Sie entspricht einem Box-Plot, mit dem Zusatz einer gedrehten Darstellung der Kerndichte auf jeder Seite. Violindigramme ähneln Boxdiagrammen, mit dem Unterschied, dass sie auch die Wahrscheinlichkeitsdichte der Daten bei verschiedenen Werten zeigen, normalerweise geglättet durch eine Kerndichte-Schätzung. In der Regel enthält ein Violindiagramm alle Daten, die auch in einem Box-Plot enthalten sind: Eine Markierung für den Median der Daten, eine Box oder eine Markierung, die den Interquartilsbereich angibt, und möglicherweise auch alle Stichprobenpunkte, wenn die Anzahl der Stichproben nicht zu hoch ist.“*

*Ein Violindiagramm ist informativer als ein einfaches Box-Plot. Während ein Box-Plot nur zusammenfassende Statistiken wie Mittelwert oder Median und Interquartilsbereiche anzeigt, zeigt der Violindiagramm die vollständige Verteilung der Daten. Der Unterschied ist besonders nützlich, wenn die Datenverteilung multimodal ist (mehr als eine Spitze). In diesem Fall zeigt ein Violindiagramm das Vorhandensein verschiedener Peaks, ihre Position und die relative Amplitude.“*

# Danksagung

Herzlich bedanken möchte ich mich bei meiner Betreuungsperson Dr. Daniel Schwarz Badertscher für die stets konstruktive, zielführende und dennoch raumgebende Unterstützung und Zusammenarbeit innerhalb der Master-Thesis und meines gesamten Studiums vom *Bachelor of Science in Wirtschaftsinformatik* bis hin zum *Master of Science in Business Administration*.

Nach bereits mehrfach erfolgreicher und immer spannender Zusammenarbeit im Rahmen von Projekten wie der CASE-Fallstudie<sup>2</sup>, der Bachelor-Thesis<sup>3</sup> und auch innerhalb weiterführender Zusammenarbeit rund um die automatisierte Berichterstellung von *smartvote*-Berichten<sup>4</sup> durfte ich mit meiner Master-Thesis ein weiteres, spannendes Projekt von hochaktueller Relevanz mit Dr. Daniel Schwarz Badertscher erfolgreich zu Ende führen.

Weiter bedanken möchte ich mich für die Möglichkeit zur Nutzung des *smartvote*-Newsletters als Versandkanal meiner Online-Umfrage. Durch die Zustellung meiner Umfrage an eine hohe Anzahl an *smartvote*-Abonnent:innen konnte ich eine im Kontext von Master-Thesen verhältnismässig umfangreiche Stichprobe erlangen. Erst durch diese breite Datenbasis war es überhaupt möglich, die herausfordernde Gewichtung der Stichprobe sinnvoll vorzunehmen und eine empirische Forschung mit Relevanz für die schweizerische Bevölkerung durchzuführen.

Ebenfalls möchte ich mich herzlich bei meiner Familie für ihre Unterstützung in Form des Korrektorats meiner Master-Thesis bedanken.

Abschliessend hoffe ich, durch meine Master-Thesis eine Forschungsarbeit hervorgebracht zu haben, welche unter wissenschaftlichen Gesichtspunkten einen wertvollen Beitrag für die wissenschaftliche Community als auch für sämtliche an den Thematiken dieser Master-Thesis interessierten Personen im Allgemeinen leisten konnte.

---

<sup>2</sup>[https://drive.google.com/file/d/1yjGEvK6\\_d7MkXGPW2zU2vyHaXZUv0p8i/view?usp=sharing](https://drive.google.com/file/d/1yjGEvK6_d7MkXGPW2zU2vyHaXZUv0p8i/view?usp=sharing)

<sup>3</sup>[https://drive.google.com/file/d/1Fmrbt9ErkyN0H1dl5xp7h1gmVD8\\_9nsz/view?usp=sharing](https://drive.google.com/file/d/1Fmrbt9ErkyN0H1dl5xp7h1gmVD8_9nsz/view?usp=sharing)

<sup>4</sup><https://github.com/wackt1>

## **Eidesstattliche Erklärung**

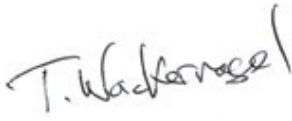
Hiermit erkläre ich, die vorliegende Master-Thesis eigenständig und ohne Benutzung anderer als der innerhalb dieser Master-Thesis und im Literaturverzeichnis angegebenen Quellen und Hilfsmittel angefertigt zu haben. Die Stellen der Arbeit, die anderen Werken dem Wortlaut oder dem Sinne nach entnommen sind, sind als Zitate gekennzeichnet und mit dem genauen Hinweis auf ihre Herkunft versehen.

Umfang dieser Arbeit von der Einleitung bis und mit der Konklusion (Titelblatt, Abstract, Management Summary, sämtliche Verzeichnisse, Anhang, Danksagung, Selbstreflexion und Eidesstattliche Erklärung ausgenommen):

114 Seiten, 33'692 Wörter, 232'753 Zeichen exkl. Leerzeichen.

Ort, Datum: Allschwil, 05.06.2022

Unterschrift:

  
Tim Wackernagel