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

4

Polit-ökonomische Evaluation einer Blockchain-basierten Identitätsnachweislösung

Tim Wackernagel und Daniel Schwarz

Zusammenfassung

Die digitale ID gilt als wichtige Voraussetzung zur Realisierung ökonomischer, sozialer und politischer Potenziale in einer digitalen Welt. Nach der Ablehnung der E-ID-Vorlage in einer Volksabstimmung am 7. März 2021 versucht die Schweizer Politik, im Rahmen der Konzeption neuer E-ID-Lösungen die Interessen von Wissenschaft, Wirtschaft und Zivilgesellschaft besser zu berücksichtigen. Der Beitrag befasst sich mit einem E-ID-Lösungsansatz auf der Basis von Blockchain-Technologie. Die Forschungsergebnisse einer quantitativ-empirischen Befragung unter 1730 Stimmberechtigten zeigen, dass die Bevölkerung einer derartigen Lösung positiv gegenüberstehen würde. Dieser Befund gilt sowohl geschlechter-, sprach- als auch annähernd parteiübergreifend. Ferner zeigt sich, dass die Bevölkerung dem Einsatz der Blockchain-Technologie auch in anderen Anwendungsbereichen nicht generell ablehnend gegenübersteht und die teils vorhandene Skepsis mittels allgemein verständlicher Erklärungen zu überwinden ist.

T. Wackernagel
Basel-Landschaft, Schweiz

D. Schwarz (✉)
Berner Fachhochschule Wirtschaft, Bern, Schweiz
E-Mail: daniel.schwarzbadertscher@bfh.ch

K. O. Tokarski et al. (Hrsg.), *Transformationen gestalten*,
https://doi.org/10.1007/978-3-658-42775-7_4

4.1 Einleitung

Die digitale ID gilt als wichtige Voraussetzung für die Realisierung ökonomischer, sozialer und politischer Potenziale in einer digitalen Welt. Die Einführung von Lösungen zum eindeutigen und sicheren digitalen Identitätsnachweis ist deshalb unausweichlich. Dies gilt nicht nur für privatwirtschaftliche Anwendungen, sondern auch im öffentlichen Sektor.

Am 7. März 2021 hat die Bevölkerung der Schweiz in einer Volksabstimmung die Gesetzesgrundlage für einen elektronischen[1] Identitätsnachweis (E-ID) abgelehnt. Als Folge davon versucht die Politik, im Rahmen der Konzeption neuer E-ID-Lösungen das Fachwissen und die Interessen von Wissenschaft, Wirtschaft und Zivilgesellschaft besser zu berücksichtigen. Denn die E-ID kann als richtungsweisender Enabler einer tiefgreifenderen Transformation der digitalen Wirtschaft und Demokratie nur erfolgreich sein, wenn sie von der Bevölkerung akzeptiert wird.

Das abgelehnte 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). Der Widerstand der Bevölkerung basierte gemäß der gfs.bern-Studie (gfs.bern, 2021) auf zwei Motiven: Datenschutzbedenken sowie die Erwartungen an die Rolle des Staats im Rahmen von Identitätsausweisen bzw. Skepsis gegenüber privaten Unternehmen als Herausgeber:innen der E-ID (S. 30). Gleichzeitig kommt die Studie zum Schluss, dass das ablehnende Votum der Bevölkerung nicht als Digitalisierungs- oder Fortschrittskritik zu deuten sei (S. 5 und 31–32). Fast zwei Drittel der Bürger:innen assoziieren mit einer rein staatlichen E-ID-Lösung eine garantierte Einhaltung des Datenschutzes und würden einer E-ID-Lösung zustimmen, wenn deren Konzept ihr Vertrauen gewinnen kann.

Für die Digitalisierung des Staats und der schweizerischen Demokratie heißt dies, dass der Staat die Rollenerwartung seitens der Bürger:innen erfüllen muss. Zudem muss die technische Lösung für den digitalen Identitätsnachweis Vertrauen und Transparenz schaffen können. An diesem Punkt kommt die Technologie der Blockchain ins Spiel, die sich als eine Alternative zu der im abgelehnten Gesetz vorgesehenen Lösung anbietet. Gleichzeitig schlägt der Technologie aufgrund ihrer Verbindung zu Kryptowährungen wie dem Bitcoin in der Öffentlichkeit auch viel Skepsis entgegen. Es stellt sich somit die Frage, ob eine Blockchain-basierte digitale Identitätsnachweislösung innerhalb der Bevölkerung der Schweiz auf Akzeptanz stoßen könnte. Damit einhergehend stellen sich Fragen rund um die Wahrnehmung sowie Einstellung der schweizerischen Bevölkerung gegenüber der Blockchain-Technologie und insbesondere gegenüber dem Einsatz von Blockchain-Technologie zum Zwecke eines digitalen Identitätsnachweises.

[1] Die Begriffe elektronisch und digital lassen sich im Kontext des Identitätsnachweises als Synonyme verstehen.

Dieser Beitrag basiert auf der wissenschaftlichen Arbeit von Wackernagel (2022) mit dem Titel „*Die Blockchain-ID: Eine mehrheitsfähige Lösung für den digitalen Identitätsnachweis innerhalb der schweizerischen Demokratie?*“ und befasst sich mit einem alternativen E-ID-Lösungsansatz auf Basis der Blockchain-Technologie. Um die aufgestellten Fragestellungen zu beantworten, widmet sich der Beitrag in einem ersten Schritt den theoretischen Grundlagen der (digitalen) Identität, der Blockchain-Technologie sowie möglichen Chancen und Risiken eines Blockchain-Identitätsnachweises. In einem zweiten Schritt werden die Ergebnisse einer quantitativ-empirischen Umfrage unter 1730 Schweizer Stimmberechtigten über die Haltung gegenüber einer staatlichen und Blockchain-basierten E-ID-Lösung präsentiert. Dieser empirische Teil hat zum Ziel, die Einstellung von in der Schweiz stimmberechtigten Personen gegenüber diversen Fragestellungen rund um eine Blockchain-basierte Identitätsnachweislösung empirisch zu erfassen. Der Beitrag schließt mit den Schlussfolgerungen und einem Ausblick.

4.2 Theoretischer Teil

Um einen theoretischen Wissensrahmen rund um die Thematik des digitalen Identitätsnachweises zu schaffen, werden im Folgenden grundlegende Begriffe und Konzepte erläutert, die für das Verständnis der digitalen Identität und der Blockchain-Technologie zentral sind.

4.2.1 Definition zentraler Begriffe

Zu den nachfolgend erläuterten Begriffen gehören die *Identität*, die *digitale Identität* sowie das *Identitätsmanagement*. Ebenfalls definiert wird der Begriff der *Blockchain-Technologie*. Eines der zentralen Ziele der Synthese von digitaler Identität und Blockchain-Technologie ist die Realisierung von selbstbestimmter Identität im digitalen Raum, der sog. *Self-Sovereign Identity*.

4.2.1.1 Identität, digitale Identität und Identitätsmanagement

Der Begriff der Identität wird in der Literatur sowohl aus ideengeschichtlicher, philosophischer und rechtlicher Perspektive als sehr vielschichtig und nicht eindeutig definierbar beschrieben (vgl. Nicke, 2018; Sullivan & Burger, 2019, S. 235; Zwitter et al., 2020, S. 3). Dennoch ist es wichtig, im Rahmen dieses Beitrags ein relevantes und einheitliches Verständnis des Begriffs zu schaffen. Identität wird hier als ein Kernelement zur eindeutigen Identifikation von Menschen verstanden. 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, wel-

ches 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 & Windisch, 2018, S. 4).

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. 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 die digitale Identität im Sinne einer Zugangsprämisse 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. Das National Institute of Standards and Technology (NIST) definiert die digitale Identität generell als einzigartige Repräsentation eines in einer digitalen Transaktion beteiligten Subjekts (Grassi et al., 2017, S. 2). Das World Economic Forum (WEF) definiert die digitale Identität als Sammlung von Einzelattributen, welche 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 (2022) 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 Authentifikatoren[2] valide sind und ob diese zur Nutzung von Dienstleistungen berechtigen. Digitales Identitätsmanagement wird hier als Sammlung von Regeln, Prozeduren und technischen Mitteln verstanden, 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).

Auch wenn sich die digitale Identität präziser als der Begriff der allgemeinen Identität definieren lässt, unterliegt sie dennoch einer eigenen Ambiguität: Einerseits kann digitale Identität ein einfaches, anonymes und pseudonymisiertes Log-in im Sinne einer Authentifizierungsmethode beschreiben. Andererseits wird das Konzept der digitalen Identität auch als ein Äquivalent zu einem staatlich anerkannten Ausweisdokument verstanden. Die

[2] Ein Element, das zur Bestätigung der Identität von Subjekten dient.

vorgängige Auslegung des Begriffs als Benutzer-Log-in unterscheidet sich grundlegend davon, wie wir Identität in der physischen Welt interpretieren und handhaben (Toth & Anderson-Priddy, 2019, S. 18; Sullivan, 2016, S. 475). Im digitalen Raum kann eine Entität mehrere digitale Identitäten besitzen. Im Gegensatz dazu basieren Transaktionen in der physischen Welt auf der Prämisse, dass eine Person legitimerweise genau eine Identität besitzt (Sullivan & Burger, 2019, S. 234 f.). In dieser Form ist die digitale Identität als eine dem physischen Ausweisdokument in Form eines Passes gleichwertige Identifikationsmöglichkeit zu betrachten.

4.2.1.2 Blockchain-Technologie

Der Kunstbegriff Blockchain beschreibt eine Technologie, welche Informationen als Kette (Chain) von Blöcken (Block) darstellt (Rauschenbach & Stucki, 2020, S. 7). Ihren Ursprung hat die Blockchain als die der digitalen (Krypto-)Währung Bitcoin zugrundeliegende Technologie, welche inmitten der Finanzkrise 2008 publiziert wurde (Ammous, 2016, S. 1; Poblet et al., S. 1). Als Schöpfer:in von Bitcoin und dem zugehörigen Blockchain-Protokoll gilt die unter dem Pseudonym Satoshi Nakamoto auftretende Person. Nakamoto (2008) beschreibt 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. Die Blockchain-Technologie gilt als die potenziell wichtigste Neuerung seit der Erfindung des Internets selbst (Crosby et al., 2016, S. 8; Efanov & Roschin, 2018, S. 116–120). Während nach Efanov und Roschin (2018) das Internet ermöglicht hat, digitale Geschäftsprozesse zu realisieren, soll 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 Judmayer et al. (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 & Muthukkumarasamy, 2016, S. 1392; Poblet et al., 2020, S. 1–2).

Die Blockchain-Technologie gilt als Vertrauensmaschine (Trust Machine) (Poblet et al., 2020, S. 2), da sie die Fähigkeit besitzt, 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 & Roschin, 2018, S. 116 f.). 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). Transaktionsprozesse auf einer Blockchain sind transparent, rückverfolgbar und manipulationssicher, womit durch die Nutzung einer Blockchain ein robustes Vertrauenssystem aufgebaut werden kann (Yang & Li, 2020, S. 5). Dieses ermöglicht eine sichere Methode, um Güter, Dienstleistungen, Verträge sowie Informationen jeglicher Art auszutauschen und dadurch neue, globale Netzwerke und Geschäftsmodelle aufzubauen (Ahram et al., 2017, S. 1–5; Underwood, 2016, S. 15). Mit diesen und weiteren Eigenschaften birgt die Blockchain das Potenzial, die technologische Basis einer digitalen ID der Zukunft zu stellen.[3]

4.2.1.3 Self-Sovereign Identity

Fragen nach der wahren Identität von Menschen und dem Vertrauen in Identitätssysteme stellen sich der Menschheit schon seit Jahrhunderten (Takemiya & Vanieiev, 2018, S. 582). Neue technische Entwicklungen, allen voran die Entwicklung des Internets, haben das Risikopotenzial im Rahmen von Identitätsdaten und -nachweisen stetig verschärft. Während die Fragmentierung von Identitätsdaten im digitalen Raum 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 & Vanieiev, 2018, S. 582; Wolfond, 2017, S. 36).

Zentralisierte Identitätssysteme bieten den Nutzer:innen zwar meistens eine einfache und bequeme Nutzungserfahrung, unterliegen aber dem technischen Konzept geschuldeten 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, geraten immer stärker in die Kritik (Stokkink & Pouwelse, 2018, S. 1336; Toth & Anderson-Priddy, 2019, S. 17).

Bakre et al. (2017, S. 379 f.) haben vier aufeinander aufbauende Stufen der Entwicklung von digitalen Identitätsmanagementsystemen definiert: Centralized Identity (zentralisierte Identität), Federated Identity (föderierte 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 & Petitcolas, 2018, S. 21). Die Wissenschaft ist sich hingegen im Grundtenor einig, dass neue Lösungen für den digitalen Identitätsnachweis bestrebt sein müssen, die rechtliche Identität wieder in die Hände der besitzenden Person zurückzugeben, was den Aufbau von möglichst dezentralisierten, transparenten und eigenständig verwalt- und kontrollierbaren Identitätssystemen bedingt (Dunphy & Petitcolas,

[3] Für eine tiefgreifende Einführung in die Thematik vgl. Wackernagel (2022) sowie Berentsen und Schär (2017).

2018, S. 21; Lips, 2010, S. 278–279). Wenn Identitäts-besitzende Personen wieder die vollständige Kontrolle über ihre Identitätsdaten erlangen sollen, kommt das Konzept der sogenannten Self-Sovereign Identity zum Zuge (Dunphy & Petitcolas, 2018, S. 21; Stokkink & Pouwelse, 2018, S. 1337).

Self-Sovereign Identity – zu Deutsch sinngemäß als vollständig selbstbestimmte Identität übersetzt – bedeutet, dass Identitätssysteme den Besitzenden einer Identität die Schaffung, Verwaltung, Nutzung und Verteilung der Identität und Identitätsdaten vollständig autonom erlauben (Allen, 2016; Stokkink & Pouwelse, 2018, S. 1336; Takemiya & Vanieiev, 2018, S. 582; Toth & Anderson-Priddy, 2019, S. 18). Davon verspricht man sich große Fortschritte bezüglich der Privatsphäre, dem Datenschutz und der Sicherheit von Identitätsdaten. Das Konzept der Self-Sovereign Identity verlangt nach technischen Lösungen, die in der Lage sind, diesen prinzipiellen Anforderungen gerecht zu werden (Wolfond, 2017, S. 36). Ein mittels Blockchain-Technologie aufgebautes Vertrauenssystem kann diesen hohen Ansprüchen gerecht werden, indem es die Konzeption von (dezentralen) Identitätssystemen erlaubt, welche den Nutzer:innen die vollständige Kontrolle über ihre Identitätsdaten ermöglichen (Rivera et al., 2017, S. 1; Takemiya & Vanieiev, 2018, S. 582).

4.2.2 Digitale Demokratie und 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 jeher 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. 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. Für Lips (2010, S. 275 f.) 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. Als kritisches, bisher vernachlässigtes Element der digitalen Ära bildet die digitale Identität ein Grundstein für das Fortschreiten der digitalen Demokratie.[4]

[4] Als digitale Demokratie werden demokratische Prozesse und Institutionen im digitalen Raum verstanden; spezifisch beinhaltet dies die Informationssuche, -verbreitung und -verarbeitung mit Blick auf politische Entscheidungen, die Meinungsbildung und Entscheidungsfindung sowie die politische Partizipation mittels Wahlen, Abstimmungen und anderen Formen der Bürger:innenbeteiligung (Fivaz & Schwarz, 2021, S. 76 f.).

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, 2018, S. 724). Die 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, gleichzeitig wächst aber auch das Bewusstsein über den Wert und Schutzbedarf ihrer eigenen Identitätsdaten.

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. (2021, S. 52) ermöglicht eine digitale ID zusätzlich die Weiterentwicklung von virtuellen Behördenschaltern. 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 (vgl. Melin et al., 2016, S. 73; Rauschenbach & Stucki, 2020, S. 34; Fivaz & Schwarz, 2021, S. 86).

Um den digitalen Staat in der Schweiz steht es nicht zum Besten (Bühler et al., 2022, S. 3; Fivaz & Schwarz, 2021, S. 77 f.). Obwohl sehr gute technische und rechtliche Rahmenbedingungen vorherrschen, haben Digitalisierungsprojekte in der Schweiz oft einen schweren Stand (Neuroni et al., 2019, S. 177; Fivaz & Schwarz, 2021, S. 77 f. und 86). Zwar bieten die Behörden den Bürger:innen diverse Dienstleistungen auf Bundes-, Kantons- und Gemeindeebene bereits heute digital an, oftmals erfordert dies aber parallel zur Online-Beantragung die analoge Einreichung von weiteren ID-Dokumenten. Ebenfalls großes Potenzial birgt die digitale Identität bei jenen Anwendungen im Rahmen der digitalen Demokratie, welche die zweifelsfreie Feststellung der Identität der stimmberechtigten Person voraussetzen (Cap & Maibaum, 2001, S. 805). Die elektronische Stimmabgabe bei Abstimmungen und Wahlen (E-Voting) ist ein Beispiel für einen solchen Anwendungsfall, welcher erst durch die Existenz einer digitalen ID auf nutzer:innenfreundliche Weise umgesetzt werden kann (Bühler et al., 2022, S. 44). Während dies im derzeitigen analogen Prozess mit individuell adressierten und auf postalischem Wege zugestellten Abstimmungsunterlagen umgesetzt wird, werden 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 aber 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. Im Rahmen des E-Collecting könnte die digitale ID als technisch zwingende Voraussetzung für die Digitalisierung des Unterschriftensammelns den gesamten demokratischen Prozess im Vergleich zur aktuellen Handhabung sogar sicherer und transparenter machen (Fivaz & Schwarz, 2021, S. 91; Bisaz & Serdült, 2017, S. 3). Des Weiteren könnte der Bereich der elektronischen Partizipation (E-Partizipation) profitieren. E-Partizipation bezeichnet die Beteiligung von Bürger:innen mittels digitaler Hilfsmittel an politischen Willensbildungs- und Mitbestimmungsprozessen, die über formelle Wahlen und Abstimmungen hinausgehen (Bühler et al., 2022, S. 44). Durch eine digitale ID könnten neue, die Demokratie stärkende Partizipationsformen realisierbar werden, die auf die Identifizierung von partizipierenden Bürger:innen angewiesen sind.

4.2.3 Chancen und Risiken des Blockchain-basierten Identitätsnachweises

In den vorangehenden Abschnitten wurde die digitale Identität mit technologischen Potenzialen wie der Blockchain-Technologie, dem Konzept der Self-Sovereign Identity sowie den Anforderungen einer modernen, digitalen Verwaltung und Demokratie in Kontext gesetzt. Im Zentrum dieses Kapitels steht die Synthese von digitaler Identität, Blockchain-Technologie ist deren Ziel der Realisierung von selbstbestimmter Identität im digitalen Raum.

Zu allgemeinen Chancen und Vorteilen der Digitalisierung von Identitätsnachweislösungen gehören unter anderem Potenziale in der digitalen Welt der Zukunft wie ökonomische Mehrwerte, neue Geschäftsmodelle, gesteigerte Benutzer:innenfreundlichkeit sowie erhöhte Transparenz und Inklusion (Wackernagel, 2022, S. 10 ff.). 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).

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.

Als spezifische Chancen und Vorteile eines Blockchain-basierten Identitätssystems gelten die Schaffung von Vertrauen und Transparenz, die Gewährleistung von autonomer Kontrolle und Datenhoheit, die Ermöglichung von dezentralen und hochgradig verfügbaren Systemen, Effizienzsteigerungs- und Kosteneinsparungspotenziale sowie vielschichtig positive Eigenschaften in den Bereichen der Daten- und Informationssicherheit (Wackernagel, 2022, S. 47 ff.).

Auf der anderen Seite stehen den generellen sowie Blockchain-spezifischen Chancen der digitalen ID auch generelle sowie Blockchain-spezifische Risiken gegenüber. Generell geltende Risiken der Digitalisierung von Identitätsdaten umfassen die Sicherheit und Integrität von sensiblen Daten bei deren digitaler Speicherung und Transaktion, die Gewährleistung der Verfügbarkeit von Identitätsdaten sowie auch ein inhärentes Missbrauchspotenzial und Risiken der Machtkonzentration durch die zentralisierte Hoheit über digital gespeicherte Identitätsdaten (Wackernagel, 2022, S. 8 ff.).

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 f.). Trotz ihrer revolutionären und vielversprechenden Potenziale sollte die Blockchain-Technologie nicht als Patentlösung für technische Anwendungsbereiche wie Identitätsnachweislösungen betrachtet werden (Dunphy & 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, 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 blindem 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 können und sollten die vorgängig aufgeführten positiven Potenziale eines Blockchain-basierten Identitätsnachweises relativierend hinterfragt werden (Wackernagel, 2022, S. 49 ff.).

4.3 Empirischer Teil

Der empirische Teil dieses Beitrags geht der Frage nach, wie sich die Schweizer Bevölkerung gegenüber der digitalen ID im Allgemeinen und einer Blockchain-basierten E-ID im Besonderen positioniert. Es sollen Erkenntnisse darüber gewonnen werden, ob das Konzept einer Blockchain-Lösung zum Identitätsnachweis in der Schweiz innerhalb der Bevölkerung auf Akzeptanz stoßen könnte. Auch dieser Teil basiert auf der wissenschaftlichen Arbeit von Wackernagel (2022), welche die vollständigen Forschungsergebnisse sowie ausführliche Informationen zu den angewendeten Erhebungs- und Analysemethoden enthält.

4.3.1 Datenerhebung

Die empirische Datenerhebung basiert auf einer Online-Befragung von in der Schweiz stimmberechtigten Personen. Zu diesem Zweck wurde an die Abonnent:innen des Newsletters der Online-Wahlhilfe *smartvote* (Politools, 2022) ein Link zum Online-Fragebogen versendet, der zwischen dem 31. März und 9. April 2022 zur Beantwortung geöffnet war. Insgesamt wurden auf diese Weise 54.529 Newsletter-Abonnent:innen angeschrieben, davon rund 79 % in deutscher Sprache und 21 % in französischer Sprache. Total konnten nach der Aufbereitung 1730 vollständig ausgefüllte und validierte Datensätze als Stichprobe erfasst werden. Die Rücklaufquote der Umfrage, bezogen auf die vollständigen und verwertbaren Datensätze, beträgt somit 3,2 %.

Auch wenn mit der erlangten Datengrundlage kein Anspruch auf Repräsentativität erhoben werden kann, bietet es sich zwecks Ausgleichs statistischer Verzerrungen an, die erhobenen Daten mittels statistischer Gewichtungsverfahren möglichst nahe an die tatsächliche Bevölkerungsstruktur der Schweiz anzugleichen [vgl. für Details Wackernagel (2022, S. 63 ff.)]. Einschränkend zu beachten ist, dass aufgrund der angeschriebenen Grundgesamtheit (Nutzer:innen einer Online-Wahlhilfe) und der Selbstselektion zur Umfrageteilnahme von einem stark überdurchschnittlichen Interesse sowohl an politischen Themen im Allgemeinen als auch an spezifischen Fragestellungen rund um die Thematiken E-ID und Blockchain ausgegangen werden muss. Dieser Verzerrung sollte die Gewichtung entgegenwirken, sodass aussagekräftige Ergebnisse zumindest in Bezug auf die politisch interessierten und sich an politischen Entscheidungen beteiligenden Bevölkerungsteile erzielt werden können.

4.3.2 Einstellung der Bevölkerung zur Blockchain-basierten E-ID

In einem ersten Schritt werden nachfolgend die deskriptiven Ergebnisse ausgewählter Fragestellungen vorgestellt. Sämtliche Auswertungen basieren auf n = 1730 gewichteten Datensätzen. Die Auswertungen werden jeweils nach der in der Umfrage angegebenen Parteinähe der Teilnehmenden dargestellt.

Ein größerer Teil der Fragestellungen verlangte von den Teilnehmenden Angaben in Form von Zustimmungswerten gegenüber unterschiedlichsten Aussagen. Diese Zustimmungswerte lassen sich wie folgt interpretieren:

- Werte > 0 entsprechen einer (durchschnittlichen) Zustimmung zur Aussage. Je näher ein Wert am Maximum von 100 liegt (vollständige Zustimmung), desto stärker fällt die Zustimmung zur Aussage aus.
- Werte = 0 entsprechen im Durchschnitt einer neutralen Haltung gegenüber der Aussage.
- Werte < 0 entsprechen einer (durchschnittlichen) Ablehnung zur Aussage. Je näher ein Wert am Minimum von −100 liegt (vollständige Ablehnung), desto stärker fällt die Ablehnung zur Aussage aus.

4.3.2.1 Vertrauen in den Staat

Die erste Gruppe von Fragestellungen behandelt das Vertrauen der Umfrageteilnehmenden in den Staat im Kontext einer E-ID. Abb. 4.1 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.

Während Anhänger:innen der SVP auch beim Vertrauen in die staatliche Wahl einer passenden Technologie und der Bereitschaft zur Nutzung einer staatlichen E-ID-Lösung (vgl. Abb. 4.2) nur noch knapp positive Zustimmungswerte erreichen, sind Befragte, die sich der glp, Mitte oder FDP nahe fühlen, trotz unterdurchschnittlicher Zustimmung zur staatlichen Herausgabe einer E-ID in überdurchschnittlichem Masse 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.

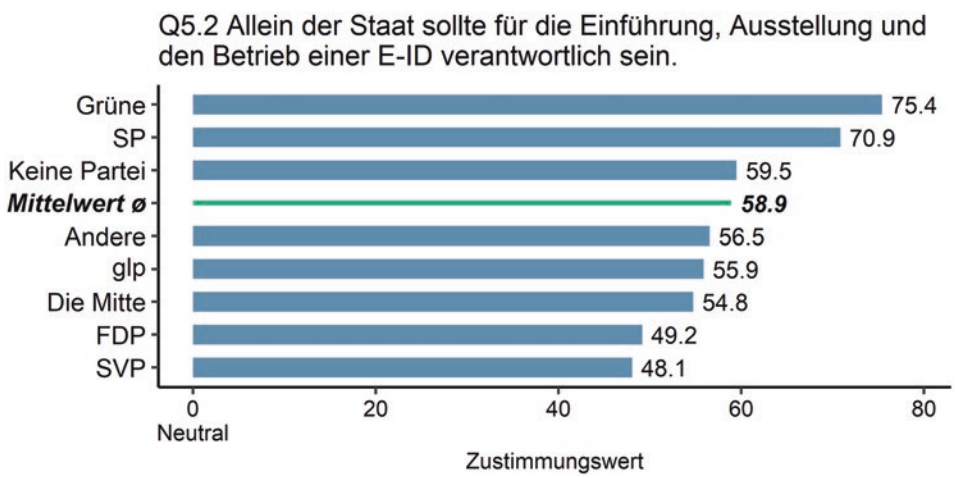

Abb. 4.1 Auswertung der Fragestellung Q5.2

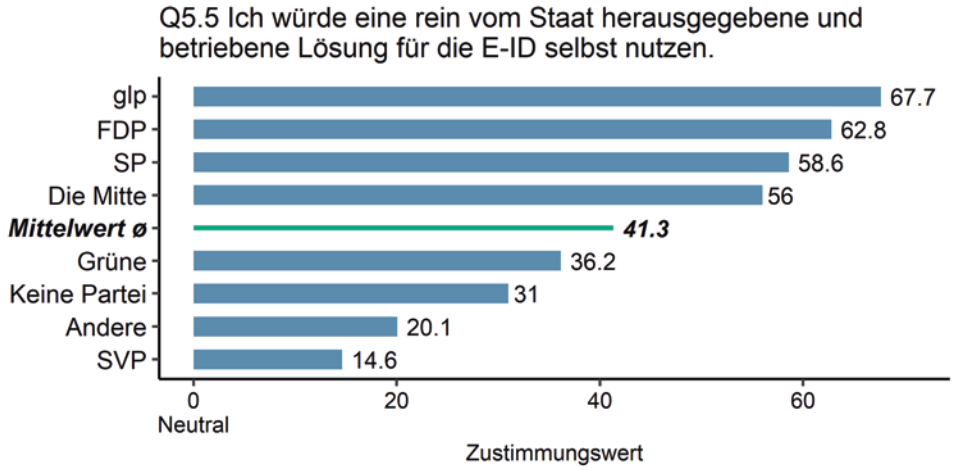

Abb. 4.2 Auswertung der Fragestellung Q5.5

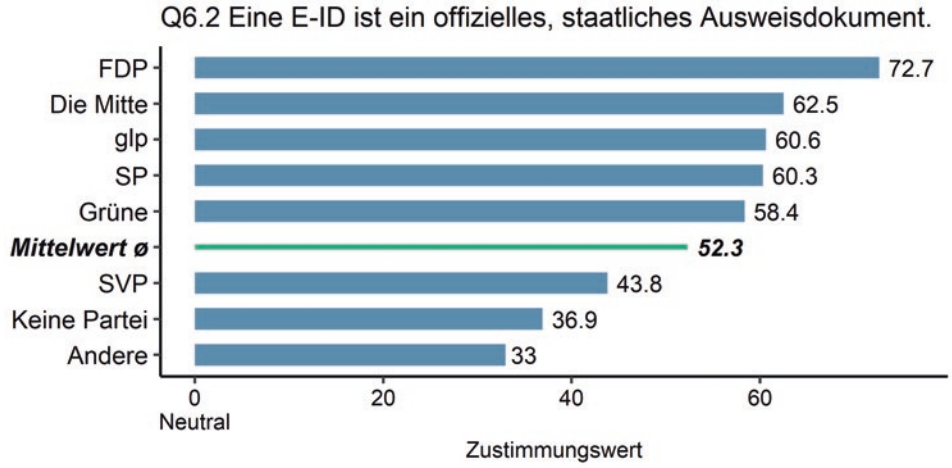

Abb. 4.3 Auswertung der Fragestellung Q6.2

4.3.2.2 Wahrnehmung und Einordnung der digitalen ID

Die Befragten wurden gebeten, ihre Wahrnehmung und Einschätzung hinsichtlich einer digitalen ID im Kontext von Log-in-Lösungen und offiziellen Ausweisdokumenten anzugeben. Dabei bestätigt sich, dass eine E-ID als offizielles und staatliches Ausweisdokument wahrgenommen wird: Der diesbezügliche Zustimmungswert liegt über sämtliche Teilnehmenden betrachtet bei einem hohen Mittelwert von 52,3 (vgl. Abb. 4.3).

4.3.2.3 Anwendungsbereiche der digitalen ID im öffentlichen Sektor und in der digitalen Demokratie

Die Umfrageteilnehmenden wurden des Weiteren danach befragt, für wie wichtig sie digitale Dienstleistungen des öffentlichen Sektors sowie die digitale Demokratie empfinden. Die Resultate der Befragung zeigen, dass Dienstleistungen über virtuelle Behördenschalter eine hohe Wichtigkeit attestiert wird (Mittelwert = 57,7). Die elektronische Partizipation (E-Partizipation) an politischen und demokratischen Prozessen erreicht über sämtliche Teilnehmenden betrachtet immerhin eine mittelhohe Wichtigkeit (Mittelwert = 28,6).

Elektronisches Abstimmen und Wählen (E-Voting, Mittelwert = 21,7) und elektronisches Unterschriftensammeln für Initiativen und Referenden (E-Collecting, Mittelwert = 17,3) erreichen Werte, welche zwar immer noch im positiven Bereich liegen, aber eher für eine moderate Bedeutung sprechen. Dabei zeigt sich, dass Anhänger:innen der SVP die einzige parteipolitische Gruppe darstellen, die sowohl beim E-Voting (−6,1) als auch beim E-Collecting (−1,5) eine leicht ablehnende Haltung einnehmen.

Mit einer weiteren Frage wurde zu eruieren versucht, inwieweit die Befragten die Notwendigkeit für eine E-ID als Voraussetzung für vollständig elektronische Behördendienstleistungen und elektronische Demokratie-Instrumente wie E-Voting und E-Collecting betrachten (vgl. Abb. 4.4). Dies vor dem im Theoriekapitel ausgeführten Hintergrund, dass aus technologischer Sicht eine digitale Transformation von Verwaltungs- und Demokratiedienstleistungen ohne eine digitale ID nicht umsetzbar ist. Die Resultate der Befragung, welche lediglich mittelhohe Zustimmungswerte von durchschnittlich 24,7 resp. 31,4 aufweisen, weisen darauf hin, dass diesbezüglich noch ein erhebliches Aufklärungspotenzial vorliegt.

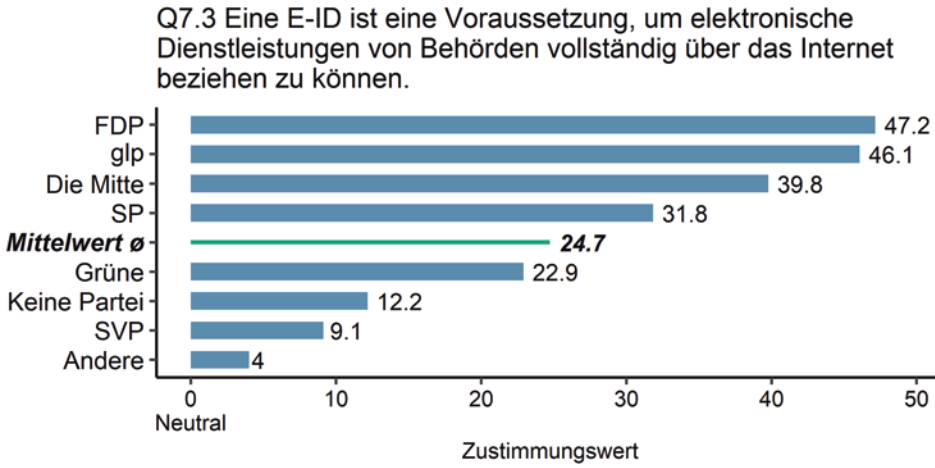

Abb. 4.4 Auswertung der Fragestellung Q7.3

4.3.2.4 Vorkenntnisse und Einstellung gegenüber der Blockchain-Technologie

Wie in Abb. 4.5 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 (bewussten) Berührungspunkte mit Anwendungen oder Systemen, welche auf der Blockchain-Technologie basieren.

Die Ergebnisse der Umfrage zeigen zudem, dass die Befragten gegenüber der Blockchain keine negative Einstellung hegen. Der Durchschnittswert von − 7,7 in Abb. 4.6 zeigt an, dass die Befragten die Aussage, dass sie den Begriff Blockchain mit etwas Negativem verbinden, insgesamt leicht ablehnen. Der Begriff Blockchain scheint damit im Mittel ziemlich neutral oder leicht positiv beurteilt zu werden, was sich auf die Einstellung der Befragten gegenüber der Blockchain-Technologie im Allgemeinen übertragen lässt.

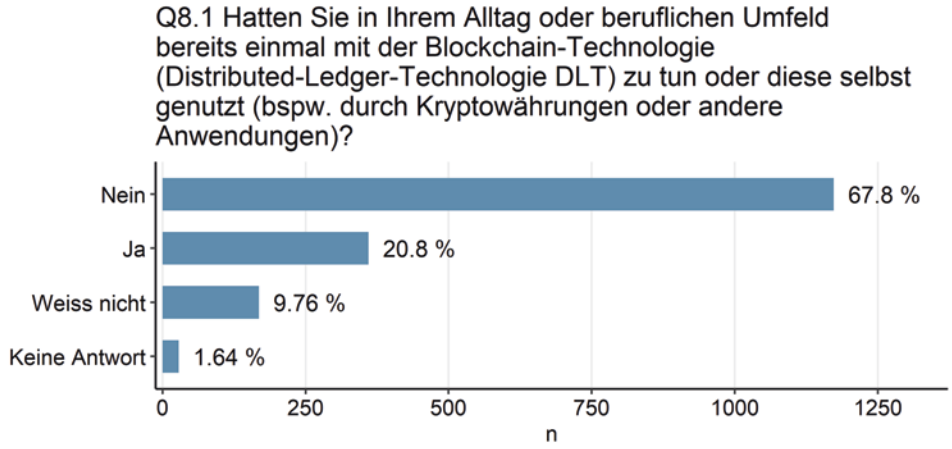

Abb. 4.5 Auswertung der Fragestellung Q8.1

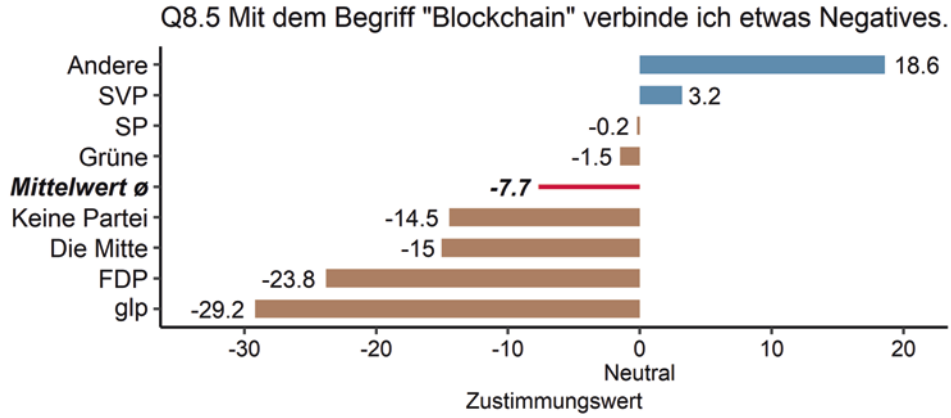

Abb. 4.6 Auswertung der Fragestellung Q8.5

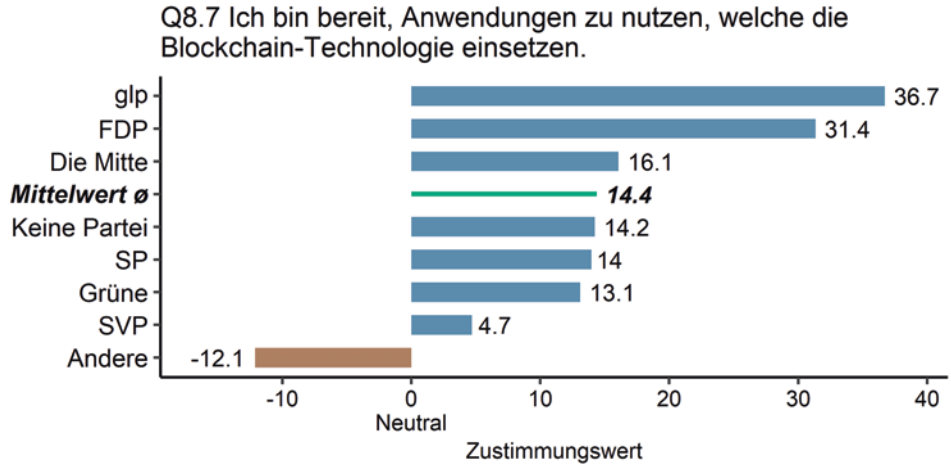

Abb. 4.7 Auswertung der Fragestellung Q8.7

Nicht nur sehen die Befragten die Blockchain-Technologie leicht positiv, sie zeigen auch die Bereitschaft, auf Blockchain-Technologie basierende Anwendungen zu nutzen (vgl. Abb. 4.7). Insgesamt scheint somit die Bereitschaft, Blockchain-Anwendungen verschiedenster Art zu nutzen oder deren Nutzung zumindest anwendungsspezifisch in Erwägung zu ziehen, im Durchschnitt durchaus vorhanden zu sein.

4.3.2.5 Einstellung gegenüber der Self-Sovereign Identity

Das innerhalb des theoretischen Teils beschriebene Konzept der Self-Sovereign Identity – also die vollständig selbstbestimmte Identität – war Bestandteil einer weiteren Frage. Die Analyse der Daten macht deutlich, dass die Befragten die Kernaspekte von Self-Sovereign Identity unabhängig der Verbundenheit mit einer bestimmten Partei 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. Weiter ist mit einem Spitzenwert von 92,2 die Zustimmung zur vollständigen Transparenz über die Verwendung der eigenen Identitätsdaten beinahe absolut. Bezüglich Datenhoheit, also der Präferenz bezogen auf die die eigenen Identitätsdaten verwaltenden Akteure, gehen die Meinungen ein wenig stärker auseinander. Dies zeigt sich bei der Auswertung von Q9.1 (vgl. Abb. 4.8).

4.3.2.6 Einstellung gegenüber einer digitalen ID auf Basis von Blockchain-Technologie

Nach den Fragestellungen rund um die Thematik der Self-Sovereign Identity werden in diesem Abschnitt spezifische Fragen zur Einstellung gegenüber einer digitalen ID auf Basis von Blockchain-Technologie analysiert. Die erste Frage in Abb. 4.9 erfasst die Ein-

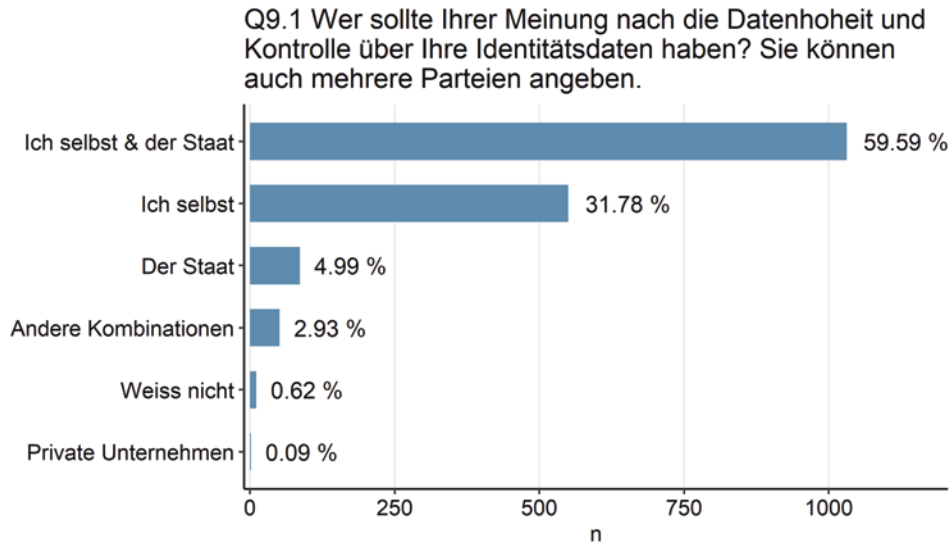

Abb. 4.8 Auswertung der Fragestellung Q9.1

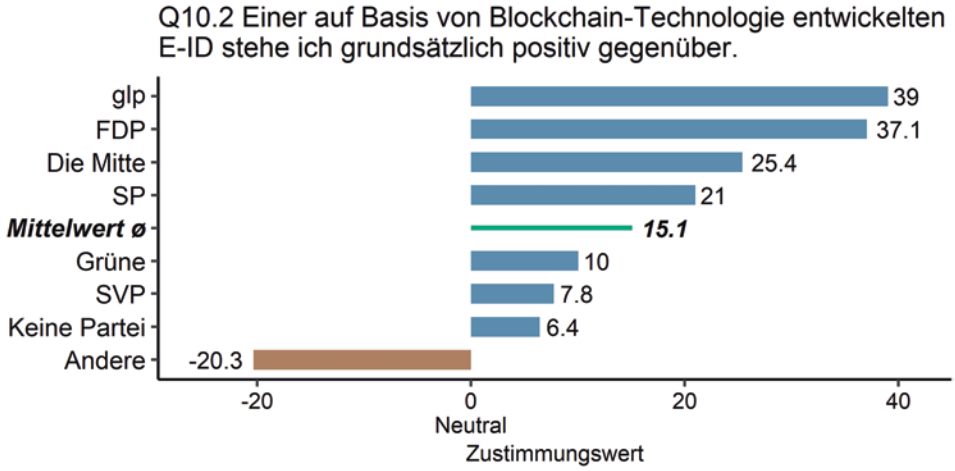

Abb. 4.9 Auswertung der Fragestellung Q10.2

stellung der Teilnehmenden gegenüber einer E-ID auf Basis von Blockchain-Technologie – ungeachtet der Aspekte von Datenhoheit, Ausstellungsinstanz etc.

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.

Um die Umfrageteilnehmenden auf einen gemeinsamen Wissensstand über die technologischen Potenziale zu bringen, wurde anschließend 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.*

Um den Effekt dieser kurzen Erklärung des Self-Sovereign-Identity-Potenzials erfassen zu können, wurde die vormals gestellte Frage in analoger Weise nochmals gestellt (vgl. Abb. 4.10).

Wie die Auswertung zeigt, steigert bereits eine kurze Aufklärung über das technologische Potenzial der Blockchain-Technologie zur Entwicklung einer E-ID-Lösung 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 die Anhängerschaft von FDP, glp und Die Mitte sogar stark zustimmen.

4.3.2.7 Abstimmungsabsicht bezüglich einer staatlichen und Blockchain-basierten ID-Lösung

Zentrales Ziel der Umfrage ist es, Aussagen über die Einstellung der Bevölkerung gegenüber einer Blockchain-basierten E-ID machen zu können. Damit sollen ebenfalls Aus-

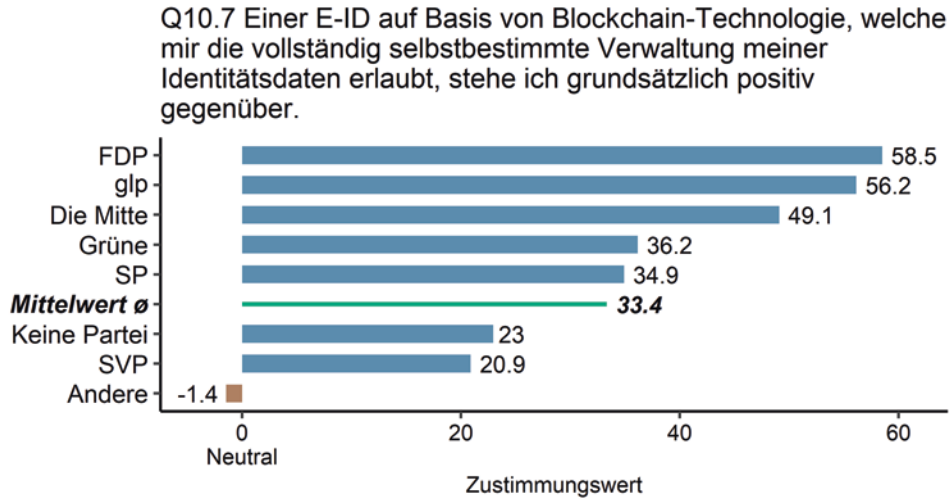

Abb. 4.10 Auswertung der Fragestellung Q10.7

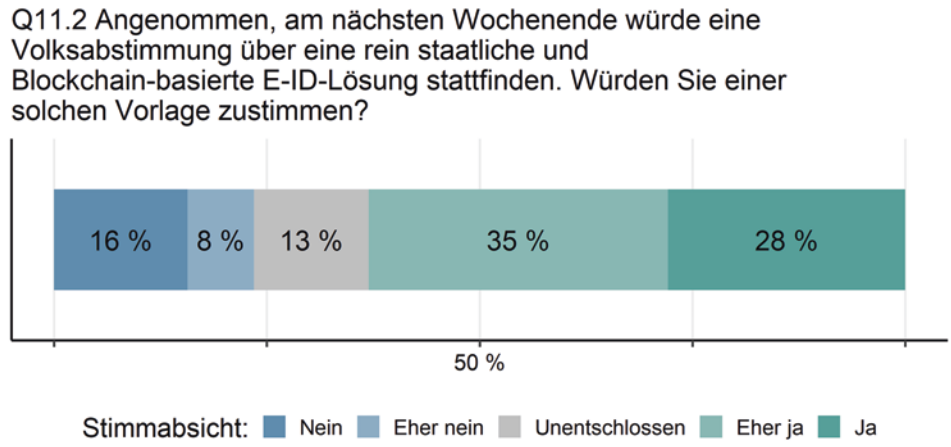

Abb. 4.11 Auswertung der Fragestellung Q11.2

sagen über eine potenzielle Mehrheitsfähigkeit einer derartigen Lösung gemacht werden können. Die Befragten wurden deshalb nach ihrer Stimmabsicht bei einer hypothetischen Volksabstimmung über eine rein staatliche und Blockchain-basierte E-ID-Lösung befragt (vgl. Abb. 4.11). Im Gegensatz zum vorherigen Abschnitt wird hier zusätzlich der Staat exklusiv als die eine E-ID herausgebende Instanz definiert.

Die Gesamtauswertung zeigt die Stimmabsicht sämtlicher Teilnehmenden der Umfrage (n = 1730). 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 % unter den Stimmberechtigten. Der Anteil Unentschlossener beläuft sich auf 13 %. Mit 16 % bzw. 8 % machen diejenigen, welche eine derartige Vorlage ganz bestimmt oder eher ablehnen würden, nur rund einen Viertel der Befragten aus. Unter den Teilnehmenden scheint eine staatliche und Blockchain-basierte E-ID folglich realistische Chancen für eine Mehrheit in der stimmberechtigten Bevölkerung aufweisen zu können.

4.3.2.8 Gründe für und gegen eine staatliche und Blockchain-basierte ID-Lösung

Die Teilnehmenden wurden zudem nach den Gründen für und gegen eine staatliche und Blockchain-basierte ID-Lösung gefragt.

Zu den meistgenannten Zustimmungsgründen zählen die Ermöglichung einer vollständig selbstbestimmten Verwaltung der eigenen Identität, die Befürwortung einer rein staatlichen Lösung (im Gegensatz zur abgelehnten Vorlage von 2021), die Verbesserung von Angebot und Nutzung digitaler Dienstleistungen der Behörden sowie die Stärkung der Demokratie durch neue digitale Instrumente. Der Verbesserung von digitalen Dienstleistungen in der Privatwirtschaft sowie der Ermöglichung einer innovativen wirtschaftlichen Zukunft durch eine Blockchain-ID kommt lediglich eine sekundäre Bedeutung zu.

Auf der Gegenseite wurden als meistgenannte Ablehnungsgründe generelle Datenschutz- und Sicherheitsbedenken bei einer E-ID, fehlendes Wissen über die und bestehende Skepsis gegenüber der Blockchain-Technologie sowie auch die grundlegende Ablehnung jeglicher E-ID-Lösungen ungeachtet der technologischen Basis genannt. Hervorzuheben ist zudem ein weiteres Ergebnis der Befragung: Ablehnende Personen sehen zu 52 % absolut keine Zustimmungsgründe, während unter den befürwortenden Personen lediglich 11 % absolut keine Gründe gegen die vorgeschlagene Lösung sehen. Dies deutet darauf hin, dass die Gegner:innen einer solchen Vorlage in ihrer ablehnenden Haltung tendenziell gefestigter sind, als die Befürworter:innen in ihrer positiven Haltung.

4.3.2.9 Einfluss der Kompetenz auf den Zustimmungsgrad

Der zuvor dargestellte Effekt des kurzen Erklärungstextes auf die Zustimmung zur Blockchain-basierten E-ID hat bereits auf einen positiven Zusammenhang zwischen der wahrgenommenen Informiertheit und der Stimmabsicht hingewiesen. In diesem Abschnitt soll dieser Aspekt nochmals vertieft werden, indem mittels inferenzstatistischer Methoden die folgende Hypothese getestet wird: 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.

Die Auswertung ergibt, dass die Selbsteinschätzung der Befragten bezüglich ihrer Blockchain-Kompetenz signifikant positiv mit der Stimmabsicht bei einer hypothetischen Volksabstimmung korreliert ($r_s = 0{,}127$, $p = < 0{,}001$, $n = 1629$). Allerdings 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 offenbart eine interessante Korrelationstendenz (vgl. Abb. 4.12). Die rötlich gekenn-

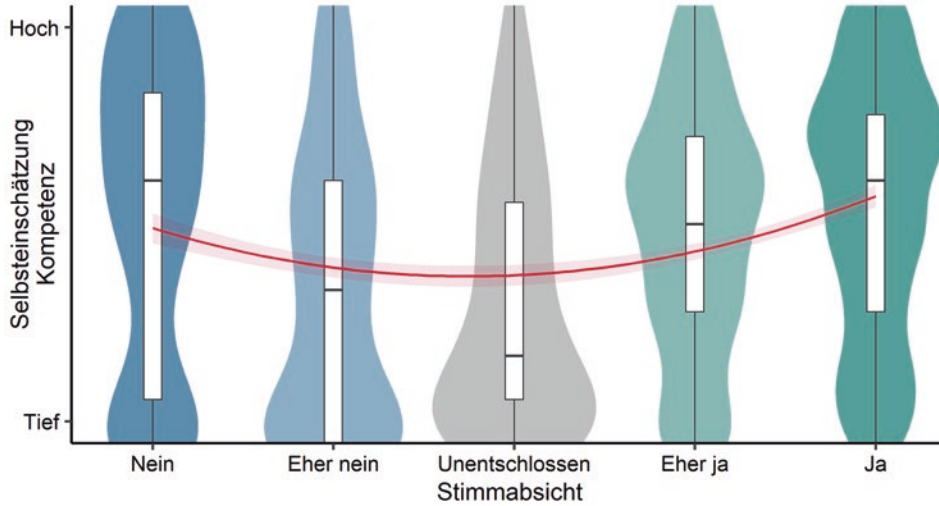

Abb. 4.12 Rangkorrelation nach Spearman von Kompetenz und Zustimmung. (Quelle: Eigene Darstellung)

zeichnete 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 vorliegenden Rahmen lediglich spekuliert werden. Eine mögliche Interpretation wäre, dass die Blockchain-Technologie stark polarisierende Eigenschaften aufweist, sodass sich gut informierte Personen entweder klar für oder gegen den Einsatz der Technologie im Rahmen einer E-ID stellen.

Basierend auf diesen Ergebnissen kann die zuvor formulierte Hypothese bedingt angenommen werden. Einerseits fällt die Korrelation zwischen der Selbsteinschätzung der technologischen Kompetenz in Bezug auf die Blockchain-Technologie und der Zustimmung gegenüber einer staatlichen, Blockchain-basierten E-ID eher schwach aus. Andererseits ist die Korrelation zwischen Selbsteinschätzung der Kompetenz und der Stimmabsicht – wie in der Abbildung gesehen – nicht eindeutig positiv, sondern von einer Dualität der beiden Polpositionen geprägt. Ebenfalls muss festgehalten werden, dass die Kompetenz lediglich auf einer Selbsteinschätzung der Teilnehmenden und nicht auf einer objektiven Messung basiert.

4.4 Schlussfolgerungen

Der Beitrag ging im Kontext der Digitalisierung von Identität sowie der Technologie Blockchain und deren Einsatzmöglichkeiten der Frage nach, wie die Haltung von Schweizer Stimmberechtigten gegenüber einer staatlichen und Blockchain-basierten E-ID-Lösung ist.

Dank der hohen Rücklaufquote der Umfrage konnte eine breite Datenbasis bestehend aus Antwort-Datensätzen von 1730 Teilnehmenden gewonnen werden. Trotz Annäherung der Stichprobe an die tatsächliche Bevölkerungsstruktur durch das angewandte Gewichtungsverfahren erhebt die Untersuchung keinen Anspruch auf Repräsentativität bezogen auf die schweizerische Bevölkerung. Dennoch scheint es zulässig, die empirischen Resultate im weiteren Verlauf als Erkenntnisse zu betrachten, welche der tatsächlichen Realität im Kontext einer E-ID zumindest nahekommen dürften.

Vor diesem Hintergrund zeigen die empirischen Auswertungen, dass für die Bevölkerung die exklusiv staatliche Datenhoheit, Kontrolle, Herausgabe sowie ein rein staatlicher Betrieb einer digitalen ID weitgehend unbestritten ist und von einem Großteil der Bevölkerung vorausgesetzt wird. Als mögliche Begründung dieser Präferenz lässt sich eine enge Assoziation der E-ID mit dem Offizialcharakter eines staatlichen Ausweisdokuments anführen: Die Auswertungen rund um die Wahrnehmung und Einordnung einer digitalen ID zeigen, dass die E-ID von vielen als eine dem Pass oder der Identitätskarte äquivalentes Ausweisdokument interpretiert wird.

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 eher 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. Auch das Bewusstsein zur Notwendigkeit einer E-ID für vollständig digitale Behördendienstleistungen seitens der Bevölkerung scheint eher niedrig. Da vollständig digitale Verwaltungen und digitale Instrumente wie E-Voting oder E-Collecting aus technologischer Sicht ohne eine digitale ID kaum sinnvoll umsetzbar sind, deuten die Ergebnisse auf ein Informationsdefizit seitens der schweizerischen Bevölkerung hin.

Der Hauptfokus der empirischen Untersuchungen lag hauptsächlich darin, die Zustimmung oder Ablehnung der Bürger:innen gegenüber einer staatlichen und Blockchain-basierten ID-Lösung zu evaluieren. Sowohl insgesamt betrachtet als auch beinahe parteiübergreifend (mit Ausnahme von Personen, die sich der SVP nahe fühlen) konnte eine vergleichsweise hohe Offenheit und Zustimmung gegenüber einer staatlichen und Blockchain-basierten E-ID eruiert werden. In einer hypothetischen Volksabstimmung über eine staatliche, Blockchain-basierte E-ID hätte diese E-ID-Variante gemäß der empirischen Erhebung eine Zustimmung von etwa 63 % erreicht. Aufgrund der beschriebenen Zurückhaltung bezüglich Digitalisierung und technischer Innovationen in der schweizerischen Bevölkerung handelt es sich um ein Resultat, das nicht unbedingt erwartet werden konnte.

Der wichtigste Grund für diese Zustimmung gegenüber der Blockchain-ID stellt für die Bevölkerung die Ermöglichung der vollständig selbstbestimmten Verwaltung der eigenen Identität dar. Ebenfalls wichtig sind 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 sowohl 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. Die Gegner:innen einer E-ID sind in ihrer ablehnenden Haltung somit gefestigter als die Befürworter:innen in ihrer positiven Haltung.

Ebenfalls spannend zu sehen ist, dass Wirtschaftsaspekte für die Bürger:innen eine stark untergeordnete Rolle spielen. Die ökonomischen Potenziale einer digitalen ID scheinen keine große Relevanz für die Bevölkerung zu besitzen. Hier besteht augenscheinlich ein weiteres Informationsdefizit seitens der breiten Bevölkerung, woraus sich ein starkes Aufklärungspotenzial seitens Behörden und insbesondere auch des privatwirtschaftlichen Sektors als Profiteure einer E-ID ergibt.

Im theoretischen Teil der wissenschaftlichen Arbeit von Wackernagel (2022) 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 Schaf-

fung 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 die der Technologie inhärenten Risiken und Nutzungshürden abgewogen werden.

Die Wahrnehmung des Begriffs Blockchain innerhalb der Bevölkerung offenbarte sich in der Befragung als relativ neutral bis leicht positiv, was in Anbetracht der Neuartigkeit und dem in der Öffentlichkeit aufgrund der Debatte um Kryptowährungen nicht immer unumstrittenen Image nicht unbedingt zu erwarten war. Dies zeigt sich auch 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 könnte.

Trotz dem festgestellten großen Vertrauen in den Staat als die E-ID ausstellende und betreibende Instanz 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.

Für die Praxis, insbesondere mit Blick auf die Umsetzung der E-ID in der Schweiz, bedeutet dies, dass gestützt auf die empirischen Ergebnisse das Konzept einer sowohl staatlichen als auch Blockchain-basierten E-ID wohl als eine mehrheitsfähige Option unter verschiedenen anderen Umsetzungsmöglichkeiten in Erwägung gezogen werden könnte. Insbesondere die Erkenntnis, dass die Bevölkerung das Konzept der selbstbestimmten Verwaltung der eigenen Identitätsdaten als gewichtigstes Argument für die Zustimmung zu einer E-ID erachtet, dürfte für die behördliche Ausarbeitung von technologischen Lösungsvarianten interessant sein.

Die generelle Einführung einer digitalen ID birgt sowohl für die Demokratie und den öffentlichen Sektor als auch für den privaten Wirtschaftssektor große Potenziale. Grundsätzlich ist die Einführung einer digitalen ID im Kontext einer fortschreitenden Digitalisierung und Technologisierung des alltäglichen Lebens unumgänglich, um neben der erwünschten digitalen Transformation des öffentlichen Sektors und der Demokratie auch die mit der E-ID einher gehenden Potenziale aus ökonomischer Sicht 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. Von einer grundsätzlichen Offenheit der schweizerischen Bevölkerung gegenüber künftigen Anwendungen und Dienstleistungen auf der Basis von Blockchain-Technologie darf aufgrund der Ergebnisse dieser Untersuchung ausgegangen werden.

Literatur

Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., & Amaba, B. (2017). Blockchain technology innovations. In 2017 IEEE Technology & Engineering Management Conference (TEMSCON) (S. 137–141).

Allen, C. (2016). The path to self-sovereign identity. In CoinDesk. https://www.coindesk.com/markets/2016/04/27/the-path-to-self-sovereign-identity/. Zugegriffen am 31.05.2022.

Ammous, S. H. (2016). Blockchain technology: What is it good for? *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2832751

Bakre, A., Nikita, P., & Sakshum, G. (2017). Implementing decentralized digital identity using blockchain. *International Journal of Engineering Technology Science and Research, 4*(10), 379–385.

Berentsen, A., & Schär, F. (2017). *Bitcoin, Blockchain und Kryptoassets: Eine umfassende Einführung*. Books on Demand.

Bisaz, C., & Serdült, U. (2017). E-Collecting als Herausforderung für die direkte Demokratie der Schweiz. LeGes: Gesetzgebung. *Evaluation, 28*(3), 531–545.

Biswas, K., & Muthukkumarasamy, V. (2016). 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) (S. 1392–1393).

Bühler, G., Hermann, M., & Krähenbühl, D. (2022). Digitaler Staat in der Schweiz: Einschätzungen und Bedürfnisse der Bevölkerung. Sotomo. https://www.swico.ch/media/filer_public/99/19/9919fe71-b4c7-4024-bc6a-e1aa9743c06f/sotomo_swico_digitaler_staat.pdf?vgo_ee=FQkJhwU4Mu1Ew7yl4DU8sE5I2jKxc%2Bu7z1tNMUbX0LI%3D. Zugegriffen am 31.05.2022.

Camp, L. J. (2004). Digital identity. *IEEE Technology and Society Magazine, 23*(3), 34–41.

Cap, C. H., & Maibaum, N. (2001). Digital identity and its implication for electronic government. In B. Schmid, K. Stanoevska-Slabeva, & V. Tschammer (Hrsg.), *Towards the e-society* (S. 803–816). Kluwer Academic Publishers.

Cohen, J. (1992). A power primer. *Psychological Bulletin, 112*(1), 155–159.

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *AIR Applied Innovation Review, 2016*(2), 6–19.

Dunphy, P., & Petitcolas, F. A. (2018). A first look at identity management schemes on the blockchain. *IEEE Security & Privacy Magazine, 16*(4), 20–29.

Efanov, D., & Roschin, P. (2018). The all-pervasiveness of the blockchain technology. *Procedia Computer Science, 123*, 116–121.

Fivaz, J., & Schwarz, D. (2021). Die digitale Demokratie in der Schweiz. In J. Stember, W. Eixelsberger, A. Spichiger, A. Neuroni, F.-R. Habbel, & M. Wundara (Hrsg.), *Aktuelle Entwicklungen zum E-Government* (S. 75–96). Springer Fachmedien.

gfs.bern. (2021). VOX-Analyse März 2021: Nachbefragung und Analyse zur eidgenössischen Volksabstimmung vom 7. März 2021. Bern. https://vox.gfsbern.ch/wp-content/uploads/2021/04/d_vox_schlussbericht_def.pdf. Zugegriffen am 31.05.2022.

Goode, A. (2019). Digital identity: solving the problem of trust. *Biometric Technology Today, 2019*(10), 5–8.

Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017). *Digital identity guidelines: Revision 3*. NIST.

Hou, H. (2017). The application of blockchain technology in e-government in China. In: 26th International Conference on Computer Communication and Networks (ICCCN) (S. 1–4).

Irani, Z., & Kamal, M. (2016). Transforming government: People, process, and policy. *Transforming Government: People, Process and Policy, 10*(2), 190–195.

Judmayer, A., Stifter, N., Schindler, P., & Weippl, E. (2019). Blockchain: Basics. In H. Treiblmaier & R. Beck (Hrsg.), *Business transformation through blockchain, volume II* (S. 339–356). Palgrave Macmillan.

Lips, M. (2010). Rethinking citizen – Government relationships in the age of digital identity: Insights from research. *Information Polity, 15*(4), 273–289.

Melin, U., Axelsson, K., & Söderström, F. (2016). Managing the development of e-ID in a public e-service context. *Transforming Government: People, Process and Policy, 10*(1), 72–98.

Mir, U. B., Kar, A. K., Dwivedi, Y. K., Gupta, M. P., & Sharma, R. S. (2020). Realizing digital identity in government: Prioritizing design and implementation objectives for Aadhaar in India. *Government Information Quarterly, 37*(2), 101442.

Müller, A., & Windisch, A. (2018). E-Identity-Lösungen in Europa: Ein europäischer Vergleich. asquared Blog Post (3/2018). 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. Zugegriffen am 31.05.2022.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *SSRN Electronic Journal*. https://bitcoin.org/bitcoin.pdf. Zugegriffen am 31.05.2022.

Neuroni, A., Kissling-Näf, I., & Riedl, R. (2019). E-Government und smarter Staat: Die Schweiz auf halbem Weg. In J. Stember, W. Eixelsberger, A. Spichiger, A. Neuroni, F. R. Habbel, & M. Wundara (Hrsg.), *Handbuch E-Government* (S. 163–180). Springer Gabler.

Nicke, S. (2018). Der Begriff der Identität. Bundeszentrale für politische Bildung. https://www.bpb.de/themen/parteien/rechtspopulismus/241035/der-begriff-der-identitaet/. Zugegriffen am 31.05.2022.

OECD (2022). Digital identity management and electronic authentication. https://www.oecd.org/sti/ieconomy/digitalidentitymanagementandelectronicauthentication.htm. Zugegriffen am 31.05.2022.

Pilkington, M. (2016). Blockchain technology: Principles and applications. In F. Olleros & M. Zhegu (Hrsg.), *Research handbook on digital transformations* (S. 225–253). Edward Elgar Publishing.

Poblet, M., Allen, D. W. E., Konashevych, O., Lane, A. M., Diaz, V., & Carlos, A. (2020). From Athens to the Blockchain: Oracles for digital democracy. *Frontiers in Blockchain, 3*. https://doi.org/10.3389/fbloc.2020.575662

Politools. (2022). smartvote – Online-Wahlhilfe. https://smartvote.ch/de/home. Zugegriffen am 31.05.2022.

Prashanth Joshi, A., Han, M., & Wang, Y. (2018). A survey on security and privacy issues of blockchain technology. *Mathematical Foundations of Computing, 1*(2), 121–147.

Rauschenbach, R., & Stucki, S. (2020). Studie zum Einsatz der Blockchain-Technologie in der kantonalen Verwaltung. Staatskanzlei Kanton Zürich. https://www.zh.ch/content/dam/zhweb/bilder-dokumente/organisation/staatskanzlei/digitale-verwaltung-und-e-government/studie_blockchain.pdf. Zugegriffen am 31.05.2022.

Rivera, R., Robledo, J. G., Larios, V. M., & Avalos, J. M. (2017). How digital identity on blockchain can contribute in a smart city environment. 2017 International Smart Cities Conference (ISC2) (S. 1–4).

Rüthi, T., Holenstein, M., Stübi, N., & Köng, A.-L. (2021). Mobiliar #Digital Barometer 2020/21: Die Stimme der Schweizer Bevölkerung. 2020. Stiftung Risiko-Dialog. https://www.digitalbarometer.ch/de/digitalbarometer#downloads. Zugegriffen am 31.05.2022.

Stokkink, Q., & Pouwelse, J. (2018). Deployment of a blockchain-based self-sovereign identity. 2018 IEEE International Conference on Internet of Things (iThings); IEEE Green Computing and Communications (GreenCom); IEEE Cyber, Physical and Social Computing (CPSCom); IEEE Smart Data (SmartData) (S. 1336–1342).

Sullivan, C. (2016). Digital citizenship and the right to digital identity under international law. *Computer Law & Security Review, 32*(3), 474–481.

Sullivan, C. (2018). Digital identity – From emergent legal concept to new reality. *Computer Law & Security Review, 34*(4), 723–731.

Sullivan, C., & Burger, E. (2019). Blockchain, digital identity, e-government. In H. Treiblmaier & R. Beck (Hrsg.), *Business transformation through blockchain, Volume II* (S. 233–258). Palgrave Macmillan.

Takemiya, M., & Vanieiev, B. (2018). Sora identity: Secure, digital identity on the blockchain. 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC) (S. 582–587).

Toth, K. C., & Anderson-Priddy, A. (2019). Self-sovereign digital identity: A paradigm shift for identity. *IEEE Security & Privacy Magazine, 17*(3), 17–27.

Underwood, S. (2016). Blockchain beyond bitcoin. *Communications of the ACM, 59*(11), 15–17.

Wackernagel, T. (2022). Die Blockchain-ID: Eine mehrheitsfähige Lösung für den digitalen Identitätsnachweis innerhalb der schweizerischen Demokratie? Master-Thesis an der Berner Fachhochschule. https://github.com/wackt1/MATH_publication/blob/main/Thesis_Wackernagel_Tim_Polit-Oekonomische_Evaluation_Blockchain-E-ID_Schweiz_20220605.pdf. Zugegriffen am 31.01.2023.

Wolfond, G. (2017). A blockchain ecosystem for digital identity: Improving service delivery in Canada's public and private sectors. *Technology Innovation Management Review, 7*(10), 35–40.

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). *Blockchain technology overview*. NIST.

Yang, X., & Li, W. (2020). A zero-knowledge-proof-based digital identity management scheme in blockchain. *Computers & Security, 99*, 102050.

Zwitter, A. J., Gstrein, O. J., & Yap, E. (2020). Digital identity and the blockchain: Universal identity management and the concept of the "Self-Sovereign" individual. *Frontiers in Blockchain, 3*. https://doi.org/10.3389/fbloc.2020.00026

Tim Wackernagel (M.Sc.) Masterstudium in Business Administration mit Vertiefung in Corporate & Business Development an der Berner Fachhochschule, davor Bachelorstudium in Wirtschaftsinformatik mit Vertiefung in Business Analysis an der Berner Fachhochschule. Hauptberuflich derzeit als Project & Business Controlling Expert / Project Management Officer beim Kanton Basel-Stadt tätig.

Dr. Daniel Schwarz Wissenschaftlicher Mitarbeiter am Institut Public Sector Transformation des Departements Wirtschaft der Berner Fachhochschule sowie am Kompetenzzentrum für Public Management der Universität Bern. Mitbegründer der Online-Wahlhilfe „smartvote". Forschungsschwerpunkte: Digitale Demokratie, Parlaments- und Parteienforschung.