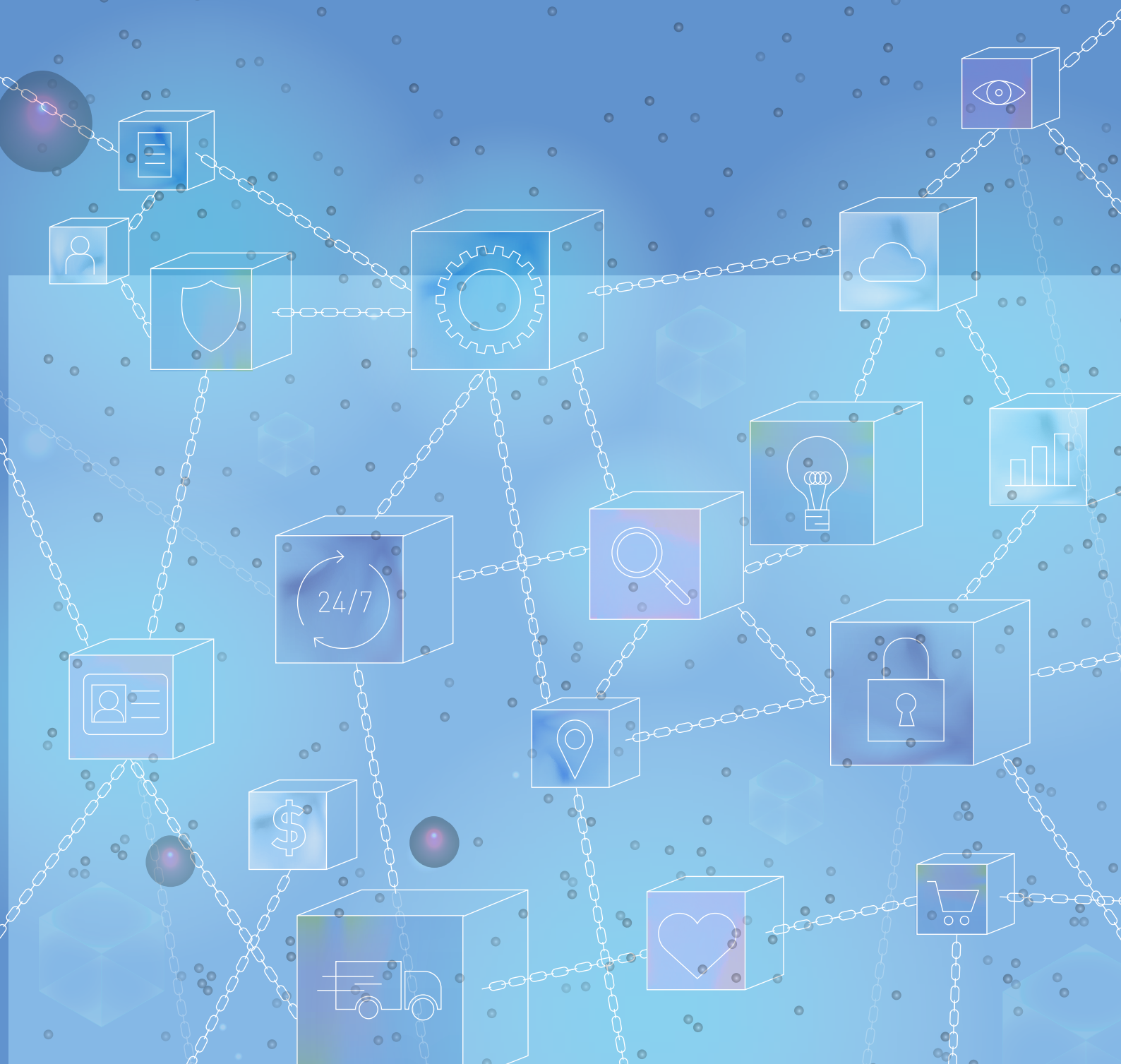
GDI GOTTLIEB DUTTWEILER INSTITUTE
CREATING FUTURES

HYPE ODER HILFE?

Was die Blockchain wirklich leistet

Von Jan Bieser und Daniel Fasnacht



Impressum

Autoren
Dr. Jan Bieser, Dr. Daniel Fasnacht

Lektorat
Karola Klatt

Korrektorat
Die Lektoren (Maja Kunze)

Layout/Illustration
Joppe Berlin, www.joppeberlin.com

GDI Research Board
Alain Egli, Karin Frick, Dr. Jakub Samochowiec, Christine Schäfer

ISBN: 978-3-7184-7142-3

Herausgeber
GDI Gottlieb Duttweiler Institut
Langhaldenstrasse 21
CH-8803 Rüschlikon
www.gdi.ch

Initianten
Sminds/N9 House of Innovation, Inacta, EcosystemPartners

Industrie- und Kooperationspartner
Ermöglicht wurde diese Studie durch diverse Partner, die sich mit ihrer Expertise und ihren Erfahrungen eingebracht haben: aXedras, Blockchain Nation Switzerland, Bundesamt für Energie, Generali (House of Insuretech Switzerland HITS), Green, Inacta, Kantonsspital Baden, Novartis, OVD Kinegram, Verband Schweizerischer Elektrizitätsunternehmen (VSE).

Inhalt

Vorwort

Die Schweiz wird oft als das innovativste Land der Welt angesehen. Dahinter steckt kein Geheimrezept. Eine Kombination bekannter Faktoren macht den Innovationserfolg der Schweiz aus. Dazu gehören das erstklassige Bildungssystem mit dem berühmten Schweizer Lehrlingswesen und einige der besten Universitäten der Welt, eine stabile, verlässliche und pragmatische Demokratie sowie eine reiche Geschichte leistungsstarker KMU. Darüber hinaus trägt die von der Schweizer Regierung unterstützte Bottom-up-Vision für Wissenschaft und Technologie dazu bei, dass Innovationen nicht durch schwerfällige und schlecht informierte Vorschriften erstickt werden, bevor deren wahre Chancen und Gefahren bekannt sind. Während neue Technologien wie Blockchain in dieser frühen Phase noch einige Höhen und Tiefen erleben werden, erwies sich Finanzminister Ueli Maurer als Visionär, als er die Schweiz als «Krypto-Nation» etablierte; und der Nationalrat folgte ihm im Jahr 2020, indem er durch Gesetzesanpassungen die Rahmenbedingungen für den Einsatz von Blockchain und Distributed Ledger Technology (DLT) verbesserte. Dieser Rechtsrahmen ermöglicht Innovationen, fördert die Akzeptanz der Technologie und beseitigt Hürden für Blockchain-Anwendungen in allen Branchen, während die Missbrauchsrisiken begrenzt werden. Gerade jetzt, in diesen turbulenten Zeiten, sehen wir, wie erfolgreich dieser Ansatz ist.

Innosuisse unterstützt mit der Initiative «Innovation Booster» den Bottom-up-Ansatz und fördert thematische Communities, die gemeinsam neue disruptive Ideen entwickeln und testen. Blockchain ist eines der vielversprechenden Themen, die im Rahmen dieses Programms unterstützt werden.

Für viele geht es bei Blockchain nur um Kryptowährungen und eine Möglichkeit, zu investieren und zu spekulieren. Das ist ungefähr so, wie wenn man Flugzeuge nur für militärische Zwecke nutzen würde. Blockchain ist ein perfektes Beispiel für eine digital native Technologie, die Lösungen für alte und neue Herausforderungen ermöglicht sowie reale und virtuelle Welt miteinander verbindet.

Da die Digitalisierung jeden Tag voranschreitet, können wir in diesem neuen Raum nicht einfach die alten Paradigmen der physischen Welt replizieren. Beispielsweise muss in der digitalen Welt Vertrauen neu gedacht werden. Wenn herkömmliche Computertechnologien ohne Blockchain verwendet werden, ist das Vertrauen darauf beschränkt, wie sehr man den Unternehmen und Menschen hinter den Technologien vertraut. In der Realität ist dies ein begrenztes Mass, was sich negativ auf die Akzeptanz einer Technologie auswirkt.

Das Schöne an der Blockchain-Technologie ist, dass sie ermöglicht, zentrale Vertrauensinstanzen im digitalen Raum zu beseitigen. Vertrauen wird durch eine im Netzwerk verteilte Konsensfindung nach nachvollziehbaren und überprüfbaren Regeln geschaffen, wobei die Privatsphäre gewahrt und die Kontrolle an Verbraucherinnen und Verbraucher zurückgegeben wird. Es ist ganz natürlich, dass eine solche Technologie in der Schweiz floriert, da sie gut zu den Werten des Landes passt, dessen Menschen und Institutionen Vertrauen, Fairness, Zuverlässigkeit, Privatsphäre und Pragmatismus schätzen.

Um dies zu verwirklichen, bedarf es visionärer Unternehmen und Menschen, die eher Chancen und Vorteile als Risiken und Probleme sehen. Die Vernetzung von Grossunternehmen, KMU und Startups ist ebenfalls ein Erfolgsfaktor für solche Vorhaben. Universitäten und Think Tanks wie das Gottlieb Duttweiler Institut (GDI) schaffen zusammen mit innovativen Partnern aus der

Privatwirtschaft eine starke Grundlage für interdisziplinäre Co-Innovation.

Diese Studie zeigt die Vorteile, welche Blockchain für die sichere Identifizierung von Bürgerinnen und Bürgern im digitalen Raum bringen kann und stellt den Zusammenhang mit der Vernehmlassung zur elektronischen Identität (E-ID) her, die dem Bundesrat im Juni 2022 vorgelegt wurde. Ideen für die Produktnachverfolgung mittels Blockchain sind schon seit Jahren bekannt. Doch diese Studie zeigt, welche bedeutenden Fortschritte in diesem Bereich gemacht wurden. Die skizzierten Anwendungsfälle können nicht nur in der Pharmaindustrie, sondern auch in Märkten wie dem Goldhandel oder für immaterielle Güter wie Herkunftsnachweise für Strom genutzt werden. In einer digitalisierten Welt spielen Daten und Datenmanagement eine immer wichtigere Rolle. Mittels Blockchain können Nutzende ihre sensiblen Gesundheits- oder Finanzdaten selbst verwalten, Datensilos verknüpft und besser vor Cyberangriffen geschützt werden.

Die von den Autoren identifizierten Potenziale der Blockchain sind enorm und werden, wenn sie weiter vorangetrieben werden, einen wesentlichen Beitrag zur Zukunft der Schweizer Wirtschaft leisten. Damit ist die Schweiz gut positioniert, um weiterhin zu den innovativsten Ländern der Welt zu gehören.

André Kudelski
Präsident von Innosuisse und Unternehmer

Zusammenfassung

Viele digitale Anwendungen sind heute zu einer kritischen Infrastruktur für die Wirtschaft und unseren Alltag geworden. Die Abhängigkeiten gehen weit über die Technologiebranche hinaus, denn digitale Werkzeuge werden auch für die Bereitstellung physischer Infrastrukturen und Dienstleistungen genutzt, beispielsweise im Finanz-, Gesundheits-, Transportwesen, Gebäudemanagement, der Energieversorgung oder Produktion. Häufig werden diese Anwendungen von zentralen Dienstleistern, wie IT-Unternehmen oder Netzbetreibern, bereitgestellt. Bürgerinnen und Bürger müssen darauf vertrauen, dass diese Dienstleister die Verfügbarkeit und Integrität der Systeme sicherstellen und ihre Marktmacht nicht missbrauchen.

Die Einführung von Bitcoin und der dahinterliegenden Blockchain-Technologie im Jahr 2009 weckte die Hoffnung, solche Abhängigkeiten, bei Bitcoin von (Zentral-)Banken, zu reduzieren. Seitdem wurde die Technologie kontinuierlich weiterentwickelt, um die Potenziale von Blockchain auch im Unternehmenskontext erschliessen zu können. Heute handelt es sich nicht mehr um eine spezifische Technologie für Kryptowährungen, sondern um eine Technologie, die Vorteile für digitale Anwendungen in vielen Branchen bietet. Dennoch fällt es vielen Führungspersönlichkeiten weiterhin schwer, den kurz- und langfristigen Nutzen von Blockchain für ihr Unternehmen zu bewerten. Ziel dieser Studie ist daher, ein differenziertes Verständnis der Einsatzmöglichkeiten sowie der Chancen und Grenzen der Blockchain-Technologie zu vermitteln.

Blockchain kann für zwei grundlegend unterschiedliche Zwecke verwendet werden:

Robustere und effizientere digitale Infrastrukturen: Der verteilte Betrieb einer digitalen Anwendung auf den Systemen mehrerer Geschäftspartner erhöht die Manipulationssicherheit und Verfügbarkeit der Anwendung. Wertgegenstände können mit Tokens digital abgebildet und gehandelt, Prozesse mit sogenannten Smart Contracts automatisiert ausgeführt werden. Dies vereinfacht die organisationsübergreifende Zusammenarbeit, spart Kosten und Zeit. Sind Prozesse anhand von Blockchain manipulationssicher digitalisiert, können sich neue Geschäftsfelder eröffnen. Beispielsweise ermöglicht Blockchain die Schaffung sicherer elektronischer Identitäten, mit denen Personen, Organisationen und Objekte digital identifiziert werden können. Dies kann eine Zugangsverwaltung zu Gebäuden ohne physische Schlüssel, fälschungssichere Echtheitszertifikate für Waren, Peer-to-Peer-Marktplätze oder eine robuste Dateninfrastruktur für das Internet der Dinge ermöglichen.

Reduktion von Abhängigkeiten: Der verteilte Betrieb eröffnet zusätzlich die Möglichkeit, die Abhängigkeit von zentralen Dienstleistern abzuschaffen. In verteilten, sich selbst regulierenden, Wertschöpfungsnetzwerken treffen alle Mitglieder gemeinsam Entscheidungen und kontrollieren sich gegenseitig, ohne dass es eine zentrale Bestimmungsinstanz gibt: Internet ohne Google, Ride-Sharing ohne Uber, Zahlungen ohne Banken. Dies ist allerdings nicht nur ein technologischer, sondern auch ein gesellschaftlicher Prozess, bei dem neue partnerschaftliche Formen der Zusammenarbeit etabliert und Interessenskonflikte überwunden werden müssen. Gelingt dies, bietet Blockchain eine geeignete technologische Grundlage, diese umzusetzen.

Eine Literaturrecherche förderte mehr als 50 Anwendungen in zehn Branchen zutage. Im Unternehmenskontext dominieren Anwendun-

gen den Markt, die weiterhin über zentrale Dienstleister gesteuert werden, mit dem Ziel, die Integrität von digitalen Anwendungen, die Automatisierung und die Kosteneffizienz zu erhöhen. Oft ist das Durchdenken einer Anwendung mithilfe von Blockchain-Technologie auch ein Treiber dafür, bestehende manuelle Prozesse zu standardisieren, denn dies ist eine Voraussetzung, um sie mittels Blockchain zu digitalisieren.

Zentrale Herausforderungen in der Umsetzung von Blockchain-Projekten sind die Etablierung geeigneter Governance-Strukturen für die organisationsübergreifende Zusammenarbeit, die Beseitigung regulatorischer Unklarheiten, die Sicherstellung der Datenqualität und -sicherheit (auf Blockchains und in angrenzenden Systemen) und die Schaffung von Vertrauen und Akzeptanz in die Technologie. Wenn Unternehmen neue Partnerschaften – auch mit Wettbewerbern und Regulierern – eingehen und Anwendungen gemeinsam in der Praxis erproben, können diese Herausforderungen gemeistert werden. Die Schweiz gilt als ein internationaler Hub für Blockchain, mit zukunftsgerichteten Regulierungen, führenden Forschungszentren und über 1 100 Unternehmen, die Blockchain-Lösungen entwickeln.

Aufgrund der weiterhin stark voranschreitenden Digitalisierung von Prozessen, die nicht zuletzt durch die COVID-19-Pandemie weiter beflügelt wurde, ist von einem weiteren Bedeutungsgewinn digitaler Anwendungen auszugehen. Die Eigenschaften von Blockchain – Manipulationssicherheit und Verfügbarkeit, effizienter Datenaustausch, in Smart Contracts fixierbare Entscheidungsregeln, Wertehandel mit Tokens – bieten eine geeignete technische Grundlage für die Schaffung robuster und effizienter digitaler Infrastrukturen.

Ausgangslage

Tim Berners-Lee, der Erfinder des World Wide Web, beklagt heute, was aus dem Internet geworden ist.[1] Statt dem Gemeinwohl zu dienen und die Verbreitung von Informationen zu demokratisieren, existiert gegenwärtig eine grosse Marktkonzentration im Netz. Wenige «Big Tech»-Unternehmen (zum Beispiel Alphabet, Apple, Amazon, Meta, Microsoft, Alibaba, Tencent) stellen digitale Plattformen bereit, die exponentiell gewachsen sind und mit denen sie den Informationsfluss kontrollieren. Auch ausserhalb der Technologiebranche werden zunehmend digitale Anwendungen zur Optimierung von Produkten und Prozessen und zur Entwicklung von neuen Geschäftsmodellen eingesetzt. Intelligente Algorithmen in Kombination mit Daten versprechen Finanztransaktionen effizienter abzuwickeln, Maschinenausfälle vorherzusagen, Lieferketten zu optimieren oder Krankheiten zu diagnostizieren. Ob im Transportwesen, bei der Energieversorgung, im Gebäudemanagement, Finanz- oder Gesundheitswesen – überall werden digitale Anwendungen genutzt. In einer Umfrage aus dem Jahr 2022 gaben rund zwei Drittel der Schweizer Unternehmen an, eine Datenstrategie einzuführen oder bereits umzusetzen.[2] Die Digitalisierung und die Nutzung von Daten sind bei Schweizer KMU ein Dauerthema und werden hiesige Unternehmen in den nächsten Jahren mehr beschäftigen als die Inflation, Lieferkettenprobleme oder der Fachkräftemängel.[3]

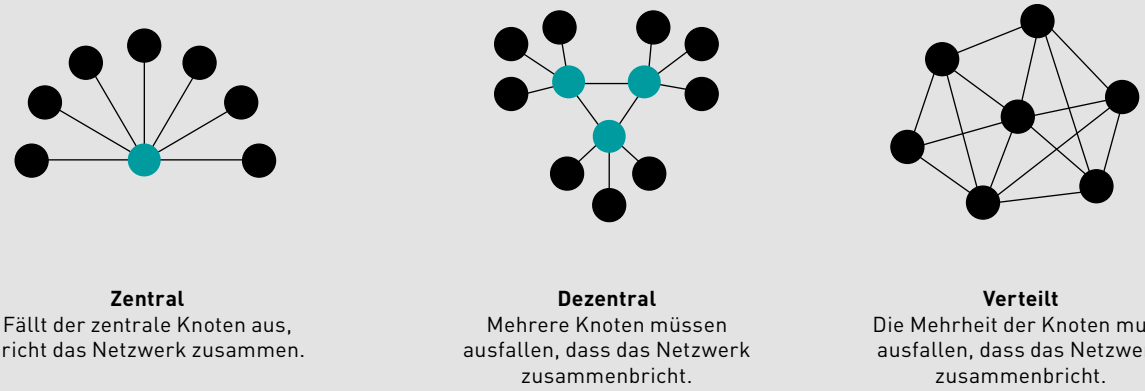
Viele digitale Anwendungen sind zu einer kritischen Infrastruktur für die Wirtschaft und unseren Alltag geworden. Würden beispielsweise die Services von Google und Meta gleichzeitig ausfallen, würden rund 92% aller Suchanfragen im Internet keine Ergebnisse liefern, und die Sofortnachrichten von rund drei Milliarden Nutzenden würden nicht beim Empfänger ankommen.[4] Wirtschaftlich bedeutsame Ausfälle kritischer digitaler Infrastrukturen hat es bereits gegeben: In der Schweiz sind schon mehrmals die Systeme zentraler Zahlungsdienstleister ausgefallen, was zu grossen Umsatzverlusten in Supermärkten und Restaurants geführt hat.[5] Im Juni 2022 wurde der Schweizer Spitalverband H+ Opfer einer Cyberattacke und hat daraufhin aus Sicherheitsgründen sämtliche Server heruntergefahren.[6]

Meist bilden sich um digitale Anwendungen sogenannte Wertschöpfungsnetzwerke, in denen Unternehmen (auch aus verschiedenen Sektoren) Güter, Geld und Informationen austauschen, um gemeinsam Wert zu schaffen. Daten werden von verschiedenen Akteuren generiert, zwischen diesen ausgetauscht und auf unterschiedliche Weise genutzt. In diesem Zusammenhang sprechen wir heute auch oft von Ökosystemen. Da dieser Begriff inflationär benutzt wird und wir der Meinung sind, dass ein Wertschöpfungsnetzwerk den Kontext von Blockchain besser umschreibt, benutzen wir diesen Begriff.

Wertschöpfungsnetzwerke sind häufig um einen zentralen Dienstleister strukturiert. Dieser übernimmt die Rolle des Intermediärs, das heisst des Mittlers, der den Datenaustausch im Netzwerk koordiniert und die Interaktionsregeln und -bedingungen bestimmen kann. Beispielsweise können Banken Transaktionsgebühren festlegen, Uber die Fahrpreise und Vermittlungskommissionen und Google die Bedingungen für die Weiterverwendung gesammelter Nutzerdaten. Wer die Angebote eines Intermediärs nutzen will, hat meist keinen Einfluss auf die Regeln. Sie müssen schlicht akzeptiert werden.

Als Bitcoin im Jahr 2009 verwirklicht wurde, entstand in der Folge nicht nur ein Hype um Kryptowährungen, sondern auch um die dahinterliegende Blockchain-Technologie. Mit Blockchain werden digitale Anwendungen nicht von

Zentrale, dezentrale und verteilte Netzwerke



Zentral
Fällt der zentrale Knoten aus, bricht das Netzwerk zusammen.

Dezentral
Mehrere Knoten müssen ausfallen, dass das Netzwerk zusammenbricht.

Verteilt
Die Mehrheit der Knoten muss ausfallen, dass das Netzwerk zusammenbricht.

Abbildung 1: Eigene Darstellung basierend auf Baran (1962).[7]

einem Intermediär, sondern verteilt auf den Systemen mehrerer am Netzwerk Teilnehmender betrieben. Die Hoffnung ist, die Abhängigkeit und Macht von Intermediären zu reduzieren und einen Wandel von zentralen zu dezentralen und verteilten Wertschöpfungsnetzwerken anzustossen (siehe Abbildung 1). Die Idee des Bitcoins war beispielsweise, eine Währung zu schaffen, die von keiner zentralen Instanz (wie Zentralbanken) kontrolliert wird.

Seit der Veröffentlichung dieser Idee wurde die Technologie kontinuierlich weiterentwickelt, um die Potenziale von Blockchain auch im Unternehmenskontext erschliessen zu können. Heute handelt es sich nicht mehr um eine spezifische Technologie für Kryptowährungen, sondern um eine Technologie, die Vorteile für Anwendungen in vielen Branchen bietet. Diskussionen über die Einsatzmöglichkeiten von Blockchain sind jedoch immer noch stark von Kryptowährungen und seit 2021 auch von sogenannten Non-Fungible Tokens (NFT) geprägt. Kein Wunder, dass es Führungspersönlichkeiten schwerfällt, in diesem Spannungsfeld den kurz- und langfristigen Nutzen der Technologie für ihr Unternehmen zu bewerten. Fragen, auf die Antworten gesucht werden, sind:

> Was genau sind die Vor- und Nachteile von Blockchain?
> Welchen konkreten Mehrwert bietet Blockchain in der Unternehmenspraxis?
> Wie kann dieser Mehrwert zielgerichtet erschlossen werden?

Um einen gewinnbringenden Einsatz von Blockchain zu ermöglichen, ist es essenziell, sich von pauschalen Beurteilungen zu lösen und ein differenziertes Verständnis der Technologie, ihrer Einsatzmöglichkeiten sowie von Chancen und Risiken für Unternehmen und die Gesellschaft aufzubauen. Das Ziel dieser Studie ist, hierzu einen Beitrag zu leisten. Um dies zu erreichen, gehen wir in dieser Studie auf drei Aspekte ein:

> Die Funktionsweise sowie Einsatzmöglichkeiten von Blockchain
> Ob und wie Blockchain zu einem Wandel von zentralen zu verteilten Wertschöpfungsnetzwerken beitragen kann sowie Chancen und Risiken dieses Wandels
> Potenziale, Herausforderungen und Erfolgsfaktoren in der Umsetzung von Blockchain-Anwendungen

In dieser Studie erwähnen wir an manchen Stellen Kryptowährungen, um wichtige Blockchain-Konzepte zu veranschaulichen. Das Hauptaugenmerk liegt jedoch auf Anwendungen jenseits von Kryptowährungen. Die Inhalte dieser Studie haben wir anhand von Literaturrecherchen, im Austausch mit Hochschulen und in enger Zusammenarbeit mit Fachleuten aus Unternehmen verschiedener Branchen erarbeitet. Die Zusammenarbeit mit den Industriepartnern erfolgte über bilaterale Gespräche, Projektsitzungen und drei Workshops, in denen branchenspezifische Anwendungen hinsichtlich Chancen und Herausforderungen intensiv diskutiert und bewertet wurden. Eine Übersicht der Partner findet sich im Anhang. Zur leichteren Lesbarkeit wird bei der Beschreibung grundlegender bzw. hinreichend bekannter (Blockchain-) Konzepte auf Quellenangaben verzichtet.


24/7

Eine Einführung in Blockchain

Die Blockchain-Technologie

Blockchain wurde 2008 von einer unbekannten Person oder Gruppe mit dem Pseudonym Satoshi Nakamoto mit der Anwendung Bitcoin ins Leben gerufen und 2009 erstmalig implementiert. Um eine Währung einzuführen, die von keiner zentralen Instanz kontrolliert wird, wurde ein System geschaffen, das sich selbst reguliert und Machtkonzentration vorbeugt: die Blockchain.

Traditionell werden digitale Anwendungen von einem Unternehmen betrieben. Dieses kann die Systemregeln bestimmen und festlegen, wer die Anwendung unter welchen Bedingungen nutzen kann. Zumindest theoretisch könnte es auch die enthaltenen Daten manipulieren. Liegt ein Programmfehler vor oder wird ein Cyberangriff erfolgreich durchgeführt, kann es dazu kommen, dass die Anwendung ausfällt oder die Dateninteg-

rität beeinträchtigt wird. Das heisst, jede Person oder Organisation, die eine digitale Anwendung und darauf basierende Dienstleistungen nutzt, muss darauf vertrauen, dass der Betreiber die Schutzziele der IT-Sicherheit – Verfügbarkeit, Vertraulichkeit und Integrität – gewährleisten kann (Abbildung 2). Das macht man meist unbewusst, wenn man zum Beispiel ein Bankkonto eröffnet oder bei einem Arztbesuch die Krankengeschichte mitteilt. Man vertraut darauf, dass die Systeme sicher sind, die Kontostände, Transaktionen, Blutwerte oder Röntgenbilder speichern, und verlässlich funktionieren.

Schutzziele der IT-Sicherheit

Verfügbarkeit
Informationssysteme und Daten sind verfügbar.

Vertraulichkeit
Nur berechtigte Akteure haben Zugriff.

Integrität
Die Daten sind komplett und unverändert.

Abbildung 2: Eigene Darstellung basierend auf Laudon und Laudon (2019).[8]

Verteilte Anwendungen, Distributed-Ledger-Technologie und Blockchain

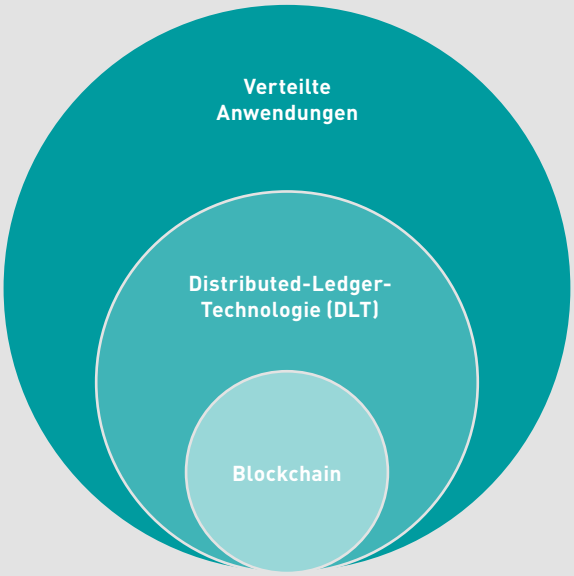


Abbildung 3: Eigene Darstellung basierend auf Hileman und Rauchs (2017).[10]

Blockchain bricht mit dem Paradigma zentral betriebener Anwendungen. Stattdessen werden Anwendungen auf die Computersysteme vieler Parteien, die auch Endnutzende sein können, verteilt. Nicht nur einer, sondern mehrere Beteiligte haben Einblick und können sicherstellen, dass die Anwendungen und darin enthaltenen Daten nicht unbemerkt manipuliert werden. Auch wenn die Systeme einzelner Parteien ausfallen, zum Beispiel aufgrund von Systemfehlern, läuft die Anwendung weiterhin stabil auf den Systemen der anderen weiter. Weil sich Beteiligte gegenseitig kontrollieren, muss man nicht mehr einem einzelnen Betreiber vertrauen, und die Notwendigkeit einer zentralen Bestimmungsinstanz kann sogar entfallen. Aber wie genau kann das funktionieren? Im Folgenden erläutern wir zunächst wichtige Blockchain-Terminologien und anschliessend die Funktionsweise von Blockchain.

Blockchain und Distributed-Ledger-Technologie

Blockchain und Distributed-Ledger-Technologie (DLT) sind spezielle Formen von verteilten Anwendungen (Abbildung 3). Verteilte Anwendungen werden auf mehreren Computersystemen statt auf einem zentralen System betrieben. Konventionelle verteilte Anwendungen werden in der Regel von einer Partei verwaltet, der alle Nutzenden vertrauen müssen. Das besondere an Blockchain und DLT ist, dass sie für den Einsatz von mehreren Parteien konzipiert sind, die sich nicht unbedingt gegenseitig vertrauen. Sie stellen die Funktionsweise einer Anwendung sicher, auch wenn einzelne Akteure versuchen diese zu manipulieren oder einzelne Systeme aufgrund technischer Fehler ausfallen.

Blockchain ist eine besondere Ausprägung der DLT, bei der Transaktionen (Änderungen an Daten) in Blöcke gebündelt und auf einer Blockchain gespeichert werden. Es gibt jedoch auch

Unterschiede zwischen offenen und zugangsbeschränkten Blockchains

KATEGORIE	OFFEN	ZUGANGSBESCHRÄNKT
Steuerung des Netzwerks	Gemeinschaft	Zentraler Dienstleister oder Konsortium aus Geschäftspartnern
Zugang zum Netzwerk	Nicht eingeschränkt	Nur zugelassene Parteien
Wichtigste Anwendungsbereiche	Offene Plattformen, auf die viele Parteien zugreifen, die sich nicht alle kennen	Organisationsübergreifende Unternehmensprozesse
Hauptziele	Abschaffung von Intermediären Erhöhung der Integrität, Manipulationssicherheit und Verfügbarkeit digitaler Infrastrukturen	Digitalisierung und Automatisierung von Unternehmensprozessen Erhöhung der Integrität, Manipulationssicherheit und Verfügbarkeit digitaler Infrastrukturen Entwicklung neuer Geschäftsfelder
Anonymität	Teilnehmende sind meist anonym	Teilnehmende sind meist nicht anonym und kennen sich auch ausserhalb der Blockchain
Datenhoheit und -einsicht	In der Regel sieht jeder alle Daten und Transaktionen Bei Bedarf kann durch Off-chain-Datenspeicherung die Einsicht eingeschränkt werden (siehe Abschnitt «Datenschutz» im folgenden Kapitel)	Datenhoheit liegt meist beim Eigentümer zur Wahrung der Vertraulichkeit Bei Bedarf kann dieser Daten teilen, zum Beispiel für Transaktionen mit direkten Geschäftspartnern

Tabelle 1: Eigene Recherche.

andere Arten der DLT, die keine Blockchains sind. Heute werden beide Begriffe jedoch häufig synonym verwendet.[9] In dieser Studie verwenden wir den Begriff Blockchain, wobei viele unserer Aussagen auch auf DLT insgesamt zutreffen.

Offene und zugangsbeschränkte Blockchains[11]

Blockchain-Technologie wird seit ihrer Einführung kontinuierlich weiterentwickelt, um den Anforderungen verschiedener Anwendungen gerecht zu werden. Heute können zwei grundsätzlich unterschiedliche Arten von Blockchains unterschieden werden: offene (englisch «permissionless») und zugangsbeschränkte (englisch «permissioned») Blockchains. Es gibt allerdings auch Mischformen.

Bei offenen Blockchains kann jede Person oder Organisation am Netzwerk teilnehmen, Transaktionen tätigen und Rechenleistung für den Betrieb der Anwendung bereitstellen. In der Regel kennen sich die Teilnehmenden nicht persönlich und treten anonym auf. Daher wird die Teilnahme am Netzwerk durch Anreizmechanismen belohnt. Das bekannteste Beispiel sind Kryptowährungen. Auf Bitcoin erhalten Miner, die Transaktionen prüfen, hierfür Bitcoins. Wichtige Ziele offener Blockchain-Anwendungen sind, die Abhängigkeit von zentralen Bestimmungsinstanzen zu vermeiden und vielen Personen oder Organisationen den Zugang zu ermöglichen.

Bei zugangsbeschränkten Blockchains darf nicht jeder Teil des Netzwerks werden. Wer mitmachen will, muss eine Mitgliedschaft beantragen und zugelassen werden. Zugangsbeschränkte Blockchains werden häufig für Unternehmensanwendungen genutzt (sogenannte Enterprise Blockchains). Hier gehen Personen oder Organisationen ausserhalb einer Blockchain Vertragsbeziehungen ein, weswegen zusätzliche Anreizmechanismen auf einer Blockchain nicht zwingend notwendig sind. Ein Beispiel ist ein System für die Rückverfolgbarkeit von Produkten, auf das bestimmte Akteure entlang der Lieferkette, wie Hersteller, Zulieferer, Transporteure oder Händler, zugreifen können. Datenintegrität und -verfügbarkeit, die Erhöhung der Effizienz in der Zusammenarbeit, Automatisierung und Kostensenkungen stehen im Vordergrund.

Häufig sind zugangsbeschränkte Systeme keine Blockchains im engeren Sinne, da weiterhin zentrale Bestimmungsinstanzen existieren. Dies kann ein Unternehmen, ein Konsortium von Unternehmen oder ein unabhängiger Serviceprovider sein, welcher zum Beispiel über die Aufnahmen neuer Mitglieder ins Netzwerk entscheidet. Diese werden dennoch als Blockchain- oder DLT-Projekte vermarktet, da sie mehrere Funktionalitäten von Blockchains einsetzen (zum Beispiel den verteilten Betrieb oder digitale Signaturen) und ohne den Hype um Blockchain vermutlich nicht zustande gekommen wären. Laut der «2nd Global Enterprise Blockchain Benchmarking Study» aus dem Jahr 2019 werden mehr als 80 % der weltweit von Unternehmen eingesetzten zugangsbeschränkten Blockchain-Anwendungen von einer zentralen Instanz gesteuert. Viele planen jedoch, später im Laufe des Projekts die Entscheidungsmacht auf mehrere Teilnehmende im Netzwerk zu verteilen.[11]

Tabelle 1 fasst die wichtigsten Eigenschaften und Einsatzbereiche von offenen und zugangsbeschränkten Blockchains zusammen. Zu berücksichtigen ist, dass weitere Ausprägungen existieren und die Tabelle nur nur gängige Einsatzbereiche und Eigenschaften darstellt.

Die Funktionsweise von Blockchain

Nachfolgend beschreiben wir die grundlegende Funktionsweise von Blockchain. In der Praxis werden verschiedene Ausprägungen und Kombinationen der genannten Techniken eingesetzt. Wir gehen besonders auf Unterschiede zwischen offenen und zugangsbeschränkten Blockchains ein.

Verteilter Betrieb

Der wichtigste Unterschied zu herkömmlichen Anwendungen ist, dass Blockchain-Anwendungen nicht auf einem zentralen Computersystem, sondern auf den Systemen mehrerer Teilnehmenden betrieben werden. Jeder dieser Teilnehmenden, auch Knoten genannt, speichert die gesamte Blockchain. Verändert nun ein Knoten unrechtmässig Daten, würden die anderen Knoten die Änderung nicht akzeptieren. Fällt ein Knoten aus, läuft die Anwendung auf den anderen Knoten stabil weiter.

Verteilter Zugriff

Bei offenen Blockchains können alle Knoten einer Blockchain auf die Daten von ihren eigenen Systemen aus zugreifen. Es gibt keine zentrale Stelle, die kontrolliert, wer die Daten einsehen darf. Bei zugangsbeschränkten Blockchains kann der Datenzugriff allerdings eingeschränkt werden und die Datenhoheit beim Eigentümer der Daten bleiben. Beispielsweise ist es möglich, dass ein Knoten nur die eigenen Transaktionen sehen kann. Das ist wichtig, um die Vertraulichkeit von Informationen wahren zu können.

Konsensmechanismus

Vereinfacht gesagt sind Konsensmechanismen Algorithmen, die sicherstellen, dass eine Übereinstimmung über Transaktionen zwischen allen Knoten gefunden wird. Im Rahmen dieser Validierung stellen sie sicher, dass eine Transaktion mit einem Wertgegenstand rechtmässig ist und nicht zwei Mal durchgeführt wird.

Auf offenen Blockchains kann in der Regel jeder Knoten alle Daten einsehen und die Rechtmässigkeit einer Transaktion prüfen. «Proof of Work» und «Proof of Stake» (siehe Box) sind derzeit die bekanntesten Konsensmechanismen auf offenen Blockchains. Bei zugangsbeschränkten Blockchains kann die Dateneinsicht eingeschränkt werden, um die Vertraulichkeit zu wahren, weswegen andere Mechanismen verwendet werden. Auf der Enterprise-Blockchain-Plattform Corda werden beispielsweise automatische Notardienste genutzt. In diesem Fall müssen nur die beteiligten Geschäftspartner eine Transaktion bestätigen, und ein Notardienst prüft automatisiert die Rechtmässigkeit der Transaktion und dass keine Konflikte mit anderen Transaktionen bestehen.

«Proof of Work» und «Proof of Stake»

Beim «Proof of Work» überprüfen Knoten Transaktionen, indem sie kryptografische Rätsel lösen. Wer das Rätsel am schnellsten löst und damit eine Transaktion validiert, erhält dafür eine Belohnung in Form einer Kryptowährung. Dieser Vorgang nennt sich «Mining» und stellt somit einen Wettbewerb dar. Grosse Chancen, die Aufgabe schnell zu lösen und die Belohnung zu erhalten, haben Miner, die über grosse Rechenleistungen verfügen. Da viele Miner parallel versuchen, das Rätsel zu lösen und die Belohnung zu

→

erhalten, ist der Stromverbrauch beim «Proof of Work» sehr hoch. Bitcoin ist eine der bekanntesten Anwendungen des «Proof of Work». Theoretisch könnte eine böswillige Person oder Gruppe von Minern versuchen, mindestens 51 % der Rechenleistung im Netzwerk bereitzustellen und damit die Kontrolle über den Konsensmechanismus erlangen (sogenannter 51 %-Angriff).

Beim «Proof of Stake» müssen Knoten einen Einsatz («Stake») in der systemeigenen Kryptowährung bieten, um als Teilnehmende in Betracht gezogen zu werden, die Transaktionen validieren dürfen. Ein Algorithmus bestimmt auf Basis des Zufallsprinzips, wer eine bestimmte Transaktion prüfen darf und eine Belohnung dafür erhält. Je höher der Einsatz, desto grösser ist die Wahrscheinlichkeit, dass man ausgewählt wird.

Verkettung

Einmal akzeptierte Transaktionen sind nicht mehr veränderbar, um sicherzustellen, dass diese im Nachhinein nicht abgestritten werden können. Hierzu werden Transaktionen verkettet gespeichert. In der Praxis spricht man in diesem Zusammenhang von «single source of truth». Wenn Daniel das Eigentum an einem Wertgegenstand an Jan überträgt und dieser es an Karin weitergibt, dann wird der Übergang des Eigentums auch in dieser Reihenfolge festgehalten.

Verschlüsselung und Anonymität

Bei offenen Blockchains sind alle auf einer Blockchain gespeicherten Daten von allen Knoten einsehbar. Allerdings will man auch hier häufig nicht, dass die Daten zu viel preisgeben. Daher treten die Teilnehmenden nicht mit ihrer echten Identität, sondern anonymisiert mit einer alphanumerischen Adresse, dem sogenannten öffentlichen Schlüssel, auf. Das Netzwerk kennt nur diesen öffentlichen Schlüssel und nutzt ihn für die Abwicklung von Transaktionen. Alle Mitglieder haben zusätzlich einen privaten Schlüssel, den nur sie selbst kennen. Alles, was mit dem privaten Schlüssel verschlüsselt wird, kann ausschliesslich mit dem zugehörigen öffentlichen Schlüssel entschlüsselt werden und umgekehrt. Darüber wird sichergestellt, dass nur diejenige Person, die im Besitz eines privaten Schlüssels ist, tatsächlich Transaktionen im Namen des zugehörigen öffentlichen Schlüssels durchführen kann. Diese Technik wird auch digitale Signatur genannt.

Digitale Signaturen werden auch auf zugangsbeschränkten Blockchains verwendet. Hier müssen Akteure allerdings erst zugelassen werden, bevor sie Teil des Netzwerks werden können. Der Zulassungsprozess kann deren Identität offen legen. Daher ist die Anonymität nicht zwingend gegeben. Bei Unternehmensanwendungen ist auch häufig gewünscht, dass man weiss, mit wem man Geschäfte abschliesst. Um dennoch die Vertraulichkeit der Daten zu wahren, können die Zugriffsrechte eingeschränkt werden. Zum Beispiel kann auf der Blockchain-Plattform Corda der Zugriff so eingeschränkt werden, dass jeder Knoten nur die Transaktionen sieht, in die er selbst als Partei involviert war.

Datenschutz

Auch unter Gewährleistung der Anonymität sollen auf Blockchains nicht alle Daten, beispielsweise Vertragskonditionen oder Preise, von anderen eingesehen werden. Dies kann durch sogenannte Hashfunktionen sichergestellt werden. Eine Hashfunktion erstellt einen Hashwert, eine Art Fingerabdruck von Daten. Werden Daten verändert, so

verändert sich auch der Hashwert. Vom Hashwert kann man nach heutigem Stand nicht zurück auf die Daten schliessen.

Hashfunktionen bieten die Möglichkeit, die eigentlichen Daten ausserhalb einer Blockchain zu speichern («off-chain»), zum Beispiel bei einer Institution, die Nutzungsrechte an den Daten hat. Um zu vermeiden, dass die Daten unrechtmässig manipuliert werden, wird der Hashwert auf einer Blockchain gespeichert. Über diesen kann geprüft werden, dass die Daten zwischen der Hinterlegung des Hashwerts und der Bereitstellung für einen bestimmten Zweck nicht verändert wurden.

Smart Contracts

Smart Contracts («selbstausführende Verträge») sind Prozessschritte, die in Form eines Programmcodes auf Blockchains geschrieben werden und automatisiert ablaufen, sobald vordefinierte Bedingungen eintreten. Zum Beispiel könnten Temperatursensoren an Produktverpackungen von Arzneimitteln kontinuierlich die Umgebungstemperatur messen, um sicherstellen zu können, dass Kühlketten eingehalten werden. Liegt die Temperatur zu lange über einem kritischen Wert, könnte über einen Smart Contract das Produkt automatisch als fehlerhaft markiert und aus der Lieferkette genommen werden. Da diese Logik fest auf Blockchains geschrieben ist, ist die Einhaltung der «Verträge» sichergestellt.

Tokens und Tokenisierung

Ein Token ist ein Wertgegenstand, der auf einer Blockchain digital abgebildet wird und handelbar ist. Das bekannteste Token ist der Bitcoin, der wie eine Währung gehandelt werden kann und deshalb als ein «Payment» oder «Currency Token» bezeichnet wird.

Es gibt allerdings auch noch andere Arten von Tokens. «Utility Tokens» bilden Rechte wie Abstimmungs- oder Zugangsrechte ab. Zum Beispiel können Plattformanbieter solche Tokens an Personen verkaufen, die Zugriff auf die Plattform erhalten möchten. Im Rahmen der Zugangskontrolle werden die Tokens beim Login verlangt. Denkbar wäre auch, dass ein Führerausweis als ein Utility Token abgebildet wird. Beim Mieten eines Autos müsste man dieses Token mithilfe des Smartphones vorzeigen. «Security Tokens» sind eine Art von Wertpapieren. «Equity Tokens» sind eine Art von «Security Tokens», die direkt mit Unternehmensanteilen und Abstimmungsrechten verknüpft sind.[12]

Unter «Tokenisierung» wird im Blockchain-Umfeld die Abbildung realer Güter auf einer Blockchain in Form von Tokens verstanden. Beispielsweise könnte ein Gebäude im Wert von zehn Millionen Schweizer Franken in 100 000 digitalen Tokens zu je 100 Schweizer Franken abgebildet werden, die dann gehandelt werden können.[13] Über Smart Contracts könnte sichergestellt werden, dass Personen, die solche Tokens besitzen, auch einen Anteil der Mieteinnahmen des Gebäudes erhalten. Die Aufteilung des Eigentums an Wertgestenständen nennt man auch «Fraktionalisierung». Tokens können aber auch weniger wertvolle Gegenstände abbilden, etwa Waren, die zwischen Unternehmen entlang einer Lieferkette weitergegeben werden, um deren Herkunft zu überwachen und Fälschungen zu identifizieren.[14]

Zu berücksichtigen ist, dass Blockchain nicht sicherstellen kann, dass Transaktionen mit realen Gütern, die auf einer Blockchain stattfinden, auch tatsächlich in der realen Welt durchgeführt werden. Das bedeutet: Immer wenn eine Blockchain genutzt wird, um Werte oder Gegenstände, die in der realen Welt existieren, zu verwalten, sind

Mechanismen ausserhalb einer Blockchain («off-chain») notwendig, um die Einhaltung von Transaktionen sicherzustellen. Solche Mechanismen können beispielsweise Audits sein.[15]

Kryptowährungen

Eine Kryptowährung ist eine virtuelle Währung, die durch die Nutzung von Blockchain gemeinsam von einem Netzwerk betrieben und somit von keiner zentralen Instanz gesteuert wird. Ein Ziel von Kryptowährungen ist, die Abhängigkeit von (Zentral-)Banken abzubauen und somit staatliche Eingriffe in das Geldsystem zu vermeiden. Die mit Kryptowährungen verbundene Hoffnung ist die Schaffung eines verteilten und robusten Finanzsystems, in dem Zahlungen schneller und günstiger durchgeführt werden können als im herkömmlichen Bankensystem.

Bitcoin und Ether sind die bekanntesten Kryptowährungen, wobei auf CoinMarketCap mittlerweile nahezu 10 000 Kryptowährungen gelistet sind.[16] Kryptowährungen werden jedoch auch häufig aufgrund fehlender Regulierbarkeit, ihrer immensen Wertschwankungen, ihres hohen Stromverbrauchs und ihres Einsatzes für illegale Aktivitäten kritisiert. Manche Ökonomen sagen auch, dass Kryptowährungen niemals echte Währungen werden. Dies liegt unter anderem daran, dass es unwahrscheinlich ist, dass sie von Regierungen akzeptiert werden, weshalb sie nicht für wichtige Finanztransaktionen wie Steuern genutzt werden können.[17]

Non-fungible Tokens

NFTs stehen für einzigartige, nicht ersetzbare Wertgegenstände. Ein Bitcoin, ein sogenanntes Payment Token, kann mit jedem anderen Bitcoin getauscht werden. Ein NFT repräsentiert digital einen Wertgegenstand, der nur einmal oder wenige Male existiert und dessen Eigentumsrechte geschützt werden sollen. NFTs werden vor allem für den Schutz von Eigentumsrechten immaterieller Wertgegenstände (zum Beispiel digitaler Kunst) eingesetzt, da diese häufig auf einfache Weise kopiert werden können und die Eigentumsrechte schlecht geschützt sind. Sie können aber auch eingesetzt werden, um das Eigentum an materiellen Wertgegenständen abzubilden. NFTs ermöglichen beispielsweise Kunstschaffenden, ihre Kunst direkt ohne Auktionshäuser oder Galerien zu verkaufen, die herkömmlicherweise die Echtheit von Werken bestätigen und das Vertrauen von Kaufinteressierten geniessen. Zusätzlich können über Smart Contracts Bedingungen festgelegt werden, etwa Lizenzgebühren, die automatisch jedes Mal bezahlt werden müssen, wenn ein Werk weiterverkauft wird. Im Jahr 2021 betrug das Marktvolumen für NFTs 41 Milliarden US-Dollar.[18]

Ein prominentes Beispiel ist die NFT-Kollektion des Kunstfälschers Wolfgang Beltracchi. Der Künstler kam zu zweifelhaftem Ruhm, weil er jahrelang Bilder grosser Meister gefälscht und über bekannte Auktionshäuser verkauft hatte. Nun hat er 4 608 verteilt auf einer Blockchain gespeicherte

→

digitale Kunstwerke geschaffen, von denen jedes in unterschiedlichem künstlerischem Stil auf dem Gemälde «Salvator Mundi» von Leonardo da Vinci basiert. Während das Originalbild 2017 für eine Rekordsumme von 450 Millionen US-Dollar versteigert wurde, bot Beltracchi seine NFTs für insgesamt 55 Millionen Schweizer Franken zum Verkauf an.[19]

Leistungsfähigkeit und Stromverbrauch

Die Leistungsfähigkeit von Blockchains hinsichtlich des Durchsatzes (Transaktionen pro Sekunde) und der Geschwindigkeit bzw. Latenz (Dauer bis zum Abschluss eine Transaktion) wird kritisch diskutiert. Das sogenannte Blockchain-Trilemma besagt, dass eine hohe Skalierbarkeit, das heisst die Erhöhung des Transaktionsvolumens ohne Beeinträchtigung der Geschwindigkeit, im Konflikt mit der Dezentralität und Sicherheit von Blockchains steht. Bei zugangsbeschränkten Blockchains sind der Durchsatz und die Geschwindigkeit in der Regel ausreichend hoch, die Dezentralität und Sicherheit aber niedriger als auf offenen Blockchains.

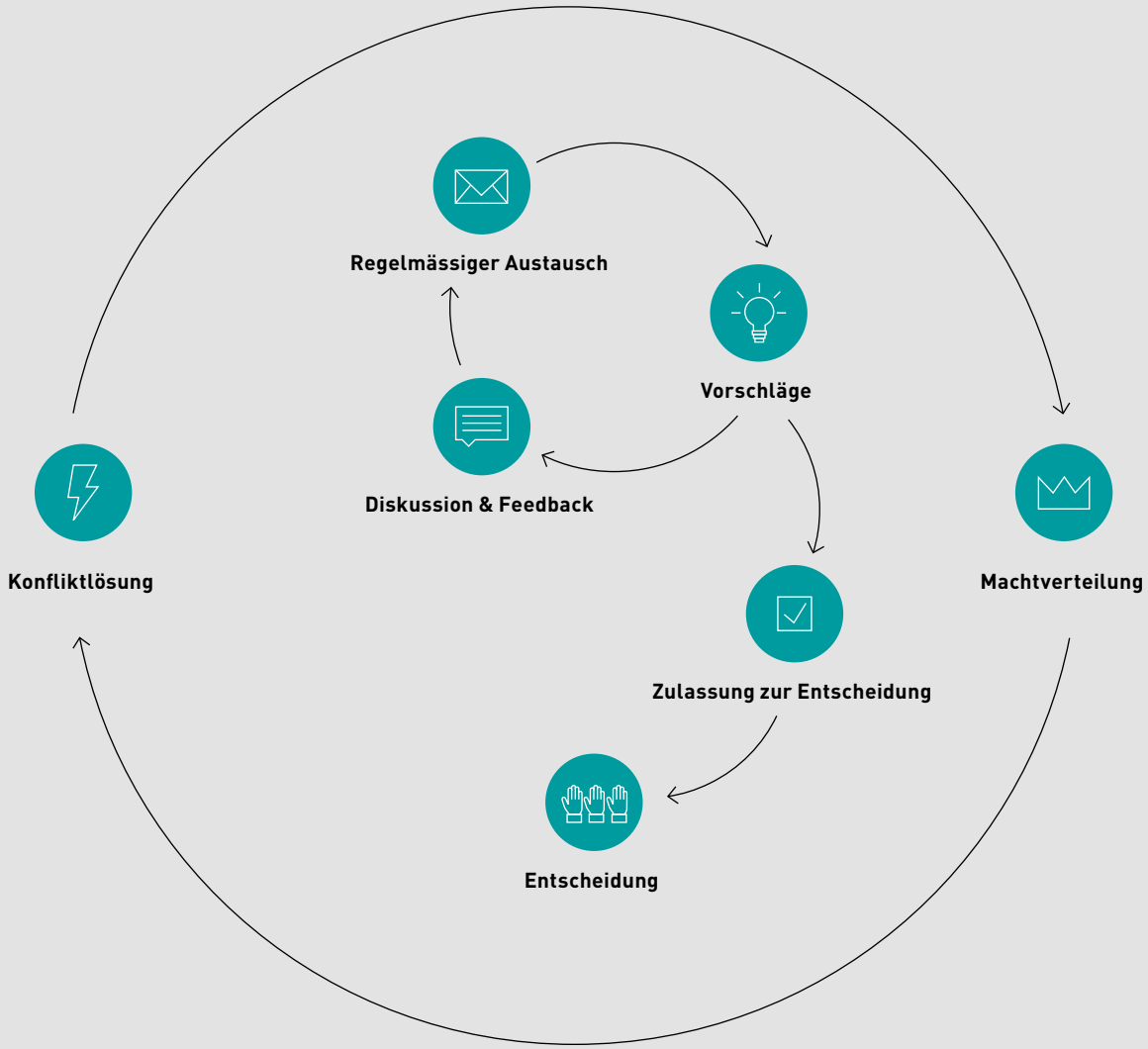
Der Stromverbrauch ist hauptsächlich bei offenen Blockchains, welche den «Proof-of-Work»-Konsensmechanismus verwenden, sehr hoch. Schätzungen gehen davon aus, dass das Bitcoin-System pro Jahr mehr als doppelt so viel Strom verbraucht wie die ganze Schweiz.[24] Bei offenen Blockchains mit «Proof-of-Stake»-Konsensmechanismus oder bei zugangsbeschränkten Blockchains ist dieser bedeutend geringer. Die Ethereum Foundation, welche im September 2022 von «Proof-of-Work» auf «Proof-of-Stake» umstellte (sogenannter «Merge»), erwartet, dass damit der Stromverbrauch von Ethereum um 99,95 % sinkt.[25] Der Nachteil ist allerdings, dass Mitglieder mit grösseren finanziellen Mitteln einen grösseren Einfluss auf das Netzwerk haben, da der «Stake» an der Währung über deren Zuteilung entscheidet. Letztlich muss für jede Anwendung individuell entschieden werden, welches Konstrukt sich am besten eignet.

Blockchain-Governance

Wenn Entscheidungen im Netzwerk von vielen Mitgliedern getroffen werden, stellt sich die Frage, wie die Entscheidungsfindung funktioniert. Governance im engeren Sinne beschäftigt sich mit genau dieser Frage. Dabei geht es weniger um prozessuale Entscheidungen wie die Prüfung von Transaktionen. Denn diese sind Bestandteil der Ablauforganisation, also der Regeln und Prozesse, welche die grundsätzliche Funktionsweise einer Anwendung sicherstellen. Vielmehr geht es um Entscheidungen, wie sich diese Ablauforganisation verändern lässt, um flexibel auf sich ändernde Bedingungen reagieren zu können. Beispiele für solche Entscheidungen sind der Wechsel des Konsensmechanismus von «Proof of Work» zu «Proof of Stake» in offenen Netzwerken oder die Aufnahme neuer Mitglieder in zugangsbeschränkten Netzwerken.

Die Governance-Mechanismen legen fest, wer auf welche Weise Einfluss auf das System nehmen kann, und beeinflussen somit massgeblich die Akzeptanz und langfristige Tragfähigkeit einer Anwendung. Bei der Ausgestaltung dieser Mechanismen spielen nicht nur die Interessen der Gründungsmitglieder eine Rolle, sondern auch die aller zukünftigen potenziellen Netzwerkmitglieder, um Vertrauen in die Lösung zu schaffen. Die Herbeiführung von Entscheidungen fängt lange vor

Wichtige Governance-Mechanismen bei Blockchain-Projekten



Wie werden Mitglieder über Entwicklungen und Änderungen informiert und können sich über diese austauschen.

Wer kann Änderungsvorschläge über welchen Kanal erreichen?

Wer kann über welchen Kanal Feedback zu Änderungsvorschlägen einbringen?

Wie werden Änderungsvorschläge zur Entscheidung zugelassen?

Wie wird über zugelassene Änderungsvorschläge entschieden?

Was geschieht bei Konflikten, die nicht von den Mitgliedern selbst gelöst werden können, oder bei böswilligem Verhalten einzelner Akteure?

Wie wird sichergestellt, dass kein Akteur andere Akteure zu sehr beeinflusst und ein unangemessen grosses Maas an Entscheidungsmacht auf sich vereint?

Abbildung 4: Eigene Darstellung inspiriert durch Barrera (2019).[20]

On-chain-Abstimmungsmechanismen von drei Blockchain-Lösungen

NAME	BESCHREIBUNG DER ABSTIMMUNGSMECHANISMEN
DASH	Jeder kann für einen Preis von einem Token Vorschläge einreichen. Masterknoten können über Vorschläge abstimmen, wobei jeder Masterknoten eine Stimme hat. Jeder kann Masterknoten werden sofern er/sie mindestens 1 000 Tokens besitzt. Vorschläge werden angenommen, wenn die Differenz zwischen der Anzahl an Zustimmungen und Ablehnungen mindestens 10% aller verfügbaren Stimmen entspricht.
TEZOS	Token-Besitzer können Tokens sogenannten «Bakern» zuweisen, die ihre Interessen am besten vertreten. «Baker» kann jeder Knoten werden, der mindestens 6 000 Token besitzt. «Baker» können Änderungen vorschlagen und darüber entscheiden. Der Vorschlag wird angenommen, wenn eine Mindestanzahl von Tokens abgestimmt hat und eine qualifizierte Mehrheit zustimmt.
EOS	Token-Besitzer wählen kontinuierlich 21 «Block Producer». Diese können Entscheidungen treffen wenn mindestens 15 «Block Producer» über eine Periode von 30 Tagen zustimmen.

Tabelle 2: Zusammenfassung nach Watson Law (n. d.)[21] und weiteren Recherchen.

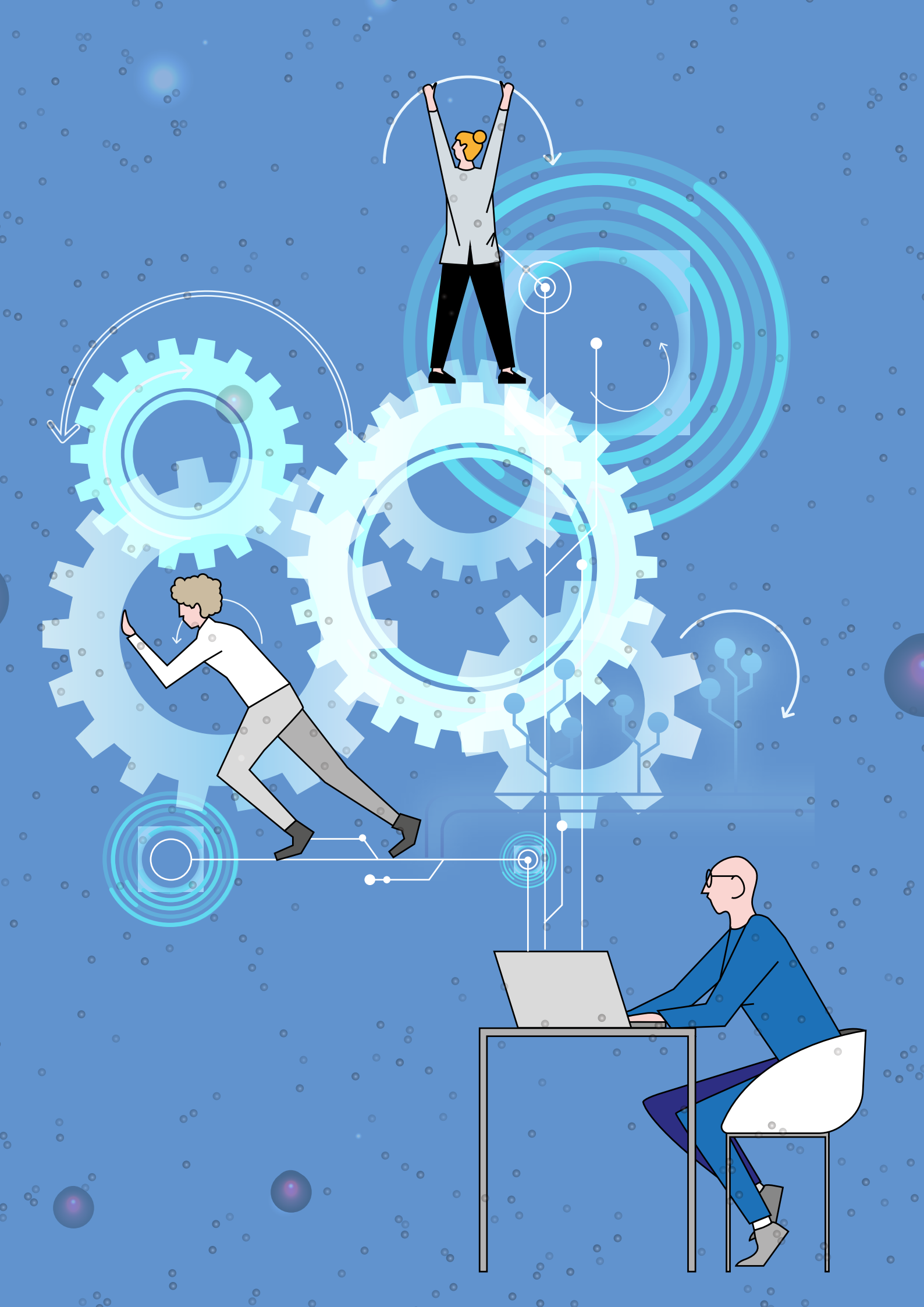
dem eigentlichen Treffen der Entscheidung an, wie in Abbildung 4 dargestellt wird.

Blockchain differenziert zwei Arten von Entscheidungsmechanismen: On-chain-Mechanismen werden fest in den Programmcode einer Blockchain geschrieben. Bei Off-chain-Mechanismen werden Entscheidungen ausserhalb einer Blockchain, zum Beispiel in Meetings oder auf Konferenzen, getroffen.

On-chain-Entscheidungen müssen in Form klarer Regeln abgebildet werden. Meist handelt es sich dabei um Abstimmungen. On-chain-Abstimmungen werden vor allem auf offenen Blockchains eingesetzt, da sich die Netzwerkmitglieder hier untereinander nicht kennen. Tabelle 2 zeigt beispielhaft On-chain-Abstimmungsmechanismen von drei Blockchain-Lösungen vor.

Bei Unternehmensanwendungen in zugangsbeschränkten Blockchains werden Entscheidungen häufig off-chain getroffen. Die Fixierung der Mechanismen on-chain ist hier weniger wichtig, da die am Netzwerk teilnehmenden Unternehmen sich meist auch ausserhalb der Blockchain kennen und dort Vertragsbeziehungen, die rechtlich bindend sind, eingehen.[22]

On-chain- und Off-chain-Mechanismen können auch beliebig kombiniert werden. Zum Beispiel werden Änderungsvorschläge häufig ausserhalb der Blockchain eingereicht und diskutiert (zum Beispiel in Foren), bevor auf der Blockchain darüber abgestimmt wird. Beim Kryptowährungsprojekt Decred wird zum Beispiel über unbedeutendere Entscheidungen on-chain abgestimmt, während strategische Entscheidungen nach definierten Regeln off-chain getroffen werden.[23]



Nutzen der Blockchain-Technologie

«Distributed-Ledger-Technologie gab uns die Möglichkeit, die Transparenz und B2B-Effizienz in der globalen Gold-Wertschöpfungskette zu erhöhen und zugleich die Daten- und Transaktionshoheit der Businesspartner zu wahren. Das Vertrauen in Gold wird, dank dem unveränderbaren Integritätszertifikat, wieder gestärkt.»

Urs Rööslı, CEO, aXedras Group

Im Folgenden stellen wir Ziele des Einsatzes von Blockchains vor und fassen anschliessend Blockchain-Anwendungen, die in der Literatur diskutiert und von Unternehmen entwickelt werden, zusammen.

Ziele des Einsatzes von Blockchain

Entlang der Dimensionen «Automatisierungsgrad» und «Machtkonzentration» unterscheiden wir vier Ziele von Blockchains: Integrität, Automatisierung, Kooperation und die Schaffung verteilter Wertschöpfungsnetzwerke (Abbildung 5).[24]

Integrität

Das Hauptziel der Integrität ist es, ein manipulationssicheres Datenregister zu erstellen. Dies wird durch den verteilten Betrieb einer Blockchain-Anwedung sichergestellt: Unrechtmässige Änderungen würden bemerkt werden, und eine hohe Verfügbarkeit des Systems ist gewährleistet, da es auch dann weiterläuft, wenn einzelne Knoten ausfallen. Beispiele für Blockchain-Anwendungen mit dem Ziel der Integrität sind digitale Grundbücher, Echtheitszertifikate für Wertgegenstände zur Vermeidung von Fälschungen oder Herkunftsnachweise von Waren wie Nahrungsmittel. Tendenziell steigt der Bedarf nach integren Informationen zu Produkten und Organisationen. Zum Beispiel berücksichtigen private und institutionelle Anlegende zunehmend Nachhaltigkeitskriterien in ihren Investitionsentscheidungen. Hierzu müssen Daten entlang der gesamten Lieferkette erfasst werden, und zwar vom Produktionsort bis zu allen Zulieferern, inklusive der Herkunft von Inhaltsstoffen und der genutzten Transportmittel.

Automatisierung

Ein weiteres Ziel der Blockchain-Technologie ist, möglichst viele Prozessschritte zu automatisieren, auch unter Nutzung von Smart Contracts. Tokens können genutzt werden, um physische Waren und virtuelle Werte wie Eigentums- oder Zugangsrechte abzubilden und handelbar zu machen. Effizienzsteigerung und Vermeidung von menschlichen Fehlern in manuellen Prozessen stehen im Vordergrund. Beispielsweise können auf sichere Weise digitale Zwillinge, digitale Abbilder von physischen Objekten, erstellt werden und hierdurch Produktions-, Lager- und Auditprozesse digitalisiert und automatisiert werden.

Eine Voraussetzung für Automatisierung ist, dass sich die Prozesse mit bedingungsabhängiger Logik darstellen lassen. Je strukturierter ein Prozess ist, desto grösser ist das Potenzial für Automatisierung. Zur Illustration ein Beispiel: Nach dem Erhalt einer Zahlung unter Angabe der Auftragsnummer kann automatisiert eine Zahlungseingangsbestätigung ausgestellt und die entsprechende Forderung aus dem verteilten Buchhaltungssystem ausgebucht werden.

Wenn physische Objekte eine Rolle spielen, lassen sich nicht alle Schritte über Blockchain automatisieren. Es muss eine Schnittstelle zur realen Welt zur Verfügung gestellt werden, da die Blockchain nur in der digitalen Welt existiert. Hier sind Offchain-Mechanismen wie Audits zur Einhaltung der Vereinbarungen, Produktidentifizierungsmerkmale und allenfalls angebrachte Sicherheitstechnologien notwendig.

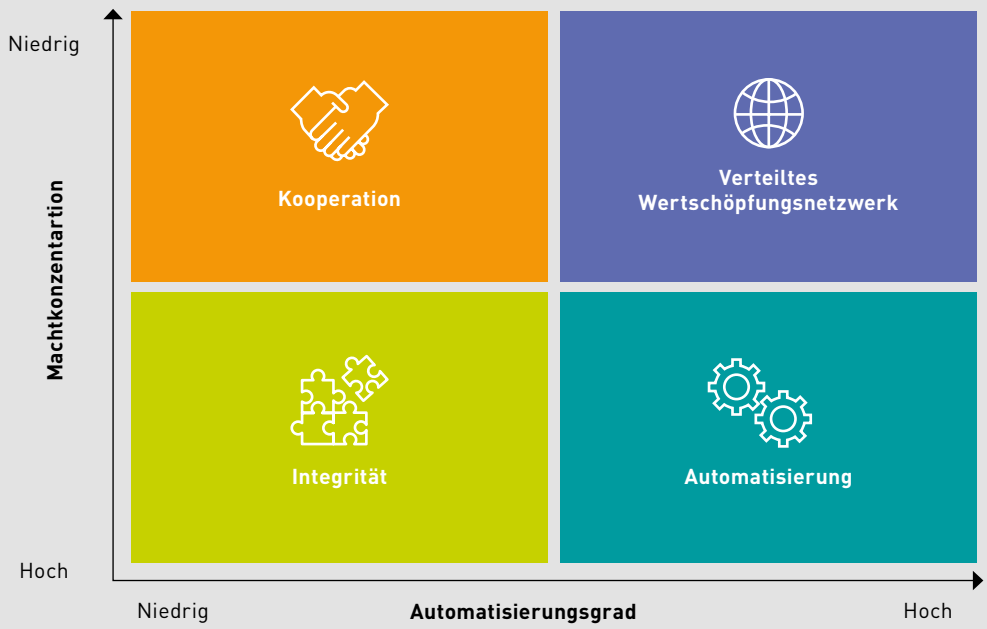


Abbildung 5: Eigene Darstellung basierend auf Heines und Gürpinar (2022).[26]

Kooperation

Ein weiteres Ziel für den Einsatz von Blockchain-Technologie ist, Koordinationsaufwände zu reduzieren und die effiziente Zusammenarbeit vieler Parteien zu ermöglichen. Die Prozesse der Zusammenarbeit werden hierfür als Logik formalisiert direkt on-chain in den Programmcode einer Blockchain geschrieben, wodurch sie manipulationssicher werden. Ein Beispiel sind Systeme für die Produktnachverfolgung. Über Blockchain teilen Hersteller, Zulieferer, (Zwischen-)Händler, Transportdienstleister sowie Verkaufsstellen Informationen über Produkte, ihre Herkunft und Lieferwege, um Transparenz sowie Planungs- und Produktsicherheit zu erhöhen. Neben der operativen Zusammenarbeit kann auch das Treffen von strategischen Entscheidungen durch Blockchain-Technologie unterstützt werden. Beispielsweise können Abstimmungen zwischen allen Personen oder Organisationen, die Tokens besitzen, stattfinden.

Verteilte Wertschöpfungsnetzwerke

In zentral organisierten Wertschöpfungsnetzwerken stellt eine Instanz eine Infrastruktur bereit, mit der Nutzende interagieren und über die sie Daten austauschen. In verteilten Wertschöpfungsnetzwerken bilden die Systeme der Teilnehmenden diese sogenannte digitale Plattform. Gemeinsam können sie über die Teilnahmebedingungen und Interaktionsregeln entscheiden. Zusammenarbeits- und Geschäftsprozesse werden möglichst vollständig in den Programmcode einer Blockchain geschrieben. Hierdurch sinken die Transaktionskosten, wodurch die Lösung einfach skaliert werden kann und mehr Personen oder Organisationen Zugang zum System erhalten. Im Unterschied zu konventionellen marktplatzorientierten Plattformen wie Uber, Facebook oder AirBnB liegen die Entscheidungsbefugnisse nicht in den Händen einzelner mächtiger Organisationen, sondern sind auf viele Schultern verteilt. Möglich wäre beispielsweise eine Peer-to-Peer-Carsharing-Lösung, bei der Veränderungen am System

über Abstimmungen unter allen Mitgliedern beschlossen werden. Die Prüfung des Führerausweises findet automatisch im Hintergrund statt, und die Zahlung wird beim Aufschliessen des Autos in Kryptowährung ausgelöst.

Abbildung 6 beschreibt Leitfragen, die helfen sollen, Ziele für den Einsatz von Blockchain-Technologie zu identifizieren. Diese Darstellung basiert auf einer Analyse bestehender Entscheidungsmodelle für den Einsatz von Blockchain.[27] Wir haben die Komplexität dieser Modelle vereinfacht und die Leitfragen den vier zuvor genannten Zielsetzungen zugeordnet. Jede Entscheidung, Blockchain-Technologie zu nutzen, bedarf selbstverständlich einer tiefer gehenden Analyse.

Dezentralisierte Autonome Organisationen

Um das Ziel eines verteilten Wertschöpfungsnetzwerkes zu erreichen, wie im Zielframework skizziert, braucht es eventuell neue Organisationsformen. Eine Form, die durch Blockchain-Technologie umgesetzt wird, sind Dezentrale Autonome Organisationen (DAO). Gesteuert werden sie durch ihre eigenen Mitglieder auf ein gemeinsames Ziel hin. In einer DAO existieren keine klassischen Managementfunktionen, stattdessen treffen die Mitglieder, häufig Personen, die Anteile an der DAO halten, durch Abstimmungen Entscheidungen. Operative Prozesse werden so weit wie möglich unter Nutzung von Smart Contracts automatisiert, sodass die Organisation ihren Zweck eigenständig erfüllen kann.[28]

→

DAOs reduzieren die Abhängigkeit von zentralen Instanzen, sind transparent und effizient, da alle Prozesse in Form von Codes einsehbar und automatisiert sind. Allerdings sind Fragen der Haftung bei DAOs noch ungeklärt, und im Falle von unvorhersehbaren Ereignissen sind gegebenenfalls doch Eingriffe von Menschen erforderlich. Beispielsweise wurde 2016 infolge eines DAO-Hacks auf Ethereum, bei dem mehr als 3,6 Millionen Ether gestohlen wurden, eine tiefgreifende Veränderung im Programmcode vorgenommen (ein sogenannter «Hard Fork»), um den Hack rückgängig zu machen.[29] Diese Protokolländerung führte dazu, dass es seitdem Ethereum Classic und Ethereum gibt. Letztere hat neben Bitcoin die grösste Marktkapitalisierung und ist das Rückgrat von NFTs und der dezentralen Finanzwelt (Decentralized Finance, DeFi).

Blockchain in der Unternehmenspraxis

Zu berücksichtigen ist, dass in der Praxis oft Kombinationen der vier Ziele verfolgt werden und die Ziele aufeinander aufbauen. Die integre Speicherung und Verarbeitung von Daten ist eine Minimalvoraussetzung für die Automatisierung und Kooperation mit Blockchain, welche wiederum Voraussetzungen für die Schaffung verteilter Wertschöpfungsnetzwerke sind.

Diskussionen über die Einsatzmöglichkeiten von Blockchain-Technologie drehen sich häufig um die vollständige Abschaffung von Intermediären durch verteilte Wertschöpfungsnetzwerke. Wer-

Blockchain-Zielframework

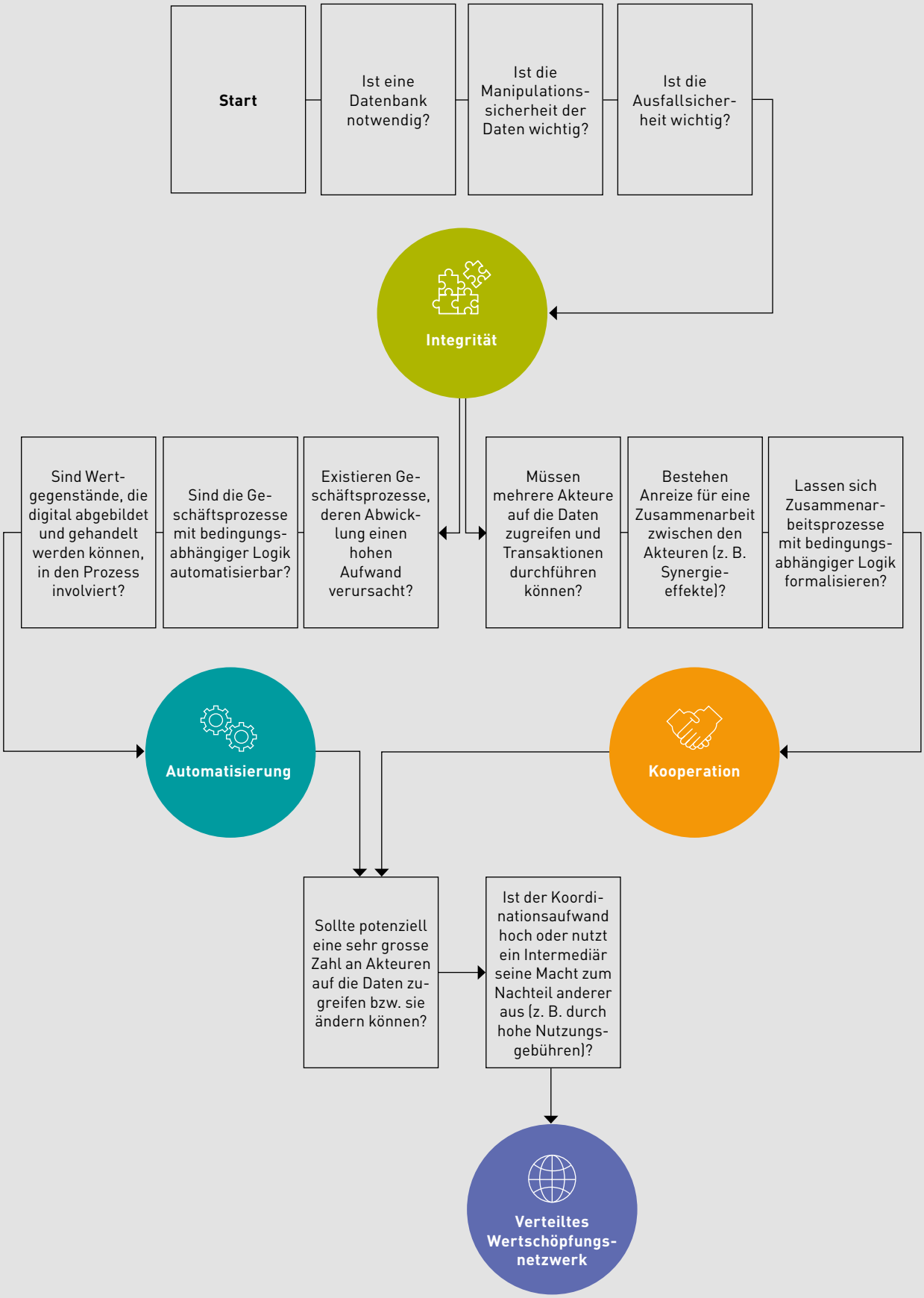


Abbildung 6: Eigene Darstellung inspiriert durch Meunier (2016).[27]

Beliebteste Blockchain-Plattformen

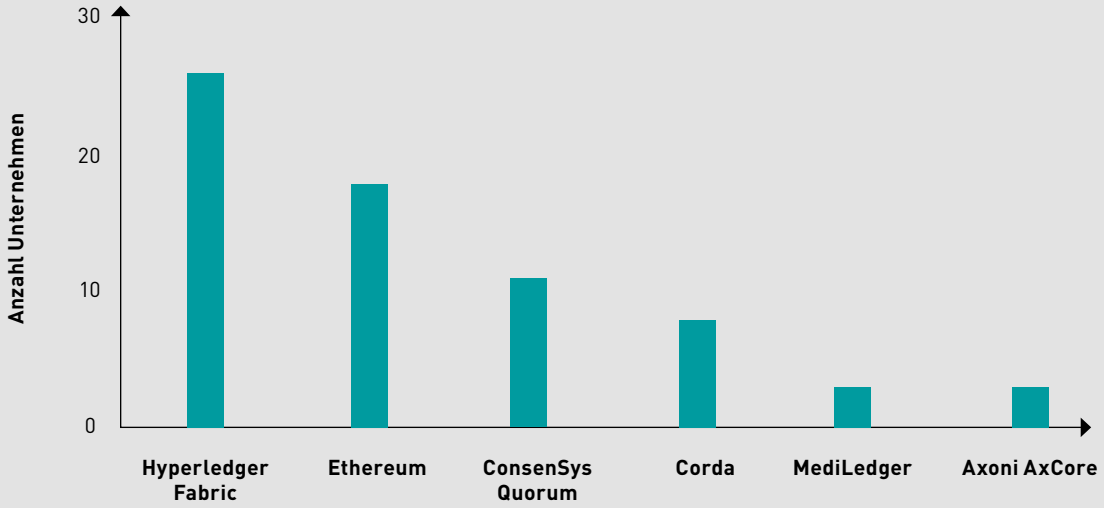


Abbildung 7: Blockckdata (2021).[31] Anzahl der 100 grössten börsennotierten Unternehmen, die eine entsprechende Blockchain-Plattform nutzen.

den durch Blockchain die integre Speicherung und Verarbeitung von Daten, die Automatisierung oder eine effizientere Kooperation verfolgt, ist allerdings weiterhin möglich, dass eine zentrale Instanz oder ein Konsortium aus Geschäftspartnern das Netzwerk steuert. Wie weiter oben beschrieben, wurden im Jahr 2019 mehr als 80 % der weltweit von Unternehmen eingesetzten zugangsbeschränkten Blockchain-Anwendungen von einer zentralen Instanz gesteuert.[30] Demnach müssen bewährte Strukturen wie zentrale Dienstleister nicht zwingend aufgelöst werden, um Blockchain gewinnbringend einzusetzen. Es können auch so robustere und effizientere digitale Infrastrukturen geschaffen werden, die dabei helfen, die Sicherheit und Effizienz in Unternehmensprozessen, speziell in der organisationsübergreifenden Zusammenarbeit, zu erhöhen.

Für Unternehmensanwendungen spielen heute zugangsbeschränkte Blockchains eine grosse Rolle. Hier möchte ein Netzwerk aus Geschäftspartnern weiterhin die Kontrolle über das Wertschöpfungsnetzwerk haben und sicherstellen können, dass die Vertraulichkeit der Daten gewährleistet ist. Das System wird verteilt auf den Computersystemen mehrerer zugelassener Organisationen betrieben, um die Manipulations- und Ausfallsicherheit zu erhöhen. Durch klar definierte Schnittstellen und Smart Contracts wird der Datenaustausch zwischen den Organisationen sicher automatisiert. Viele technologische Dienstleister bieten Blockchain-Infrastrukturen und Entwicklungsumgebungen an, mit denen Unternehmen zugangsbeschränkte (aber auch offene) Blockchain-Systeme entwickeln können. Abbildung 7 zeigt die beliebtesten Blockchain-Plattformen in Grossunternehmen.

Oft ist das Durchdenken einer Anwendung mithilfe von Blockchain-Technologie auch ein Treiber dafür, bestehende manuelle Prozesse zu standardisieren, denn dies ist eine Voraussetzung, um sie mittels Blockchain zu digitalisieren. Sind Unternehmensprozesse anhand von Blockchain manipulationssicher abgebildet, können sich viele neue Anwendungen und Geschäftsmodelle eröffnen. Ein Beispiel hierfür sind elektronische Identitäten (E-IDs). Anhand von Blockchain können Personen, Organisationen oder Objekte im digitalen Raum eindeutig und sicher identifiziert werden. Dies biete viele neue Möglichkeiten wie eine Zugangsverwal-

tung zu Gebäuden ohne physische Schlüssel, fälschungssichere Echtheitszertifikate für Waren, Peer-to-Peer-Marktplätze oder eine robuste Dateninfrastruktur für das Internet der Dinge. Nach der «2nd Global Enterprise Blockchain Benchmarking Study» verfolgen die meisten Unternehmen durch den Einsatz von Blockchain im ersten Schritt das Ziel der Kostenreduktion und anschliessend auch das Ziel der Entwicklung neuer Geschäftsfelder und der Steigerung des Umsatzes.[32]

Rückverfolgung von Gold mittels digitaler Zwillinge

Die Schweiz spielt eine massgebende Rolle im globalen Goldmarkt. Über ein Drittel des Goldes werden in der Schweiz raffiniert und Zürich ist neben London einer der wichtigsten globalen Handelsplätze für Gold. Der Datenaustausch entlang der Wertschöpfungskette ist geprägt von Datensilos und fehlenden Datenstandards, worunter Transparenz, Effizienz und Fälschungssicherheit leiden. Eine zentrale Herausforderung ist daher, Transparenz über den Ursprung des Goldes herzustellen und gleichzeitig die Vertraulichkeit hinsichtlich Besitzverhältnissen, Preisen und Bezugsmengen zu wahren.

aXedras wurde von Spezialisten der Edelmetall- und IT-Industrie gegründet, um eine spezifische Produktplattform für diese Herausforderungen zu entwickeln. Die Lösung wurde in einem zugangsbeschränkten DLT-System gefunden, über das bereits 30 Mitglieder global Daten zu physischen Produkten austauschen und gleichzeitig die Hoheit über die vertraulichen Transaktionsdetails behalten. Jedes physische Produkt erhält einen digitalen Zwilling mit Integritätszertifikat, das eine manipulationssichere Dokumentation über die Herkunft und Stationen entlang der Lieferkette enthält. Hierdurch erhöhen sich für Mitglieder die Effizienz in der Zusammenarbeit entlang der Lieferkette sowie die Transparenz gegenüber Abnehmern (Unternehmen der Industrie, aus der Schmuck- und Uhrenbranche) und Finanzinvestoren.

Die grösste Schwierigkeit in der Umsetzung bestand darin, die unabhängigen Akteure in der weltweiten Wertschöpfungskette zu überzeugen, dem Netzwerk beizutreten. Dabei halfen die gute Vernetzung in der Industrie sowie die neutrale Position von aXedras als reiner Technologieanbieter. Die Plattform wird nun weiter ausgebaut, um in Zukunft Lieferketten anderer hochwertiger Produkte zu digitalisieren und damit für mehr Transparenz, Effizienz und Vertrauen zu sorgen.

Blockchain-Anwendungen in zehn verschiedenen Branchen

Die oben beschriebenen Nutzen von Blockchain bieten Vorteile in vielen Branchen. Aufgrund der weiterhin stark voranschreitenden Digitalisierung von Prozessen, die nicht zuletzt durch die COVID-19-Pandemie weiter beflügelt wurde, ist davon auszugehen, dass Blockchain-Anwendungen in Zukunft nach Anzahl und Art weiterhin zunehmen werden. Abbildung 8 veranschaulicht Anwendungsmöglichkeiten der Blockchain-Technologie in zehn verschiedenen Branchen.

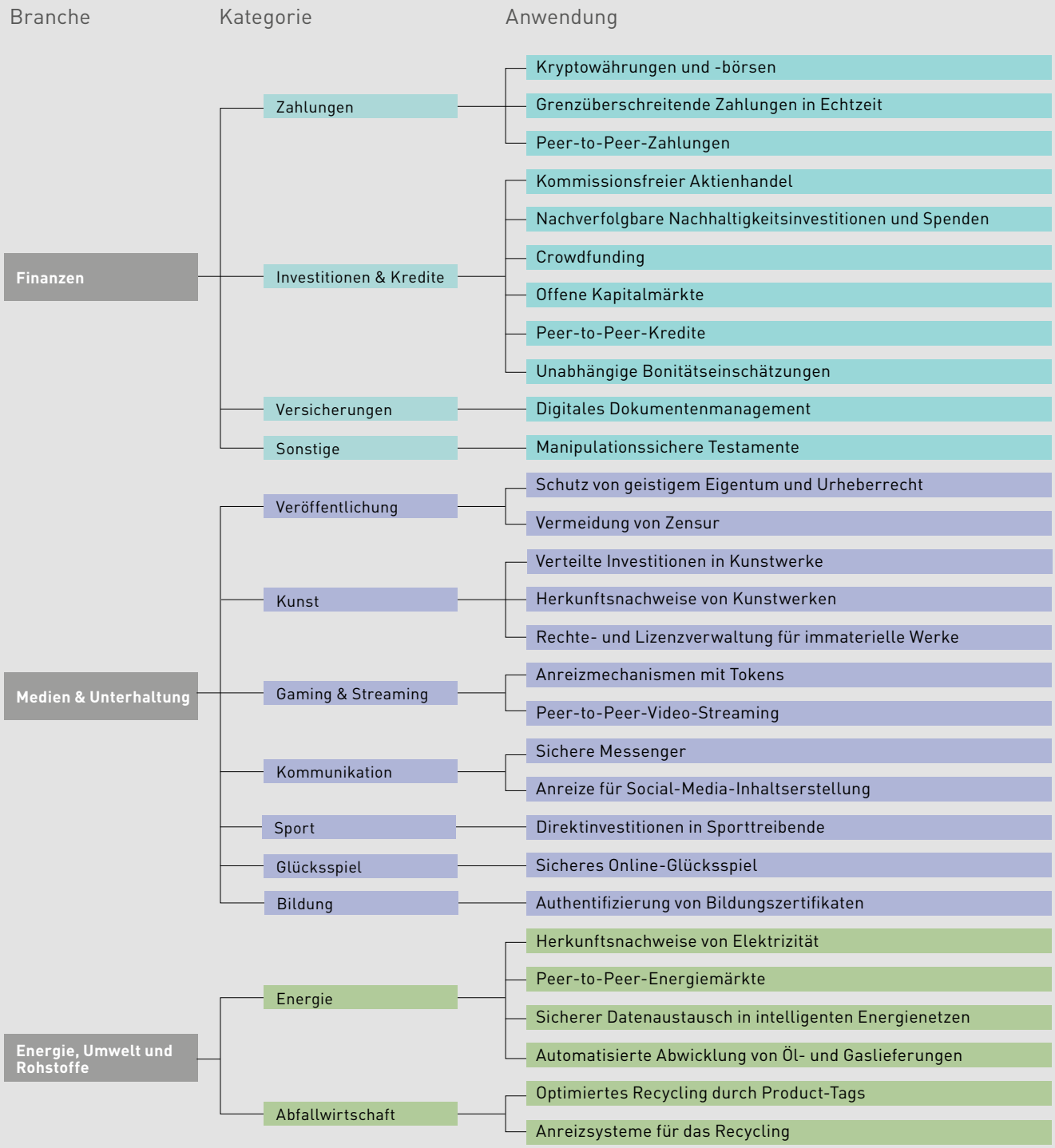
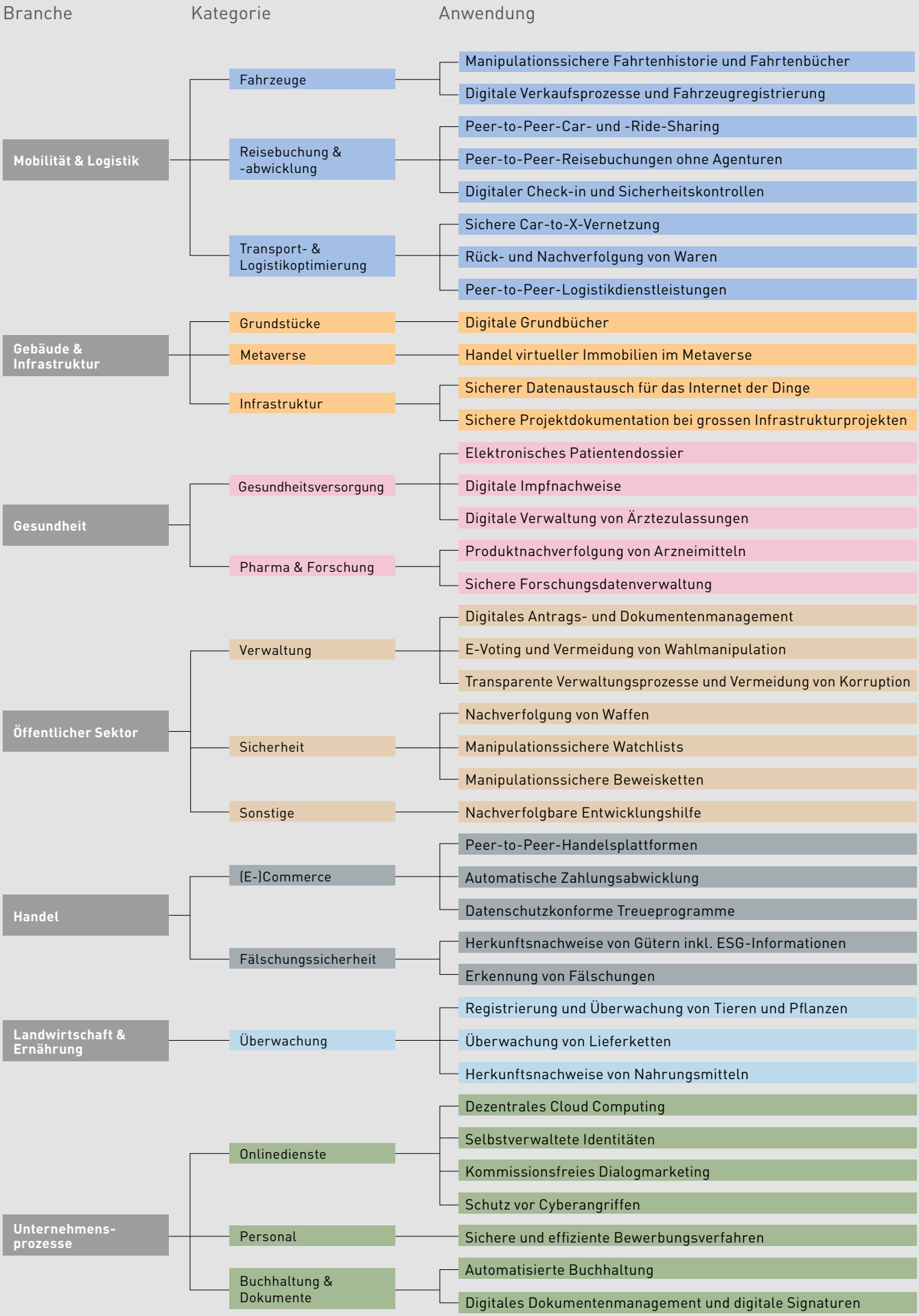


Abbildung 8: Eigene Zusammenstellung basierend auf CB Insights (2022)[33] und weiteren Recherchen.


Branche
Kategorie
Anwendung
Mobilität & Logistik
Fahrzeuge
Manipulationssichere Fahrtenhistorie und Fahrtenbücher
Digitale Verkaufsprozesse und Fahrzeugregistrierung
Reisebuchung & -abwicklung
Peer-to-Peer-Car- und -Ride-Sharing
Peer-to-Peer-Reisebuchungen ohne Agenturen
Digitaler Check-in und Sicherheitskontrollen
Transport- & Logistikoptimierung
Sichere Car-to-X-Vernetzung
Rück- und Nachverfolgung von Waren
Peer-to-Peer-Logistikdienstleistungen
Gebäude & Infrastruktur
Grundstücke
Digitale Grundbücher
Metaverse
Handel virtueller Immobilien im Metaverse
Infrastruktur
Sicherer Datenaustausch für das Internet der Dinge
Sichere Projektdokumentation bei grossen Infrastrukturprojekten
Gesundheit
Gesundheitsversorgung
Elektronisches Patientendossier
Digitale Impfnachweise
Digitale Verwaltung von Ärztezulassungen
Pharma & Forschung
Produktnachverfolgung von Arzneimitteln
Sichere Forschungsdatenverwaltung
Öffentlicher Sektor
Verwaltung
Digitales Antrags- und Dokumentenmanagement
E-Voting und Vermeidung von Wahlmanipulation
Transparente Verwaltungsprozesse und Vermeidung von Korruption
Sicherheit
Nachverfolgung von Waffen
Manipulationssichere Watchlists
Manipulationssichere Beweisketten
Sonstige
Nachverfolgbare Entwicklungshilfe
Handel
(E-)Commerce
Peer-to-Peer-Handelsplattformen
Automatische Zahlungsabwicklung
Datenschutzkonforme Treueprogramme
Fälschungssicherheit
Herkunftsnachweise von Gütern inkl. ESG-Informationen
Erkennung von Fälschungen
Landwirtschaft & Ernährung
Überwachung
Registrierung und Überwachung von Tieren und Pflanzen
Überwachung von Lieferketten
Herkunftsnachweise von Nahrungsmitteln
Unternehmens-prozesse
Onlinedienste
Dezentrales Cloud Computing
Selbstverwaltete Identitäten
Kommissionsfreies Dialogmarketing
Schutz vor Cyberangriffen
Personal
Sichere und effiziente Bewerbungsverfahren
Buchhaltung & Dokumente
Automatisierte Buchhaltung
Digitales Dokumentenmanagement und digitale Signaturen

Blockchain in der Schweiz und international

Seit der Einführung der Blockchain-Idee im Jahr 2008 ist die Zahl an Blockchain-Unternehmen kontinuierlich gestiegen. Auch der Umfang der Investitionen in solche Unternehmen stieg erheblich. Nach Informationen des Portals Blockdata wurden 2021 mit Abstand die meisten Investitionen in Blockchains in den USA getätigt, es folgen das Vereinigte Königreich, Hongkong, Kanada und Frankreich.[34] 81 der weltweit grössten 100 börsennotierten Unternehmen nutzten oder erprobten laut Blockdata im September 2021 bereits Blockchain-Technologie.[35]

Die Schweiz gilt global als führender Standort im Bereich Blockchain. Vorteile, die mit der Schweiz verbunden werden, sind neben der Verfügbarkeit von Fachleuten und einer hohen politischen und wirtschaftlichen Stabilität auch die Offenheit gegenüber neuen Technologien sowie klare und pragmatische Regulierungen im Bereich Blockchain.[36] Beispielsweise hat die Eidgenössische Finanzmarktaufsicht im Jahr 2018 als erste Regulierungsbehörde eine Wegleitung für die Klassifizierung von Tokens und für sogenannte Initial Coin Offerings (eine Methode zur Kapitalakquisition über Tokens) veröffentlicht.[37] Seit August 2021 ist in der Schweiz auch ein Gesetz für verteilte elektronische Register in Kraft, das Gleiche gilt für DLT-Handelssysteme.[38] In der Forschung von Blockchain steht die Schweiz an der Spitze. Das Blockchain Center der Universität Zürich erreichte 2022 in einem internationalen Ranking, durchgeführt von CoinDesk und dem MIT, den ersten Platz in der westlichen Welt.[39]

Besonders Zug ist ein Hub für Blockchain-Unternehmen, da hier das Crypto-Valley, ein vom Bund geförderter Verband für Blockchain und Kryptografie, angesiedelt ist. Laut einer Studie von CV VC waren in der Schweiz im Jahr 2022 über 1 100 Blockchain-Unternehmen aktiv. Eine eigene Auswertung auf der Unternehmensdatenbank Crunchbase zeigt, dass die meisten Schweizer Blockchain-Unternehmen Anwendungen für die Finanzbranche entwickeln. Danach folgen Unternehmen, die Blockchain-Technologie im Allgemeinen weiterentwickeln, zum Beispiel in Form von Plattformen, die für Anwendungen in vielen Branchen genutzt werden können. Dies bestätigt, dass in der Schweiz viel Know-how für die Entwicklung von Blockchain-Anwendungen in der Finanzbranche und darüber hinaus existiert.

Im Folgenden stellen wir globale und Schweizer Statistiken zum Einsatz von Blockchain dar. Die in den Statistiken genutzten Branchenklassifizierungen unterscheiden sich, da diese aus unterschiedlichen Quellen stammen.

Globale Blockchain-Statistiken

Blockchain-Investitionen von Venture Capital Funds, Banken und grossen Unternehmen nach Branchen und Wirtschaftsbereichen in 2021

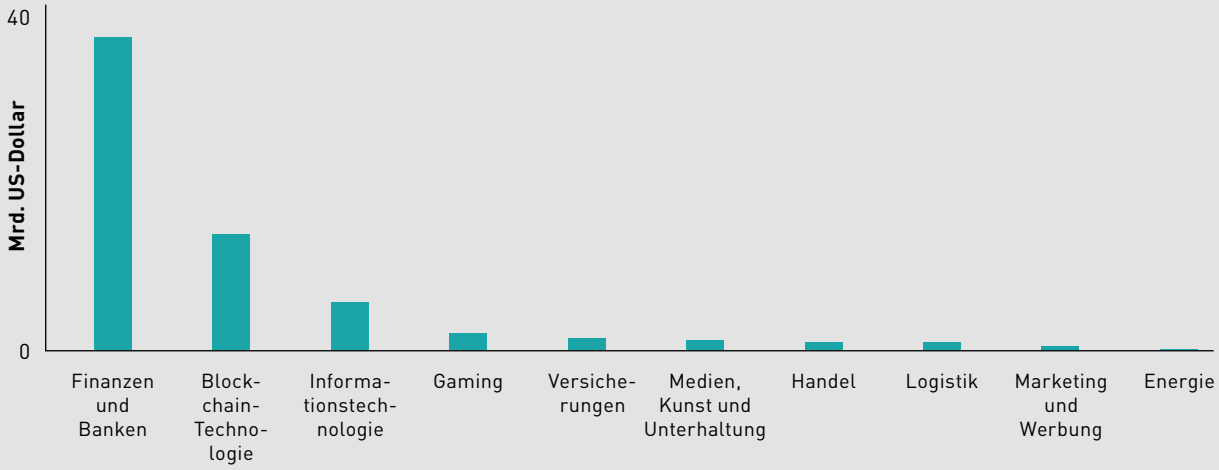


Abbildung 9: Eigene Darstellung basierend auf Blockdata (2021).[40]

Operative Enterprise Blockchains
nach Branche im Jahr 2019

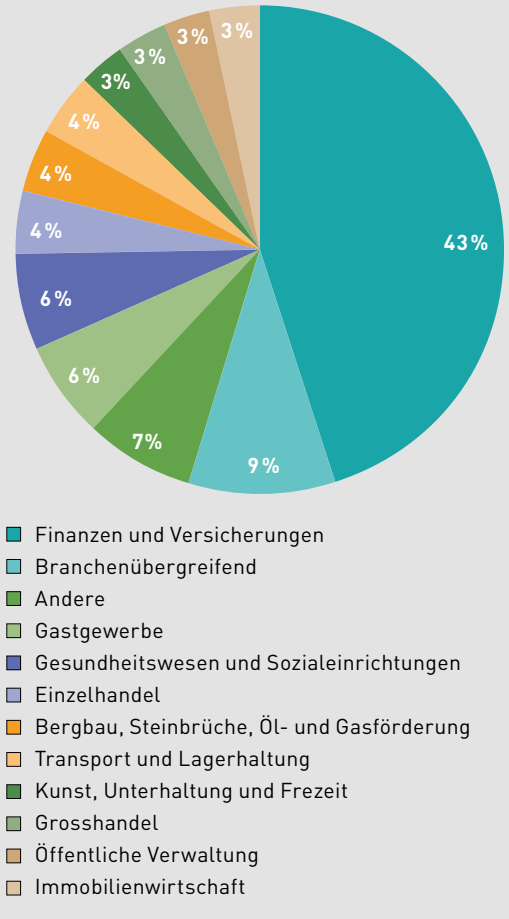


Abbildung 10: Rauchs et al. (2019).[41] Basierend auf einer Studie zu 67 operativen, zugangsbeschränkten Blockchain-Anwendungen im Unternehmenskontext.

Operative Enterprise Blockchains
nach Anwendungsfällen im Jahr 2019

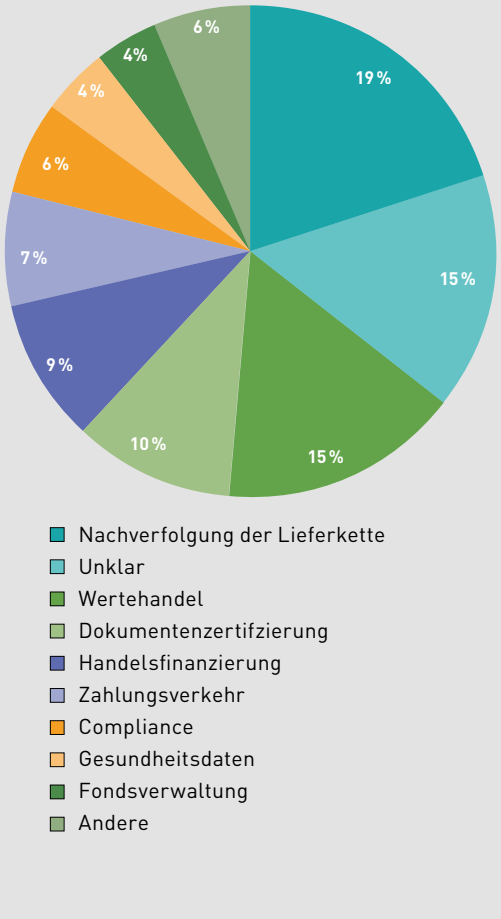


Abbildung 11: Rauchs et al. (2019).[42] Basierend auf einer Studie zu 67 operativen Blockchain-Anwendungen im Unternehmenskontext.

Schweizer Blockchain-Statistiken

Unternehmen und Beschäftigte

1 135

Anzahl an Blockchain-Unternehmen in der Schweiz und Liechtenstein im Jahr 2021

5 766

Beschäftigte

Abbildung 12: CV VC (2023).[43]

Blockchain-Unternehmen in der Schweiz nach Branchen und Wirtschaftsbereichen

Abbildung 13: Eigene Abfrage auf Crunchbase.com (Stand: 19.10.2022).

Blockchain-Unternehmen in der Schweiz und Liechtenstein nach Kantonen im Jahr 2022

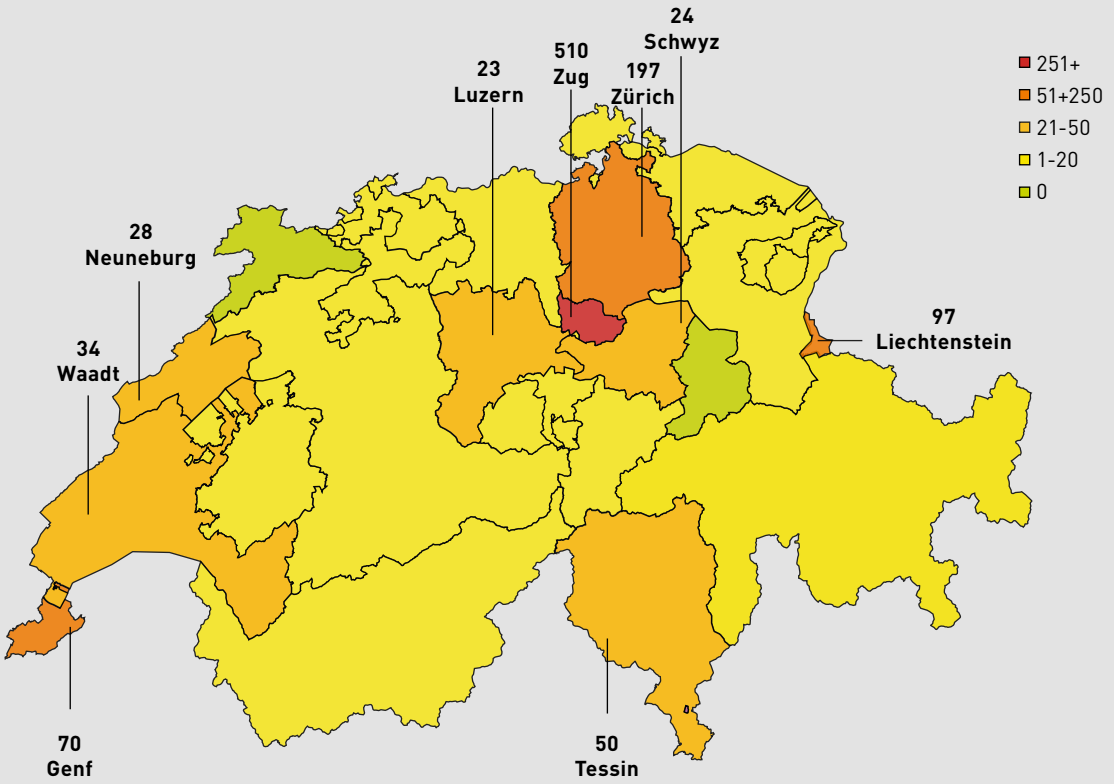


Abbildung 14: CV VC (2023).[44] Nur Kantone mit mehr als 20 Unternehmen sind genannt.

Der Wandel zu verteilten Wertschöpfungsnetzwerken

«Blockchain ermöglicht ganz neue Geschäftsmodelle, da dank dieser Infrastruktur-Technologie effizient, resilient, transparent und sicher Daten und Werte gespeichert und gehandelt werden können.»

Roger Süess, CEO, Green

Heute verfolgen die meisten Unternehmen mit dem Einsatz von Blockchain die Ziele, die Integrität und Verfügbarkeit von digitalen Infrastrukturen zu erhöhen, Effizienz- sowie Kostensenkungspotenziale zu heben und neue Geschäftsfelder zu erschliessen. Viele Fachleute vertreten die Meinung, dass sich mittels Blockchain langfristig existierende zentral organisierte Strukturen und Denkmuster in vielen Branchen komplett zugunsten verteilter Wertschöpfungsnetzwerke auflösen liessen. Viele Unternehmen entwickeln auch bereits Anwendungen mit dem Ziel, zentrale Strukturen komplett abzuschaffen. Ob, wie, wann und mit welcher Wahrscheinlichkeit diese Szenarien tatsächlich eintreten werden, wird dabei meistens offengelassen. Dieser Wandel wäre auch sowohl ein technologischer als auch ein gesellschaftlicher Prozess, bei dem viele Interessenskonflikte überwunden werden müssen. Daher sollten solche Vorhersagen kritisch hinterfragt werden. Dennoch ist es wichtig, die Zielvorstellungen solcher Visionen wahrzunehmen, um eine Diskussion über Chancen und Risiken der Technologie führen zu können.

Im Folgenden illustrieren wir anhand von Beispielen aus vier Branchen, welche Hoffnungen in verteilte Wertschöpfungsnetzwerke gesetzt werden, und diskutieren anschliessend Vor- und Nachteile verteilter Wertschöpfungsnetzwerke.

Was ist das Web 3.0?

Mit «Web 1.0» wird das Internet der Vergangenheit bezeichnet, in dem man hauptsächlich auf statischen Webseiten surfte, ohne selbst Inhalte zu erstellen oder zu teilen. «Web 2.0» beschreibt das heutige Internet, über das kommuniziert wird und Nutzende auch selbst Inhalte teilen. Die Interaktionen finden vor allem auf grossen Plattformen statt, die von wenigen Unternehmen kontrolliert werden. Diese Unternehmen erwirtschaften Gewinne aus gesammelten Nutzerdaten. «Web3» oder «Web 3.0» sind Sammelbegriffe für viele Zukunftsvisionen des Internets, in denen digitale Inhalte und mit Daten generierte Umsätze gerecht unter Nutzenden und Anbietenden geteilt werden. Plattformen sind nicht im Besitz einzelner mächtiger Unternehmen, sondern der Teilnehmenden, die sich an der Entwicklung beteiligen und dadurch Anteile erhalten. Umgesetzt werden sollen solche Visionen durch Blockchain-Technologie, die es ermöglicht, Besitzverhältnisse und Transaktionen zwischen vielen Teilnehmenden manipulationssicher und automatisiert zu organisieren.[45]

Visionen verteilter Wertschöpfungsnetzwerke

Sharing Economy

Heute

Die Sharing Economy hat das Ziel, die Auslastung von Gütern durch eine geteilte Nutzung zu erhöhen und damit die Anzahl an Gütern, die bereitgestellt werden müssen, zu senken. Auch wenn die Sharing Economy häufig als ein Gemeinschaftsprojekt gesehen wird, ist die Realität eine andere, denn ein Grossteil des geteilten Konsums wird heute von zentralen Intermediären koordiniert. Zum Beispiel organisiert Uber das Teilen von Fahrten und AirBnB das Teilen von Unterkünften. Diese Anbieter haben eine so grosse Marktmacht erlangt, dass sie die Konditionen für das Teilen diktieren können. Beispielsweise stand Uber wiederholt wegen prekärer Beschäftigung in der Kritik. Auch verlangen Sharing-Plattformen hohe Entgelte für ihre Leistungen. Bei Uber sind es 25 % des Fahrpreises.[46]

Oft werden die Güter nicht zwischen den Nutzenden geteilt, sondern von Unternehmen für Nutzende bereitgestellt. Dies ist zum Beispiel beim Car-Sharing der Fall, wenn von Unternehmen neue Autos auf die Strassen gebracht werden, die man per App buchen kann. Ob dies tatsächlich zu einer Reduktion der Anzahl von Autos auf den Strassen und der gefahrenen Autokilometer führt, ist umstritten.

Zukunft

Privatpersonen stellen ihr Eigentum anderen zur Nutzung zur Verfügung, speziell Produkte, bei denen es sich nicht lohnt, sie selbst zu kaufen, da sie kostspielig sind und nur selten gebraucht werden. Dies sind nicht nur Autos oder Unterkünfte, sondern auch Gegenstände wie Bohrmaschinen, Parkplätze oder Zelte. Die Anbahnung von Sharing-Geschäften findet auf einer Plattform statt, die von einem Netzwerk an Organisationen und Privatpersonen mithilfe von Blockchain-Technologie bereitgestellt und gesteuert wird. Die Gebührenstruktur ist kostendeckend, aber nicht gewinnorientiert. Die Sharing-Verträge werden direkt zwischen den Teilenden und Nutzenden abgeschlossen (Peer-to-Peer). Die Vertragsbedingungen für das Teilen können die Parteien direkt unter sich ausmachen. Notwendige Voraussetzungen für das Teilen, wie Führerausweise beim Autoteilen, können automatisiert über die elektronischen Identitäten der Mitglieder, die ebenfalls über Blockchain realisiert sind, überprüft werden. Alle abgeschlossenen Geschäfte und die bezahlten Entgelte sind für Finanzämter transparent und manipulationssicher dokumentiert, sodass anfällige Steuern automatisch berechnet werden können.

Online-Veröffentlichungen und Werbung

Heute

Im Internet werden überall gratis Inhalte angeboten: auf Streaming-Plattformen, News-Webseiten, in Blogs, auf Social-Media-Plattformen. Inhalte von Quellen werden häufig weitergegeben, ohne dass die Personen der Urheberschaft gefragt werden oder eine Gegenleistung dafür erhalten. Nur wenige, sehr erfolgreiche und populäre «Content Creators» oder «Influencer» verdienen gut mit ihrer Onlinepräsenz. Die meisten Autorinnen und Autoren von Inhalten verdienen nichts oder nur wenig daran, dass sie originelle Inhalte erstellen und ihr Wissen mit anderen teilen. Gleichzeitig existiert eine geringe Anzahl an Unternehmen, die erheblich davon profitieren, dass die Allgemeinheit freiwillig Inhalte im Internet teilt und konsumiert. Sie sammeln möglichst viele Informationen über die Nutzenden ihrer Plattformen, um ihnen gezielt Werbung anzeigen zu können, die möglichst genau den persönlichen Interessen entspricht. Pro Werbeklick fliesst Geld von den Werbetreibenden zu den Internetunternehmen und nur wenig davon bleibt bei den Erstellern der Inhalte hängen. Die Nutzenden der digitalen Angebote wissen nicht, welche Daten über sie gesammelt und wie diese im Hintergrund monetarisiert werden. Die Nutzerfreundlichkeit des Internets leidet stark unter diesem Modell, da nicht nur ständig Werbung eingeblendet wird, sondern auch Aufforderungen, einen Account zu eröffnen oder einen Newsletter zu abonnieren, den Zugang zu den erwünschten Inhalten blockieren.

Zukunft

Jeder Beitrag, der im Internet veröffentlicht wird, ist standardmässig und eindeutig über selbstverwaltete Identitäten, die mit Blockchain realisiert sind, einer Person oder Organisation zugeordnet, die ihn erschaffen hat.

Die Nutzenden des Internets haben volle Transparenz, welche Informationen an welcher Stelle über sie gesammelt werden, und können ihre Daten freiwillig oder für eine Gegenleistung teilen. Die Konditionen können sie selbst festlegen. So entsteht ein offener Markt für Inhalte und Daten. Beispielsweise erhalten Personen eine finanzielle Entschädigung, wenn sie ihre Nutzungsdaten für Werbezwecke bereitstellen und erlauben, dass ihnen personalisierte Werbung angezeigt wird. Die durch die Werbung erzielten Einnahmen werden automatisiert unter den datenteilenden Personen, den Betreibenden von Portalen oder Blogs und den Personen aufgeteilt, die Inhalte beigetragen haben. Verwendet man im Internet das geistige Eigentum anderer, wird dies erkannt, und ein Teil der Einnahmen fliesst automatisch zum Inhabenden der Urheberrechte. Mithilfe von Kryptowährungen und Smart Contracts gelingt die Monetarisierung.

Stromhandel

Heute

Strom wird hauptsächlich in zentralen Kraftwerken erzeugt, von Netzbetreibern verteilt und von Energielieferanten an die Haushalte verkauft. Die Herkunft des Stroms – aus welchem Kraftwerk er kommt, welcher Energieträger eingesetzt wurde – wird in Form von Zertifikaten, sogenannten Herkunftsnachweisen, bestätigt und in zentralen Registern konsolidiert. So kann der Strommix überwacht und sichergestellt werden, dass Erzeuger und Lieferanten nur Strom verkaufen, der tatsächlich hergestellt wurde. Laut einer Verordnung des Eidgenössischen Departements für Umwelt, Verkehr, Energie und Kommunikation haben Stromlieferanten die Pflicht, ihre Kundschaft sowie die Öffentlichkeit einmal pro Kalenderjahr darüber zu informieren, welche Energieträger für die Stromproduktion eingesetzt wurden und ob der verkaufte Strom in der Schweiz oder im Ausland produziert wurde.[47] In der Regel wissen die Endverbrauchenden jedoch nicht, mit welchen Anlagen ihr Strom genau produziert wurde. Fallen die zentralen Systeme zur Überwachung der Nachweise aus, besteht die Gefahr, dass wichtige Informationen verloren gehen. Kleine Stromerzeugungsanlagen, zum Beispiel Fotovoltaikanlagen auf Häuserdächern, werden im System nicht erfasst.

«Blockchain könnte in einem zukünftigen Energie-Ökosystem, in dem viele Akteure und Geräte wie PV-Anlagen, Speicher, Elektromobile, Wärmepumpen und Gebäude über Internet-of-Things-Technologie verknüpft sind, eine Rolle spielen, um beispielsweise eindeutig Stromnachweise zu liefern.»

Dr. Matthias Galus, Leiter Digital Innovation Office, Bundesamt für Energie

Zukunft

Zentrale Kraftwerke sind kaum noch vorhanden, und Strom wird in vielen verteilten Anlagen erzeugt und zwischengespeichert. Die Herkunft von Strom wird automatisiert über Messgeräte an Erzeugungsanlagen erfasst und in einem manipulationssicheren, hochverfügbaren Blockchain-Register gespeichert. Hierdurch wird sichergestellt, dass erzeugter Strom nur einmal mit den korrekten Eigenschaften verkauft wird. Privathaushalte, die Strom sowohl konsumieren als auch selbst erzeugen, können überschüssigen Strom direkt – ohne Umwege über Stromlieferanten – an Verbrauchende (Peer-to-Peer) verkaufen.

Verbrauchende haben über Blockchain Einblick in die Herkunft des bezogenen Stroms, können flexibel die Bezugsquelle wechseln und sich ihren individuellen Strommix bis hin zur Erzeugungsanlage selbst zusammenstellen. Der Strompreis wird automatisch und in Echtzeit aus dem aktuellen Angebot und der Nachfrage berechnet. Wird das Stromangebot knapp, steigt der Preis unmittelbar, wodurch Anreize für den Ausbau erneuerbarer Energien geschaffen werden. Das System kann praktisch nicht ausfallen, da es nicht von einer zentralen Instanz, sondern auf vielen verteilten Knoten eines Blockchain-Netzwerks betrieben wird.

Zahlungsverkehr

Heute

Das Bankwesen wimmelt von Intermediären, die dafür zuständig sind, Zahlungen zwischen verschiedenen Parteien abzuwickeln. Banken führen Zahlungen im Auftrag von Personen und Organisationen aus. Über das Swiss-Interbanking-Clearing-System, das von der SIX betrieben wird, werden Transaktionen zwischen Banken abgewickelt. Kreditkartenunternehmen stellen sicher, dass man bargeldlos bei vielen Händlern im In- und Ausland bezahlen kann. An einer einzigen Kreditkartenzahlungen sind drei Instanzen beteiligt, welche die Zahlung zwischen Kaufenden und Handelnden abwickeln.[48] Jede dieser Instanzen möchte Geld verdienen, und die Kosten dafür werden von Händlern und den Karteninhabenden getragen. Obwohl aus technischer Sicht Echtzeit-Überweisungen mit Ländern wie den USA bereits möglich sind, ist der internationale Zahlungsverkehr durch viele Regularien mühsam, langsam und teuer. Vergeben Banken Kredite oder verwalten Investitionen, werden dafür ebenfalls erhebliche Gebühren berechnet. Fallen die Systeme eines zentralen Intermediärs aus, sind viele Dienstleistungen nicht mehr verfügbar.

Zukunft

Menschen können sich direkt (Peer- to-Peer) über eine digitale sogenannte Wallet (deutsch: «Brieftasche») Geld von Smartphone zu Smartphone schicken, ohne dass dabei Intermediäre ins Spiel kommen (bereits heute möglich). Die Überweisung ist kostenfrei und funktioniert in Echtzeit, auch über Landesgrenzen hinweg. Auch können sich Menschen gegenseitig rund um die Uhr und von überall auf der Welt Geld leihen und die Konditionen dafür untereinander abmachen. Investitionen in Unternehmen werden ebenfalls nicht mehr über Dienstleister abgewickelt, sondern direkt und gebührenlos zwischen den Geldgebenden und den Unternehmen. Da alles vollautomatisiert abläuft, sind die Kosten niedrig, wodurch auch Investitionen in kleinere Unternehmen, die nicht an der Börse gehandelt werden, möglich sind. Möglich wurde dies dank rechtssicherer, selbstverwalteter Identitäten und der Automatisierung von Zahlungs- und Investitionsprozessen mittels Blockchain und Smart Contracts. Das System kann praktisch nicht ausfallen, da es nicht von einer zentralen Instanz, sondern verteilt, von vielen Teilnehmenden gemeinschaftlich betrieben wird.

Was ist Decentralized Finance?

Decentralized Finance («dezentrale Finanzwirtschaft», kurz: DeFi) ist ein offenes Blockchain-System für die Verwaltung digitaler Vermögenswerte, welches ohne Zwischenhändler (Peer-to-Peer) betrieben wird. Über das System sollen fast alle klassischen Bankdienstleistungen abgewickelt werden, wie Kontoführung, Überweisung, Kreditgeschäft oder Wertpapierhandel. Durch die Nutzung von Blockchain und den Wegfall von Intermediären steigt die Geschwindigkeit des Systems und die Kosten sinken.[49]

Vor- und Nachteile verteilter Wertschöpfungsnetzwerke

Wird eine digitale Anwendung nicht mehr auf den Computersystemen einer zentralen Instanz, sondern auf den Systemen von mehreren Teilnehmenden betrieben, erhöhen sich dadurch die Ausfall- und Manipulationssicherheit sowie (in Kombination mit dem Einsatz von Kryptographie) der Schutz vor Cyberangriffen. In verteilten Wertschöpfungsnetzwerken wird allerdings nicht nur der Systembetrieb, sondern auch die Entscheidungsbefugnis auf viele Schultern verteilt, um Machtkonzentration vorzubeugen. Zukunftsszenarien verteilter Netzwerke legen den Fokus meist auf die Vorteile, etwaige Nachteile werden ausser Acht gelassen. Dabei kann die Konzentration der Entscheidungsbefugnisse bei manchen Entscheidungen auch Vorteile mit sich bringen. Zwei Beispiele hierfür sind:[50]

> Entscheidungen, die viel Expertenwissen und Erfahrung erfordern: Dies kann zum Beispiel der Fall sein bei Entscheidungen in Investitionen in radikale Innovationen, deren langfristige Vorteile heute nur schwer abschätzbar sind.
> Entscheidungen, die darauf abzielen, eine Organisation langfristig gesund zu erhalten, sich jedoch kurzfristig für viele nachteilig auswirken können: Die Entscheidung eines Automobilherstellers, komplett auf E-Mobilität und Mobility-as-a-Service zu setzen, kann langfristig gewinnbringend für die Organisation sein. Viele, die in der Herstellung von Verbrennungsmotoren beschäftigt sind, würden diese Entscheidung jedoch nicht zwingend mittragen.

Mit der Konzentration von Entscheidungsbefugnissen will man die Beständigkeit und Berechenbarkeit von Organisationen und Systemen sicherstellen und den Fokus auf das langfristige Wohl und nicht auf das Wohl einer jeden Person oder Organisation legen.[51] Dies erhöht jedoch die Abhängigkeit von den Führungspersönlichkeiten, und das Potenzial für Machtmissbrauch wächst. Beispielsweise können bei grossen Plattformen, zu denen kaum Alternativen existieren, die Plattformbetreiber die Nutzungsbedingungen diktieren. Grossen Vermittlungsplattformen wie Booking.com oder Uber wird regelmässig vorgeworfen, ihre marktbeherrschende Stellung zulasten von Hotels oder Personen, die Fahrdienste übernehmen, auszunutzen.[52] Durch die Verteilung der Entscheidungsbefugnisse auf viele Netzwerkteilnehmende (zum Beispiel Hotels oder Taxiverbände) liesse sich dem entgegenwirken.

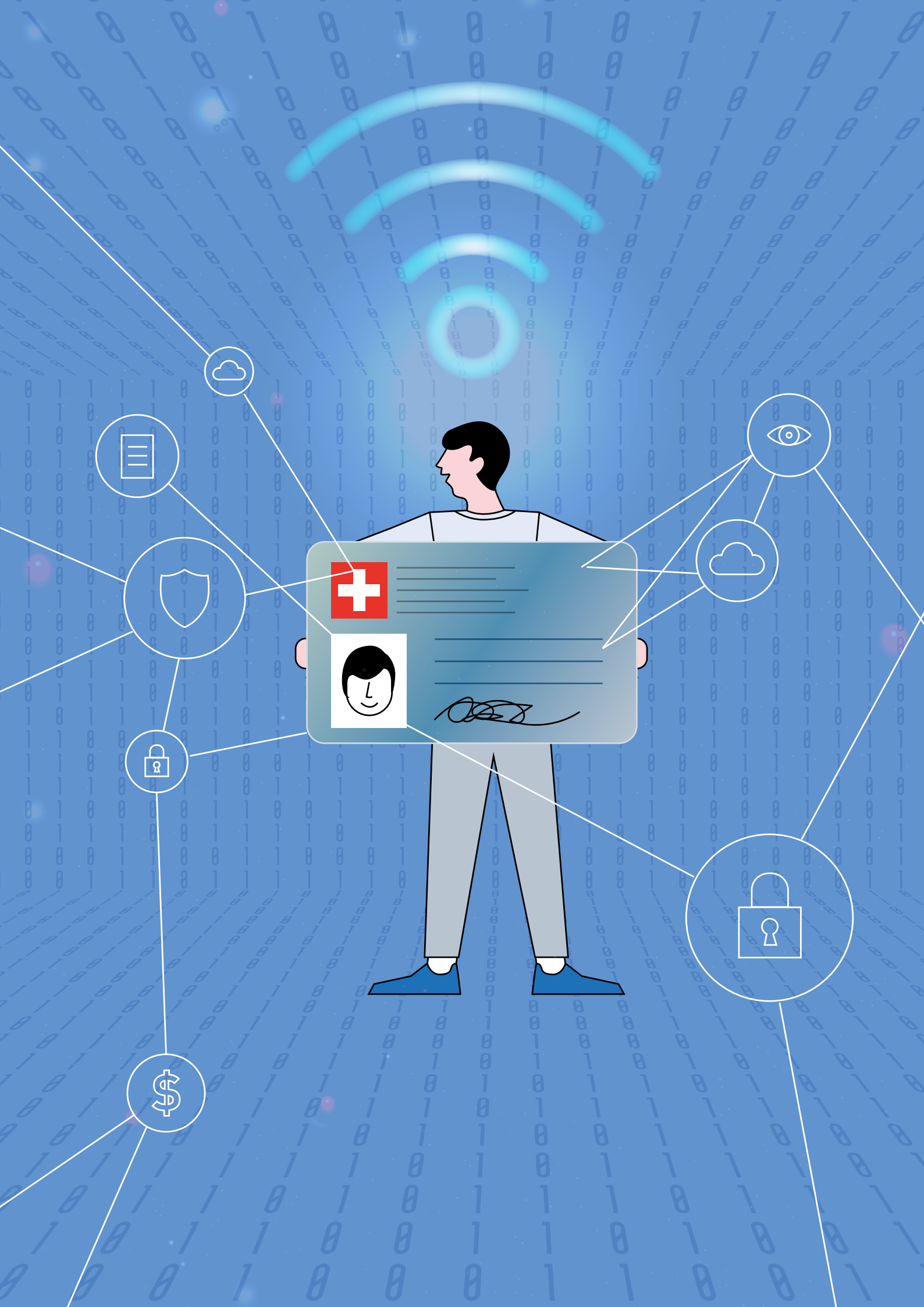
Es gibt keine allgemeingültige Antwort auf die Frage, wie stark strategische Entscheidungsbefugnisse konzentriert oder verteilt werden sollten. Demokratische Systeme versuchen, die Vorteile von verteilten und konzentrierten Entscheidungen zu vereinen: Bürgerinnen und Bürger wählen in regelmässigen Abständen ihre politische Vertretung und übertragen ihr damit Entscheidungsbefugnisse für einen bestimmten Zeitraum. Durch die Gewaltenteilung kontrollieren sich verschiedene Staatsorgane gegenseitig. Auch auf unternehmerischer Ebene existieren ähnliche Systeme: Bei schweizerischen und deutschen Aktiengesellschaften überwachen Verwaltungsräte respektive Aufsichtsräte die Geschäftsleitungen, wobei beide Organe von den Aktionärshauptversammlungen kontrolliert werden. Hierdurch wird versucht, die Vorteile konzentrierter Entscheidungen zu nutzen und gleichzeitig Machtmissbrauch durch Kontrollmechanismen vorzubeugen.

Blockchain und Machtkonzentration

Selbst wenn Entscheidungsbefugnisse im Netzwerk verteilt werden, können sich Strukturen im Netzwerk oder in dessen Umfeld etablieren, die Machtkonzentration fördern, wie das Beispiel des Bitcoins zeigt. Beim Bitcoin entscheiden Miner mit der Installation von Software-Updates, ob sie eine Veränderung in der Funktionsweise akzeptieren. Nur wenn die Mehrheit der Miner ein bestimmtes Software-Update installiert, sind die darin enthaltenen Änderungen quasi angenommen. Prinzipiell kann jeder Miner selbst seine Entscheidung treffen. In der Praxis haben jedoch manche deutlich mehr Einfluss als andere, denn welche Änderungen von der Gemeinschaft der Miner akzeptiert werden, hängt stark davon ab, ob sie die Unterstützung einer Bitcoin-Elite erhalten. Den grössten Einfluss haben Kernentwickelnde die laufend den Code des Bitcoins begutachten, und grosse Miner, die viel Rechenleistung für das Blockchain-Netzwerk bereitstellen.[53] Die 50 grössten Miner (das sind 0,1 % aller Miner) kontrollieren etwa 50 % der für das Mining eingesetzten Rechenleistung.[54] In der Vergangenheit ist es schon mehrmals vorgekommen, dass die Gruppe der Kernentwickelnden versucht hat, grosse Miner zu überzeugen, ein bestimmtes Update zu unterstützen.[55]

Auch möchten nicht unbedingt alle Handelnden bei der Bereitstellung digitaler Dienste mitwirken und an allen Entscheidungen beteiligt sein. Für viele Konsumierende ist vor allem wichtig, dass ein vertrauenswürdiger und nutzerfreundlicher Service zu Verfügung steht. Man ist froh, wenn man sich keine Sorgen um technische Fragestellungen machen muss. Private gewinnorientierte Unternehmen haben dies erkannt, stellen Dienste bereit, um den Umgang mit Blockchain- Anwendungen zu erleichtern und haben dadurch eine grosse Machtkonzentration erlangt. Coinbase, eine der grössten Handelsplattformen für Kryptowährungen, ist ein privates gewinnorientiertes Unternehmen, das grossen Einfluss auf den Markt für Kryptowährungen hat. Der sogenannte Coinbase Effekt beschreibt, dass der Kurs einer Kryptowährung steigt, sobald angekündigt wird, dass sie auf Coinbase handelbar wird. Allerdings scheint der Effekt abzunehmen, je mehr Kryptowährungen auf Coinbase gehandelt werden.[56] Dennoch lautet eine goldene Regel für viele Kryptowährungen: «Werde auf Coinbase gelistet und dein Preis wird in die Höhe schnellen.»[57]

Um effektiv Machtkonzentration vorzubeugen, ist es notwendig, die Entscheidungsbefugnisse in übergreifenden Wertschöpfungsnetzwerken, die aus vielen Blockchain-Anwendungen bestehen können, auf möglichst viele Organisationen zu verteilen. Gleichzeitig müssen Anreizmechanismen geschaffen werden, die sicherstellen, dass Teilnehmende kooperieren, auch bei Interessenskonflikten. Blockchain-Technologie löst per se keine Interessenskonflikte. Sie ist aber durchaus ein Vehikel, das in vielen Bereichen eine Aufbruchsstimmung zu verteilten Wertschöpfungsnetzwerken ausgelöst hat. Die technischen Eigenschaften von Blockchain – verteilter Betrieb, Manipulationssicherheit, in Smart Contracts fixierbare Entscheidungsregeln – sind förderlich für die Entwicklung verteilter Governance-Strukturen. Viele Blockchain-Unternehmen, beispielsweise Tezos, haben bereits bewiesen, dass Machtkonzentration tatsächlich vorgebeugt werden kann. Hier kann sich jede Person oder Organisation, die mindestens einen Token besitzt, an Abstimmungen beteiligen.[58] Manchmal entscheidet in solchen Systemen die Anzahl an Tokens, die Mitglieder besitzen, über eine Gewichtung ihrer Stimmen, was wiederum Machtkonzentration fördern kann.



Das Potenzial von Blockchain-Anwendungen im Detail

Um die Chancen des Einsatzes von Blockchain und die Herausforderungen bei der Umsetzung von Blockchain-Projekten zu identifizieren, haben wir drei potenzielle Blockchain-Anwendungen genauer untersucht:

> Selbstverwaltete Identitäten
> Verteilte Verwaltung von sensiblen Daten am Beispiel von Gesundheitsdaten
> Rück- und Nachverfolgung von Waren am Beispiel von Arzneimitteln

Für jede dieser Anwendungen beschreiben wir den heutigen Status quo ohne Nutzung von Blockchain-Technologie, entwickeln ein Zielbild einer möglichen Blockchain-Lösung und identifizieren auf der Basis von Fachliteratur und Expertenworkshops mit Industriepartnern Chancen, Risiken und Hürden in der Umsetzung.

Selbstverwaltete Identitäten

Status quo und Herausforderungen

Viele Interaktionen mit Organisationen über das Internet machen es notwendig, dass man sich identifizieren kann. Dafür werden Authentifizierungstechniken eingesetzt. Neben Benutzernamen und Passwörtern werden in den letzten Jahren Techniken wie biometrische Authentifizierung (Fingerabdrücke, Gesichtserkennung), Multi-Faktor-Authentifizierung[59] oder die Online-Video-Identifikation[60] eingesetzt. Im Zuge der COVID-19-Pandemie wurde Authentifizierung über das Internet noch wichtiger, zum Beispiel die Identifikation bei einer Kontoeröffnung per Live-Video und Fotos von Ausweisdokumenten.

Heute muss man eine Vielzahl von Accounts für die Authentifizierung gegenüber Organisationen im Internet anlegen. Die Speicherung personenbezogener Daten in all diesen Systemen ist ineffizient und erzeugt Sicherheitsrisiken, da potenziell viele Personen oder Organisationen die Möglichkeit hätten, die Daten für andere Zwecke und ohne Zustimmung der Datengebenden zu missbrauchen. Zudem lagern viele die Identitätsverwaltung über den sogenannte Social Login an Dritte, in der Regel private Unternehmen, aus. Beispielsweise wird der Facebook-, LinkedIn- oder Google-Login heute häufig auch für die Authentifizierung gegenüber anderen Plattformen oder Internetseiten verwendet. Auch wenn dies eine komfortable Alternative zur Erstellung vieler unterschiedlicher Logins ist, so wirft diese Praxis Bedenken hinsichtlich des Datenschutzes auf, da die Identitätsdienstleister nachverfolgen können, wo und wann man sich bei anderen Diensten anmeldet.[61] Der Fall des Unternehmens Cambridge Analytica, das personenbezogene Daten von Facebook zur Wahlbeeinflussung in den USA und im Vereinigten Königreich nutzte, hat eindrücklich gezeigt, welche Missbrauchsmöglichkeiten solche Daten bieten.[62]

In der Schweiz gab es bereits mehrere Vorstösse, ein geeigneteres System zur Identitätsverwaltung und Authentifizierung anhand elektronischer Identitäten, kurz E-IDs, zu schaffen. Die SwissID ist beispielsweise ein System der Schweizerischen Post, das zur elektronischen Identifizierung sowie Signierung von Dokumenten genutzt werden kann. Im März 2021 hat die Schweizer Stimmbevölkerung das Bundesgesetz über elektronische Identifizierungsdienste abgelehnt, hauptsächlich da private Unternehmen aus Sicht der Bevölkerung nicht als Identitätsanbieter agieren sollen.[63] Daraufhin hat der Bundesrat die Entwicklung eines neuen Gesetzes in Auftrag gegeben, das folgende Grundsätze umfassen soll:[64]

> Datenschutz durch Technikgestaltung (englisch «Privacy by Design»): Datenschutz soll durch das System selbst sichergestellt werden.

> Datensparsamkeit: Datenflüsse sollen minimiert werden.
> Verteilte Speicherung: Daten sollen verteilt gespeichert werden.
> Staatlicher Identitätsanbieter: Der Ausstellungsprozess von Identitäten und der Betrieb der Infrastruktur sollen in staatlicher Hand liegen.

Die darauffolgende Konsultation ergab, dass eine Mehrheit die Nutzung einer selbstverwalteten Identität (englisch «Self-Sovereign Identity», kurz: SSI) zur Realisierung der Lösung präferiert.[65] Zusätzlich wurde mehrheitlich gefordert, dass das sogenannte Ambitionsniveau 3 angestrebt werden soll, bei dem sowohl staatliche als auch private Stellen E-IDs ausstellen können. Konkret bedeutet das, der Staat stellt die Infrastruktur für E-IDs bereit, nutzt sie auch selbst für die Ausstellung staatlicher E-IDs (Ausweise), stellt sie aber auch anderen für ihre Nachweise zur Verfügung, zum Beispiel Ausbildungsnachweise, Arbeitszeugnisse, Mitarbeiter- und Mitgliederausweise.[66] Seit Ende Juni 2022 läuft eine Vernehmlassung zum E-ID-Gesetz.[67]

Zielbild

Im Gegensatz zum traditionellen Identitätsparadigma mit einer zentralen Identitätsbehörde ist die SSI ein Konzept, das Personen, Organisationen oder Maschinen erlaubt, eine E-ID digital zu erzeugen und vollständig selbst zu verwalten, üblicherweise in einer SSI-fähigen App, einer sogenannten Wallet, auf dem Smartphone.

Aussteller erteilen sogenannte überprüfbare Nachweise (englisch «Verifiable Credentials») an Berechtigte, welche diese in ihren Wallets auf dem Smartphone speichern. Im Fall von Identitätsnachweisen wäre der Aussteller der Staat, bei Führerausweisen das Strassenverkehrsamt, bei Studienabschlusszeugnissen die Hochschule und bei personalisierten Konzerttickets die Verkaufsstelle. Die Bürgerinnen und Bürger übermitteln den prüfenden Personen ihre Nachweise von der Smartphone-Wallet über einen gesicherten Kanal. Die Echtheit eines Nachweises ergibt sich durch einen «kryptografischen Beweis», der in einem Register gespeichert ist. Das Register ist als Blockchain realisiert, um die Unveränderbarkeit der Daten sicherzustellen und die Existenz eines «Single-Point-of-Failure» zu vermeiden.

«Anhand von Blockchain können wir Identifizierungslösungen schaffen, mit welchen wir in der digitalen Welt sicher und vertraulich interagieren können, selbst wenn wir unser Gegenüber nicht kennen.»

Orlando Hirt, Managing Director, OVD Kinegram

Um die Prinzipien der Datensparsamkeit sicherzustellen, können die Bürgerinnen und Bürger immer selbst entscheiden, welche Daten sie mit welchen prüfenden Personen oder Institutionen teilen. Datensparsamkeit wird zusätzlich durch sogenannte Null-Wissen-Beweise (englisch «zero-knowledge proof») unterstützt. Sie stellen sicher, dass nur die für eine Interaktion minimal notwendigen Informationen geteilt werden.[68] Dies ist zum Beispiel bei heutigen physischen Ausweiskontrollen nicht möglich, da immer der ganze Ausweis bereitgestellt werden muss, auch wenn nur eine bestimmte Information, beispielsweise das Geburtsdatum, geprüft wird.

Der Vorteil gegenüber herkömmlichen Identitätsprüfungsverfahren ist, dass prüfende Personen nicht direkt beim Aussteller eines Nachweises anfragen müssen, ob dieser echt ist, sondern die Echtheit selbstständig über das Register prüfen können. Somit erlangt weder ein Aussteller noch ein soziales Netzwerk über seinen Social-Login-Dienst Kenntnis darüber, mit wem Nachweise

Architektur der SSI

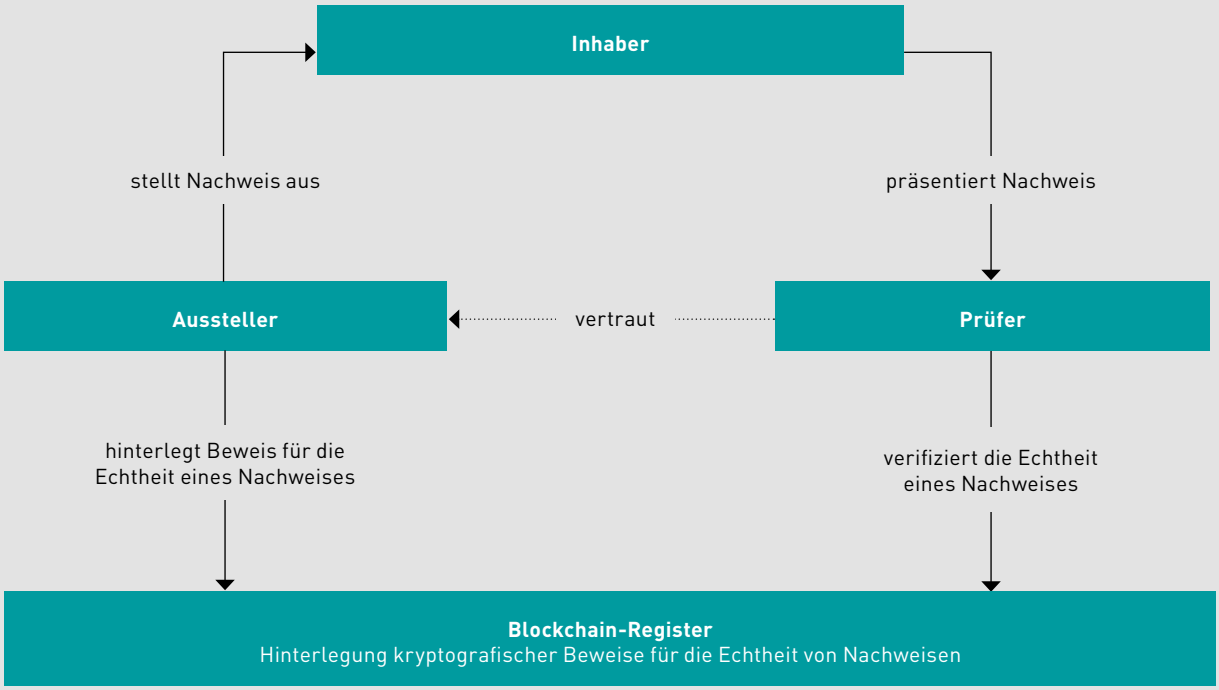


Abbildung 15: Eigene Darstellung basierend auf Bundesamt für Justiz (2021).[70]

geteilt werden. Um das Prinzip Privacy by Design zur realisieren, werden im Register selbst nicht die eigentlichen Daten, sondern lediglich die kryptografischen Beweise (sogenannte Hashwerte) zur Überprüfung der Echtheit der Daten gespeichert. Die Nachweise selbst werden ausschliesslich auf den Smartphones der Bürgerinnen und Bürger («off-chain») gespeichert, sodass ohne ihr Wissen niemand anderes darauf Zugriff hat. Hierfür werden besonders geschützte Bereich auf Smartphones («Secure Elements») genutzt, die allerdings noch nicht auf allen Modellen verfügbar sind.[69] Sollte ein Nachweis seine Gültigkeit verlieren, kann dies ebenfalls im Register hinterlegt werden. Bürgerinnen und Bürger können unabhängig von ihrer staatlichen Identität auch selbst Nachweise erzeugen, zum Beispiel Pseudonyme für den Login bei Streaming-Plattformen. Prinzipiell kann die SSI sowohl zur Identifizierung von Personen als auch von Organisationen und Maschinen, beispielsweise für das Internet der Dinge (englisch «Internet of Things», kurz: IoT), genutzt werden. Abbildung 15 zeigt die grundsätzliche Architektur der SSI. Die Lösung könnte auch in

Architektur der SSI auf Grundlage der angedachten Lösung in der Schweiz

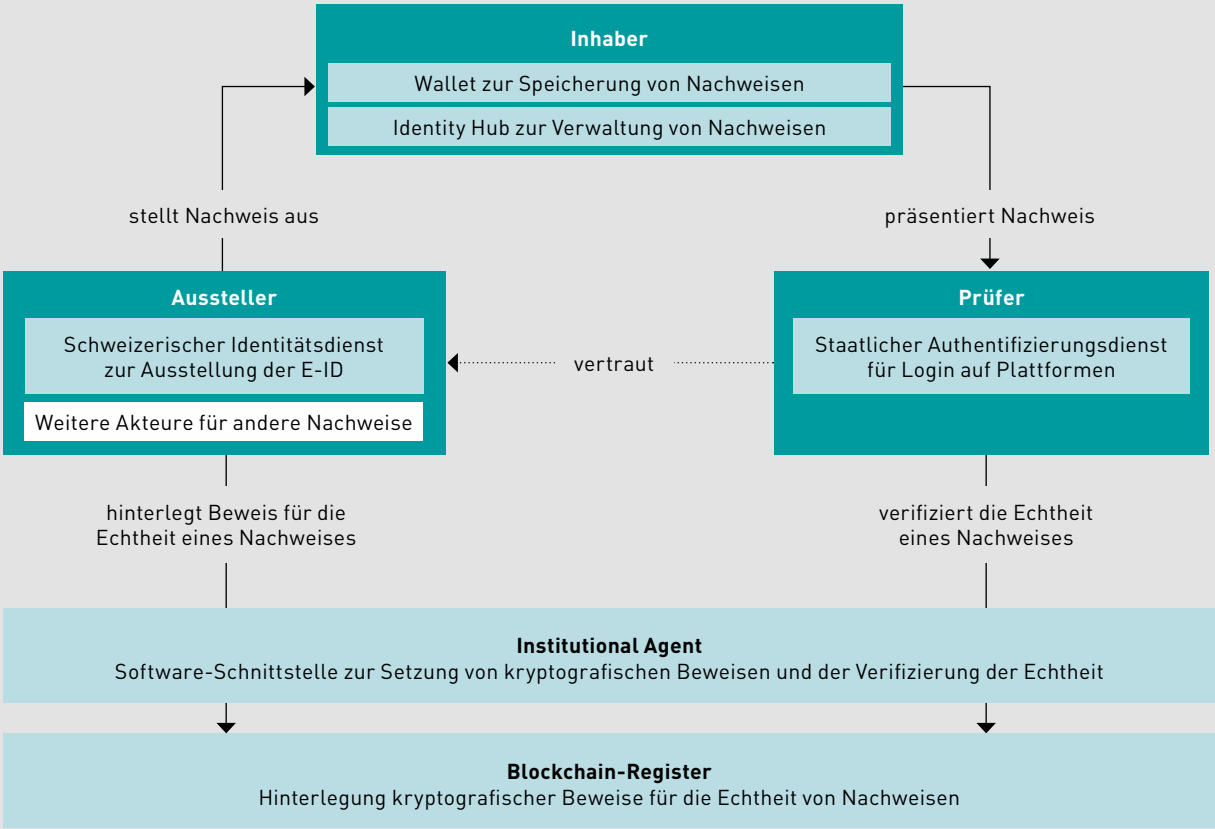


Abbildung 16: Eigene Darstellung basierend auf Bundesamt für Justiz (2021).[73] Die staatlicherseits bereitgestellten Funktionalitäten sind hellblau unterlegt.

der physischen Welt eingesetzt werden, zum Beispiel für die Zutrittsverwaltung zu Räumen ohne physische Schlüssel.

Laut dem «Diskussionspapier zum Zielbild E-ID» des Bundesamtes für Justiz würde der Staat bei der Umsetzung der SSI mehrere Funktionalitäten bereitstellen:[71] einen automatisierten Prozess zur Ausstellung von E-IDs durch den Schweizerischen Identitätsdienst, eine Software zum Ausstellen und Verifizieren von staatlichen E-IDs und anderen Nachweisen («Institutional Agent») sowie eine sichere Wallet zur Speicherung der Nachweise auf den Smartphones der Bürgerinnen und Bürger. Auch das Register würde der Staat in Form einer verteilten Speicherung bereitstellen, zudem einen Identity-Hub, der den Menschen die Verwaltung ihrer eigenen Identitäten ermöglicht (inkl. Backups), sowie einen Authentifizierungsdienst, der von staatlichen und privaten Plattformen als Login-Dienst genutzt werden kann.[72] Der Minimalanwendungsfall der Ausstellung und Verifizierung von staatlichen EI-Ds soll ausschliesslich mit staatlich bereitgestellten Komponenten reali-

Prozesse und Anwendungen die durch SSI vereinfacht oder ermöglicht werden

SEKTOR	ANWENDUNG
Online-Dienste (zum Beispiel E-Banking, E-Commerce)	Nutzerfreundlicher und sicherer Login in Online-Dienste Schnelleres Onboarding von Neukunden inkl. Legitimationsprüfungen («know your customer») Sicherer Online-Handel Sichere Peer-to-Peer Marktplätze ohne Intermediär
Gesundheit	Digitale Impfzertifikate Elektronisches Patientendossier Digitale Medikamentenrezepte Medizinische Online-Beratung
Transport	Sicheres Peer-to-Peer Car- und Ride-Sharing Digitale Identifizierung von Autos für die Interaktion mit Tankstellen oder Mautstellen Digitales Fahrtenbuch
Gebäude	Zugangskontrolle zu Gebäuden und Räumen Sichere Liegenschafts- und Raumvermietungen
Reisen und Veranstaltungen	Kontaktloser Hotel Check-In Schnellerer Check-In an Flughäfen Personalisierte, digitale Eintrittstickets
Öffentlicher Sektor	E-Voting Digitale Dokumente wie Wohnsitzbestätigungen, Betreibungsregisterauszüge oder Zeugnisse Schnellere Aufnahme von Flüchtlingen

Tabelle 3: Eigene Recherche.

siert werden. Dennoch ist das Ziel, dass auch weitere Applikationen anderer Anbieter auf die staatlicherseits bereitgestellte Infrastruktur zugreifen und sie nutzen können (zum Beispiel weitere Wallets mit Nachweisen). Bei Applikationen von Dritten ist jedoch darauf zu achten, dass diese die geforderten Prinzipien einhalten, zum Beispiel Datensparsamkeit oder Privacy by Design. Die Abbildung 16 veranschaulicht die Funktionen, die der Staat laut dem «Zielbild E-ID» bereitstellen will.

Chancen

Die Industriepartner dieser Studie sehen als Vorteile der SSI vor allem den Datenschutz und die Datensicherheit. Nur die Bürgerinnen und Bürger haben Zugriff auf ihre Nachweise und können selbst entscheiden, mit wem sie diese teilen. Dadurch liegen weniger personenbezogene Daten auf den Systemen anderer Unternehmen, wodurch die Missbrauchsgefahr sinkt. Hackerangriffe auf personenbezogene Daten werden durch den zunehmenden Rückgang zentraler Kundendatenbanken unattraktiver. Die Partner sehen die SSI auch als ein Mittel, um die Bevölkerung hinsichtlich des Datenschutzes zu sensibilisieren. Heute gehen viele Bürgerinnen und Bürger noch zu sorglos mit ihren Daten um, seien es Gesundheitsdaten, die über Health Tracker von privaten Unternehmen gesammelt werden, oder sensible Dokumente, die in die Cloud eines privaten Anbieters hochgeladen werden. Die SSI könnte aufzeigen, dass datengetriebene Dienste auch erbracht werden können, ohne dass private Unternehmen Zugriff auf viele personenbezogene Daten erhalten. Schliesslich könnten durch SSI bestehende Medienbrüche geschlossen werden. Zum Beispiel könnten Wohnsitzbescheinigungen oder Betreibungsregisterauszüge ausschliesslich digital statt per Post beantragt und ausgestellt werden, da Bürgerinnen und Bürger elektronisch eindeutig identifizierbar sind und die Dokumente ebenfalls sicher als Nachweise in der Wallet gespeichert werden können.[74] Auch bei der Interaktion mit privaten Unternehmen können Medienbrüche vermieden werden, zum Beispiel beim Check-in am Flughafen.[75]

Tabelle 3 zeigt eine Übersicht bestehender Prozesse und neuer Anwendungen, die durch eine funktionierende SSI vereinfacht oder erst ermöglicht werden. Letztlich könnte das Vertrauen der Bevölkerung in digitale Dienstleistungen insgesamt wachsen, wenn die Identitätsverwaltung statt von einzelnen Unternehmen von einer verteilten Infrastruktur erbracht wird, ohne dass eine privatwirtschaftliche Organisation darüber die Kontrolle hat. Eine Offenlegung des Codes («Open Source») würde das Vertrauen in die Anwendung weiter stärken.

Hürden und Risiken

Die grössten Herausforderungen sehen die Industriepartner in Bezug auf die Governance und Akzeptanz der Lösung. Eine Kernfrage ist, wie dezentral eine SSI wirklich sein kann, wenn die dafür notwendige Infrastruktur und die Prozesse hauptsächlich vom Staat bereitgestellt werden. Dadurch könnte einerseits die Gefahr bestehen, dass Bürgerinnen und Bürger sowie Unternehmen der Lösung nicht vollumfänglich vertrauen, worunter die Akzeptanz leiden könnte. Andererseits hat die Schweizer Stimmbevölkerung eine Lösung abgelehnt, die von privaten Identitätsanbietern koordiniert wird. Deshalb spricht viel für die Schaffung einer verteilten Lösung, die weder alleinig vom Staat noch von privaten Unternehmen gesteuert wird. Die Schaffung solch eines Ökosystems wird auch von DigitalSwitzerland, einem Verband zur Stärkung digitaler Innovation in der Schweiz, vorgeschlagen.[76] Eine Anregung einer verteilten Lösung ist IDUnion, ein Projekt

zur Entwicklung einer SSI-Lösung, an dem über 50 öffentliche und private Akteure im deutschsprachigen Raum beteiligt sind.[77]

Zusätzlich ist für die Förderung der Akzeptanz auch Aufklärungsarbeit zur Funktionsweise und Sicherheit der SSI nötig, um das Vertrauen in die Technologie zu steigern. Findet die Lösung keine breite Akzeptanz, besteht die Gefahr der parallelen Existenz vieler untereinander inkompatibler Identifizierungslösungen, worunter die Nutzerfreundlichkeit leidet. Letztlich wäre es wünschenswert, dass eine SSI-Lösung nicht nur in einigen wenigen, sondern in vielen Ländern funktioniert.[78] Die Entwicklung einer internationalen SSI-Lösung erfordert jedoch erheblichen Koordinationsaufwand, vor allem weil auch Regulierungen angepasst werden müssen, die international noch nicht kompatibel sind. Dabei ist eine Kernfrage, welche Daten von Nutzerinnen und Nutzern abgefragt werden dürfen.

Die Decentralized Identity Foundation und das World Wide Web Consortium treiben die Entwicklung globaler Standards im Internet für SSI voran.[79] Auch auf EU-Ebene wird im Rahmen des «European Self-Sovereign Identity Frameworks» an einer internationalen Lösung gearbeitet.[80] KILT ist ein weiteres privatwirtschaftlich vorangetriebenes Projekt zur Blockchain-basierten Umsetzung einer SSI-Lösung, bei der statt Intermediären die Gemeinschaft über die Funktionsweise der Lösung entscheidet.[81]

Die Gestaltung der Governance beeinflusst auch die Datensicherheit. Je weniger Akteure in die Bereitstellung der SSI involviert sind (zum Beispiel nur der Staat oder nur die Schweiz), desto eher besteht die Gefahr, einen «Single-Point-of-Failure» zu schaffen. Beispielsweise könnte bei einer Lösung, die auf die Schweiz beschränkt ist, eine Störung in den Telekommunikationsnetzen der Schweiz zu einem Ausfall der SSI führen.

Eine SSI-Lösung kann die Einhaltung des Datenschutzes nicht vollständig garantieren. Wie Organisationen mit den Informationen umgehen, die sie über das Teilen eines Nachweises mithilfe einer SSI erhalten, lässt sich nicht kontrollieren. Eine mögliche Lösung dieses Problems ist, dass Nachweise bei jeder Transaktion neu übermittelt werden müssen. Zum Beispiel müsste bei der Buchung eines geteilten Autos jedes Mal aufs Neue der Führerausweis geteilt werden und dürfte nicht für künftige Transaktionen im System des Car-Sharing-Anbieters gespeichert werden. Allerdings kann auf technische Weise nicht sichergestellt werden, dass ein Anbieter sich an diese Vorgabe hält.[82]

Organisationen können deutlich mehr personenbezogene Informationen verlangen, als sie eigentlich zur Authentifizierung benötigen. Dies ist heute häufig der Fall. Beispielsweise fordert der Facebook-Messenger Zugriff auf Telefonnummern, Textnachrichten, getätigte Anrufe, E-Mails und andere gespeicherte Profile – alles Informationen, die eigentlich nicht zur Erbringung des Messenger-Dienstes not wendig sind.[83] Prinzipiell ist es auch mit einer SSI möglich, dass bei der Authentifizierung mehr Daten verlangt werden als unbedingt nötig. Zudem nehmen die Möglichkeiten, Daten von Bürgerinnen und Bürgern zu sammeln, auch deshalb zu, weil mithilfe einer SSI immer mehr manuelle Prozesse digitalisiert werden können. So könnte der Betreiber eines Zugangssystems zu Räumen, das den herkömmlichen Einlass mithilfe von Schlüsseln oder Codes ablöst, bei der Zugangskontrolle per SSI Daten über eintretende Personen sammeln.

Werden die Nachweise ausschliesslich auf den Smartphones der Bürgerinnen und Bürger gespeichert, so würden sie beim Verlust des Endgeräts verloren gehen. Die Erstellung eines Backups an einem anderen Ort könnte die datenschutzrechtlichen Vorteile der SSI wieder aufheben. Hier wird derzeit an Lösungen gearbeitet.[84] Wichtig ist dabei, dass auch hier die Bürgerinnen und Bürger selbst entscheiden können, ob und wo ein Backup gespeichert wird.[85]

Einige Industriepartner äusserten Bedenken, ob die Leistungsfähigkeit von Blockchains hinsichtlich Durchsatz, Geschwindigkeit und Skalierbarkeit für SSI ausreicht. Aufgrund der kontinuierlichen Weiterentwicklung der Technologie betrachten Teilnehmende an unseren Workshops wie auch die einschlägige Fachliteratur diese Herausforderung jedoch als lösbar. Entscheidend sei hier die Lösungsarchitektur.[86]

Zusammenfassung

SSI bietet klare Vorteile gegenüber den heute üblicherweise genutzten Authentifizierungslösungen wie Logins mit E-Mail-Adressen und Passwörtern oder dem Social Login: Bürgerinnen und Bürger sind selbst in der Lage, die eigenen Identitäten zu verwalten (Selbstverwaltung), und können darüber entscheiden, mit wem welche Informationen geteilt werden. Aussenstehende erlangen keinen Einblick, für welche Zwecke Identitäten genutzt werden («Privacy by Design»). Dennoch besteht auch bei SSI weiterhin die Möglichkeit, dass Datenschutzprinzipien verletzt werden, da die Bürgerinnen und Bürger nicht kontrollieren können, was mit einmal geteilten Daten geschieht. Auch weiterhin können Unternehmen unnötig viele Daten anfordern und sammeln. Daher sollte die Einhaltung der Prinzipien des Datenschutzes (speziell der Datensparsamkeit) nicht rein über die Technik, sondern auch anhand geeigneter Regularien (zum Beispiel durch Sanktionen) sichergestellt werden. Trotz der noch zu lösenden Herausforderungen wäre eine funktionierende SSI eine deutliche Verbesserung gegenüber dem heutigen Status quo und würde die informationelle Selbstbestimmung stärken.

Die Fähigkeit, Personen, Organisationen und Gegenstände digital eindeutig identifizieren zu können, gilt auch als «Enabler» vieler neuer Anwendungen und Geschäftsmodelle, speziell für Peer-to-Peer-Geschäfte. Zum Beispiel ermöglicht eine sichere und automatisierte Identifizierung, Verträge für das Teilen von Fahrzeugen direkt zwischen Anbietenden und Nachfragenden abzuschliessen und so die Abhängigkeit von Plattformbetreibern, die Vermittlungskommissionen verlangen, zu reduzieren. Eine funktionierende SSI-Lösung könnte zusätzlich in der physischen Welt eingesetzt werden, beispielsweise für die Zutrittsverwaltung zu Räumen ohne Schlüssel oder für Sicherheitskontrollen an Flughäfen ohne physische Ausweise.

Für eine erfolgreiche Umsetzung der SSI ist zentral, dass eine Lösungsarchitektur und Governance-Struktur gefunden werden, denen sowohl private Organisationen als auch Bürgerinnen und Bürger vertrauen. Da SSI und Blockchain Konzepte sind, denen Viele aufgrund fehlender Informationen skeptisch gegenüberstehen, ist weitere Aufklärungsarbeit notwendig. Zusätzlich sollte angestrebt werden, eine international kompatible und offene Lösung zu schaffen, bei der länderübergreifend sowohl staatliche als auch private Organisationen Identitäten und identitätsbezogene Dienstleistungen anbieten können. Die Tatsache, dass dem E-ID-Gesetz eine Vernehmlassung nachgestellt wurde, zielt darauf ab, dass eine Lösung gefunden wird, die breite Zustimmung erlangt.

Einsatz von Blockchain in Estland

Estland ist ein Vorreiter von Blockchain-Anwendungen. Vor zehn Jahren wurde Blockchain-Technologie in den Bereichen E-Government und E-Health erstmals eingesetzt. Heute werden in Estland Ausweisdokumente mit Blockchain verwaltet. Weitere Anwendungen sind das elektronische Patientendossier mit Arztberichten, E-Rezepte, digitale Steuererklärungen, digitale Verwaltungsdienstleistungen oder E-Voting. Sensible Daten werden dabei nicht direkt auf der Blockchain, sondern in Regierungssystemen gespeichert. Mithilfe von Blockchain wird allerdings die Integrität der Daten sichergestellt. Unautorisierte Änderungen an Daten sind nicht möglich beziehungsweise sehr unwahrscheinlich.

Das Vertrauen der Bevölkerung in digitale Technik ist in Estland sehr hoch. Das Land gehört zu den ersten Staaten, die eine elektronische Identität (E-ID) einführten – und das bereits vor 20 Jahren. Fast 50 % der Bevölkerung haben bei den Kommunalwahlen 2021 ihre Stimme online abgeben.[87]

Der Kanton Jura in der Schweiz hat die von Estland entwickelte Blockchain-Lösung KSI erprobt, um digital ausgestellte amtliche Dokumente fälschungssicher zu machen, und setzt sie seit Februar 2022 für Betreibungsregisterauszüge ein.[88]

Verteilte Verwaltung von sensiblen Daten am Beispiel von Gesundheitsdaten

Die Menge an personenbezogenen Daten, die digital erfasst und verarbeitet werden, nimmt kontinuierlich zu. Trotz der Überarbeitung der Datenschutzgesetze in der Schweiz und in der EU machen sich viele Bürgerinnen und Bürger Sorgen über die Verwendung ihrer Daten im Internet. Laut einer Umfrage in Deutschland aus dem Jahr 2021 war die Sorge um mangelnde Privatsphäre der zweitwichtigste Grund, warum Personen sich von sozialen Netzwerken abgewandt haben.[89] Dies scheint auch gerechtfertigt, denn viele Online-Dienste haben gegen das Datenschutzgesetz verstossen und mussten infolgedessen hohe Strafen zahlen.[90] Blockchain kann dabei helfen, den Schutz von sensiblen Daten und die informationelle Selbstbestimmung zu stärken. Nachfolgend analysieren wir dies am Beispiel von Gesundheitsdaten.

Status quo und Herausforderungen

In der Schweiz wie auch in den Nachbarländern werden derzeit Systeme zur zentralen Speicherung von Gesundheitsdaten in Form von elektronischen Patientendossiers (EPD) entwickelt. Hierbei spielt der rechtliche Rahmen eine tragende Rolle.[91] Da laut Schweizer Datenschutzgesetz Gesundheitsdaten besonders schützenswerte (sensible) Personendaten sind, gelten für deren Verarbeitung sehr hohe Anforderungen. So ist eine ausdrückliche persönliche Zustimmung für die Erhebung von Gesundheitsdaten notwendig, und ein Datensammler muss betroffene Personen informieren, auch wenn die Beschaffung von Gesundheitsdaten über Dritte erfolgt.[92]

Bislang wurden Gesundheitsdaten meist nur in den Systemen der Institutionen gespeichert, die sie erhoben haben (zum Beispiel in Arztpraxen oder in Spitälern). Hierdurch werden die gleichen Daten von verschiedenen Institutionen immer wieder neu aufgenommen, ein Datenaustausch erfolgt allenfalls manuell. Es entstehen verstreute, nicht verknüpfte Datensilos, die ein komplettes Bild von einer persönlichen Gesundheitshistorie unmöglich machen, worunter die Qualität der medizinischen Diagnose und Behandlung sowie die Patientensicherheit leiden können.[93] Wenn einzelne Akteure des Gesundheitswesens ihre Systeme nicht ausreichend schützen, besteht ausserdem die Gefahr des Datendiebstahls durch Cyberangriffe. Gestohlene Gesundheitsdaten sind im Darknet ein grosses Geschäft.[94]

Ziel des EPD ist es, diese Probleme durch eine zentrale Verwaltung der Daten zu lösen. Im Zentrum steht die informationelle Selbstbestimmung: Ein EPD kann nur mit persönlicher Einwilligung erstellt werden. Patientinnen und Patienten haben die volle Kontrolle darüber, welche Daten in ihren EPDs gespeichert werden und wer auf diese Daten zugreifen darf. Jede Bearbeitung der Daten muss protokolliert werden. Da in der Schweiz das Gesundheitswesen in der Verantwortung der Kantone liegt, mit unterschiedlichen Anforderungen je nach Kanton, wurde eine dezentrale EPD-Struktur gewählt: Sogenannte Stammgemeinschaften (das sind technisch-organisatorische Zusammenschlüsse von medizinischem Fachpersonal und seinen Einrichtungen[95]) können EPD-Systeme anbieten, die von einer Zertifizierungsstelle hinsichtlich technischer und regulatorischer Anforderungen überprüft werden. Zusätzlich werden weitere Dienstleister für die eindeutige Identifizierung von Personen genutzt (zum Beispiel SwissID). Stand November 2022 haben in der Schweiz acht Stammgemeinschaften die Zertifizierung bestanden, und es wurden insgesamt etwa 13 000 EPDs eröffnet. Das Projekt ist gegenüber der ursprünglichen Planung deutlich in Verzug geraten, insbesondere aufgrund der Komplexität der Zertifizierungsverfahren.[96]

Gleichzeitig arbeiten mehrere Akteure in der Schweiz darauf hin, ein wertorientiertes Gesundheitssystem einzuführen. Heutzutage erfolgt die Abrechnung der erbrachten medizinischen Leistungen mit den Kostenträgern (zum Beispiel Krankenversicherung) oft manuell und auf Basis fester Kostensätze.[97] In einem wertorientierten Gesundheitssystem soll sich die Leistungsabrechnung auch daran orientieren, ob eine Behandlung zu einer Verbesserung der Gesundheit geführt hat. Um dies zu erreichen, ist es notwendig, auch nach einer Behandlung Daten über die Gesundheit von Personen zu sammeln. Um die Effizienz in der Gesundheitsversorgung zu erhöhen, wird auch diskutiert, wie Patientinnen und Patienten dazu angeregt werden können, Krankheiten bereits vor ihrem Entstehen durch Verhaltensveränderungen vorzubeugen (Prävention) und beim Eintreten einer Erkrankung diese, sofern möglich, selbst zu behandeln (Selbstversorgung).[98] Für die Überwachung des Gesundheitszustands und zur Prävention nutzen Menschen zunehmend kommerzielle mobile Gesundheitsdienste. Bereits heute werden von grossen Technologieunternehmen über die Nutzung von Fitness- und Gesundheits-Apps im grossen Stil Gesundheitsdaten gesammelt. In einer Umfrage aus dem Jahr 2021 in der Schweiz gaben 36 % der Befragten an, Apps für Fitness und Bewegung zu nutzen.[99]

Ein EPD müsste im Sinne einer wertorientierten und präventiven Gesundheitsversorgung somit

eine zentrale Sicht auf die sicher gespeicherten Gesundheitsdaten schaffen. Die volle Kontrolle über die personenbezogenen Gesundheitsdaten müsste bei den Patientinnen und Patienten liegen. Sie könnten verschiedenen Institutionen des Gesundheitswesens (zum Beispiel Spitälern, Arztpraxen, Versicherungen) selektiv oder vollumfänglich den Zugriff auf diese Daten erlauben. Die in einem solchen System gespeicherten Gesundheitsdaten wären auch für die Gesundheitsforschung interessant oder für weitere datengetriebene Geschäftsmodelle, beispielsweise Prämienrabatte von Versicherungen für gesunde Lebensstile.

Zielbild

Im Folgenden illustrieren wir unter Berücksichtigung der aktuellen Literatur und der Meinungen unserer Experten eine Möglichkeit, das oben beschriebene System unter Nutzung von Blockchain-Technologie abzubilden.[100]

Für alle Beteiligten steht eine Frontend-Applikation bereit, wobei sich die Funktionalität je nach Bedarf unterscheidet. Wenn ein Leistungserbringer neue Daten über eine Person erzeugt, kann er diese mit deren Zustimmung in der zentralen Patientenakte, die durch Blockchain realisiert wird, hinterlegen. Die eigentlichen Gesundheitsdaten, wie Laborergebnisse, Röntgenbilder und Vitalparameter, verbleiben off-chain in der Datenbank des Leistungserbringers. Auf der Blockchain selbst werden einzig Metadaten (Verweise zu den Speicherorten der Daten), Zugriffsbedingungen (wer darf auf die Daten zugreifen) sowie der Hashwert der Daten hochgeladen. Dies ist notwendig, da laut Datenschutzgesetz Personendaten löschbar sein müssen (sogenanntes Recht auf Vergessen), was im Widerspruch zur Unveränderbarkeit von Daten auf Blockchains steht. Statt verteilt in den Systemen der Leistungserbringer könnte die Speicherung der Daten auch in einer zentralen Datenbank stattfinden, die von einer vertrauenswürdigen Partei betrieben wird. Dies hat allerdings Konsequenzen für die Verfügbarkeit, Integrität und Vertraulichkeit der Daten, die es zu prüfen gilt.[101]

«Im Gesundheitswesen existieren viele Datensilos. Blockchain bietet eine Möglichkeit, diese effizient und sicher zu managen, was wiederum die Diagnose- und Behandlungsqualität erhöht.»

Dr. Daniel Heller, Präsident des Verwaltungsrates, Kantonsspital Baden AG

Patientinnen und Patienten können die eigenen Daten einsehen und bestimmen, wer auf welche Daten zugreifen kann. Da sie Zugriffsrechte auch wieder entziehen können, spricht man bei diesem Konzept von «dynamischer Einwilligung» (englisch «dynamic consent»).[102] Bei allen Datenverarbeitungen oder Zugriffsanfragen, die nicht bereits persönlich genehmigt wurden (zum Beispiel für Forschungszwecke), erhalten die Betroffenen eine Benachrichtigung und müssen explizit zustimmen. Die Einhaltung der Zugriffsrechte und der automatische Datenaustausch wird über Smart Contracts realisiert. In diesen selbstausführenden Verträgen werden die eindeutigen Verweise zu den verteilten Gesundheitsdaten der Patientinnen und Patienten hinterlegt genauso wie die Zugriffsbedingungen, die diese für Behandelnde und andere Akteure des Gesundheitswesens festgelegt haben. Wenn beispielsweise ein Versicherer auf die Daten zugreifen möchte, wird über den Smart Contract automatisiert geprüft, ob dieser dazu berechtigt ist. Nur wenn das der Fall ist, werden die Daten aus dem Off-chain-Speicher bereitgestellt. Gleichzeitig wird über den Hashwert geprüft, ob die Daten unverändert sind. Optional könnten in den Smart Contracts auch Anreizmechanismen für die Bereitstellung von Daten, zum Beispiel als Datenspende für For-

Architektur eines Systems für die verteilte Verwaltung von Gesundheitsdaten

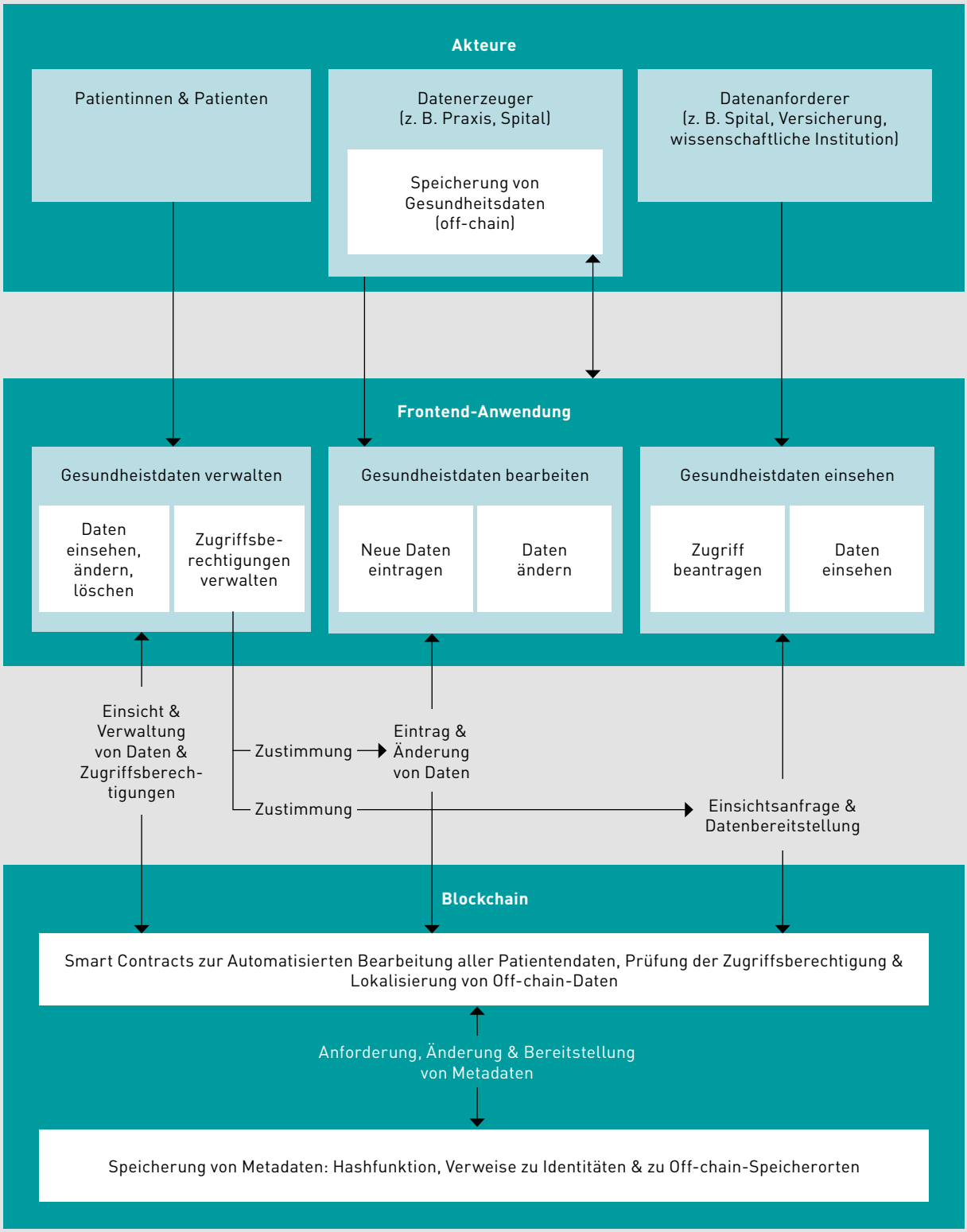


Abbildung 17: Eigene Darstellung.

schungszwecke, hinterlegt werden, beispielsweise die Zahlung eines finanziellen Betrags in einer Kryptowährung.

Die eindeutige Identifizierung aller an einem EPD Beteiligten ist für diesen Anwendungsfall ebenfalls relevant, wird an dieser Stelle jedoch nicht weiter erörtert. Grundsätzlich bietet Blockchain Möglichkeiten zur eindeutigen Identifizierung von Personen, Organisationen und Maschinen im Internet, wie im Anwendungsfall «selbstverwaltete Identitäten» näher erläutert wird. Abbildung 17 zeigt die grundsätzliche Architektur des Systems.

Chancen

Die Kombination der Off-chain-Speicherung der sensiblen Daten mit einer Zugriffsverwaltung, die über Blockchain realisiert wird, ist nach Einschätzung der Industriepartner aus technischer Sicht eine machbare und grundsätzlich geeignete Lösung. Da die Patientinnen und Patienten den Zugang zu ihren sensiblen Daten selbst verwalten, führt die Lösung zu mehr Eigenverantwortung. Die vollständige Sicht auf alle Gesundheitsdaten einer Person, inklusive aller Impfungen und Medikationen, hat viele Vorteile, zum Beispiel:

> Verbesserte Diagnose und Therapie in Praxen und Spitälern
> Hochwertigere und massgeschneiderte Behandlungen für Patientinnen und Patienten
> Entwicklung von neuen Therapien und Präventionsmassnahmen in der medizinischen Forschung
> Kosteneinsparungen für Versicherer und Versicherte aufgrund verbesserter Prävention und Behandlungen

Die Regelung der Zugriffsrechte über Smart Contracts eliminiert manuelle Datenübertragungsprozesse und vermeidet redundante Datenabfragen. Gleichzeitig behalten die Patientinnen und Patienten die Kontrolle über ihre Daten und verwalten die Zugriffsberechtigungen selbst. Ungewollte Manipulationen an den Daten werden durch die Nutzung von Hashwerten erschwert. Schafft man es, rund um die Gesundheitsdaten auf diesem System zusätzlich einen Marktplatz aufzubauen, so könnten Patientinnen und Patienten ihre Daten anonymisiert für eine Gegenleistung anderen Organisationen, beispielsweise Forschungsinstituten, anbieten.

Hackerangriffe auf Blockchains sind eher unattraktiv, da die Daten verteilt und nicht zentral gespeichert sind. Die auf den IT-Systemen der Datenerzeuger gespeicherten Daten (zum Beispiel in der Praxis oder im Spital) bleiben jedoch potenziell verwundbar.

Hürden und Risiken

Die hier identifizierten Hürden decken sich zu einem erheblichen Teil mit den Herausforderungen selbstverwalteter Identitäten. Dies liegt daran, dass beide Anwendungsbereiche das Ziel haben, personenbezogene Daten vertraulich und manipulationssicher zu speichern und Bürgerinnen und Bürger zu ermächtigen, den Zugriff darauf zu verwalten. Eine grosse Herausforderung besteht deshalb auch hier darin, ein System zu schaffen, dem die Patientinnen und Patienten sowie alle anderen Beteiligten im Gesundheitswesen vertrauen.

Um das Vertrauen der Bevölkerung zu gewinnen, ist Aufklärungsarbeit notwendig. Zu berücksichtigen ist hier das Privatsphäre-Paradox. Es besagt, dass die meisten Menschen trotz grosser Bedenken hinsichtlich der Wahrung der Privatsphäre im Internet gewillt sind, Daten zu teilen. Dies ist zum Beispiel bei der Nutzung von Social-Media-Plattformen oder Health Trackern zu beobachten, über die Technologieunternehmen bereits heute viele Gesundheitsdaten sammeln. Das Paradox

wird unter anderem damit erklärt, dass Menschen eher gewillt sind, ihre Bedenken beiseitezuschieben und Informationen zu teilen, wenn damit ein konkreter Mehrwert für sie verknüpft ist. Deshalb sollte man bei der Kommunikation einer EPD-Lösung einen konkreten und schnell eintretenden Nutzen in den Vordergrund stellen, beispielsweise für Patientinnen und Patienten die Möglichkeit einer verbesserten Diagnose durch eine Gesamtsicht auf die Gesundheitshistorie oder personalisierte Empfehlungen. Stellt man in der Kommunikation stattdessen Fragen des Datenschutzes zu sehr in den Vordergrund, besteht die Gefahr, dass Patientinnen und Patienten skeptisch werden. Als Anreiz könnten sie auch finanzielle Vorteile für das Teilen von Daten erhalten. Krankenversicherer gewähren bereits heute schon Rabatte, wenn die Versicherten bestimmte Gesundheitsdaten mit ihnen teilen.[103]

Eine ähnlich grosse Herausforderung ist es, die anderen Beteiligten im Gesundheitssystem von der Lösung zu überzeugen, das heisst die Leistungserbringer (Spitäler, Arztpraxen, Hilfs- und Pflegedienste, Apotheken, Labore, Pharmaunternehmen), Partner (Technologieunternehmen, Krankenkassen, Forschungsinstitutionen) und sonstigen Stakeholder (Bundesamt für Gesundheit, Interessensgruppen). Datenformate und Austauschwege müssten standardisiert werden, was Investitionen erfordert. Auch könnten nicht alle Organisationen gewillt sein, ihre Hoheit über erhobene Patientendaten aufzugeben. Wenn die Kontrolle über die Daten vollständig in den Händen der Patientinnen und Patienten liegt, könnten diese auch andere Institutionen mit Datenspenden begünstigen.

Um diese Probleme zu lösen, muss nach Ansicht der Industriepartner eine geeignete Governance-Struktur gefunden werden, bei der keine der beteiligten Parteien allein, sondern alle gemeinschaftlich die Kontrolle über das System und die Entscheidungsmechanismen haben. Die gewählte Form der Zusammenarbeit muss gerecht verteilte Anreize und Vorteile für alle beteiligten Stakeholder gegenüber dem Status quo bieten. Gleichzeitig muss eine kritische Masse im Gesundheitssystem die Lösung nutzen, sodass tatsächlich eine relevante Sammlung von Gesundheitsdaten mit dem System erfasst wird. Die Governance-Struktur und die Kommunikation bei der Markteinführung beeinflussen wiederum die Akzeptanz der Lösung unter Patientinnen und Patienten. Einerseits kann eine verteilte Governance, bei der keine Partei einzeln die Kontrolle über das System hat, vertrauensbildend wirken, da die Parteien sich gegenseitig kontrollieren und Manipulationen am System weitestgehend ausgeschlossen werden können. Andererseits könnten Patientinnen und Patienten eher gewillt sein, ihre Gesundheitsdaten dem System einer benennbaren Organisation, der sie vertrauen, zu überlassen. Dies ist heute zum Beispiel bei Banken der Fall, welche die Finanzdaten und transaktionen ihrer Kundinnen und Kunden zentral verwalten und abwickeln. Dies spricht wieder dafür, dass den Patientinnen und Patienten ein klarer Mehrwert angeboten werden muss, damit sie gewillt sind, eine EPD-Lösung zu nutzen.

Wie bei der SSI besteht auch hier die Herausforderung, dass Patientinnen und Patienten nicht kontrollieren können, was diejenigen, denen sie Zugriff auf ihre Daten erteilt haben, mit diesen machen. Beispielsweise hat in den USA eine App für das Überwachen des Menstruationszyklus personenbezogene Daten an Facebook verkauft.[104] In einem anderen Fall wurden GPS-Daten von Menschen, die Abtreibungskliniken besucht haben, online verkauft.[105] Auch wenn diese Daten anonymisiert sind, lassen sich häufig Verknüpfungen mit anderen Datensätzen herstellen, sodass

dann doch wieder die eindeutige Identifikation von Personen möglich wird.[106] Wenn Datenanforderer die erhaltenen Gesundheitsdaten über Patientinnen und Patienten auch auf ihren eigenen Systemen speichern, wären diese wiederum attraktiv für Hackerangriffe, und die Datensicherheit sinkt. Schliesslich besteht zudem die Gefahr, dass Daten nicht verfügbar sind oder verloren gehen, sollte das System eines Datenerzeugers ausfallen oder der Datenerzeuger die Daten versehentlich löschen oder verlieren. Hierzu gibt es Lösungsansätze[107] und auch Smart Contracts können helfen. Smart Contracts sind im juristischen Sinne nach dem Grundsatz «Code is Law» zwar verbindlich, allerdings sind Haftung und Klagemöglichkeit in Rechtsfällen unklar, was zu Unsicherheiten führt.

«Blockchain ermöglicht, die Kontrolle über sensible Gesundheits- und Finanzdaten zurückzuerlangen und so die informationelle Selbstbestimmung von Bürgerinnen und Bürgern zu stärken.»

Dr. Samyr Mezzour, Chief Innovation Officer, House of Insurtech Switzerland HITS

Zusammenfassung

Die Frage ist nicht, ob, sondern wann und wie ein geeigneteres System zur Verwaltung von Gesundheitsdaten eingeführt wird, da der Status quo mit vielen Nachteilen verbunden ist: Die herkömmliche verteilte und fragmentierte Speicherung von Gesundheitsdaten ist ineffizient, sie ermöglicht weder die eigenverantwortliche Selbstverwaltung von Gesundheitsdaten noch einen vollständigen Blick auf die Gesundheitshistorie einer Person, was die Qualität von Diagnosen und Therapien beeinträchtig. Der Hauptvorteil der oben beschriebenen Blockchain-Lösung ist, dass sie eine konsolidierte Sicht auf Gesundheitsdaten ermöglicht und Patientinnen und Patienten ihre Daten und den Zugriff darauf selbst verwalten können. Die Nutzung von Blockchain stellt dabei sicher, dass die Daten nicht unbemerkt von Dritten manipuliert werden können und ein hohes Mass an Automatisierung im Datenaustausch durch die Nutzung von Smart Contracts erreicht werden kann. Damit würde der Übergang von der institutionellen zur patientenorientierten Datenhaltung in einem «Continuum of Care»-Ökosystem – von der Prävention über die Früherkennung und Diagnose bis zur Therapie und Nachsorge – unterstützt werden.[108]

Allerdings kann auch hier nicht blind auf die Technik vertraut werden, denn was mit einmal geteilten Daten geschieht, kann nicht technisch, sondern nur durch andere Kontrollmechanismen, zum Beispiel Audits, kontrolliert werden. In der Umsetzung ist die grösste Herausforderung, dass die Vielzahl unterschiedlicher Interessen im Gesundheitssystem gemeinsam an einer Lösung arbeitet und die Mehrwerte der Lösung gerecht verteilt. Branchenverbände könnten hier möglicherweise unterstützen. Erst wenn das System von allen wichtigen Stakeholdern genutzt wird, kann eine wirkliche Konsolidierung der Gesundheitsdaten stattfinden. Letztlich sind auch das Vertrauen in die Datensicherheit und die Benutzerakzeptanz entscheidend. Einige Partner schlugen vor, eine entwickelte EPD-Lösung zunächst in kleinem Rahmen zu testen, damit sich der Nutzen am konkreten Beispiel demonstrieren lässt.

Teilweise fehlendes Vertrauen in zentrale Instanzen, der Druck zur Effizienzsteigerung, veränderte Kundenbedürfnisse und Datensicherheitsaspekte sind auch Herausforderungen in anderen Branchen. Die Finanzbranche ist ähnlich stark reguliert wie die Gesundheitsbranche und weist Parallelen bezüglich des Schutzinteresses von Daten auf. Funktionierende Systeme für die verteilte Verwaltung von sensiblen Daten haben auch

in dieser Branche grosse Zukunft. Im traditionellen Finanzsystem werden die Verwahrung und der Handel von Werten durch Intermediäre bewerkstelligt. Mit einer verteilten Blockchain-Lösung lassen sich klassische Finanzprodukte, wie das Verleihen von Kryptowährungen, selbstständig über Smart Contracts verwalten. Die Hoffnung von Decentralized Finance (DeFi) mittels Blockchain-Technologie ist, das Finanzsystem vertrauenswürdiger, effizienter, kostengünstiger und transparenter zu gestalten.

Rück- und Nachverfolgung von Waren am Beispiel von Arzneimitteln

Das Ziel der Rück- und Nachverfolgbarkeit in Lieferketten ist, Transparenz über die Herkunft, Weitergabe, Verarbeitung und Nutzung von Waren und Informationen zu schaffen. Dies ermöglicht, Prozesse zu überwachen und zu optimieren. Kundinnen und Kunden profitieren von grösserer Fälschungs- und Produktsicherheit sowie mehr Transparenz.[109] Das Bedürfnis, Transparenz über die Herkunft von Waren zu schaffen, existiert in vielen Branchen, wie zum Beispiel für Nahrungsmittel, Luxusgüter wie Uhren oder Rohstoffe wie Gold. Konsumenten möchten heute wissen, woher das Lithium in Batterien kommt, und der Regulator möchte wissen, welchen CO_2-Ausstoss die Lieferanten von Grosskonzernen verursachen. Blockchain bietet die Möglichkeit, physische Produkte im digitalen Raum abzubilden und effiziente Systeme für die Rück- und Nachverfolgung von Waren zu schaffen, ohne dass ein Akteur eine dominante Rolle einnimmt und viel Marktmacht auf sich vereint. Nachfolgend erläutern wir dies am Beispiel von Arzneimitteln.

Status quo und Herausforderungen

GS1 ist eine internationale, private, nicht gewinnorientierte Standardisierungsorganisation, die Systeme für die Rückverfolgbarkeit von Produkten anbietet. Laut eigenen Angaben deckt das GS1-System heute fast 100 % aller in der Schweiz zugelassenen Arzneimitteln ab.[110] Das GS1-System definiert sogenannte Nummernkreise, die zur eindeutigen Identifikation von Produkten, Betrieben, logistischen Einheiten und weiteren Objekten genutzt werden. Die Nummern können Hersteller selbst erstellen und an Verpackungen von Waren in Form eines zweidimensionalen Barcodes anbringen. Diese Barcodes werden gescannt, um im Datensatz weitere Information zu Prozessschritten, die mit den Waren durchgeführt wurden, zum Beispiel Transport oder Umverpackung, zu hinterlegen. Bei der Herausgabe von Arzneimitteln können Apotheken oder Spitäler die Herkunft der Arzneimittel rückverfolgen und sicherstellen, dass nur originale Arzneimittel herausgegeben werden. Sobald eine bestimmte Einheit eines Arzneimittels in der Schweiz verkauft wird, wird dies im GS1-System vermerkt, um sicherzustellen, dass die Nummern nicht kopiert und für andere Produkteinheiten verwendet werden können. Versiegelungen sollen vermeiden, dass einmal verpackte Arzneimittel entlang der Lieferkette ausgetauscht werden können. Prinzipiell wäre es zwar möglich, dass Hersteller falsche Daten zu produzierten Arzneimitteln an das GS1-System übermittelten und stattdessen möglicherweise gefälschte Produkte verpackten. Bei grossen Herstellern wäre diese Gefahr jedoch vernachlässigbar, da ein solches Vorgehen bei Aufdeckung der Reputation erheblich schaden könnte. Die Schweizer Zulassungsbehörde (Swissmedic) sowie RefData, eine Datenbank, in der Informationen zu allen zugelassenen Arzneimitteln veröffentlicht werden,

Produktnachverfolgung und Zulassung von Arztneimitteln in der Schweiz

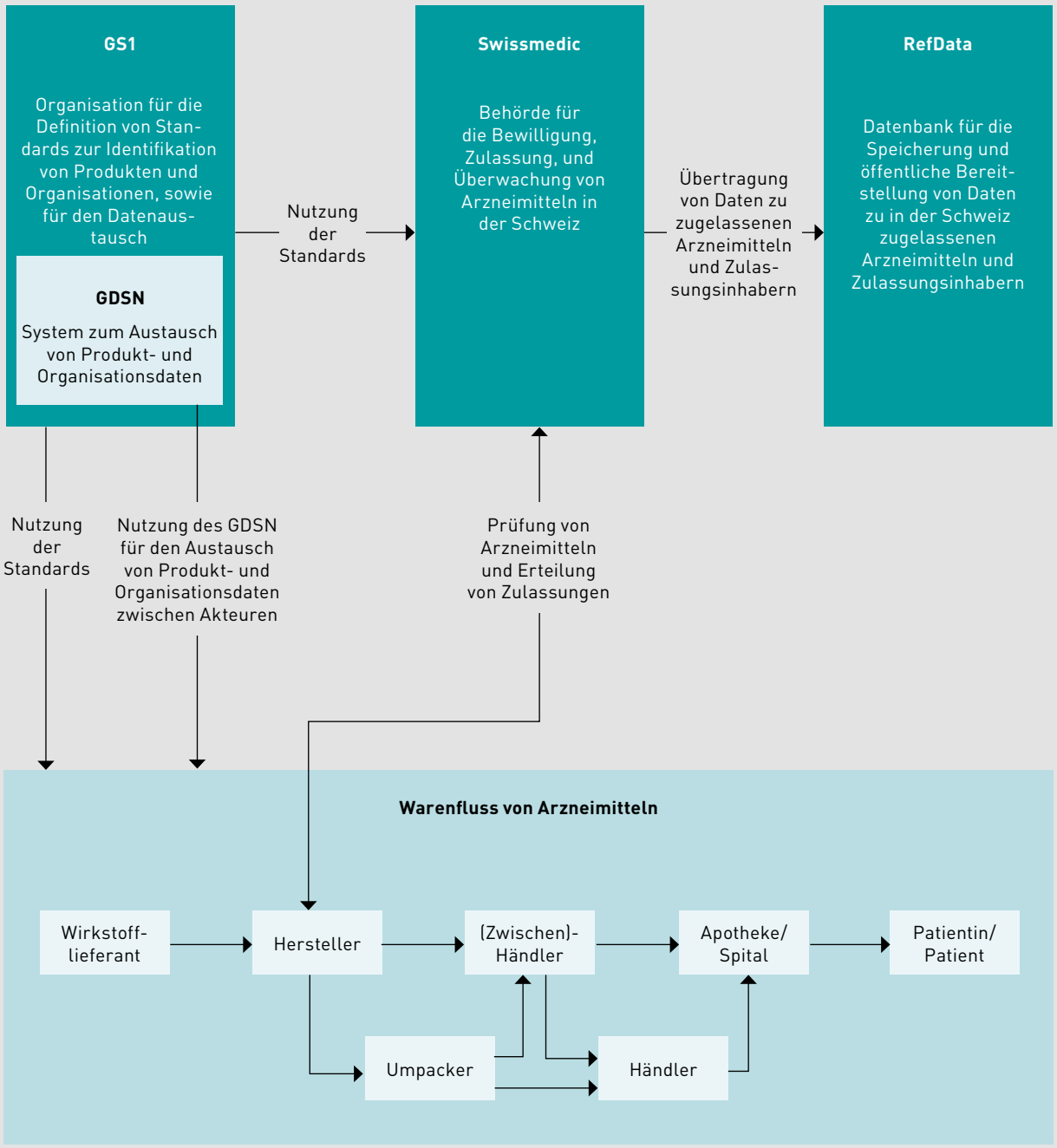


Abbildung 18: Eigene Darstellung basierend auf der Funktionsweise des GS1-Systems.

nutzen ebenfalls das nationale GS1-Kennzeichnungssystem.

Für den Datenaustausch zwischen den Akteuren kann das sogenannte «Global Data Synchronization Network» (GDSN) von GS1 genutzt werden, das aus 49 zertifizierten Datenpools (Stand September 2022) und einem Global Registry zur Verbindung der Datenpools besteht.[111] Führt ein Akteur einen Prozessschritt an Artikeln durch, lädt er diese Information in einen der Datenpools. Fordert ein Akteur Zugriff auf Artikeldaten, sendet er eine Anfrage an seinen Datenpool. Über diesen wird eine Anfrage an das Global Registry gesendet, um herauszufinden, in welchem Datenpool die Artikelinformationen liegen. Nun wird geprüft, ob der Datenempfänger berechtigt ist, auf die Daten zuzugreifen. Verfügt er über die erforderlichen Zugriffsrechte, werden die Daten bereitgestellt. Das GDSN nutzt ein Datenmodell, das Produkte in Kategorien einteilt und definiert, welche Attribute zu welchen Produkten hinterlegt werden können. Abbildung 18 stellt das heutige System dar.

Eine Herausforderung des heutigen Systems ist nach Auskunft der GS1, dass kleinere Produzenten nicht ans GS1-System angeschlossen sind, da der Aufwand zu hoch sei. In diesen Fällen werde auf den Produkten lediglich die Swissmedic-Zulassungsnummer angebracht, die eine Überwachung der Herkunft der Arzneimittel nicht zulasse. Auch wären nicht alle Spitäler an das GS1-System angeschlossen und nutzten teilweise eigene Systeme, unter anderem da das GS1-System nicht überall bekannt und vom Gesetzgeber kein landesweiter Standard für die Nachverfolgbarkeit von Arzneimitteln definiert sei. Zusätzlich würden in der Schweiz Arzneimittel auch über das Internet von nicht offiziell zugelassenen Verkaufsstellen verkauft. Auch auf diesem Wege könnten Fälschungen auf den Markt gelangen.

Aufgrund der Vielzahl an (teils manuellen) Schnittstellen ist die Reaktionszeit des Systems nach Ansicht einiger unserer Industriepartner und den Angaben einer US-amerikanischen Quelle in manchen Fällen relativ lang.[112] Dies kann zum Beispiel bei Produktrückrufen problematisch sein, da unter Umständen noch Arzneimittel verkauft werden, bevor die Rückrufinformation in den Ausgabestellen ankommt. In den USA kann das bis zu drei Tagen dauern. Das heutige System erlaubt zudem nicht das «Forward Tracking», also dass Hersteller einsehen können, welchen Weg ihre Arzneimittel bis zur Ausgabestelle zurücklegen und wann sie ausgegeben werden.

Zielbild

Unser Zielbild illustriert eine Möglichkeit, das oben beschriebene System unter Nutzung von Blockchain-Technologie abzubilden. Dabei haben wir uns an dem US-amerikanischen Pilotprojekt «FDA DSCSA Blockchain Interoperability Pilot» von IBM, KPMG, Merck und Walmart orientiert.[113] Abbildung 19 stellt das System dar.

Akteure greifen über Frontend-Applikationen auf das System zu. Sie können Produktereignisse erstellen, beispielsweise das Herstellen, Versenden oder Ausgeben eines Arzneimittels. Ausserdem können sie Massnahmen zur Gewährleistung der Produktsicherheit ergreifen, zum Beispiel die Produktherkunft überprüfen oder einen Rückruf starten. Über definierte Schnittstellen kommunizieren die Frontend-Applikationen mit den Backend-Applikationen, welche die Produkt- und Organisationsdaten in ein Blockchain-Register schreiben und von ihm abrufen. Das Backend stellt auch sicher, dass nur berechtigte Akteure Zugriff auf die Daten haben und nur Daten im richtigen Format auf die Blockchain geschrieben werden. Über die Schnittstelle können für den automatisierten Datenaustausch zudem externe System angebun-

den werden, wie das GS1-System, sodass die standardisierten Nummernkreise weiterhin verwendet werden können, oder andere Drittsysteme der Akteure, zum Beispiel ERP-Systeme.

Es gibt grundsätzlich zwei Optionen für den Speicherort der Warendaten: Einerseits könnten alle Daten auf einer Blockchain gespeichert werden. Diese Variante wurde im oben erwähnten Pilotprojekt in den USA gewählt. Sie hat den Vorteil, dass die Daten dann tatsächlich unveränderbar sind. Nachteilig ist jedoch, dass die Daten vermutlich redundant auf den Systemen der Datenerzeuger und einer Blockchain gespeichert werden, die Daten nicht löschbar sind und die in einer Blockchain gespeicherten Datenvolumen sehr gross werden können. Die auf einer offenen Blockchain gespeicherten Daten können zudem von allen Akteuren eingesehen werden, was unter Umständen zur Offenlegung von Geschäftsgeheimnissen wie Produktionsvolumen führen kann.[114]

Eine andere Möglichkeit wäre, auf einer Blockchain nur Metadaten zu den Produkten zu speichern, wie einen Verweis zum Speicherhort der Daten, die Zugriffsbedingungen sowie den Hashwert der Daten. Die eigentlichen Daten würden bei dieser Umsetzung off-chain in der Datenbank des Datenerzeugers bleiben und nicht auf einer Blockchain gespeichert werden.[115] Fordert ein Akteur Daten an, würde über die Metadaten zunächst geprüft werden, ob der Akteur zugriffsberechtigt ist, bevor die Daten mithilfe des Verweises vom Speicherort abgerufen und über den Hashwert auf ihre unveränderte Echtheit geprüft werden können. Diese Lösung hätte einige Vorteile: Absolut gesehen müssten weniger Daten mittels Blockchain gespeichert werden, die off-chain gespeicherten Daten wären löschbar und könnten nicht von jedem eingesehen werden. Falls jemals personenbezogene Daten Eingang in das System finden würden, wäre die Off-chain-Speicherung zwingend notwendig, da solche Daten laut Schweizer und Europäischem Datenschutzgesetz zwingend löschbar sein müssen.

Über Smart Contracts könnten in Zukunft weitere Geschäftsprozesse automatisiert werden. Zum Beispiel könnten bei der Beschädigung eines Produkts während des Transports automatisch eine Nachbestellung oder bei Erhalt eines Produkts automatisch eine Zahlung ausgelöst werden. Die Zugriffsberechtigung auf Daten könnte, wie in der Anwendung «Verteilte Verwaltung von Gesundheitsdaten», über Smart Contracts gesteuert werden.

Zusätzlich könnten auch Sensoren an das System angeschlossen werden, die automatisiert Informationen zu Arzneimitteln in die Blockchain hochladen. Zum Beispiel könnten Temperatursensoren an Produktverpackungen kontinuierlich die Umgebungstemperatur messen, um sicherstellen zu können, dass Kühlketten eingehalten werden. Liegt die Temperatur zu lange über einem kritischen Wert, könnte über einen Smart Contract das Produkt automatisch als fehlerhaft markiert und aus der Lieferkette genommen werden. Das Schweizer Start-up Modum entwickelt solche Lösungen und wurde im Jahr 2021 vom amerikanischen Unternehmen Roambee gekauft.[116] Generell gilt, je mehr Daten automatisiert von Maschinen statt manuell durch Menschen direkt in Blockchains geschrieben werden, desto niedriger ist die Gefahr, dass sich Datenfehler bei der Dateneingabe einschleichen.

Im Pilotprojekt wurde die Lösung als zugangsbeschränkte Blockchain mit drei Knoten – Hersteller, Händler und Ausgabestelle – aufgesetzt. Laut Bericht war die Lösung erfolgreich. Alle Produktinformationen konnten im System gespeichert, die Systeme der Akteure angebunden,

Architektur eines Systems für die Produktnachverfolgung unter Nutzung von Blockchain

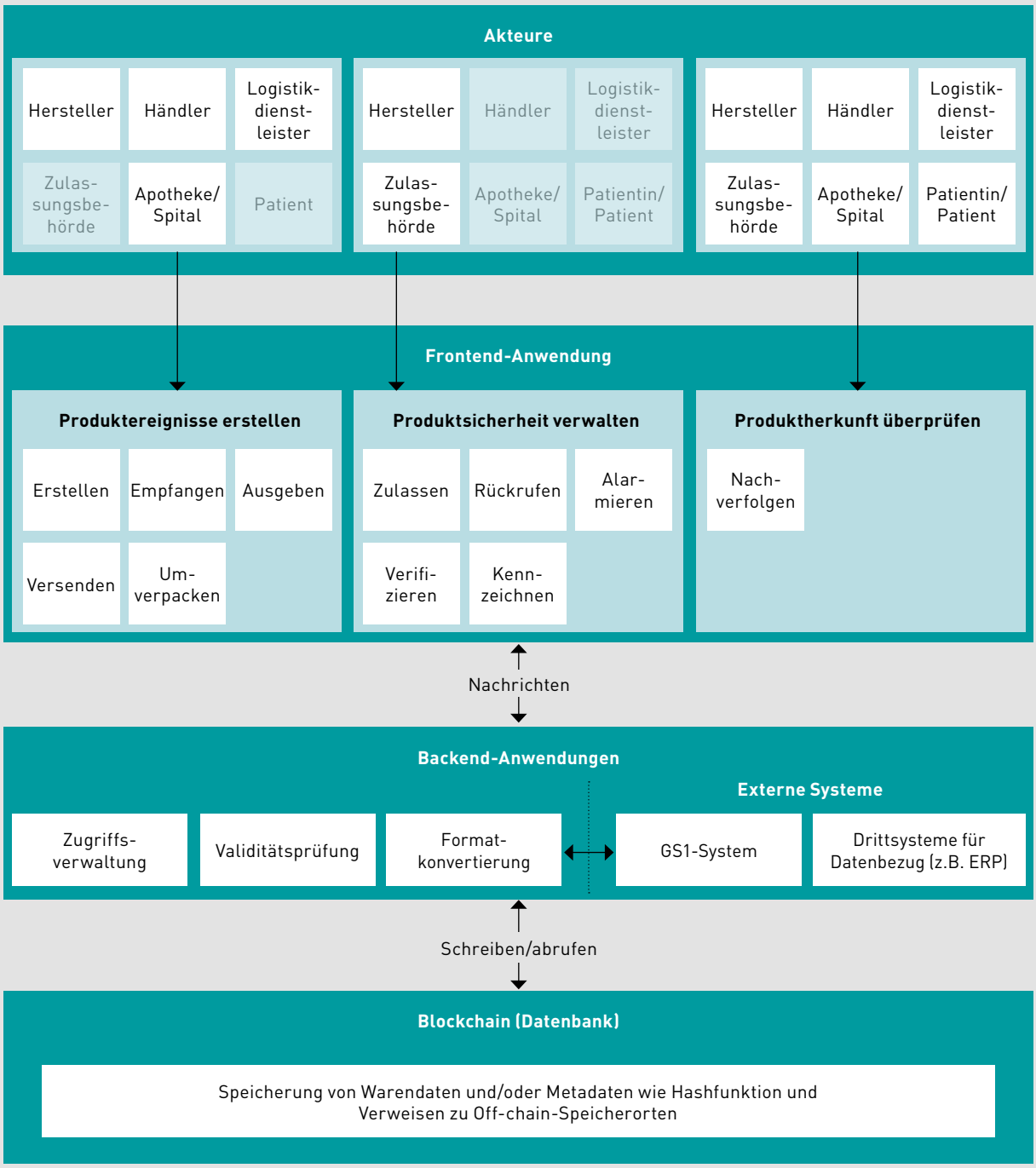


Abbildung 19: Eigene Darstellung.

Arzneimittel von allen Akteuren rückverfolgt und bei der Ausgabe entwertet werden. Auch Rückrufinformationen wurden schnell an Akteure weitergegeben.[117]

Chancen

Im Workshop zeigte sich, dass die Teilnehmenden in der Hebung von Effizienzpotenzialen die grössten Chancen der Blockchain-Lösung sehen. Diese betreffen die Abschaffung oder Vereinfachung von Datenschnittstellen, zum Beispiel werden mit der Lösung die verteilten Datenpools obsolet. Weitere Vorteile sind die schnellere Verfügbarkeit von Informationen zu Produkten, da die Synchronisierung sich über Blockchain ggf. schneller vollzieht, sowie die Automatisierung von Prozessschritten, beispielsweise der Upload von Daten. Laut dem Pilotprojekt in den USA können in maximal zehn Sekunden Rückrufinformationen an alle relevanten Akteure versandt werden, während dies heute bis zu drei Tage benötigt.[118] Allerdings kann die Latenz steigen, wenn mehr Akteure das System nutzen. Da die Hauptvorteile in der Effizienzsteigerung gesehen wurden, handelt es sich bei der Lösung nach Ansicht eines Partners nicht um eine Disruption, also eine grundlegende Veränderung von Prozessen, Technologien oder Geschäftsmodellen, sondern um eine Verbesserung eines bestehenden Systems.

Zusätzlich steigt die Manipulationssicherheit und damit die Integrität der Daten, da diese eher nicht unbemerkt verändert werden können. Dadurch erhöhen sich ebenfalls die Fälschungs- und Produktsicherheit. Im gegenwärtigen System müssen alle Akteure mindestens GS1 und den an das GDSN angeschlossenen Datenpools vertrauen. Würde die Blockchain-Lösung von einer Vielzahl an Organisationen entlang der Lieferkette gemeinschaftlich betrieben und verwaltet werden statt von einer Drittpartei, so könnten Intermediäre und die Abhängigkeit von diesen reduziert werden. Hierdurch würde auch ein «Single-Point-of-Failure» abgeschafft, wodurch sich die Ausfallsicherheit erhöht, da das System weiterläuft, auch wenn einzelne Akteure ausfallen. Heute hängt das Funktionieren des Systems stark von der Verfügbarkeit der Systeme von GS1 und den Datenpools ab.

Als weiterer Vorteil wurde eine erhöhte Transparenz hinsichtlich der Funktionsweise der Lösung genannt. Dies liegt daran, dass der Programmcode einer Blockchain theoretisch von allen beteiligten Akteuren gemeinschaftlich festgelegt und eingesehen werden kann.

Grundsätzlich bietet die Lösung das Potenzial, unter Nutzung von Smart Contracts noch mehr Prozessschritte zu automatisieren, zum Beispiel die automatisierte Abwicklung von Zahlungen, sobald Produkte eingetroffen sind, oder von Nachbestellungen, sobald Lagerbestände leerlaufen. Hierfür müssten allerdings noch weitere Systeme verknüpft werden.

Hürden und Risiken

Zwar wurden Bedenken hinsichtlich der Reife und Leistungsfähigkeit von Blockchain-Technologie geäussert, jedoch wurden diese von anderen Industriepartnern, die bereits an der Umsetzung von Blockchain-Projekten beteiligt waren, ausgeräumt. Dennoch ist bei der Entwicklung der Lösung darauf zu achten, dass eine Architektur gewählt wird, die eine ausreichend hohe Leistungsfähigkeit hinsichtlich Geschwindigkeit, Skalierbarkeit und Durchsatz ermöglicht.[119]

Als grösste Herausforderung wird die unterschiedliche Interessens- und Motivationslage der für die Umsetzung notwendigen Akteure gesehen. Das heutige System funktioniert ausreichend gut und war mit hohen Investitionen verbunden, somit

besteht kein Drang zur Veränderung. Erschwerend kommt hinzu, dass Arzneimittellieferketten global sind. Eine Vielzahl an Akteuren sind hier involviert und viele länderspezifische Regularien müssen berücksichtigt werden. Das oben beschriebene System erfordert die Entwicklung klarer Standards für die Datenhaltung und den Austausch, was im Hinblick auf die komplexen Anforderungen schwierig ist und hohe Investitionen erfordert. Schliesslich erzeugen die Entwicklung der Lösung und der notwendige Parallelbetrieb von Alt- und Neusystemen in der Übergangszeit hohe Kosten, wohingegen die erhofften Effizienzsteigerungen erst später realisiert werden können. Dies kann erschweren, zögerliche Akteure zu überzeugen. Auch hier schlagen die Industriepartner als Lösung die testweise Umsetzung in einem klar abgegrenzten Rahmen – in einem Land oder für ein spezifisches Arzneimittel – vor. Sollten sich die erwarteten Mehrwerte einstellen, könnten damit weitere Akteure überzeugt und das System skaliert werden.

Wie in der vorherigen Anwendung ist von einer breiten Nutzung des Systems nur auszugehen, wenn ein Modell der Zusammenarbeit gefunden wird, das sicherstellt, dass die durch die Lösung generierten Mehrwerte unter allen Partnern gerecht verteilt werden. Dies beinhaltet die Zusammenarbeit off-chain, zum Beispiel zur Entscheidungsfindung bei Systemanpassungen, und automatisiert on-chain, zum Beispiel hinsichtlich der Definition von Datenschnittstellen oder automatisierten Prozessen. Im Rahmen von GS1 wurde bereits ein Zusammenarbeitsmodell vieler Akteure etabliert, auf das aufgebaut werden könnte.

Zu entscheiden ist zudem, welche Daten in der Blockchain für wen einsehbar wären, und ob die beteiligten Akteure anonym sind oder nicht. Würde die Blockchain offen gestaltet werden, so könnte die Anonymität der Akteure gewahrt bleiben, da diese nur unter ihrem öffentlichen Schlüssel im Netzwerk interagieren würden. Allerdings könnten dann auch weniger vertrauenswürdige Akteure Zugang erhalten. Da alle Akteure Einsicht in die über die Blockchain abgewickelten Transaktionen haben, wäre es möglich, dass Geschäftsgeheimnisse offengelegt werden, beispielsweise Produktionsvolumen oder Kundenbeziehungen.[120] Auch besteht die Gefahr, dass über Transaktionsdaten Akteure eindeutig identifiziert werden können, auch wenn diese eigentlich anonymisiert sind. Demzufolge könnten Akteure auf Blockchains wechselnde Pseudonyme verwenden, um die Identifikation zu erschweren. Bei einer zugangsbeschränkten Blockchain würden nur zugelassene Akteure auf das System zugreifen können. Dies würde allerdings bedeuten, dass die Akteure mindestens durch das Durchlaufen des Zulassungsprozesses bekannt sind.

Eine Herausforderung ist auch, dass auch Blockchain nicht sicherstellen kann, dass nur korrekte Daten gespeichert werden. Das sogenannte GIGO-Prinzip («Garbage in, Garbage out») gilt auch für Blockchains. Es wird deshalb empfohlen, möglichst viele Datenerhebungs- und schreibprozesse zu automatisieren, sodass menschliche Fehler vermieden werden können. Das System würde auch nicht verhindern, dass weiterhin Arzneimittel über inoffizielle Wege, zum Beispiel über Internetplattformen, auf den Markt kommen.

Zusammenfassung

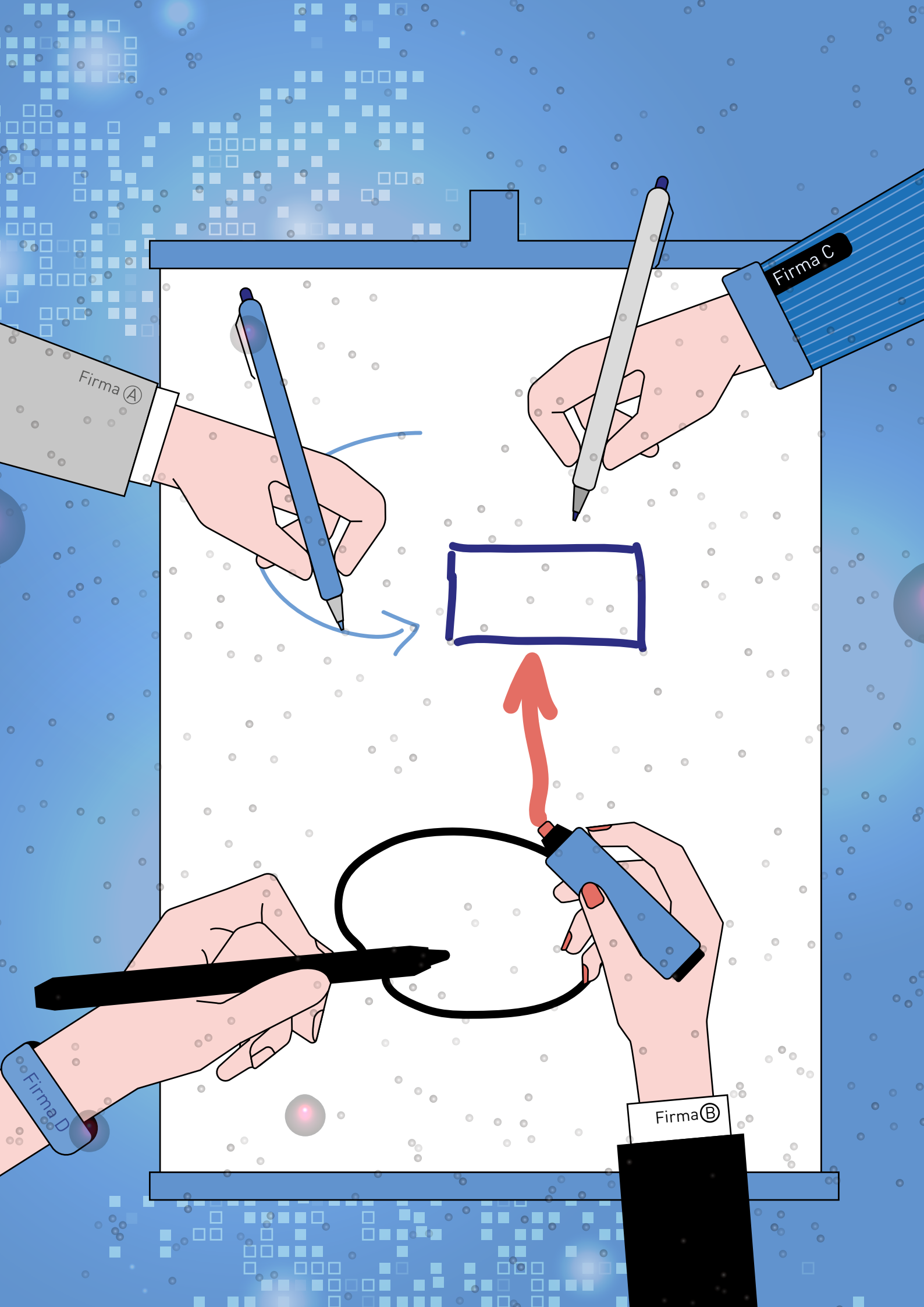
Die beschriebene Blockchain-Lösung zur Rück- und Nachverfolgung von Arzneimitteln bietet klare Vorteile gegenüber dem heutigen Status quo: Manuelle Schnittstellen würden abgeschafft, Prozesse automatisiert, der Datenaustausch erheblich beschleunigt, die Transparenz sowie Fälschungs- und Produktsicherheit erhöht. Ob in Zukunft ein

System geschaffen wird, das diese Mehrwerte realisiert, hängt vor allem vom Willen der Akteure in der Arzneimittellieferkette ab. Das Aushandeln eines geeigneten Zusammenarbeitsmodells und die Einigung auf Standards, die international kompatibel sind, erfordern viel Zeit und hohe Kosten. Auch die Entwicklung der sich heute im Einsatz befindenden Systeme hat mehrere Jahrzehnte gedauert. GS1 wurde beispielsweise schon im Jahr 1974 gegründet. Weil für dieses System bereits Zusammenarbeitsmodelle in der Arzneimittellieferkette entwickelt wurden, scheint es ratsam, für eine neue Lösung darauf aufzusetzen. Gleichzeitig scheint der Veränderungsdrang nicht so hoch zu sein wie bei den anderen beiden besprochenen Anwendungen. Das heutige GS1-System hat Verbesserungspotenzial, funktioniert jedoch grundlegend.

«Die Blockchain-Technologie passt mit ihren dezentralen Eigenschaften gut zu einer CO_2-neutralen Energielandschaft und transparenten Gesellschaft, in der Haushalte und Unternehmen immer häufiger Strom selber produzieren, speichern und handeln und über die Stromherkunft Bescheid wissen möchten.»

Markus Riner, Leiter Digitalisierung und IT,
Verband Schweizerischer Elektrizitätsunternehmen VSE

Zu berücksichtigen ist zudem, dass manche der heutigen Schwachstellen sich auch ohne den Einsatz von Blockchain lösen lassen. Darunter fallen die fehlende Möglichkeit für das Forward-Tracking, Nachbestellungen oder die Abschaffung manueller Schnittstellen. Dennoch bietet Blockchain eine geeignete Grundlage, um physische Produkte digital abzubilden und deren Weg entlang von Wertschöpfungsketten effizient und sicher zu verfolgen. Dies bietet Vorteile bei Arzneimitteln, aber auch in vielen anderen Branchen. Entsprechend sehen unsere Experten aus der Energiewirtschaft hier grosses Potenzial. Denn Blockchain kann nicht nur Warenströme von Produkten digital abbilden, sondern es könnte auch immaterielle Stromnachweise erbringen.


Firma Ⓐ
Firma C
Firma Ⓑ
Firma D

Kritische Erfolgsfaktoren von Blockchain-Projekten

Wir haben kritische Erfolgsfaktoren bei der Entwicklung und Einführung von Blockchain-Anwendungen identifiziert und in sieben Kategorien dargestellt. Abgeleitet wurden sie aus der Detailanalyse der Anwendungen im vorherigen Kapitel und der einschlägigen Fachliteratur. Abbildung 20 stellt die Faktoren dar, welche wir im Folgenden erläutern. Der Anhang enthält eine detaillierte Beschreibung der Faktoren.

Zweckmässigkeit und Wirtschaftlichkeit

Bevor mit der Umsetzung eines Blockchain-Projekts begonnen wird, sollte im Rahmen einer Business-Case-Analyse geprüft werden, ob die Eigenschaften von Blockchain für den gewählten Anwendungsfall tatsächlich Vorteile gegenüber dem Status quo bieten. Ausserdem muss der Nutzen, der durch den Einsatz von Blockchain realisiert werden soll, die Investitions- und Betriebskosten, auch unter Berücksichtigung von Unsicherheiten und Projektrisiken, deutlich übersteigen. Die durch die Lösung generierten Mehrwerte und Kosten müssen unter allen Stakeholdern gerecht aufgeteilt werden. Nur wenn alle, die für den Erfolg der Lösung von Bedeutung sind, Anreize haben, die Entwicklung und Nutzung zu unterstützen, ist eine erfolgreiche Realisierung möglich. Akteure mit starker Marktposition zu überzeugen, an einer Lösung mitzuwirken, kann besonders schwierig sein.

Projektaufbau und -umsetzung

Eine Blockchain-Lösung zu entwickeln und erfolgreich am Markt zu etablieren, ist ein aufwendiges Unterfangen, das viele Ressourcen, Koordination und Zeit erfordert. Um eine erfolgreiche Umsetzung sicherzustellen, müssen alle bedeutenden Stakeholder eine gemeinsame Projektvision und realistische Erwartungen hinsichtlich der Chancen, Risiken und der Projektdauer haben. Bei unternehmerischen Blockchain-Projekten vergehen zwischen der ersten Machbarkeitsstudie und dem produktiven Einsatz durchschnittlich 25 Monate.[121] Im Projekt müssen das notwendige technische und fachliche Wissen sowie die notwendigen Ressourcen (Zeit, Geld, Mitarbeitende) zur Realisierung der Lösung vorhanden sein. Da Blockchain weiterhin eine relativ junge Technologie ist, kontinuierlich weiterentwickelt wird und viel Gestaltungsspielraum bietet, sollte die Umsetzung schrittweise durchgeführt werden. Zwischenergebnisse sollten getestet, Feedback gesammelt und in der Entwicklung berücksichtigt werden. Erst nach einem erfolgreichen Piloten sollte die Lösung skaliert werden.

«Blockchain erlaubt Organisationen auf neue Art zusammenzuarbeiten und ermöglicht neue Geschäftsmodelle. Die Technologie ist dabei nur Enabler. Wichtig sind die richtigen Anreizsysteme und eine funktionierende Governance.»

Daniel Rutishauser, Head of Blockchain, Inacta

Technische Umsetzung

Blockchain bietet viele Gestaltungsspielräume in der technischen Umsetzung. Diese betreffen zum Beispiel Zugangsbeschränkungen, die Wahl des Konsensmechanismus, die Anzahl der Knoten, das Design von Smart Contracts oder Kombinationen von On-chain- und Off-chain-Datenspeicherungen. Daher ist es wichtig, die Architektur der Lösung genau auf die langfristigen Anforderungen des Anwendungsfalls abzustimmen.

Zusätzlich sollten möglichst viele Medienbrüche und Schnittstellen abgeschafft, Prozesse automatisiert und manuelle Schritte vermieden werden. Auch redundante Datenhaltungen gilt es abzuschaffen, wenn darunter die Verfügbarkeit nicht leidet. Da der Stromverbrauch von Blockchains in manchen Fällen sehr hoch ist, muss bei der technischen Architektur darauf geachtet werden, dass

Kritische Erfolgsfaktoren von Blockchain-Projekten

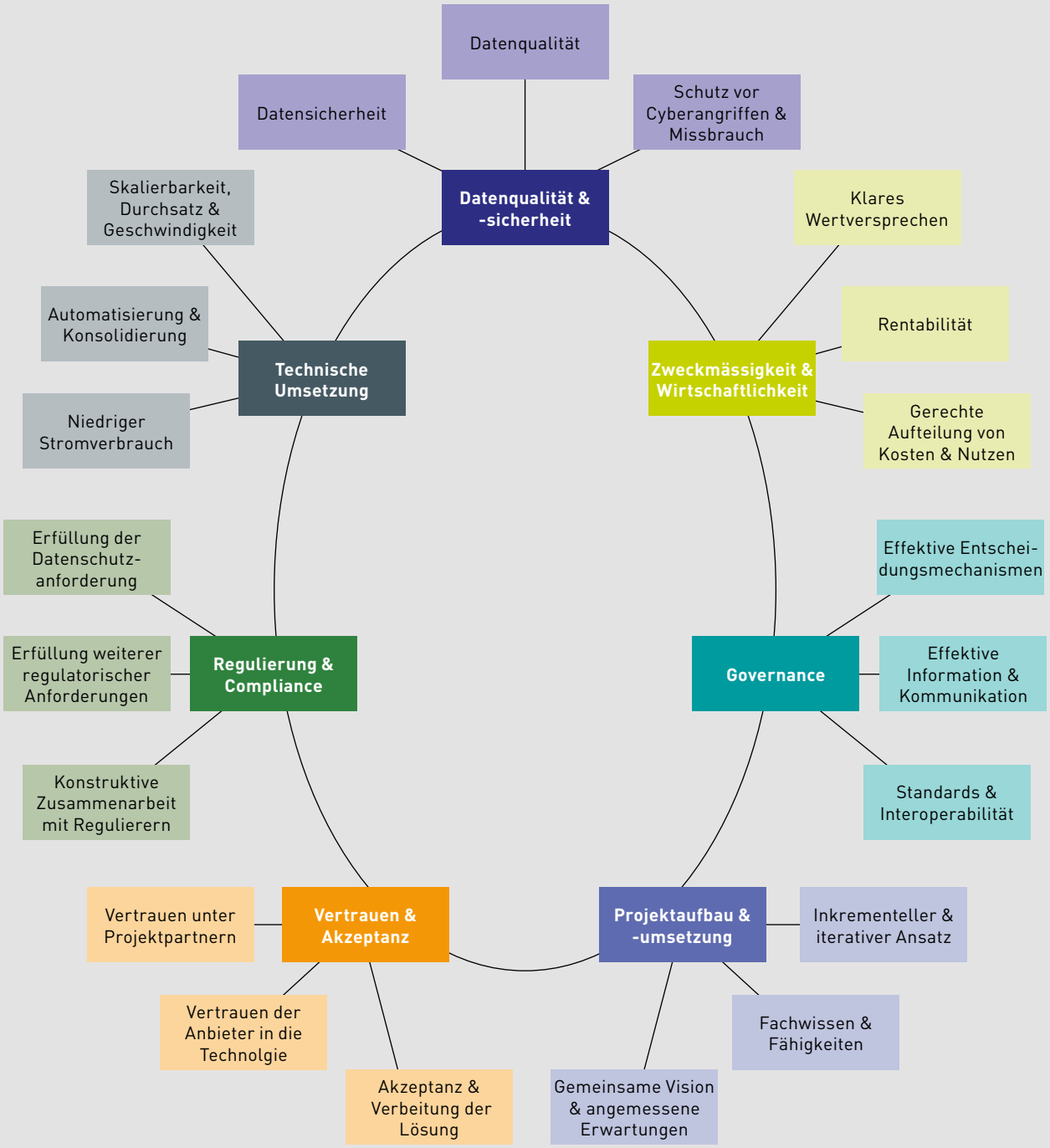


Abbildung 20: Eigene Darstellung.

der durch die Lösung generierte Mehrwert den Stromverbrauch rechtfertigt. Ein hoher Stromverbrauch ist allerdings nur bei offenen Blockchains, die den Konsensmechanismus «Proof-of-Work» einsetzen, und somit nicht bei zugangsbeschränkten Blockchains, der Fall.

Datenqualität und -sicherheit

Blockchain-Technologie erschwert es, Daten unbemerkt zu verändern. Sie kann aber nicht sicherstellen, dass nur korrekte Daten erfasst werden. Auf technischer und prozessualer Ebene ist deshalb sicherzustellen, dass die Daten, die auf Blockchains geschrieben werden, korrekt sind und menschliche Fehler weitestgehend vermieden werden, zum Beispiel indem viele Datenerhebungs- und schreibeprozesse automatisiert werden.

Weil Daten auf Blockchains verteilt gespeichert werden, sind sie für Cyberangriffe tendenziell unattraktiver als konventionelle Lösungen. Dennoch sind Cyberattacken möglich, zum Beispiel wenn es gelingt, in die Systeme der Knoten einzudringen und Zugriff auf private Schlüssel zu erhalten. Auch können die Systeme von Netzwerkmitgliedern attackiert werden, nachdem Daten aus einer Blockchain importiert wurden oder in denen Daten off-chain gespeichert werden. Daher müssen nicht nur Blockchains selbst, sondern auch die Systeme der Teilnehmenden sowie deren private Schlüssel ausreichend geschützt werden. Off-chain-Governance-Strukturen können sich auf den Datenschutz auswirken. Zum Beispiel müssen neue Mitglieder in zugangsbeschränkten Blockchains erst zugelassen werden. Die Zulassungsprozesse können die Identitäten der Prüflinge offenlegen. Aggarwal und Kumar (2020) diskutieren weitere Angriffsmöglichkeiten auf Blockchains und Schutzmechanismen dagegen.[122]

Governance

Effektive Governance-Mechanismen stellen sicher, dass alle Stakeholder über geeignete Kanäle von den für sie relevanten Entwicklungen und Entscheidungen erfahren, die Möglichkeit haben, Vorschläge einzubringen und zu diskutieren und entsprechend ihrer Rolle angemessen in Entscheidungsprozesse involviert zu werden. Sie definieren auch Vorgehensweisen, wie mit Konflikten zwischen Teilnehmenden oder unlauterem Verhalten einzelner umgegangen wird. Die Entwicklung geeigneter Governance-Strukturen ist umso herausfordernder, je mehr Stakeholder beteiligt sind, je unterschiedlicher deren Interessen sind und je weniger diese sich gegenseitig vertrauen. Zusätzlich müssen für den organisationsübergreifenden Datenaustausch Datenmodelle und Schnittstellen standardisiert werden.

Vertrauen und Akzeptanz

Bis heute ist mit Blockchain der Mythos verbunden, die Technologie mache Vertrauen unnötig. Dies liegt vor allem daran, dass die Technik sicherstellt, dass einzelne Mitglieder im Netzwerk Daten oder Transaktionen nur schwer unbemerkt verändern können. Dies bietet vor allem Vorteile bei Peer-to-Peer-Transaktionen, bei denen kein Intermediär die Vertrauenswürdigkeit der Partner und die Rechtmässigkeit und Sicherheit der Transaktion sicherstellt. Heute leistet zum Beispiel AirBnB diesen Service für Übernachtungen in Privathaushalten, und Nutzende zahlen einen Aufschlag für diesen Service. Dieser könnte in Zukunft geringer ausfallen, wenn Teile dieser Leistung durch Blockchain automatisiert werden. Für die erfolgreiche Etablierung einer Blockchain-Lösung ist dennoch viel Vertrauen notwendig: Die am Projekt beteiligten Partner müssen gewillt sein, zusammenzuarbeiten und sich gegenseitig wie auch der Technologie zu vertrauen. Für eine erfolgreiche Skalierung muss

zudem die Zielgruppe der Lösung den verwendeten Technologien und den Anbietern vertrauen. Misstrauen Patientinnen und Patienten beispielsweise einem Anbieter für elektronische Patientendossiers, werden sie ihre Gesundheitsdaten nicht teilen, auch wenn die Technologie noch so gut ist.

Nur wenn ausreichend viele aus der Zielgruppe das System nutzen, kann der parallele Betrieb mehrerer Lösungen vermieden und können die erwarteten Effizienzpotenziale tatsächlich gehoben werden. Der Marktauftritt und die Kommunikation spielen eine entscheidende Rolle für die Akzeptanz der Lösung. Die teilnehmenden Organisationen können beispielsweise ein Konsortium bilden und am Markt als neue Entität mit eigener Marke auftreten. Dadurch wird die eigentliche Identität der Anbieter verschleiert.

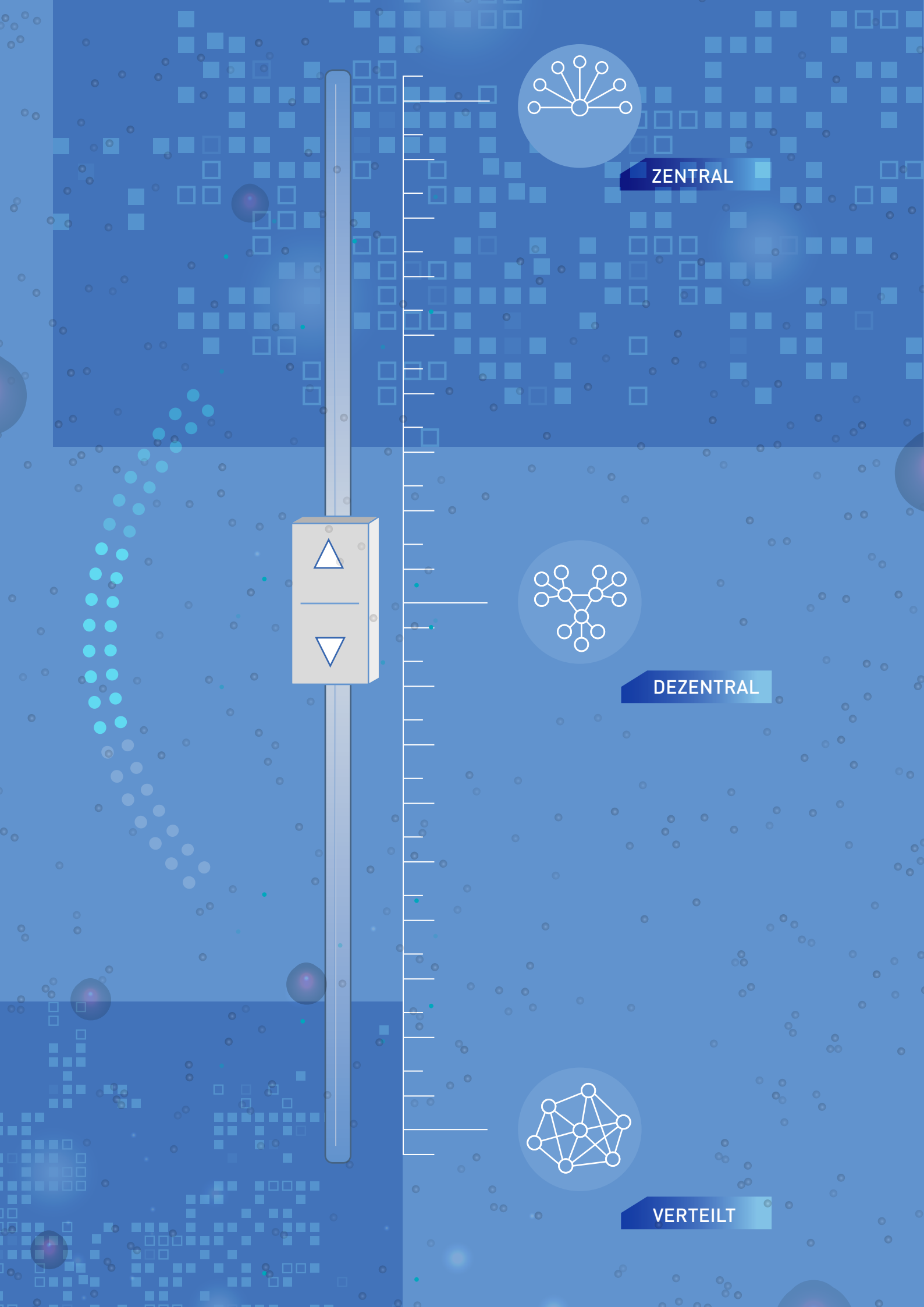
Um eine breite Akzeptanz der Lösung zu erlangen, sollten die konkreten Mehrwerte für die Nutzenden in den Vordergrund gestellt werden. Stellt man in der Kommunikation den Datenschutz oder die Manipulationssicherheit zu sehr in den Vordergrund, besteht die Gefahr, dass man Skepsis und Misstrauen erregt. Laut der Wirtschaftsinformatikerin Liudmila Zavolokina von der Universität Zürich muss eine vertrauenswürdige Blockchain «die erwartete Leistung erbringen und ihre Prozesse sowie ihr Zweck müssen nachvollziehbar sein».[123]

Regulierung und Compliance

Da Blockchains für den organisationsübergreifenden Austausch von – häufig personenbezogenen und sensiblen – Daten genutzt werden, muss zwingend sichergestellt sein, dass die Anforderungen des Datenschutzes eingehalten werden. Personenbezogene Daten müssen laut Schweizer Datenschutzgesetz immer löschbar sein, weswegen diese nie auf der Blockchain selbst, sondern nur in Offchain-Speichern hinterlegt werden dürfen.

Da viele Anwendungen länderübergreifend eingesetzt werden und sich die Datenschutzanforderungen von Land zu Land unterscheiden, stellt der Datenschutz eine grosse Herausforderung dar. Die Einhaltung der rechtlichen Vorgaben sollte so weit wie möglich auf technischer Ebene sichergestellt werden. Die Technik allein kann dies jedoch nie vollumfänglich leisten, weswegen zusätzliche Kontrollmechanismen, zum Beispiel Audits, notwendig sind. Beispielsweise ist es möglich, über Blockchain erhaltene Daten im eigenen System zu speichern und für andere unzulässige Zwecke zu nutzen. Ausserdem können weitere regulatorische Anforderungen bestehen, die berücksichtigt werden müssen. Zum Beispiel regeln die «Markets in Financial Instruments Directive» oder die Verordnung «Basel IV» besondere Anforderungen beim Umgang mit Finanzdaten.[124]

Weil viele rechtliche Aspekte des Einsatzes von Blockchain noch ungeklärt sind, muss eine konstruktive Zusammenarbeit mit Regulatoren geschaffen werden. Vor allem muss klar geregelt werden, wer in welcher Form bei Haftungsfällen zur Rechenschaft gezogen werden kann. Das sind Fragen, die in verteilten Organisationen ohne zentrale Instanz nicht einfach zu beantworten sind. Für die Schaffung von Vertrauen in Blockchain-Lösungen und ihre Anbieter ist ihre Klärung jedoch unabdingbar.[125]


ZENTRAL
DEZENTRAL
VERTEILT

Ist die Zukunft verteilt?

Verfügbarkeit, Integrität und Sicherheit der digitalen Infrastrukturen werden im Zuge der voranschreitenden Digitalisierung immer wichtiger für die Wirtschaft und unseren Alltag. Blockchain ermöglicht es, im Vergleich zu herkömmlichen Systemen eine robustere und effizientere digitale Infrastruktur zu schaffen. Auf technischer Ebene kann sichergestellt werden, dass Daten stets verfügbar und vor Manipulationen geschützt sind. Werte wie Geld, Gold, Patente oder Kunstgegenstände können mit Tokens digital abgebildet und gehandelt werden, und Prozesse werden mit sogenannten Smart Contracts automatisiert ausgeführt.

Dieses Potenzial kann nicht nur in der digitalen Welt ausgeschöpft werden, sondern auch in Wertschöpfungsnetzwerken für physische Produkte, die mit Blockchain effizienter und sicherer gesteuert werden können. Dabei müssen bewährte Strukturen, wie zentrale Dienstleister, nicht immer sofort radikal aufgelöst werden. In Unternehmensnetzwerken werden die meisten Blockchain-Anwendungen heute von einem zentralen Dienstleister gesteuert mit den Zielen, die Datenintegrität sicherzustellen und Kosten zu sparen.

Oft ist das Durchdenken einer Anwendung mithilfe von Blockchain-Technologie auch ein Treiber dafür, bestehende manuelle Prozesse zu standardisieren, zu digitalisieren und zu automatisieren. Sind Prozesse anhand von Blockchain manipulationssicher digitalisiert, können sich viele neue Anwendungen und Geschäftsfelder eröffnen. Beispielsweise ermöglicht Blockchain die Schaffung sicherer elektronischer Identitäten, mit denen Personen, Organisationen und Objekte eindeutig digital identifiziert werden können. Hierdurch kann nicht nur die Privatsphäre im Internet gestärkt werden, sondern auch eine Zugangsverwaltung zu Gebäuden und Räumen ohne physische Schlüssel, Peer-to-Peer-Marktplätze oder eine robuste Infrastruktur für das Internet der Dinge (IoT) geschaffen werden.

Die Eigenschaften von Blockchain bieten auch eine geeignete technologische Grundlage für einen Wandel zu verteilten Wertschöpfungsnetzwerken. In einem gemeinschaftlich betriebenen, sich selbst regulierenden Wertschöpfungsnetzwerk unterstützt Blockchain-Technologie alle Teilnehmenden, effizient und sicher zu interagieren und sich gegenseitig zu kontrollieren, ohne dass eine zentrale Bestimmungsinstanz notwendig ist.

Dieser Wandel ist sowohl ein technologischer als auch ein gesellschaftlicher Prozess, bei dem viele Interessenskonflikte überwunden werden müssen. Speziell bei bewährten Anwendungen kann es schwierig sein, existierende Strukturen aufzulösen. Ganz neue Anwendungen hingegen können gleich von Beginn an so geplant werden, dass möglichst wenig Abhängigkeiten entstehen.

Zentrale Herausforderungen in der Umsetzung von Blockchain-Projekten sind die Etablierung geeigneter Governance-Strukturen, die Beseitigung regulatorischer Unklarheiten, die Sicherstellung der Datenqualität und -sicherheit (auf Blockchains und in angrenzenden Systemen) und die Schaffung von Vertrauen und Akzeptanz in eine Blockchain-Lösung. Gelingt es, diese zu meistern, bietet Blockchain die Möglichkeit, digitale und physische Wertschöpfungsprozesse sicher und effizient zu gestalten und das Vertrauen in die digitale Infrastruktur zu erhöhen.

Blockchain wird kontinuierlich weiterentwickelt – und zwar technologisch, organisatorisch und regulatorisch. Über die langfristigen Auswirkungen lässt sich allerdings nur spekulieren. Eines ist jedoch sicher: Die Eigenschaften der Blockchain – Manipulationssicherheit, Verfügbarkeit, effizienter Datenaustausch, in Smart Contracts fixierbare Entscheidungsregeln oder der Wertehandel mit Tokens – bieten eine geeignete technische Grundlage für die Schaffung effizienter und robuster digitaler Infrastrukturen.

Danksagung

Wir danken allen Partnern für die Unterstützung und die gute Zusammenarbeit bei der Erstellung der Studie und Dr. Ralf Grötker für die methodische Begleitung, Karola Klatt für das Lektorat, Maja Kunze und Scribendi für das Korrektorat. Zusätzlich danken wir Anne van Berkel Meier, Dr. Roger Heines, Prof. Dr. Burkhard Stiller, Dr. Liudmila Zavolokina, Dr. Rafael Ziolkowski für Reviews und die Bereitstellung ihres Fachwissens. Ein besonderer Dank geht an Mathias Ruch und Dr. Pascal Ihle für die Integration unserer Studie in die Open-Ideation-Phase des NTN Innovation Boosters Blockchain Nation Switzerland (Innosuisse), André Kudelski für das Vorwort und Dr. Daniel Heller für die politische Unterstützung.

Anhang

Industriepartner

UNTERNEHMEN	KONTAKT
aXedras	Urs Röösli (CEO) Kathrin Wolff Schmandt (Senior Advisor)
Blockchain Nation Switzerland	Dr. Pascal Ihle (CEO)
Bundesamt für Energie	Dr. Matthias Galus (Head Digital Innovation Office)
EcosystemPartners	Dr. Daniel Fasnacht (CEO)
Generali (House of Insurtech Switzerland HITS)	Pietro Carnevale (CEO) Dr. Samyr Mezzour (CIO)
Green	Miki Mitric (Head of Business Development) Roger Süess (CEO)
Inacta	Daniel Rutishauser (Head DLT & Financial Services)
Kantonsspital Baden	Maximilian Grimm (Innovation Manager) Dr. Daniel Heller (Präsident des Verwaltungsrates)
Novartis	Marco Cuomo (Manager Applied Technology), Daniel Fritz (Domain Architect Supply Chain)
OVD Kinegram	Patrick Brouwer (Program Manager Digital Solutions) Orlando Hirt (Managing Director)
sminds/N9 House of Innovation	Sandro Schmid (CEO) Jacqueline Schleier (Member of the Executive Board)
Verband Schweizerischer Elektrizitätsunternehmen	Markus Riner (Head Digitalization & IT)

Tabelle 4.

Ausführliche Beschreibung kritischer Erfolgsfaktoren von Blockchain-Projekten

KATEGORIE	ERFOLGSFAKTOR	BESCHREIBUNG
Zweckmässigkeit und Wirtschaftlichkeit	Klares Wertversprechen	Der Nutzen, welcher mit dem Einsatz von Blockchain realisiert werden soll, muss für alle Stakeholder klar und interessant sein (zum Beispiel geringere Intermediärskosten, Unveränderbarkeit von Daten).
	Rentabilität	Der Nutzen, welcher durch dein Einsatz von Blockchain realisiert werden soll, muss die Investitions- und Betriebskosten, auch unter Berücksichtigung von Unsicherheiten und Projektrisiken, deutlich übersteigen («Business Case»).
	Gerechte Aufteilung von Kosten und Nutzen	Die durch die Lösung generierten Mehrwerte und Kosten müssen unter allen Stakeholdern gerecht aufgeteilt werden. Alle Stakeholder, welche für den Erfolg der Lösung von Bedeutung sind, müssen Anreize haben die Entwicklung und Nutzung zu unterstützen.
Governance	Effektive Information und Kommunikation	Alle Stakeholder müssen über geeignete Kanäle über für sie relevante Entwicklungen und Entscheidungen informiert werden und die Möglichkeit haben Vorschläge einzubringen und zu diskutieren.
	Effektive Entscheidungsmechanismen	Es muss ein Zusammenarbeitsmodell für alle Partner entwickelt werden («on-chain» und «off-chain») bei dem alle Partner entsprechend ihrer Rolle angemessen in Entscheidungsprozesse involviert sind.
	Standards und Interoperabilität	Für den organisationsübergreifenden Datenaustausch müssen Datenmodelle und Schnittstellen standardisiert werden.
Projektaufbau und -umsetzung	Gemeinsame Vision und angemessene Erwartungen	Alle für die erfolgreiche Umsetzung bedeutenden Stakeholder müssen eine gemeinsame Projektvision und realistische Erwartungen hinsichtlich Chancen, Risiken und der Projektdauer haben.
	Fachwissen und Fähigkeiten	Im Projekt müssen das notwendige technische und fachliche Wissen sowie die notwendigen Ressourcen (Zeit, Geld, Mitarbeiter) zur Realisierung der Lösung vorhanden sein.
	Inkrementeller und iterativer Ansatz	Die Umsetzung sollte schrittweise durchgeführt werden, da viel Gestaltungsspielraum besteht. Zwischenergebnisse sollten getestet, Feedback gesammelt und in der Entwicklung berücksichtigt werden. Erst nach einem erfolgreichen Piloten sollte die Lösung skaliert werden.
Vertrauen und Akzeptanz	Vertrauen unter Projektpartnern	Die am Projekt beteiligten Partner müssen gewillt sein zusammenzuarbeiten und sich grundlegend vertrauen.
	Vertrauen der Anbieter in die Technologie	Um die Lösung erfolgreich zu etablieren, müssen die am Projekt beteiligten Partner den für die Lösung verwendeten Technologien (zum Beispiel Kryptografie) vertrauen.
	Akzeptanz und Verbreitung der Lösung	Eine ausreichend grosse Menge an Akteuren muss das System, unabhängig von Landesgrenzen, nutzen, so dass der parallele Betrieb mehrerer Lösungen vermieden und erwartete Effizienzpotenziale tatsächlich gehoben werden. Dafür müssen die Nutzenden der Lösung der Technologie und den Anbietern vertrauen. Der Marktauftritt und die Kommunikation spielen eine entscheidende Rolle für die Akzeptanz der Lösung unter den Nutzenden.

KATEGORIE	ERFOLGSFAKTOR	BESCHREIBUNG
Regulierung und Compliance	Erfüllung der Datenschutz-anforderungen	Die Datenschutzanforderungen aller beteiligten Länder müssen erfüllt werden. Dies muss wenn möglich auf technischer Ebene, aber auch durch geeignete Kontrollmechanismen (zum Beispiel Audits), sichergestellt werden.
	Erfüllung weiterer regulatorischer Anforderungen	Weitere regulatorische Anforderungen aller beteiligten Länder müssen erfüllt werden, wie zum Beispiel besondere Anforderungen beim Umgang mit Finanzdaten («Markets in Financial Instruments Directive», Basel IV, etc.)
	Konstruktive Zusammenarbeit mit Regulierern	Da viele regulatorische Aspekte für den Einsatz von Blockchain noch ungeklärt sind muss eine konstruktive Zusammenarbeit mit Regulierern geschaffen werden.
Datenqualität und -sicherheit	Datensicherheit	Die Lösung muss sicherstellen, dass nur berechtigte Akteure Zugang zu Daten haben, die Daten immer dann verfügbar sind, wenn Zugriff auf sie benötigt wird (zum Beispiel durch die Abschaffung eines «Single-Point-of-Failure») und einmal gespeicherte Daten vollständig und unverändert sind. Dies betrifft die Inhalte von gespeicherten Transaktionsdaten und ggf. auch die Anonymität beteiligter Akteure.
	Datenqualität	Auf technischer und prozessualer Ebene muss sichergestellt werden, dass nur korrekte Daten auf die Blockchain geschrieben werden, und menschliche Fehler weitestgehend vermieden werden.
	Schutz vor Cyberangriffen und Missbrauch	Das System muss gleich oder weniger verletzbar durch Cyberangriffe sein als die Lösung vor dem Einsatz von Blockchain. Missbrauch von Daten muss soweit möglich technisch und durch Kontrollmechanismen ausgeschlossen werden.
Technische Umsetzung	Skalierbarkeit, Durchsatz und Geschwindigkeit	Die technische Architektur ermöglicht einer ausreichend grossen Anzahl an Akteuren Zugang zur Lösung, ausreichend Transaktionen gleichzeitig (Transaktionen pro Zeiteinheit), ausreichend schnell durchzuführen (Latenz).
	Automatisierung und Konsolidierung	Die technische Architektur ermöglicht einer ausreichend grossen Anzahl an Akteuren Zugang zur Lösung, ausreichend Transaktionen gleichzeitig (Transaktionen pro Zeiteinheit), ausreichend schnell durchzuführen (Latenz).
	Niedriger Stromverbrauch	Der Stromverbrauch der Lösung darf ein Mass nicht überschreiten, das nicht im Verhältnis zu dem durch die Lösung generierten Mehrwert steht.

Tabelle 5: Eigen Recherche.

Referenzen

[1] Brooker, K. (2018): "I was devastated": Tim Berners-Lee, the man who created the world wide web, has some regrets. Vanity Fair, 08/2018. https://www.vanityfair.com/news/2018/07/the-man-who-created-the-world-wide-web-has-some-regrets

[2] Kaat, C. (2022): Wo Schweizer Firmen auf dem Weg zum data-driven Business stehen. IT Markt. https://www.it-markt.ch/storys/2022-05-11/wo-schweizer-firmen-auf-dem-weg-zum-data-driven-business-stehen (abgerufen: 18.10.2022)

[3] Ryf, S.; Siegenthaler, P.; Fasnacht, D.; Fichter, C. (2022): NZZ-KMU-Barometer: Lieferkettenprobleme und Fachkräftemangel – die Zukunftsaussichten von Schweizer Unternehmen verdüstern sich. https://www.kalaidos-fh.ch/-/media/KFH2019/Dokumente/News/2022/Wirtschaft/Ergebnisbericht-NZZ-KMU-Barometer-2022.pdf (abgerufen 18.10.2022)

[4] Statcounter (o. D.): Search Engine Market Share Worldwide. https://gs.statcounter.com/search-engine-market-share (abgerufen: 18.10.2022); primäre Quelle nicht einsehbar. Zitiert nach: Statista (2022): Most popular global mobile messenger apps as of January 2022, based on number of monthly active users. https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/ (abgerufen: 18.10.2022)

[5] Watson (2019): Schweizweite Störung im elektronischen Zahlungsverkehr. https://www.watson.ch/schweiz/wirtschaft/425414560-bezahlung-mit-ec-karten-wegen-stoerung-schweizweit-ausgefallen (abgerufen: 18.10.2022); Thomi, S. (2022): Mitten im Samstagseinkauf: Störungen bei Twint, Postfinance und weiteren Banken. Luzerner Zeitung. https://www.luzernerzeitung.ch/news-service/wirtschaft/online-zahlungsmittel-mitten-im-samstagseinkauf-stoerung-bei-twint-app-postfinance-und-visa-ld.2300310 (abgerufen: 18.10.2022)

[6] Wingeier, C. (2022): Hackerangriff auf Schweizer Spitalverband. Inside IT. https://www.inside-it.ch/hackerangriff-auf-schweizer-spitalverband-20220621 (abgerufen: 21.10.2022)

[7] Baran, P. (1962): On Distributed Communications Networks. RAND Corporation, California, USA.

[8] Laudon, K.; Laudon, J. (2019): Management Information Systems: Managing the Digital Firm. 16th edition. Pearson.

[9] Rauchs, M.; Blandine, A.; Bear, K.; McKeon, S. (2019): 2nd global enterprise blockchain benchmarking study. University of Cambridge, Invesco.

[10] Hileman, G.; Rauchs, M. (2017): Global Blockchain Benchmarking Study. University of Cambridge, Visa, EY.

[11] Basiert auf: Ibit 9

[12] Schmitz, P. (2019): Was ist ein Token? Blockchain Insider. https://www.blockchain-insider.de/was-ist-ein-token-a-854928/ (abgerufen: 18.10.2022); Schiller, K. (2022): Was sind Security Token? – Die Vor- und Nachteile. https://blockchainwelt.de/security-token/ (abgerufen: 24.10.2022); Schiller, K. (2022): Was ist ein Utility Token? Beispiele und Erklärung. https://blockchainwelt.de/utility-token/ (abgerufen: 24.10.2022). Schiller, K. (2022): Equity Token und ETO: Was können sie wirklich? https://blockchainwelt.de/equity-token-eto/ (abgerufen: 24.10.2022).

[13] Lu, M. (2022): Blockchain Applications: Tokenization of Real Assets. Visual Capitalist. https://www.visualcapitalist.com/sp/blockchain-applications-tokenization-of-real-assets/ (abgerufen: 18.10.2022)

[14] Ibit 10

[15] Ibit 10

[16] CoinMarketCap (o. D.): Today's Cryptocurrency Prices by Market Cap. https://coinmarketcap.com/?page=95 (abgerufen: 18.10.2022)

[17] Martin, W. (2017): There's a 'fatal' flaw in cryptocurrencies which means they can never be real currencies. Insider. https://www.insider.com/bitcoin-cryptocurrency-ubs-wealth-management-economist-paul-donovan-2017-11 (abgerufen: 26.10.2022)

[18] Quelle nicht einsehbar. Zitiert nach: Dailey, N. (2022): NFTs ballooned to a $41 billion market in 2021 and are catching up to the total size of the global fine art market. https://markets.businessinsider.com/news/currencies/nft-market-41-billion-nearing-fine-art-market-size-2022-1 (abgerufen: 10.1.2023)

[19] Gerbl, E. (2021): Fälscher-Ikone Wolfgang Beltracchi malt jetzt digital. Bilanz. https://www.handelszeitung.ch/bilanz/falscher-ikone-wolfgang-beltracchi-malt-jetzt-digital (abgerufen: 18.10.2022)

[20] Barrera, C. (2019): A Framework for Blockchain Governance Design: The Prysm Group Wheel. Prysm Group on Medium. https://medium.com/prysmeconomics/a-framework-for-blockchain-governance-design-the-prysm-group-wheel-703279c1b0dd (abgerufen: 18.10.2022)

[21] Watson Law (o. D.): Blockchain governance: what is it, what types are there and how does it work in practice? https://watsonlaw.nl/blockchain-governance-what-is-it-what-types-are-there-and-how-does-it-work-in-practice/#:~:text=In%20the%20context%20of%20blockchain,into%20question%20contemporary%20authority%20structures (abgerufen: 18.10.2022)

[22] Ibit 10

[23] Decred Project (o. D.): Introduction to Decred Governance. https://docs.decred.org/governance/overview/ (abgerufen: 18.10.2022)

[24] Bocksch, R. (2022): Bitcoins Stromverbrauch übertrifft den der Ukraine. Statista. https://de.statista.com/infografik/18608/stromverbrauch-ausgewaehlter-laender-im-vergleich-mit-dem-des-bitcoins/ (abgerufen: 18.10.2022)

[25] Finews (2022): The Merge: Ethereum 2.0 ist geboren. https://www.finews.ch/news/finanzplatz/53360-the-merge-eth-ethereum-bitcoin-umstellung-proof-of-stake-vitalik-buterin (abgerufen: 18.10.2022)

[26] Heines, R. Gürpinar, T. (2021): Towards a typology of blockchain-based applications: a conceptualization from a business perspective. Konferenzband zum Scientific Track der Blockchain Autumn School 2021, Hochschule Mittweida. https://doi.org/10.48446/opus-13082

[27] Meunier, S. (2016): When do you need blockchain? Decision models. Medium. https://medium.com/@sbmeunier/when-do-you-need-blockchain-decision-models-a5c40e7c9ba1 (abgerufen: 18.10.2022)

[28] Schlatt, V.; Schweizer, A.; Urbach, N.; Fridgen, G. (2016): Blockchain: Grundlagen, Anwendungen und Potenziale. Fraunhofer-Instituts für Angewandte Informationstechnik FIT.

[29] Ibit 28

[30] Ibit 9

[31] Schweiger, L. (2021): 81 of the Top 100 Public Companies are using blockchain technology. Blockdata. https://www.blockdata.tech/blog/general/81-of-the-top-100-public-companies-are-using-blockchain-technology (abgerufen: 18.10.2022)

[32] Ibit 9

[33] CBInsights (2022): Banking is only the beginning: 65 big industries blockchain could transform. (abgerufen: 18.10.2022)

[34] Bijkerk, M. (2022): Blockchain Venture Funding per Country. Blockdata. https://www.blockdata.tech/blog/general/blockchain-venture-funding-per-country (abgerufen: 18.10.2022)

[35] Ibit 31

[36] Koopman, M. (2018): Blockchain in Switzerland: Opportunities for future cooperation between Switzerland and the Netherlands. Kingdom of the Netherlands.

[37] Finma (2018): Wegleitung für Unterstellungsanfragen betreffend Initial Coin Offerings (ICOs). https://www.finma.ch/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf?sc_lang=de

[38] Staatssekretariat für internationale Finanzfragen SIF (2022): Blockchain / DLT. https://www.sif.admin.ch/sif/de/home/finanzmarktpolitik/digit_finanzsektor/blockchain.html (abgerufen: 18.10.2022)

[39] CoinDesk & MIT (2022): Best Universities for Blockchain 2022. https://www.coindesk.com/layer2/2022/09/26/best-universities-for-blockchain-2022 (aufgerufen 18.10.2022)

[40] Blockdata (2021): Blockchain & Crypto in 2021 - A review in data. https://www.blockdata.tech/blog/general/blockchain-crypto-in-2021-data-review (abgerufen: 18.10.2022)

[41] Ibit 9

[42] Ibit 9

[43] CV VC (2023): Top 50 Report 2022. Erstellt in Zusammenareit mit Bank Frick.

[44] Ibit 43

[45] Edelman, G. (2021): The father of Web3 wants you to trust less. Wired. https://www.wired.com/story/web3-gavin-wood-interview/ (abgerufen: 18.10.2022)

[46] Uber Technologies (o. D.): Tracking your earnings. https://www.uber.com/us/en/drive/basics/tracking-your-earnings/#:~:text=Where%20can%20I%20see%20my,Earnings%20section%20of%20the%20app. (abgerufen: 18.10.2022)

[47] Eidgenössische Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK (2017): Verordnung des UVEK über den Herkunftsnachweis und die Stromkennzeichnung. 730.010.1.

[48] Schindele, M. (2019): Wie funktioniert eine Kreditkartenzahlung? Payment Technology Law. https://paytechlaw.com/kreditkartenzahlung/ (abgerufen: 18.10.2022)

[49] Finma (2021): Decentralized Finance (DeFi). Jahresbericht.

[50] Vantrappen, H.; Wirtz, F. (2017): When to decentralize decision making, and when not to. Harvard Business Review. https://hbr.org/2017/12/when-to-decentralize-decision-making-and-when-not-to (abgerufen: 18.10.2022)

[51] Ibit 50

[52] SRF News (2017): Nationalrat knöpft sich booking.com vor. https://www.srf.ch/news/schweiz/nationalrat-knoepft-sich-booking-com-vor (abgerufen: 18.10.2022); Kolbe, C. (2019: Uber hat seine Schweizer Fahrer um halbe Milliarde geprellt. Blick. https://www.blick.ch/wirtschaft/gewerkschaft-unia-klagt-an-uber-hat-seine-schweizer-fahrer-um-halbe-milliarde-geprellt-id15645475.html (abgerufen: 18.10.2022)

[53] Hacker, P. (2019): Corporate governance for complex cryptocurrencies? A framework for stability and decision making in blockchain-based organizations. In: Hacker, P.; Lianos, I.; Dimitropoulos, G.; Eich, S.: Regulating Blockchain: Techno-social and legal challenges. Oxford Academic.

[54] Graffeo, E. (2021): Bitcoin is still concentrated in a few hands, study finds. Time. https://time.com/6110392/bitcoin-ownership/

[55] Ibit 53

[56] Bitpush News (2021): Does the „Coinbase Effect" still exist, and what does it mean for the market. Bitpush Newson Medium. https://bitpushnews.medium.com/does-the-coinbase-effect-still-exist-and-what-does-it-mean-for-the-market-cc1a19c6fa1c

[57] Hyse, K. (2021): What is the coinbase effect? BSC news. https://www.bsc.news/post/cryptonomics-what-is-the-coinbase-effect (abgerufen: 18.10.2022, übersetzt aus dem Englischen).

[58] Ibit 21

[59] Laudon, K.; Laudon, J.; Schoder, D. (2015): Wirtschaftsinformatik. Pearson Studium.

[60] Doerk, A.; Hansen, P.; Jürgens, G.; Kaminski, M.; Kubach, M.; Terbu, O. (2020): Self Sovereign Identity Use Cases – von der Vision in die Praxis. Bitkom.

[61] Ibit 60

[62] Townsend, M. (2022): Facebook-Cambridge Analytica data breach lawsuit ends in 11th hour settlement. The Guardian. https://www.theguardian.com/technology/2022/aug/27/facebook-cambridge-analytica-data-breach-lawsuit-ends-in-11th-hour-settlement (abgerufen: 18.10.2022)

[63] Raaflaub, C. (2021): E-ID ist vom Tisch – Neustart folgt sogleich. Swissinfo. https://www.swissinfo.ch/ger/abstimmung-7_-maerz-2021-e-id/46414110 (abgerufen: 18.10.2022)

[64] Bundesamt für Justiz (2021): Diskussionspapier zum «Zielbild E-ID».

[65] Bundesamt für Justiz (o. D.): Öffentliche Konsultation zum «Zielbild E-ID». https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/staatliche-e-id/zielbild-e-id.html (abgerufen: 18.10.2022).

[66] Ibit 64

[67] Der Bundesrat (2022): E-ID: Bundesrat eröffnet Vernehmlassung. https://www.bj.admin.ch/bj/de/home/aktuell/mm.msg-id-89515.html (abgerufen: 18.10.2022)

[68] Schellinger, B.; Sedlmeir, J.; Willburger, L.; Strüker, J.; Urbach, N. (2022): Mythbusting Self-Sovereign Identity (SSI). Fraunhofer-Instituts für Angewandte Informationstechnik FIT.

[69] Ibit 64

[70] Ibit 64

[71] Ibit 64

[72] Ibit 64

[73] Ibit 64

[74] Mingot, S. (2022): Mit repräsentativen Use Cases das Potenzial von Self-Sovereign Identity ausloten. Adnovum. https://www.adnovum.com/de/blog/mit-repr%C3%A4sentativen-use-cases-das-potenzial-von-self-sovereign-identity-ausloten (abgerufen: 18.10.2022)

[75] Hotta, E. (o. D.): Self-sovereign identity use cases. Cheqd. https://cheqd.io/blog/self-sovereign-identity-use-cases (abgerufen: 18.10.2022)

[76] Digital Switzerland (2022): Building a Swiss Digital Trust Ecosystem: Perspectives around an e-ID ecosystem in Switzerland.

[77] IDunion (o. D.): IDunion. https://idunion.org/ (abgerufen: 18.10.2022)

[78] Ibit 76

[79] W3C (o. D.): W3C. https://www.w3.org/ (abgerufen: 18.10.2022)

[80] European Commission (o. D.): What is EBSI. https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/ESSIF+Functional+Scope (abgerufen: 18.10.2022)

[81] BOTLabs (o. D.): KILT. https://www.kilt.io/ (abgerufen: 18.10.2022)

[82] Loskamp, H. (2022): Mythen und Fakten. Ist Self-Sovereign Identity gefährlich? Logbook. https://jolocom.io/blog/mythen-und-fakten-ist-self-sovereign-identity-gefahrlich/ (abgerufen: 18.10.2022)

[83] Dewey, C. (2014): Yes, the Facebook Messenger app requests creepy, invasive permissions. But so does every other app. Washington Post. https://www.washingtonpost.com/news/the-intersect/wp/2014/08/04/yes-the-facebook-messenger-app-requests-creepy-invasive-permissions-but-so-does-every-other-app/ (abgerufen: 18.10.2022); Lovejoy, B. (2021): App privacy labels show stark contrasts among messaging apps. 9to5Mac. https://9to5mac.com/2021/01/04/app-privacy-labels-messaging-apps/ (abgerufen: 18.10.2022)

[84] Ibit 68

[85] Ibit 60

[86] Strüker, J.; Urbach, N.; Guggenberger, T. et al. (2021): Self-Sovereign Identity – foundations, applications, and potentials of portable digital identities. Fraunhofer-Instituts für Angewandte Informationstechnik FIT; Schellinger, B.; Sedlmeir, J.; Willburger, L.; Strüker, J.; Urbach, N. (2022): Mythbusting Self-Sovereign Identity (SSI). Fraunhofer-Institut für Angewandte Informationstechnik FIT.

[87] E-Estonia (o. D.): We have built a digital society and we can show you how. https://e-estonia.com/ (abgerufen: 18.10.2022)

[88] République et canton du Jura (o. D.): Quel était le cas d'usage pour le pilote? https://faq.jura.ch/space/CN/635175035/Quel+%C3%A9tait+le+cas+d'usage+pour+le+pilote+%3F (abgerufen: 18.10.2022)

[89] Primäre Quelle nicht einsehbar. Zitiert nach: Rabe, L. (2022): Aus welchen Gründen nutzen Sie keine sozialen Netzwerke mehr? Statista. https://de.statista.com/statistik/daten/studie/1283718/umfrage/gruende-fuer-abkehr-von-social-media-plattformen-in-deutschland/ (abgerufen: 23.10.2022)

[90] Brandt, M. (2022): Amazon und Meta führen die DSGVO-Top 10 an. Statista. https://de.statista.com/infografik/25449/fuer-verstoesse-gegen-datenschutzgesetze-verhaengte-geldbussen/ (abgerufen: 23.10.2022)

[91] Bundesversammlung der Schweizerischen Eidgenossenschaft (2013): Bundesgesetz über das elektronische Patientendossier. 816.1.

[92] Bundesversammlung der Schweizerischen Eidgenossenschaft (1992): Bundesgesetz über den Datenschutz. 235.1.

[93] Bundesamt für Gesundheit BAG (o. D.): Verbreitung und Nutzung des EPD. https://www.bag.admin.ch/bag/de/home/strategie-und-politik/nationale-gesundheitsstrategien/strategie-ehealth-schweiz/umsetzung-vollzug/verbreitung-nutzung-epd.html (abgerufen: 18.10.2022)

[94] Davis, J. (2021): Dark web analysis: healthcare risks tied to database leaks, credentials. Health IT Security. https://healthitsecurity.com/news/dark-web-analysis-healthcare-risks-tied-to-database-leaks-credentials (abgerufen: 18.10.2022)

[95] EPD (o. D.): Was ist eine Stammgemeinschaft? https://www.patientendossier.ch/eroeffnung/was-ist-eine-stammgemeinschaft (abgerufen: 18.10.2022); Konferenz der kantonalen Gesundheitsdirektorinnen und -direktoren (2019): Wer kann auf das EPD zugreifen? Gesundheitsfachpersonen nach EPDG. Factsheet.

[96] Bundesamt für Gesundheit BAG (2022): Zertifizierte (Stamm-)Gemeinschaften. https://www.bag.admin.ch/bag/de/home/strategie-und-politik/nationale-gesundheitsstrategien/strategie-ehealth-schweiz/umsetzung-vollzug/zertifizierte_stammgemeinschaften.html (abgerufen: 4.1.2023); Konferenz der kantonalen Gesundheitsdirektorinnen und -direktoren (2022): Elektronisches Patientendossier: Die Einführungsphase läuft. Factsheet.

[97] Boydak (2021): Automation in der Krankenversicherungsbranche. https://boydak.ch/de/automation-in-der-krankenversicherungsbranche/ (abgerufen: 18.10.2022)

[98] Bundesamt für Gesundheit BAG (o. D.): Prävention in der Gesundheitsversorgung. https://www.bag.admin.ch/bag/de/home/strategie-und-politik/nationale-gesundheitsstrategien/strategie-nicht-uebertragbare-krankheiten/praevention-in-der-gesundheitsversorgung.html (abgerufen: 18.10.2022); WBF/EDI (o. D.): Gesamtsicht Aus- und Weiterbildung Medizin im System der Gesundheitsversorgung.

[99] Gfs Bern (2021): Swiss eHealth Baromter 2021.

[100] Basierend auf den Workshops mit den Industriepartnern und diversen Studien: Azari, A.; Ekblaw, A.; Vieira, T.; Lippman, A. (2016): MedRec: Using Blockchain for Medical Data Access and Permission Management. 2016 2nd International Conference on Open and Big Data (OBD). https://doi.org/10.1109/OBD.2016.11; Shreshta, A.; Vassileva, J.; Deters, R. (2020): A Blockchain Platform for user data sharing ensuring user control and incentives. Frontiers in Blockchain, 3:497985, https://doi.org/10.3389/fbloc.2020.497985. Mamo, N.; Martin, G.; Desira, M.; Ellul, B.; Ebeje, J.-P. (2020): Dwarna: a blockchain solution for dynamic consent in biobanking. European Journal of Hu- man Genetics, 28, 609-626. https://doi.org/10.1038/s41431-019- 0560-9

[101] Shreshta, A.; Vassileva, J.; Deters, R. (2020): A Blockchain Platform for user data sharing ensuring user control and incentives. Frontiers in Blockchain, 3:497985, https://doi.org/10.3389/fbloc.2020.497985

[102] Mamo, N.; Martin, G.; Desira, M; Ellul, B.; Ebeje, J.-P. (2019): Dwarna: a blockchain solution for dynamic consent in biobanking. Eu- ropean Journal of Human Genetics, 28. https://doi.org/10.1038/s41431-019-0560-9

[103] Helsana (o. D.): Helsana+ App. https://www.helsana.ch/de/private/services/apps/helsana-plus.html?

[104] Schechner, S.; Secada, M. (2019): You give apps sensitive personal information. Then they tell facebook. Wall Street Journal. https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636?mod=e2tw (abgerufen: 18.10.2022)

[105] Cox, J. (2022): Data broker is selling location data of people who visit abortion clinics. Vice. https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood (abgerufen: 18.10.2022)

[106] Rocher, L.; Hendrickx, J.; de Montjoye, Y. (2019): Estimating the success of re-identifications in incomplete datasets using generative models. Nat Commun 10, 3069. https://doi.org/10.1038/s41467-019-10933-3

[107] Hepp, T.; Sharinghousen, M.; Ehret, P.; Schoenhals, A. B. (2018): On-chain vs. off-chain storage for supply- and blockchain integration. it - Information Technology, 60(5-6). https://doi.org/10.1515/itit-2018-0019

[108] Evashwick, C. (1989): Creating the continuum of care. Health Matrix, 7(1):30-9. https://pubmed.ncbi.nlm.nih.gov/10293297/

[109] Batt, J.; Da Forno, M.; Pfarrer, R. (2017): Rückverfolgbarkeit in der Lieferkette: Grundlagen und Prozesse. GS1 Switzerland.

[110] GS1 Switzerland (o. D.): Arzneimittel. https://www.gs1.ch/home/branchen/gesundheitswesen/arzneimittel (abgerufen: 18.10.2022)

[111] Bayard Consulting (o. D.): Was ist das GDSN?; ECR (o. D.): GS1 Global Data Synchronization Network (GDSN). https://www.ecr.digital/book/gs1-standards/gs1-global-data-synchronisation-network-gdsn/ (abgerufen: 18.10.2022)

[112] IBM; KPMG; Merck; Walmart (2020): FDA DSCSA: Blockchain Interoperability Pilot Project Report.

[113] Ibit 112

[114] Bischoff, O.; Seuring, S. (2021): Opportunities and limitations of public blockchain-based supply chain traceability. Modern Supply Chain Research and Applications, 3(3). https://doi.org/10.1108/MSCRA-07-2021-0014

[115] Ibit 107

[116] Modum (2021): Roambee Acquires Modum's Condition Monitoring Division. https://www.modum.io/news/roambee-acquires-modum?hsLang=en (abgerufen: 23.10.2022)

[117] Ibit 112

[118] Ibit 112

[119] Ibit 114

[120] Ibit 114

[121] Ibit 9

[122] Aggarwal, S.; Kumar, N. (2021): Chapter twenty - Attacks on blockchain. Advances in Computers, 121. https://doi.org/10.1016/bs.adcom.2020.08.020

[123] Saraga, D. (2022): Verteiltes Vertrauen. Universität Zürich. https://www.news.uzh.ch/de/articles/2022/Blockchain-Zavolokina.html (abgerufen: 18.10.2022)

[124] Krecké, E. (2019): 'Basel IV' and the stability of the financial industry. Geopolitical Intelligence Services. https://www.gisreportsonline.com/r/basel-iv/ (abgerufen: 18.10.2022)

[125] Ibit 123

Herausgeber
GDI Gottlieb Duttweiler Institute
Langhaldenstrasse 21
CH-8803 Rüschlikon
www.gdi.ch