

Bausteine für eine digitale Souveränität Europas

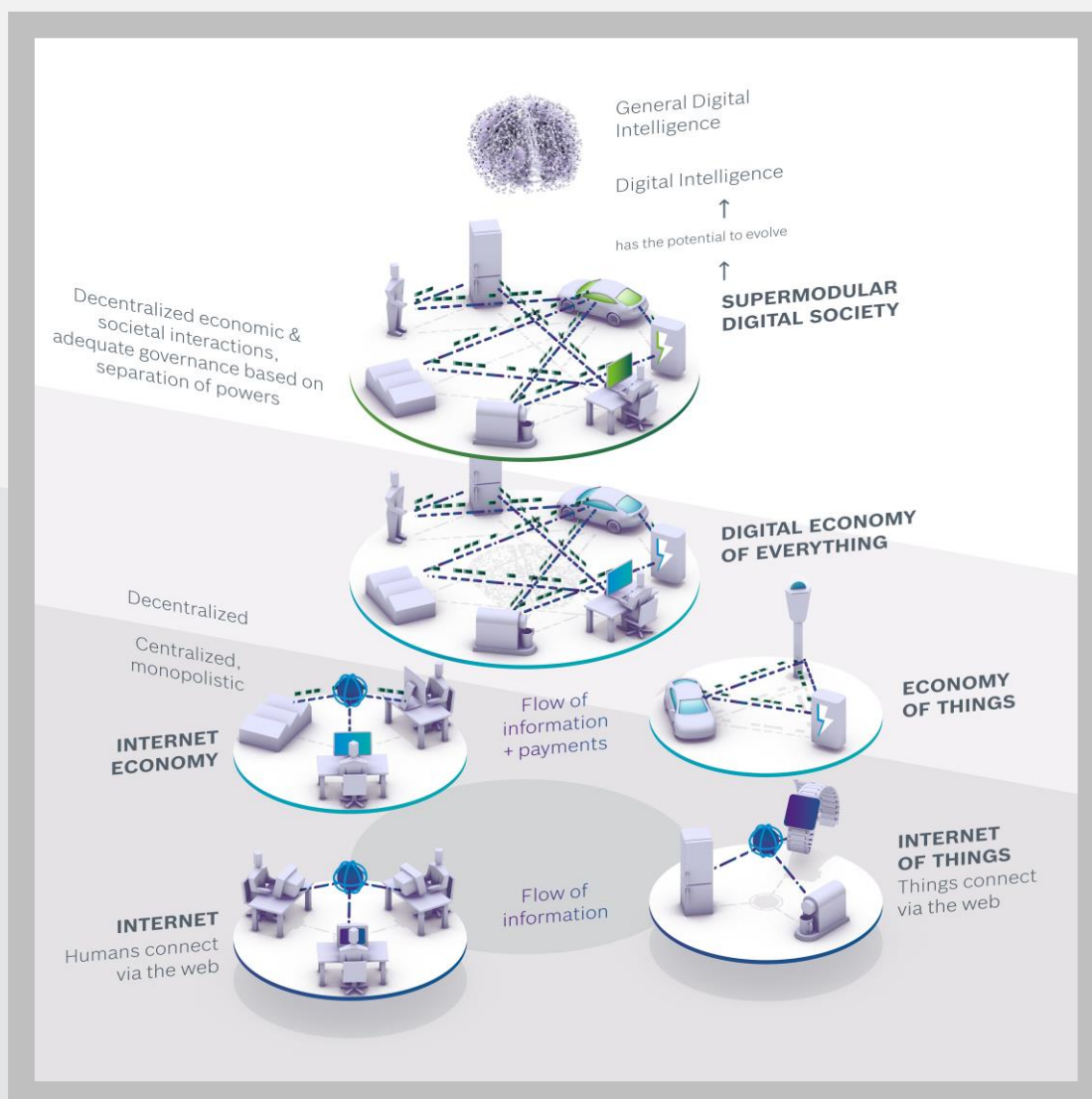
Wertekonforme, sichere und effiziente Bausteine für die Ökonomie der Zukunft:

Europas Stärken nutzen auf dem Weg in eine faire digitale Sozioökonomie.



BOSCH

Technik fürs Leben



INHALT

1	EINLEITUNG	3
1.1	ALLGEMEINE AUSGANGSSITUATION	3
1.2	EINORDNUNG DER BAUSTEINE FÜR EINE DIGITALE SOZIOÖKONOMIE	5
2	BESCHREIBUNG DER BAUSTEINE EINER DIGITALEN SOZIOÖKONOMIE	6
2.1	BAUSTEIN 1: FAIRE, MANIPULATIONSSICHERE B2B-MARKTPLÄTZE	6
2.1.1	<i>Ausgangssituation</i>	6
2.1.2	<i>Lösungsansatz: Dezentrale, offene Marktplatzlösung am Beispiel Fertigungsmarktplatz</i>	7
2.1.3	<i>Anforderungen für die Umsetzung</i>	9
2.2	BAUSTEIN 2: REGULIERUNGSKONFORME, SICHERE UND EFFIZIENTE BEZAHLSYSTEME	10
2.2.1	<i>Ausgangssituation</i>	10
2.2.2	<i>Lösungsansatz: crypto & Banken Hybrid</i>	11
2.2.3	<i>Konkreter Usecase: hybrides Brokermodell</i>	14
2.3	BAUSTEIN 3: SICHERE, DIGITALE IDENTITÄTEN	18
2.3.1	<i>Ausgangssituation</i>	18
2.3.2	<i>Lösungsansatz: Self-sovereign Identities</i>	18
2.3.3	<i>Initiativen und Förderprogramme</i>	19
2.4	BAUSTEIN 4: ORGANISATIONSSTRUKTUREN UND ANREIZSYSTEME FÜR DIGITALE ÖKOSYSTEME	19
2.4.1	<i>Ausgangssituation</i>	19
2.4.2	<i>Lösungsansatz: Digitalisierung der Ökosystem-Governance und Anreizmechanismen</i>	20
3	ZUSAMMENFASSUNG	21
4	AUTOREN	22
5	BIBLIOGRAFIE	23

1 EINLEITUNG

Dieses Dokument beschreibt Bausteine und Lösungskonzepte für eine digitale Souveränität Europas. Hierbei wird der Status-quo der Digitalisierung im Kontext der europäischen Wirtschaft erfasst und die Probleme durch zunehmende Monopolisierung von digitalen Plattformanbietern und einhergehende Informations- und Machtassymetrien aufgezeigt. Es werden Lösungskonzepte vorgestellt, welche die europäischen Werte widerspiegeln und die auf Basis innovativer technologischer und organisatorischer Bausteine eine effiziente digitale Sozioökonomie schaffen, die nicht mehr von digitalen Machtmonopolen bestimmt wird.

1.1 ALLGEMEINE AUSGANGSSITUATION

Die europäische und globale Sozioökonomie befindet sich in einem starken Wandel hin zu einer digitalen Sozioökonomie (s. auch unsere Einführung in [1]), der im Wesentlichen durch zwei Hauptströmungen gekennzeichnet werden kann.

Zum einen hat die Internet-Technologie und die voranschreitende Digitalisierung Prozesse großer Transformation eingeleitet. Diese haben die Kernbereiche der europäischen Wirtschaft und Gesellschaft zunächst nicht direkt betroffen. Das Ergebnis der ersten Phasen dieser Transformation, die digitale Informationsvernetzung und die Etablierung darauf aufbauender Geschäftsmodelle, werden heute im allgemeinen Sprachgebrauch als Entstehung des Web 2.0 bezeichnet. Web 2.0 ist, vereinfacht gesagt, dadurch gekennzeichnet, dass die Erbringung der Funktionalität grundlegend zentralisiert erfolgt, wobei die Beiträge (z.B. von Nutzerdaten), welche zur Erzeugung des Mehrwertes benötigt werden, durch eine große Zahl an Nutzern erfolgen. Diese meist freiwillig erbrachten Beiträge werden durch kostenlose Services motiviert, wobei der eigentliche Wert und die Verwendung der Beiträge für den Nutzer intransparent gehalten und nicht zugänglich gemacht werden. Zur Illustration seien hier beispielhaft soziale Medien und Internetsuche genannt, wobei der augenscheinliche Vorteil der kostenlosen Vernetzung und Suche dazu verwendet wird, eine große Zahl an Beiträgen der Nutzer zum Training von Verfahren des maschinellen Lernens zu verwenden, und damit die Möglichkeiten rund um die Themen künstliche Intelligenz voranzutreiben. So hat der Nutzer im Web 2.0 zwar einen mehr oder weniger direkten Einfluss auf die Inhalte (z.B. Beiträge in den sozialen Medien). Die eigentliche Hauptfunktionalität und der auf Grund von Netzwerkeffekten rapide wachsende Mehrwert sowie die damit verbundene Vormachtstellung entsteht jedoch in den Händen zentraler Intermediäre [2] [3], welches de facto einzelne privatwirtschaftliche Technologieunternehmen sind, die sich zu wahren Technologiegiganten (sog. *Hypercaler*) entwickelt haben.

Aus dieser Vormachtstellung heraus versuchen die Web-2.0-Giganten nun Stück für Stück in die Kernbereiche der (europäischen) Sozioökonomie einzudringen, indem die Erfahrungen und Praktiken aus dem Endnutzergeschäft (sog. business to customer, B2C) u.a. in den B2B-Bereich übertragen werden, z.B. in den Themenfeldern Marktplätze und Bezahlssysteme. Siehe hierzu auch die detaillierte Diskussion in den folgenden Kapiteln.

Neben den privatwirtschaftlichen Konzernen erarbeiten sich zunehmend auch halbstaatliche bzw. durch die aufstrebende Wirtschaftsmacht China protegierte Unternehmen große Anteile am Weltmarkt, wobei hierbei die wirtschaftlich-strategische Macht genutzt wird, ebenfalls in die zentralen sozioökonomischen Bereiche Europas vorzudringen.

Die zweite Hauptströmung ergibt sich dadurch, dass, basierend auf den Erkenntnissen über die Nachteile einer auf diese Art zentral-intermediär dominierten Wirtschaft und dem zunehmenden Vertrauensverlust in diese Intermediäre – zusätzlich befeuert durch die Finanzkrise – ein gesellschaftliches Verlangen entstanden ist, diese Nachteile zu überwinden [4] [5] [6]. Fortschritte im Bereich der Verbindung von Kryptotechnologie

mit Peer-to-Peer- (Teilnehmer zu Teilnehmer) Ansätzen erlaubten die informationstheoretisch sichere Zusammenarbeit und Werteverwaltung zwischen Teilnehmern eines Systems, wobei kein gegenseitiges Vertrauen vorausgesetzt wird (sog. *trustless* Ansätze), ohne dabei auf einen zentralen Intermediär angewiesen zu sein. Beispielhaft sei hier die wohl zentralste Arbeit von Nakamoto [7] und die Entstehung von Bitcoin genannt. Basierend auf der sog. *Distributed Ledger Technologie* (DLT) und Multi-Party Computation (MPC), hat sich ein weites wissenschaftlich, wirtschaftlich und gesellschaftlich relevantes Feld ergeben, das sich, ausgehend von sicheren, dezentral organisierten digitalisierten Wertdarstellungen über programmgesteuerte Ausführung von Werttransfer und (Geschäfts)vorgängen (z.B. via sog. *smart contracts*) bis hin zu der Frage gleichberechtigter sozialer Koordination (sog. *Governance*) und Teilhabe an den entstehenden Systemen und den damit verbundenen Wertzuwächsen erstreckt. Und all dies ohne die Unterstützung und Erlaubnis zentraler Intermediäre, bei denen die Gefahr des Machtmissbrauchs in Form von Zulassungsbeschränkung, Zensur sowie überproportionalem Wertentzug aus dem System gegeben ist [8].

Durch die Verknüpfung der wissenschaftlichen Gebiete Spieltheorie, Mechanismus-Design und Kryptographie ist auf diese Art die Möglichkeit zur Entwicklung einer sicheren und effizienten digitalen Sozioökonomie entstanden. Die Bewegung wird u.a. als *democratized Web*, *Web 3.0* oder *crypto-movement* bezeichnet.

Ausgehend von den Arbeiten Polanyis (zuerst publiziert 1944 und in der Ausgabe von 2001 mit einem Vorwort von Stiglitz [9]), dessen Theorien u.a. durch die Nobelpreisträger¹ Stiglitz, Akerloff und Spence auf die modernen ökonomischen Märkte übertragen und untermauert wurden [10] [11] [12] [13], gibt es in der Wirtschafts- und Sozialtheorie eine breite Akzeptanz der Erkenntnis, dass unregulierte Systeme / Märkte im Allgemeinen versagen. Anders gesagt, Systeme ohne Regeln und gestaltende Eingriffe kommen nicht auf magische (Stichwort *invisible hand*) Weise zu einem effizienten Zustand. Erst durch geeignetes Setzen von Regeln, basierend auf Grundwerten, kann die angestrebte Effizienz erreicht werden².

Vor diesem Hintergrund verwundert es nicht, dass auch im Bereich des jungen *crypto-movement* teilweise unvorteilhafte Auswüchse wie beispielsweise die Abwicklung verbrecherischer Machenschaften in kryptographisch geschützten Bereichen (landläufig als *DarkWeb* bezeichnet) sowie exzessive Finanzspekulationen bis hin zu kriminellen Finanzmanipulationen (sog. *Pump & Dump*, *Exit scams*,...) auftreten.

Zugleich bieten aber gerade die Ansätze des *crypto-movement* wirksame Maßnahmen, die den digitalen Technologien grundsätzlich innewohnenden Gefahren der Machtkonzentration, Überwachung und Unterdrückung entgegenzuwirken, wenn sie geeignet wertebasiert angewendet werden. Auf diese Weise ist die Chance gegeben, eine auf europäischen Werten basierende digitale Sozioökonomie so zu gestalten, dass sie auf Grund der freigesetzten Effizienz, der Bedrohung dieser Werte und dem nachteiligen Eindringen destruktiver Akteure in die Kernbereiche der europäischen Gesellschaft und Wirtschaft entgegenwirken kann (an dieser Stelle sei nochmals auf [1] verwiesen).

Diese Werte sind

- **Offenheit:** Ökosysteme, die durch die Anwendung der Bausteine entstehen, stehen dauerhaft allen Teilnehmern offen, die sich an die für alle geltenden Grundsätze halten.
- **Neutralität:** Kein einzelner Teilnehmer eines Ökosystems soll den Markt dominieren können.
- **Transparenz:** Organisationsstrukturen, Regulatorien und Entscheidungswege sind für die Ökosystemteilnehmer transparent und nachvollziehbar.

¹ Nobelpreis der Wirtschaftswissenschaften 2001

² vgl. [1]. für eine ausführlichere Darstellung der Zusammenhänge.

- **Souveränität:** Bewahrung der Hoheit über Beiträge und deren Verwendung für den Beitragenden, sowie diskriminierungsfreier und rechtlich zulässiger Zugang dazu für alle Marktteilnehmer (z.B. Daten, trainierte Modelle, usw.)
- **Integrität:** Angemessene Identifikation der Akteure, Authentizität der ausgetauschten Informationen bei gleichzeitiger Wahrung von Vertraulichkeit.

1.2 EINORDNUNG DER BAUSTEINE FÜR EINE DIGITALE SOZIOÖKONOMIE

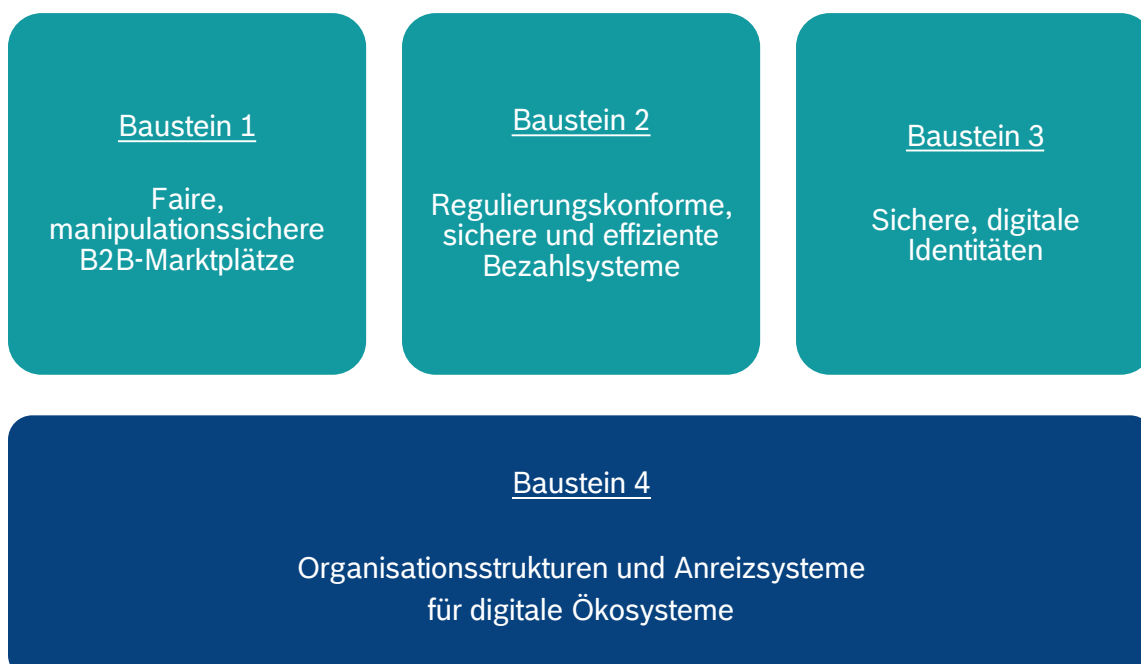


Abbildung 1 Übersicht über die Bausteine für eine digitale Sozioökonomie

Wesentliche Bausteine einer digitalen Sozioökonomie, gerade auch der vierteiligen Wertschöpfungskette, welche unsere Industrie kennzeichnet, bilden die geeignete Organisation von Marktplätzen als Handelsraum für digitale und physische Güter (Baustein 1), die digitalisierte Wertdarstellung und programmgesteuerte Ausführung von Werttransfer und (Geschäfts)vorgängen auf eine dem regulativen Rahmen entsprechenden Art und Weise (Baustein 2) und entsprechende Organisationsstrukturen und Anreizsysteme die Kooperationsmodelle und Regelwerke für digitale Ökosystemen beschreiben (Baustein 4). Darüber hinaus ist die Frage der digitalen Identitätsverwaltung (Baustein 3) von zentraler Bedeutung: Marktplätze und regulierungskonforme Bezahlungssysteme bedürfen sicherer, digitaler Identitätsverwaltungssysteme, damit Marktakteure auch ohne einen zentralen Mittelsmann sicher agieren können.

Zwischen den Bausteinen bestehen Wechselwirkungen, sodass sich insgesamt ein gut zusammenwirkendes Gesamtkonzept ergeben kann. Diese Wechselwirkungen der Bausteine muss vor dem Hintergrund der bereits oben erwähnten Prinzipien (Offenheit, Neutralität, Transparenz, Souveränität, Integrität) erfolgen.

2 BESCHREIBUNG DER BAUSTEINE EINER DIGITALEN SOZIOÖKONOMIE

2.1 BAUSTEIN 1: FAIRE, MANIPULATIONSSICHERE B2B-MARKTPLÄTZE

2.1.1 AUSGANGSSITUATION

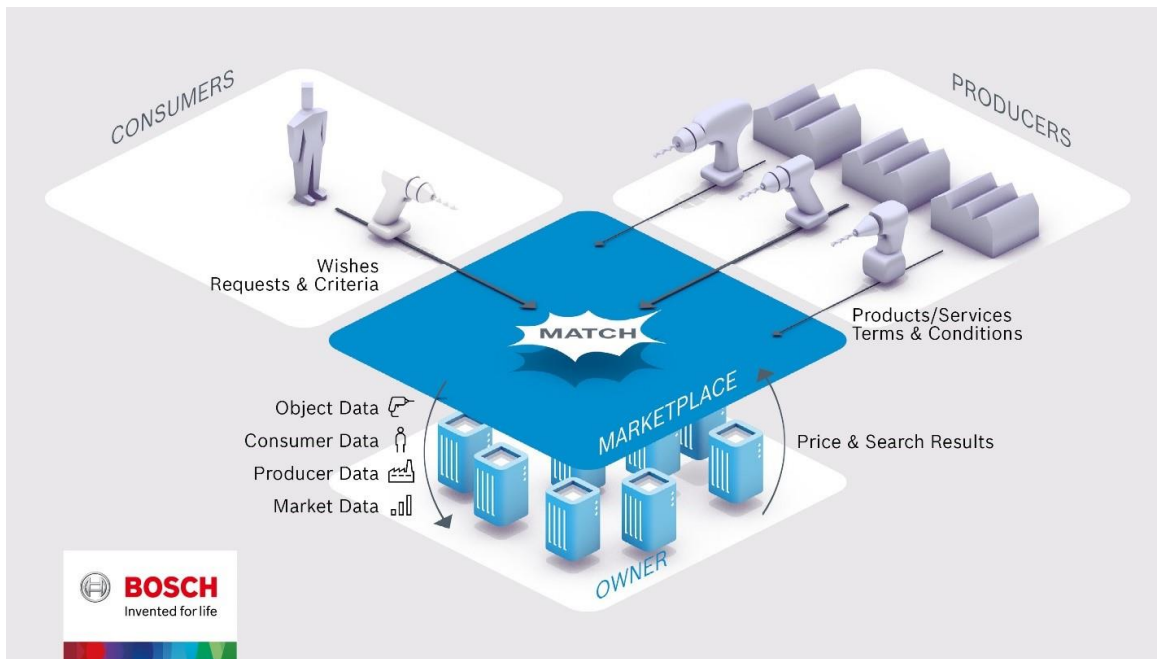


Abbildung 2 Schematische Darstellung wie Angebot und Nachfrage auf einem B2B-Marktplatz zusammengeführt werden

Im digitalen Zeitalter haben wir uns an den Erfolg von Plattformen und digitalen Marktplätzen gewöhnt. Als sogenannter Matchmaker stellen sie einen virtuellen Raum zur Verfügung, über den Konsumenten und Produzenten zusammengebracht werden. Wie bereits erwähnt ist aufgrund von Netzwerk- und Lock-In-Effekten eine Tendenz zur Monopolbildung zu erkennen, die einerseits in hohen Margen, rapidem Wachstum und einer hohen Marktkapitalisierung der Plattformbetreiber resultiert. Andererseits führen diese dominante Marktstellung und Machtkonzentration auf den Plattformbetreiber zu erheblichen Nachteilen für die Plattformnutzer, die sich transparent machen und Abhängigkeiten in Kauf nehmen.

Bisher sind diese Entwicklungen vor allem im B2C-Bereich erkennbar. Zunehmend wird jedoch auch der B2B-Bereich agitiert. Start-ups, die Plattformen zur Vermittlung von Fertigungsaufträgen bereitstellen, werden mit großem Kapitalinvestment ausgestattet. Auch sog. Hyperscaler, die im B2C-Bereich bereits erfolgreich sind, versuchen sich im lukrativen Segment der B2B-Marktplätze zu positionieren. Sie basieren auf zentralisierten Strukturen, bei denen die Governance und der Betrieb der Plattform in der Hand einer Entität konsolidiert ist. Ihre Geschäftsmodelle basieren auf Transaktionsdaten und sensiblen Kundendaten der Nutzer. Mit ihrem Wissen über die Marktsituation und den daraus resultierenden Informationsasymmetrien haben die Plattformbetreiber einen erheblichen Wettbewerbsvorteil: Basierend auf Daten des Marktplatzes können sie besonders interessante Güter identifizieren, selbst produzieren, zu attraktiven Preisen auf ihrem Handelsplatz anbieten und sich somit zwischen Kunden und Anbieter drängen. Als Betreiber können sie Suchanfragen manipulieren und ihre Produkte an die Spitze der Ergebnisliste setzen. Auch eine individuelle Preisgestaltung, bei denen unterschiedliche Preise für verschiedene Kundengruppen aufgerufen werden, ist möglich. Zusammengefasst: Plattformbetreiber profitieren überproportional von der Plattforminteraktion der Nutzer.

In produzierenden Unternehmen führt dieses ökonomische Ungleichgewicht in Verbindung mit den Winner-takes-it-all-Dynamiken der Plattformökonomie zu Hemmnissen der Plattformnutzung. Am Beispiel eines dezentralen Fertigungsmarktplatzes soll ein Ansatz verdeutlicht werden, durch den traditionelle Unternehmen ihre hohe Produktions- mit einer neuen Plattformkompetenz verbinden können. Der Ansatz beruht auf der Nutzung dezentraler Technologien sowie der Kooperation zwischen den Marktteilnehmern und soll eine faire, neutrale und offene digitale Wirtschaft ermöglichen. Die Abhängigkeit von einzelnen, dominanten Akteuren soll vermieden und die Position des Produktionsstandortes Europa gestärkt werden.

2.1.2 LÖSUNGSANSATZ: DEZENTRALE, OFFENE MARKTPLATZLÖSUNG AM BEISPIEL FERTIGUNGSMARKTPLATZ

In der Vision der Industrie 4.0 sollen Fertigungskapazitäten flexibel angeboten und angefragt werden können. Das heißt:

- a.) Fertigungsanfragen können digitalisiert eingestellt und vermittelt werden.
- b.) Produzenten und Lieferanten wollen nicht-genutzte Kapazitäten kurzfristig zur Verfügung stellen und beziehen können.

Produzenten erhoffen sich dadurch eine gesteigerte Flexibilität in der Produktion und eine höhere Effizienz ihrer Maschinenauslastung. Auch soll der Marktzugang zu neuen Kunden erleichtert werden. Auf der anderen Seite wollen Kunden aus dem Industrieumfeld diese freien Kapazitäten "on-demand" nutzen, um Teile oder komplette Produkte fertigen zu lassen. Neben einer flexiblen Reaktion auf Markt- und Kundenanforderungen soll somit die Flexibilisierung der Produktion in Richtung Losgröße 1 ermöglicht und gleichzeitig die Kapitalbindung reduziert werden.

Um diese Potenziale nutzen und effizient gestalten zu können, muss die Auftragsanbahnung und Abwicklung möglichst automatisiert und nahtlos ermöglicht werden. Heutzutage ist die Suche nach passenden Produzenten mit hohem zeitlichen Aufwand verbunden. Zudem ist die Automatisierung dieses Prozesses ein großes, noch ungelöstes Problem. Gegenwärtige Marktplatzlösungen, die sich diesem annehmen, basieren zumeist auf zentralisierten Strukturen und bürden die oben beschriebenen Hemmnisse. Ein unternehmens- und fertigungsübergreifendes Netzwerk zur Vermittlung von Fertigungsaufträgen ist aktuell – in Europa – nicht existent. Entsprechend verspricht ein solcher Ansatz einen hohen industriellen Mehrwert.

Das Ziel dieses Bausteins ist somit eine dezentrale und faire Marktplatzlösung, die grundsätzlich offen ist und auf den Grundsätzen von Fairness und neutralen Wettbewerbsbedingungen aufbaut. Durch die stärkere Vernetzung von Anbietern und Nachfragenden sollen Hemmnisse reduziert sowie die Innovationskraft und -geschwindigkeit aller Teilnehmenden gestärkt werden.

Konkret wird angestrebt, einen Marktplatz für Fertigungsaufträge zu entwickeln, der (a) dezentral betrieben wird und (b) ein hohes Maß an Automatisierung verspricht (siehe Abbildung 3). Durch einen dezentralen Fertigungsmarktplatz soll ein (domänenübergreifendes) Ökosystem von Unternehmen geschaffen werden, welches den Austausch von Fertigungsaufträgen fokussiert. Verschiedene Unternehmen kooperieren und kombinieren ihre Ressourcen, um das technische System des Marktplatzes zu entwickeln und zu betreiben, ohne dass ein einziges Unternehmen das Netzwerk kontrolliert. Dennoch konkurrieren sie auf der Ebene der Produkte und Dienstleistungen miteinander. So sollen die Prozessschritte der Auftragsanbahnung und Auftragsabwicklung eines Geschäftsprozesses vereinfacht werden, wodurch eine Kosten- und Aufwandsreduktion bei Auftraggeber und Auftragnehmer entsteht. Durch das Netzwerk aus Konsumenten und Herstellern sollen neue Geschäftsmodelle und Produkte umgesetzt werden können. Bisher nicht genutzte Kapazitäten können über der Marktplatz monetarisiert werden, um neue Anreize zu schaffen, damit weitere Teilnehmer sich dem Netzwerk anschließen.

Als Voraussetzung für Akzeptanz und schnelle Skalierung wird eine Kombination der Merkmale kooperative Governance und dezentrale Technologie gesehen. Die für erfolgreiche Marktplätze essenzielle Vermittlerfunktion wird zwar weiterhin als logisch zentraler Punkt gesehen, die Umsetzung jedoch dezentralisiert. Dabei wird der Marktplatz dezentral von verschiedenen Partnern – beispielsweise in Form eines Konsortiums mehrerer Unternehmen oder einer Gemeinschaft – betrieben. Zu diesem Zweck wird eine Umsetzung mit Hilfe von dezentralen Technologien, wie z.B. *Distributed Ledger Technologien* angestrebt. Erforderlich ist auch ein dezentral betriebenes Identitätsmanagementsystem, welches durch Baustein 3 bereitgestellt wird und damit ein standardisiertes Identitätssystem für alle Teilnehmer darstellt, welches gleichzeitig die Anforderungen nach Datensouveränität für Identitätsdaten abdeckt. Durch den Einsatz von *Open Source Agenten Software* die, stellvertretend für die Auftraggeber / Auftragnehmer, auf dem Marktplatz automatisiert handelt, soll das gewünschte Maß an Automatisierung und Skalierung erreicht werden. Die Agentensoftware ist an das jeweilige IT-Backendsystem (Legacy) des Unternehmens gekoppelt um die notwendigen Informationen über freie Fertigungskapazitäten zu erhalten.

Die Marktplatzfunktionalität des *Matchmakings* von Angebot und Nachfrage lässt sich dabei durch den Einsatz dezentraler Technologien wie DLT / MPC auf ein dezentrales Netzwerk von Berechnungsknoten auslagern. Auftragsanbahnung und Vertragsabwicklung (*settlement*) sind über den Marktplatz standardisiert abbildbar und damit transparent und sicher. Daten aus IT-Backendsystemen werden benutzt, um aggregierte Angebote erstellen zu können. Durch den Einsatz von Verschlüsselungstechniken kann die Vertraulichkeitseinhaltung von Daten (z.B. das RFQ und die Angebotsdaten) gewährleistet werden. Zudem steht der Betrieb eines Berechnungsknotens des Marktplatzes für jeden willigen Teilnehmer offen, der sich der Governance-Satzung anschließt. Durch ein entsprechendes Anreizsystem, was z.B. durch ein transparentes Transaktionskostensystem finanziert wird, ist sichergestellt, dass die Betreiberknoten die Funktion korrekt ausführen und gleichzeitig der Marktplatzmechanismus nicht unter der Kontrolle einer Entität steht. Durch den Einsatz kryptographischer Verfahren (sogenannte *Confidential Computing Plattformen*) in der Marktplatzarchitektur ist gewährleistet, dass Konsumenten und Produzenten stets Herr ihrer Daten sind und diese nicht einem Dritten zur Verarbeitung innerhalb der Marktplatzfunktion aushändigen müssen, wie dies bei zentralisierten Lösungen der Fall ist. Die Eigentümer der Daten entscheiden stets selbst, welche Informationen öffentlich auf dem Marktplatz einsehbar sind. Die Vertrauenswürdigkeit der Datenhaltung ist dadurch in der gesamten Prozesskette gewährleistet.

Für die Beschreibung der Fertigungskapazitäten und -anforderungen sollte auf bereits existierenden Semantiken (siehe Standards) aufgebaut werden. Die Kommunikation zwischen den handelnden Agenten auf dem Marktplatz sollte ebenfalls standardisiert ablaufen, um eine nahtlosere Integration in bestehende IT-Systeme zu ermöglichen.

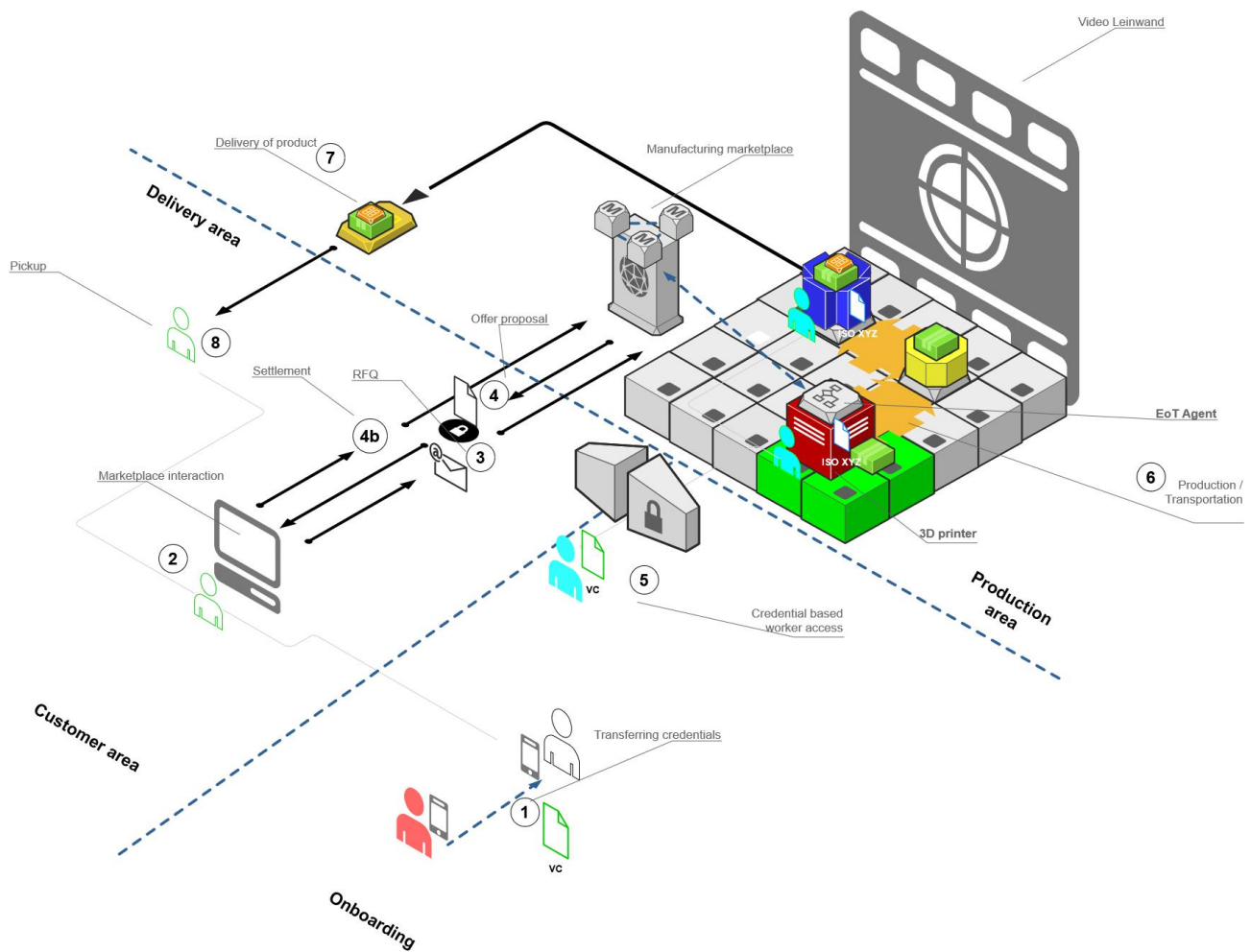


Abbildung 3 Skizze eines dezentralen Fertigungsmarktplatzes, auf dem Fertigungsaufträge gehandelt werden können

2.1.3 ANFORDERUNGEN FÜR DIE UMSETZUNG

Für die Umsetzung eines solchen Marktplatzes für Fertigungsaufträge, der (a) dezentral betrieben wird und (b) ein hohes Maß an Automatisierung verspricht, werden die folgenden Kernanforderungen definiert:

- 1) Integration eines dezentralen Identitätsmanagementsystems im Zuge der Onboarding-Phase des dezentralen Marktplatzes.
- 2) Das Matchmaking der Parteien muss in einer sicheren Umgebung stattfinden, in der kein Teilnehmer überproportionales Marktwissen erlangen kann und somit das Matchmaking beeinflussen kann.
- 3) Das Settlement zwischen den Parteien findet *peer-to-peer* statt und ist kryptographisch abgesichert gegen Manipulationen.
- 4) KI-Algorithmen für Fertigungsmarktplätze können dezentral trainiert und ausgeführt werden. Für Endnutzer bringt das denselben Vorteil wie bei zentralen Lösungen. Für Produzenten bietet es den Vorteil, Daten für das Trainieren eines KI-Modells zu nutzen, ohne diese offenlegen zu müssen.

2.2 BAUSTEIN 2: REGULIERUNGSKONFORME, SICHERE UND EFFIZIENTE BEZAHLSYSTEME

2.2.1 AUSGANGSSITUATION

Die moderne Wirtschaft ist gekennzeichnet durch vierteilige, transnationale Wertschöpfungsketten. Hierbei spielt die Aufgabe der Vermittlung (durch sog. *Broker*) sowie die Erbringung von Funktionen klassischer Banken, gestützt auf regulierte Währungssysteme, eine wesentliche Rolle.

Auch in diesen Bereichen ist, auf Grund von Netzwerk- und Lock-In-Effekten, eine Tendenz zur Monopolbildung sowie das Eindringen von *Hyperscalern* zu beobachten.

Einerseits üben neuartige Bezahlungsdienstleister, sog. *payment service provider* (PSP), im Bereich der Zahlungsabwicklung in den üblichen Währungseinheiten (FIAT Geld) bereits heute einen erheblichen Druck, sowohl auf die klassischen Banken, als auch auf die Industrie aus. Kurz gesagt ist dieser Druck möglich, da vergleichbare Geschäftsstrategien wie aus den Themen rund um Web 2.0 bekannt (Kartendienstleistung, Smartphone-Dienste, soziale Medien, B2C-Marktplätze) angewendet wurden – z.B. attraktive Gebührenmodelle (wie beispielsweise kostenloses *instant-payment*) für Verbraucher, bei hoher Servicequalität – um zunächst eine weite Verbreitung und Akzeptanz beim Verbraucher zu erreichen. Die daraus erwachsende Vormachtstellung wird nun verwendet, um von der Geschäftsseite (also z.B. den Händlern, Marktplatzbetreibern usw.) hohe Gebühren für die Zahlungsabwicklung zu erheben. Darüber hinaus werden z.T. auch die Herausgabe der Meta-Information (vereinfacht: „Wer kauft unter welchen Randbedingungen was ?“) verlangt. Letzteres greift wiederum das Kernfeld der Industrie (sowohl im B2C- als auch B2B-Bereich) an: den Kunden zu verstehen und das Angebot entsprechend (weiter) zu entwickeln. Es ist zu erwarten, dass die Erkenntnisse aus den Meta-Informationen von den PSP nicht nur zur Verbesserung der Servicequalität der eigentlichen Bezahlungsdienstleistung, sondern früher oder später auch zur Etablierung eigener Angebote im Kernfeld der Industrie führen wird. Als Analogie seien hier die bereits weiter oben erwähnten Vorgänge bei den B2C-Marktplätzen angeführt, bei denen der zentrale *Matchmaker* die Informationen über die von Händlern erfolgreich angebotene Produkte nutzt, um diese Produkte dann in der Folge selbst herzustellen und anzubieten.

Neben der Industrie kommen durch solche Vorgänge auch die klassischen Geschäftsbanken unter Druck, welche jedoch neben dem reinen Bezahlendienst weitere wichtige Aufgaben, wie z.B. Verwahrung von Krypto-Werten oder Kreditvergabe, in einer funktionierenden Sozioökonomie übernehmen müssen.

Zusätzlich zur Frage der Vormachtstellung im Bereich der klassischen Zahlungsabwicklung gewinnt der Aspekt der Digitalisierung von Wertdarstellungen sowie die programmgesteuerte Ausführung von Geschäftsvorgängen und Werttransfer (z.B. via sog. *smart contracts*) stark an Bedeutung.

Die zu Grunde liegende Wertdarstellung kann sich einerseits auf die digitale Darstellung der üblichen im Regulierungsrahmen (wie Bankenregulierung, Verhinderung von Geldwäsche und Terrorfinanzierung, Exportkontrolle und steuerrechtliche Aspekte) befindlichen Währungseinheiten (FIAT) stützen. Auf Grund der komplexen Auswirkung auf das Gefüge des Zentral- und Geschäftsbankensystems sowie der Stabilität des Wirtschaftssystems ist jedoch zumindest in Europa keine zügige Umsetzung einer allgemein verfügbaren Lösung, z.B. auf Basis von CBDC (wie z.B. der programmierbare Euro) in Sicht. Andererseits finden sog. Kryptotoken zum Wertausgleich bei vollautomatischer Geschäftsabwicklung via *smart contracts* im Bereich der Distributed Ledger Technologie (DLT, auch Blockchain genannt, z.B. Bitcoin und Ethereum etc.) bereits heute eine breite Verwendung. Hierbei ist die Konformität mit dem Regulierungsrahmen weitestgehend nicht gegeben bzw. ungeklärt. Deshalb, und auf Grund weiterer Aspekte wie z.B. hohe Preisvolatilität, finden

Kryptotoken basierte Darstellungen bisher weder beim Endverbraucher, noch bei industriellen Anbietern – welche sich notwendigerweise innerhalb des Regulierungsrahmens bewegen – keine breite Anwendung. Für eine detaillierte Diskussion dieser Thematik verweisen wir auf unser Papier [14].

Nichtsdestotrotz bietet die den DLT-Systemen zu Grunde liegende Technologie (kryptographische Methoden zur sicheren Wertdarstellung und programmgesteuerten Geschäftsabwicklung) ein hohes Maß an Bedeutung für die künftige digitale Sozioökonomie. Diese ist zum einen durch automatische Abwicklung einer großen Zahl an vierteilig verzahnten, quasi instantanen Micro-Geschäftsvorgängen gekennzeichnet (beispielhaft seien Industrie 4.0 und Maschinenökonomie genannt), beinhaltet jedoch auch (tokenbasierte) Mechanismen zur Geschäftsanbahnung sowie die Koordination und Selbstverwaltung der komplexen Wertschöpfungsketten (s. dazu auch [15] [16]).

In die durch den vorhandenen Bedarf bei fehlendem Angebot gegebene Lücke stoßen nun einerseits Nationalstaaten wie China mit der programmierbaren digitalen Variante des Yan, eine Vielzahl von privaten Initiativen bis hin zu Vereinigungen von Tech-Giganten wie Libra [17].

Bleibt weiterhin eine auf dem europäischen Regulierungsrahmen basierende, an den gesamtwirtschaftlichen Interessen orientierte Lösung aus, so ist zu erwarten, dass sich eine der zuvor genannten Bestrebungen erfolgreich eine Vormachtstellung erarbeiten wird. Neben den üblichen gesamtwirtschaftlich und gesellschaftlich destruktiven Effekten (überproportionaler Wertenzug durch einzelne Quasi-Monopolisten zum Schaden der Sozioökonomie als Ganzes), ergäbe sich dadurch eine weitere Dimension negativer Auswirkungen auf das europäische Wirtschafts- und Gesellschaftsgefüge. Die Unterwanderung der Währungshoheit schränkt die Effektivität sowohl von Geldpolitik als auch Steuerung durch Regulierung stark ein. Nicht zuletzt deshalb, ist der Libra-Vorstoß zur Errichtung einer übernationalen digitalen Währung nicht nur in Europa auf heftige Gegenwehr gestoßen. Denn hier würden die Mechanismen der geldpolitischen Steuerung in der Hand einer Vereinigung von Tech-Giganten liegen und nicht mehr in der Hand der staatlichen Zentralbanken[18] [19] [20].

Es zeigt sich also, dass es sich bei der Situation rund um die für eine stabile Sozioökonomie bedeutsamen Themen digitale und programmierbare Wertdarstellung sowie Zahlungs- und Geschäftsabwicklung um eine komplexe Gemengelage handelt, für welche aus europäischer Sicht zügig Lösungsmöglichkeiten erarbeitet werden müssen. Ansonsten könnten Datensouveränität, die Souveränität der Geld- und Finanzpolitik, die Effektivität der Steuerung durch Regulierung und damit letztlich die Stabilität des europäischen Wirtschaftssystems gefährdet sein.

2.2.2 LÖSUNGSANSATZ: CRYPTO & BANKEN HYBRID

Wie in der Darstellung der Ausgangssituation beschrieben, kommt einer auf dem europäischen Regulierungsrahmen basierenden Ermöglichung von sicheren digitalen und programmierbaren Wertdarstellungen sowie Zahlungs- und Geschäftsabwicklungen eine gewisse Dringlichkeit zu. Aufgrund der Komplexitäten rund um die Einführung eines programmierbaren Euros ist eine baldige Lösung auf diesem Wege nicht in Aussicht [21] [22]. Um diese Situation zu überwinden, bietet sich jedoch eine Kombination der Vorteile von kryptobasierten Lösungsansätzen mit den Stärken eines etablierten Bankensystems an. Diese Hybridlösung wurde in [14]³ detailliert dargestellt und soll im Folgenden kurz skizziert werden.

³ Insbesondere Kapitel V.

Trustless channels

Aus dem Feld der krypto-basierten DLT ist das Konzept der sicheren Zusammenarbeit, z.B. zur Verwaltung von Wertdarstellungen und fälschungssicheren Ausführung von Programmen (z.B. via sog. *smart contracts*), in nicht-kooperativen Umfeldern bekannt. Die Sicherheit wird dabei informationstheoretisch bzw. kryptographisch erbracht, sodass keinerlei Vertrauen in teilnehmende Parteien oder Intermediäre notwendig ist (sog. *trustless* Ansätze). Im Prinzip sind mittels dieser Ansätze sichere, effiziente und hochfrequente Mikro-Geschäftsvorgänge realisierbar. Eine naive Anwendung der DLT, z.B. auf Basis von *on-chain* Ausführungen, wie in manchen Vorschlägen zu hybriden Lösungsansätzen (sog. DLT-Banken- Konnektoren) angedacht, führt jedoch weder zur notwendigen Zeit-, noch Kosteneffizienz.

Sogenannte 2nd-Layer-Technologie (also zweite Schicht zum DLT-System), wie *payment-, state- und generalized state channels* sind vielversprechende Ansätze, die Anzahl der notwendigen zeit- und kostenintensiven *on-chain* Interaktionen stark zu reduzieren, während die Sicherheit der zu Grunde liegenden DLT erhalten bleibt [23] [24]. Die unterschiedlichen Verfahren wie *time- & hash locks* [25] [26], *forceMove* [27] und *Perun* [28] ermöglichen, kurz gesagt, eine *on-chain* Verankerung so, dass sichere und *off-chain* Interaktionen direkt zwischen den betroffenen Teilnehmern (*peer-to-peer*) ermöglicht werden. Erst dadurch ist die notwendige Kosten- und Zeiteffizienz darstellbar.

Justified Trust

Üblicherweise werden den kryptobasierten *trustless* Technologien die klassischen, vertrauensbasierten Ansätze des etablierten Wirtschaftssystems als Kontrapunkt gegenübergestellt. Bzgl. der Letzteren besteht prinzipiell die Gefahr des Vertrauensmissbrauchs, welcher nicht wie bei Ersteren, per Konstruktion informationstheoretisch verhindert werden kann. Gleichzeitig wird aus Sicht der DLT-Community die komplexe Regulierungssituation als unnötige Bürde empfunden. Jedoch erfüllt dieser Regulierungsrahmen wichtige Funktionen wie beispielsweise Verhinderung von Geldwäsche und Terrorfinanzierung, und dient gerade auch dem Zweck der Absicherung vertrauensbasierter Zusammenarbeit. Abgesichert durch den einbettenden, regulativen Rahmen können die Teilnehmer (z.B. Bankkunden) gerechtfertigter Weise Vertrauen in die korrekte Ausführung der Interaktionen haben. Dies ist möglich, da es einen etablierten Satz an Regeln sowie zugehörige Instanzen der Adjudikation gibt, sodass die einzelnen Parteien im Zweifel eine Klärung herbeiführen und ihre Rechte durchsetzen können. Dieser als *justified trust* bezeichnete Umstand ist daher nicht als nachteiliges Gegenbeispiel zu *trustless* Ansätzen zu betrachten. Vielmehr bietet eine geeignete Kombination große Synergieeffekte.

Trustless & justified trust Hybrid

Die kryptobasierten *trustless* Technologien ermöglichen einerseits eine fälschungssichere und für alle Beteiligten (auch z.B. für die Regulierungsbehörden) transparente⁴, sichere, effiziente und hochfrequente Verwaltung und Ausführung von Mikro-Geschäftsvorgängen. Bettet man diese Technologien geeignet in den regulativen Rahmen ein, und schafft eine sichere Schnittstelle zu *justified trust* Elementen wie z.B. zum Bankensystem zum Zweck des niederfrequenten Wertausgleichs in FIAT Währung, können die Vorteile der Konformität dieser Elemente zum regulativen Rahmen mit denen der *trustless* Technologie verbunden werden. Des Weiteren ist auf dieser Basis eine baldige, legale und rechtssichere Inbetriebnahme möglich, sodass eine hohe Akzeptanz sowohl bei der Industrie als auch beim Endverbraucher erreicht werden kann.

⁴ Transparent in den Sinne daß einzelne Vorgänge bei Bedarf fälschungssicher nachgewiesen werden können, wobei generell Datensouveränität sichergestellt ist.

Darüber hinaus ist eine Evolution einzelner Aspekte des Lösungsansatzes leicht möglich, ohne die wesentlichen Bausteine jeweils neu erarbeiten zu müssen. So ist z.B. eine Anbindung zur Nutzung eines ggf. später verfügbaren digitalen Euros genauso möglich wie die Anbindung von etablierten Kryptotoken wie z.B. BTC, sobald die diesbezüglichen rechtlichen Fragen geklärt sind. Auf diese Weise wird sowohl ein Lock-In in einzelne Technologien, als auch eine starke Zerklüftung in alternative Lösungsansätze vermieden.

Abbildung 4 illustriert diese Herangehensweise. Eine detaillierte Diskussion der Architektur, sowie der zu Grunde liegenden Protokolle zur Schaffung sicherer Schnittstellen ist in [14]⁵ zu finden.

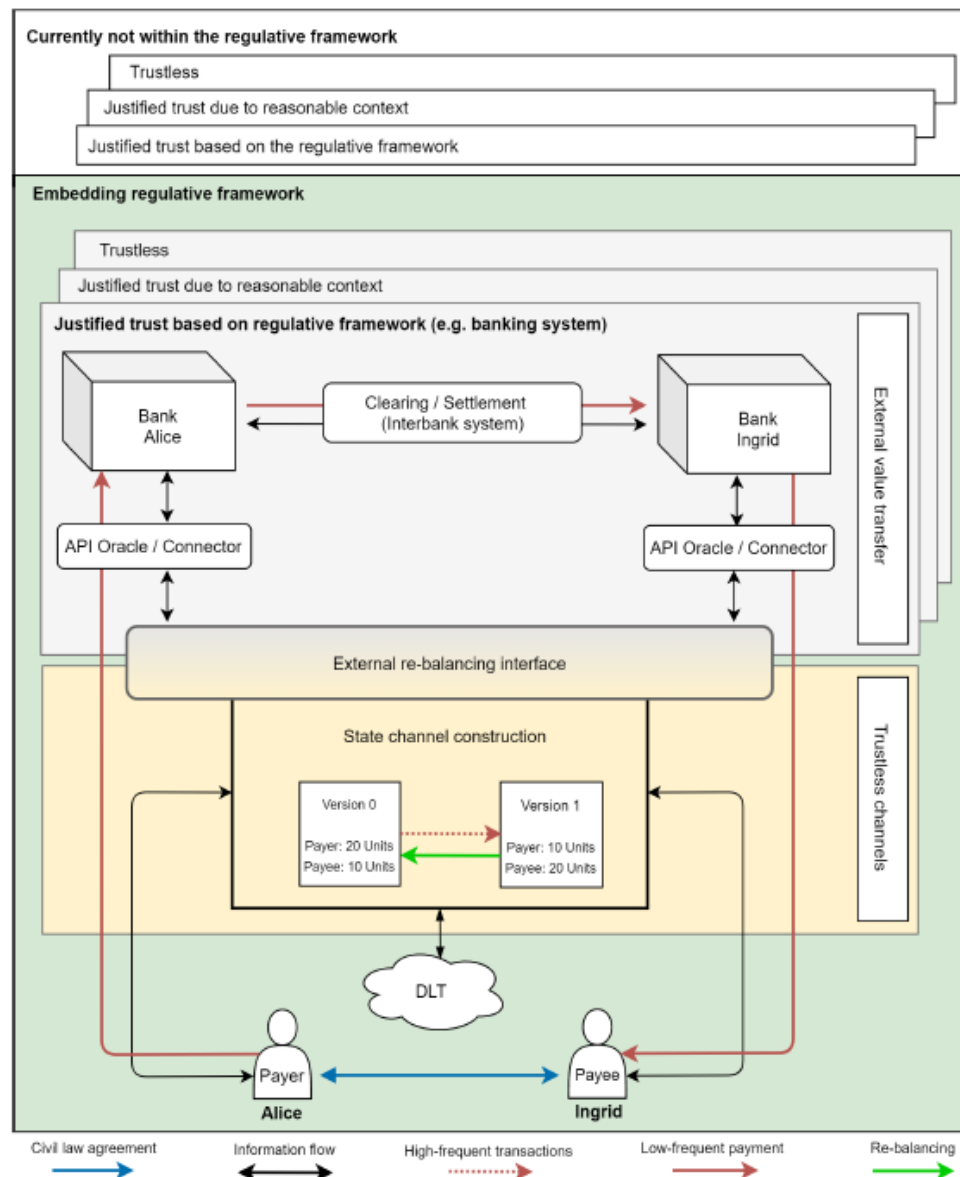


Abbildung 4 Übersicht über die Architektur der vorgeschlagenen trustless / justified trust Hybridlösung. Eine detaillierte Diskussion dieser Architektur sowie der zu Grunde liegenden Protokolle zur Schaffung sicherer Schnittstellen ist in [14] zu finden.

⁵ Kapitel V, bzw. Appendix A

2.2.3 KONKRETER USECASE: HYBRIDES BROKERMODELL

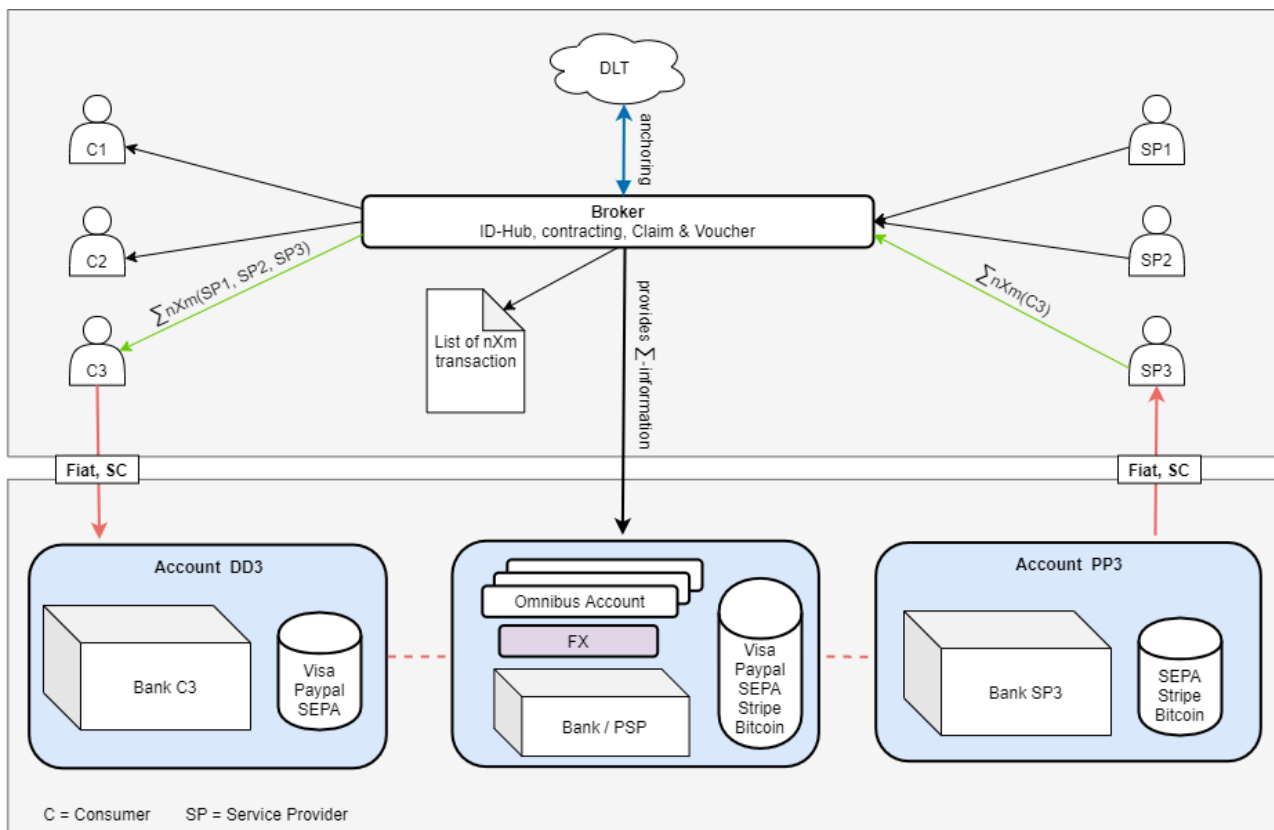


Abbildung 5 Illustration des Brokermodells, gekennzeichnet durch einen trustless Bereich (hier in der oberen Hälfte dargestellt) sowie Verknüpfung mit einem justified trust Bereich für den niederfrequenten externen Wertausgleich, analog zu Abbildung 4, mit den dann beteiligten Hausbanken / PSP.

Abbildung 5 illustriert das sog. *Brokermodell* (Vermittlermodell), welches in der vierteiligen Wirtschaft zunehmend an Bedeutung gewinnt. Es ist dadurch gekennzeichnet, dass ein Vermittler das Zustandekommen eines Geschäfts zwischen Anbietern (*service provider*) und Nutzern (*service consumer*) vermittelt und ggf. rund um die Abwicklung des Geschäfts weitere Servicedienstleistungen erbringt.

Nutzer sind hier nicht zwangsläufig Endkunden, sondern z.B. im B2B-Bereich Integratoren von Subsystemen, welche das Ergebnis der Integration dann wieder als Service im Rahmen einer vierteiligen Wertschöpfungskette zur Verfügung stellen können.

Das Brokermodell zeichnet sich – im Unterschied zum Weiterverkäufermodell – nun insbesondere dadurch aus, dass nach erfolgter Vermittlung zwischen Anbieter und Nutzer ein direktes Rechtsgeschäft zwischen diesen beiden Parteien zustande kommt. Der Vermittler selbst ist dabei nicht Teilnehmer des Geschäfts und somit nicht von etwaigen Haftungsansprüchen (welche beispielsweise aus mangelhafter Serviceerbringung, Produkthaftung etc. erwachsen) betroffen.

Das Brokermodell stellt eine spezielle Ausprägung des allgemeineren Marktplatzmodells (Baustein 1) dar, und bezieht sich insbesondere auf den Aspekt der nicht-haftenden Vermittlung und den damit einhergehenden Anforderungen aus Sicht des regulierenden Rahmens. Es verbindet die für eine vierteilige Wertschöpfungskette essentiellsten Anforderungen an digitale und programmierbare Wertdarstellungen und Zahlungs- und Geschäftsabwicklungen. In der hier gezeigten Architektur nimmt der Vermittler im Sinne der *trustless* Ansätze die Rolle eines sog. Hubs, also eines Intermediärs ein, wobei zumindest die durch den in Abbildung 4 illustrierten Anteil (kryptobasierte Verwaltung und Wertausgleich in FIAT Währung) die

Eigenschaft *trustless* gegeben ist. Die weiteren Funktionen des Vermittlers können prinzipiell, je nach Anwendungsfall, auch über dezentralisierte Ansätze erbracht werden (wie dies im Baustein Marktplätze erarbeitet wird). Da die Komplexität einer legalen und effizienten Realisierung aber gerade in der Konformität zum heute existierenden regulativen Rahmen liegt und dies durch eine weitergehende Dezentralisierung ggf. zusätzlich verkompliziert wird, sowie der oben argumentierten Dringlichkeit, soll in diesem Baustein die Realisierung mit einem Hub-Intermediär betrachtet werden.

Kurz gesagt liegt der Fokus darauf, die Tragfähigkeit der folgenden Arbeitshypothese nachzuweisen:

Durch geeignete Kombination von (2nd Layer) *trustless* Ansätzen mit *justified trust* Systemen kann einerseits das Effizienzpotenzial von programmierbaren Wertdarstellungen und Zahlungs- und Geschäftsabwicklungen konform zum regulativen Rahmen erschlossen werden. Darüber hinaus ergibt sich gerade aus den Eigenschaften der *trustless* Ansätze (neben Kosteneffizienz: Fälschungssicherheit, beweisbare Validität, Selbstsouveränität z.B. bzgl. Daten bei gegebener Transparenz, ...) die Möglichkeit, den Anforderungen des regulativen Rahmens auf effiziente Weise gerecht zu werden.

, sowie entsprechende Arbeitsergebnisse als dokumentierte *best practice*, offene Protokolle und Standards, sowie open source Referenzimplementierungen etc. der (europäischen) Wirtschaft zur Verfügung zu stellen.

Die erarbeiteten Ergebnisse bilden dann eine Ausgangsbasis für die legale Umsetzung weitergehender Dezentralisierung für Fälle, in denen dies angezeigt ist.

Diskussion des gewählten Ansatzes – Ausgangspunkt

Wie oben beschrieben, steht die Konformität zum bestehenden regulativen Rahmen im Zentrum der Aktivität. Daher bildet das klassisch realisierte Brokermodell (also ohne *trustless* Anteile), welches heute, mit einigem Aufwand, bereits legal umgesetzt werden kann, die Ausgangsbasis.

Aufgabe des Brokers, neben der reinen Vermittlung des Geschäfts zwischen Anbieter und Nutzer, ist gerade auch eine einfach zu verwendende und kostengünstige Schnittstelle zur Zahlungsabwicklung zu ermöglichen. Zwar könnte prinzipiell nach erfolgreicher Vermittlung eine Abwicklung der Zahlung vom Nutzer zum Anbieter auch direkt erfolgen. Dies ist jedoch aus verschiedenen Gründen oft nicht gewünscht. Zum einen ist die Zahlungsübermittlung mit Gebühren verbunden, sodass die Kosten für einen Ausgleich kleiner und mittlerer Summen die Rentabilität der zu Grunde liegenden Geschäftsmodelle beeinträchtigt. Darüber hinaus sind die Sekundärprozesse wie Vorgangsverfolgung, Monitoring offener Forderungen, Zuordnung von Zahlungen zu offenen Forderungen, Buchhaltung usw. bei den Beteiligten mit hohem Aufwand verbunden. Insbesondere die zunehmende Vierteiligkeit der Wertschöpfung (z.B. im Zusammenhang mit Industrie 4.0 und Maschinenökonomie) ist nun aber gerade durch eine zunehmende Zahl an Mikro-Geschäftsvorgängen gekennzeichnet. Da die Ansätze zur effizienten elektronischen Abwicklung solcher Vorgänge (z.B. mittels sog. *eBilling*) noch nicht breit etabliert sind, profitieren die Beteiligten von einer orchestrierenden Instanz (dem Broker), welcher eine Summierung und effiziente Abwicklung von mikro-Zahlungen zur Verfügung stellt.

Auch aus steuerrechtlicher Sicht ergibt sich z.T. die Anforderung, wenigstens Zahlungsanteile (z.B. Umsatzsteuer) seitens des Brokers abzuführen. Der Vermittler wird ggf. von den (Regulierungs)behörden als zentrale Instanz gesehen, welche für die Erfüllung der (steuer)rechtlichen Anforderungen in Verantwortung genommen wird. Fließen nun aber (Teil)beträge über den Broker selbst, so erbringt er ggf. einen Zahlungsdienst in Form des Finanztransfargeschäfts, welches der Bankenregulierung unterliegt. Um eine entsprechende Zulassung als Broker selbst nicht erwirken zu müssen, werden die Abwicklung der

Zahlungsdienste meist an (zugelassene) PSPs vergeben, mit all den in der Ausgangssituation beschriebenen Nachteilen, wenn es sich um PSPs mit Vormachtstellung handelt.

Diskussion des gewählten Ansatzes – vorteilhafte Erweiterung des Ausgangspunktes durch das hybride (trustless / justified trust) Brokermodell

In der dem klassischen Ausgangspunkt am weitesten entsprechenden Ausgestaltung des hybriden Brokermodells findet ein sog. *onboarding* der einzelnen Parteien (Serviceanbieter und Nutzer) beim Broker statt. Dieser Vorgang wird durch das Zustandekommen eines zivilrechtlichen Vertrages begleitet. In diesem Vertrag sind auch die Eckpunkte der *trustless* Buchführung in einer definierten Darstellung geregelt. Zugleich wird eine entsprechende *trustless channel* Verbindung zum Broker (der Broker ist zugleich Channel-Hub) etabliert.

Das *onboarding* und die Verwaltung der zugehörigen Datensätze kann vorzugsweise auf Basis von Verfahren zur selbstsouveränen Verarbeitung von elektronischen Identitäten (Self-sovereign identities (SSI)/ Decentralized identifiers (DID)) und digital unterstützt bzw. automatisiert werden. Vorzugsweise erfolgt dies über die Fähigkeiten, welche im Zusammenhang mit diesen Technologien (SSI / DID) sowie dem Baustein Marktplatz entwickelt werden.

Die in den o.g. Initiativen entstehenden, Stammdaten bezogene SSI / DID-basierten Methoden können auch leicht entsprechend den Anforderungen zur elektronischen Rechnungslegung (eBilling, bspw. nach EDIFACT ZUGFeRD, CEN16931-core invoice usage specification CIUS, etc.) erweitert werden.

Das *onboarding* beim Broker macht diesen auch zum – wenn auf SSI basiert –, sicheren Geschäftsdaten-Hub. Der Zweck davon ist, dass nicht jeder Anbieter mit jedem potentiellen Nutzer die Stammdaten austauschen muss. Im Rahmen der Vermittlung eines Geschäftes zwischen Anbieter und Nutzer kann nun der diese Parteien bindende zivilrechtliche Vertrag, orchestriert durch den Broker (Daten-Hub), automatisiert generiert werden. Die Parteien können dann, auf dem regulativen Rahmen und den Anforderungen der *trustless* Ansätze entsprechend geeigneten Weise (beispielsweise durch elektronische Signatur), diesen Vertrag akzeptieren. Auf diese Weise kommt ein zivilrechtlich bindender und durch alle Teilnehmer beweisbar eingegangener Vertrag zustande.

Als Teil dieser Verträge ist geregelt, dass und wie die Verwaltung der sich ggf. hochfrequent in Mikro-Vorgängen ergebenden Zahlungsansprüche mittels des etablierten *trustless channel* Netzwerks verwaltet werden. Für eine detaillierte Darstellung s. [14] und die darin angegebenen Referenzen. Somit sind die weiter oben beschriebene Vorteile der *trustless* Ansätze (wie Kosteneffizienz, Fälschungssicherheit, beweisbare Validität, Selbstsouveränität z.B. bzgl. Daten bei gegebener Transparenz,...) nutzbar.

Auf niederfrequenter Basis, beispielsweise am Ende der durch die Vertragspartner vereinbarten Abrechnungsperiode, findet dann ein Ausgleich der aufgelaufenen, im *trustless channel* Netzwerk kryptographisch sicher verwalteten Forderungen über den Weg des in Abbildung 1 und zugehörigem Text dargestelltem und aus Sicht des *trustless channel* externen Wertausgleichs in FIAT Währung über die Verbindung zum *justified trust* System statt. Dieser Wertausgleich ist dann per Konstruktion konform mit dem regulativen Rahmen (z.B. Bankenregulierung, Geldwäscheverordnung etc.). Etwaige Teilbeträge wie z.B. Umsatzsteuer können bei diesem Vorgang ebenfalls ausgekehrt werden. Wie oben dargestellt ist der tatsächliche Ausgleich mit Kosten und Aufwand verbunden, sodass durch die Kombination der hochfrequenten Geschäftsabwicklung mit niederfrequentem Wertausgleich erhebliche Kosteneinsparungen realisiert und somit Anwendungsfälle beispielsweise im Bereich Industrie 4.0 und Maschinenökonomie dadurch erst rentabel werden.

In einem komplexen Anwendungsfall mit vielen hochfrequenten Interaktionen zwischen vielen Parteien implementiert der Channel-Hub die notwendige Funktion der Aggregation der Mikro-Vorgänge und ermöglicht eine (niederfrequente) summierte Aufteilung (sog. *Splitting*). Dies könnte beispielsweise wie folgt gestaltet sein:

Der Broker sowie Nutzer und Anbieter besitzen im Rahmen des oben beschriebenen externen Wertausgleichs, beispielsweise über ihre Hausbank, eine geeignete Zahlungs- und Empfangsmöglichkeit für FIAT Währung. Der PSP (Hausbank) des Brokers implementiert ein Sonderkonto, dessen Rolle im Folgenden näher erläutert wird.

Angenommen Nutzer 1 nimmt an einer Vielzahl von Mikro-Geschäftsvorgängen mit einer Vielzahl an Anbietern teil. Andererseits ist Anbieter 1 an einer Vielzahl von Transaktionen mit vielen Nutzern beteiligt. Am Ende der vereinbarten Abrechnungsperiode kann nun durch den Channel-Hub eine summierte Aufstellung für Nutzer einerseits und Anbieter andererseits erstellt werden. Wichtig dabei ist, dass es sich jeweils um auf einen Gesamtbetrag lautende Darstellung handelt, wobei die einzelnen Vorgänge auf Wunsch bzw. entsprechend den gesetzlichen Anforderungen als Einzelposten aufgeführt werden können. Der Nutzer 1 kann diesen summierten Betrag nun über den oben beschriebenen externen Wertausgleich auf das Sonderkonto anweisen (bei gleichzeitig sicherem Rückausgleich des entsprechenden *trustless* channels mit dem Broker).

Auf Grund der einem PSP vorliegenden Zulassung für Finanztransfersgeschäfte kann er die erfolgten Einzahlungen auf das Sonderkonto legal verwalten. Die summierten Zahlungen an die Anbieter werden von diesem Konto, nach Vorgabe des Brokers ausgekehrt.

Auf Grund dieser Konstruktion unter Verwendung von *trustless* channels ist einerseits die Korrektheit der Summierung kryptographisch beweisbar, gleichzeitig bleiben die mit den einzelnen Mikro-Geschäftsvorgängen verbundenen Meta-Informationen (z.B. wer hat wann welchen Dienst wie genutzt) im Brokersystem und sind vor dem Zugriff durch den PSP geschützt (s. den oben diskutierten Punkt Schutz des Geschäfts-Know-hows und Datensouveränität).

Die PSPs bzw. die Hausbanken des Brokers, der Nutzer und Anbieter können somit sowohl auf geeignete Weise ihre Grundaufgabe, nämlich die Abwicklung der Zahlungsdienstleistung entsprechend dem regulativen Rahmen erbringen, als auch weitere, dem Bankenbereich zuzuordnende Servicefunktionen wie Finanzierung etc. anbieten.

Voraussetzung für eine zügige, weite Verbreitung der Lösung sind dokumentierte *best practices*, offene Protokolle und Standards, sowie *open source* Referenzimplementierungen, welche einerseits im Einklang mit den Anforderungen des regulativen Rahmens sind, und andererseits – insbesondere den externen Wertausgleich betreffend – auf etablierte Verfahren (wie SEPA) und Standards (wie R2P) aufbauen. Auf diese Weise kann ein Lock-in in Spezialverfahren bzw. individuelle Lösungen einzelner Anbieter vermieden werden.

In den vergangenen Jahren wurden im Rahmen mehrerer Projekte sowie universitären Engagements *best-in-class trustless channel* Verfahren entwickelt. Die entsprechenden Arbeitsergebnisse wurden bereits in *open source* Projekte übergeführt. Im Speziellen sei hier das Perun-Projekt, welches innerhalb der Hyperledger Organisation als Labs-Projekt etabliert wurde, und in diesem Rahmen weiterentwickelt wird, genannt [29].

Die für die Grundlagentechnologie erfolgreich erbrachten Sicherheitsbeweise müssen nun einerseits, in Zusammenarbeit mit Vertretern des Bankensektors, auf die hybride Lösung erweitert, und entsprechende Referenzimplementierungen erarbeitet werden. Dabei ist, wie oben beschrieben, eine enge Abstimmung mit den Technologien aus Baustein 3 und Baustein 1 notwendig. Des Weiteren sollten die Referenzimplementierungen den inzwischen stattfindenden Wandel weg von einzel-DLT-spezifischen Lösungen hin zu interoperablen Ansätzen, basierend auf bspw. Webassembly (wasm) aufgreifen. Dies erfordert zwar die teilweise Neuimplementierung von Protokollelementen, dient aber sowohl der Vermeidung

eines Lock-in in spezifische DLT-Systeme, als auch der leichten Verbreitung und breiten Unterstützung bei Anwendern und Entwicklern. Darüber hinaus trägt die Verwendung von durch einen Zusammenschluss großer Teile der Crypto-Community entwickelten Grundelementen (wie *crypto* Bibliotheken) zur Sicherheit des Systems bei.

Zusammenfassend kann gesagt werden, dass eine auf offenen, standardisierten und interoperablen Protokollen und Referenzimplementierungen basierende Vorgehensweise, einerseits in Bezug auf die *trustless* Ansätze und andererseits durch Realisierung der Verbindung zu *justified trust* Systemen, idealerweise auf Basis der bereits implementierten Verfahren des Bankensystems wie SEPA und dem verabschiedeten Standard *request to pay* (R2P), die zügige Etablierung einer sicheren, effizienten und dem regulativen Rahmen entsprechende Lösung ermöglichen kann, ohne in einen Lock-in zu führen.

2.3 BAUSTEIN 3: SICHERE, DIGITALE IDENTITÄTEN

2.3.1 AUSGANGSSITUATION

Für den Baustein 3 - sichere, digitale Identitäten sind ebenfalls die bereits eingangs erwähnten Probleme durch zentrale Intermediäre erkennbar. Das zur Verfügung Stellung von offensichtlichem Kundennutzen, wie einfache Verwaltung der heute üblichen Vielzahl an digitalen Konten und Log-ins durch zentrale Instanzen (sog. *single-sign-on*) ist bereits stand Heute weit verbreitet. Dies ermöglicht eine Identifikation und Auswertung des Nutzerverhaltens möglichst in alle Lebensbereiche hinein durch die zentralen digitalen Identitätsanbieter. Diesen Bestrebungen kann ebenfalls mittels den Ansätzen des *crypto-movements* (z.B. sog. *self-sovereign identity* (SSI) und *decentralized identifiers*, DID [30, 31]) entgegengewirkt werden.

2.3.2 LÖSUNGSANSATZ: SELF-SOVEREIGN IDENTITIES

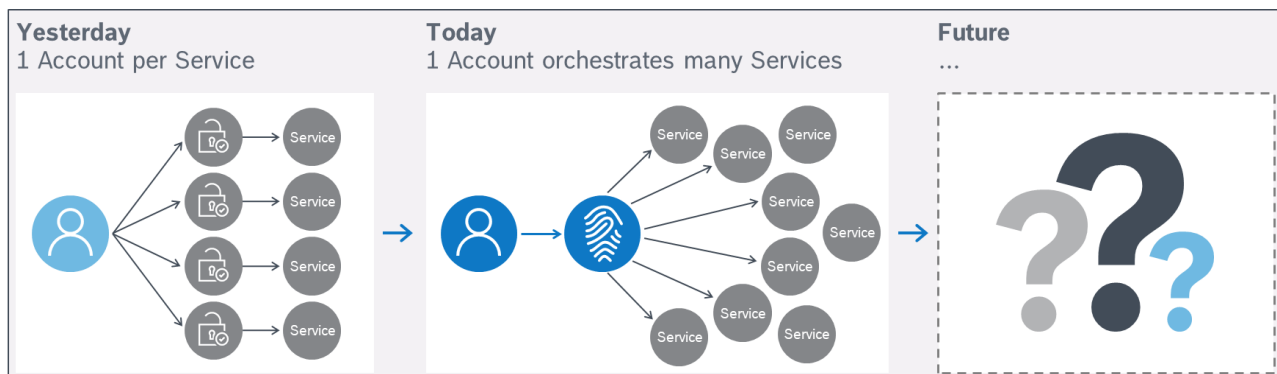


Abbildung 6 Digitale Identitäten im Wandel der Zeit

Im Unterschied zum herkömmlichen und heutzutage breit akzeptierten Ansatz der Nutzung von sogenannten Identity Providern (IDP), wie beispielsweise bekannt durch „Login with Google/Facebook/AppleID“ setzt der erwähnte Ansatz SSI auf die Souveränität des/der Einzelnen (Mensch, Maschine, Organisation). Statt einen Account bei einem IDP zu erzeugen, der entsprechend alle Informationen / Attribute für einen verwaltet, erzeugt bei SSI jede Entität selbständig ohne einen Mittelsmann eine Identität und kann sich durch andere Identitäten wie beispielsweise bekannte zertifizierte Stellen (öffentliche Stelle) bestimmte Attribute seiner selbst bestätigen lassen. Im Vergleich zum accountbasierten IDP-Ansatz liegt die Kontrolle der eigenen Identitäten sowie der ausgestellten sogenannten *credentials*, die Bestätigung von persönlichen Attributen, in der Hand der Entität selbst und erlaubt somit eine direkte Beziehung zum jeweiligen Geschäftspartner, ohne

die Notwendigkeit einer zentralen Stelle. Bei Anforderung von bestimmten bestätigten Attributen kann die jeweilige Entität selbst entscheiden, welche Informationen aus welcher Quelle offen gelegt und zur Verifikation preisgegeben werden, da diese lediglich dem jeweiligen Eigner zur Verfügung stehen und nicht durch Dritte verwaltet werden.

Dies führt zu einer wesentlichen Verschiebung der Informationstransparenz bzgl. IDPs und deren Rolle, da diese durch den Wandel zu direkten Geschäftsbeziehungen zwischen zwei Parteien keinerlei Meta-Informationen über eben dieses Zusammenspiel beziehen können – sie sind kein Teil der Beziehung. Die eigene Daten-Souveränität schafft somit Vertrauen durch Verifizierbarkeit von Attributen und Identitäten zwischen Entitäten und verringert dabei ebenfalls die Angst zur Abhängigkeit von IDPs und anderen Identitätsservices, da die Identität selbst souverän bei jedem Einzelnen verwaltet und gesteuert wird.

2.3.3 INITIATIVEN UND FÖRDERPROGRAMME

Verschiedene Initiativen und öffentlich geförderte Projekte bemühen sich bereits um eine entsprechende Entwicklung und Überführung in Anwendung, z.B. das Projekt „Self Sovereign Identity für Deutschland“ [32] und „EMIL - eIDAS ökosysteme Identity self-sovereign“ [33]. Wir verweisen deshalb auf die entsprechenden, bereits eingereichten Projektanträge.

2.4 BAUSTEIN 4: ORGANISATIONSSTRUKTUREN UND ANREIZSYSTEME FÜR DIGITALE ÖKOSYSTEME

2.4.1 AUSGANGSSITUATION

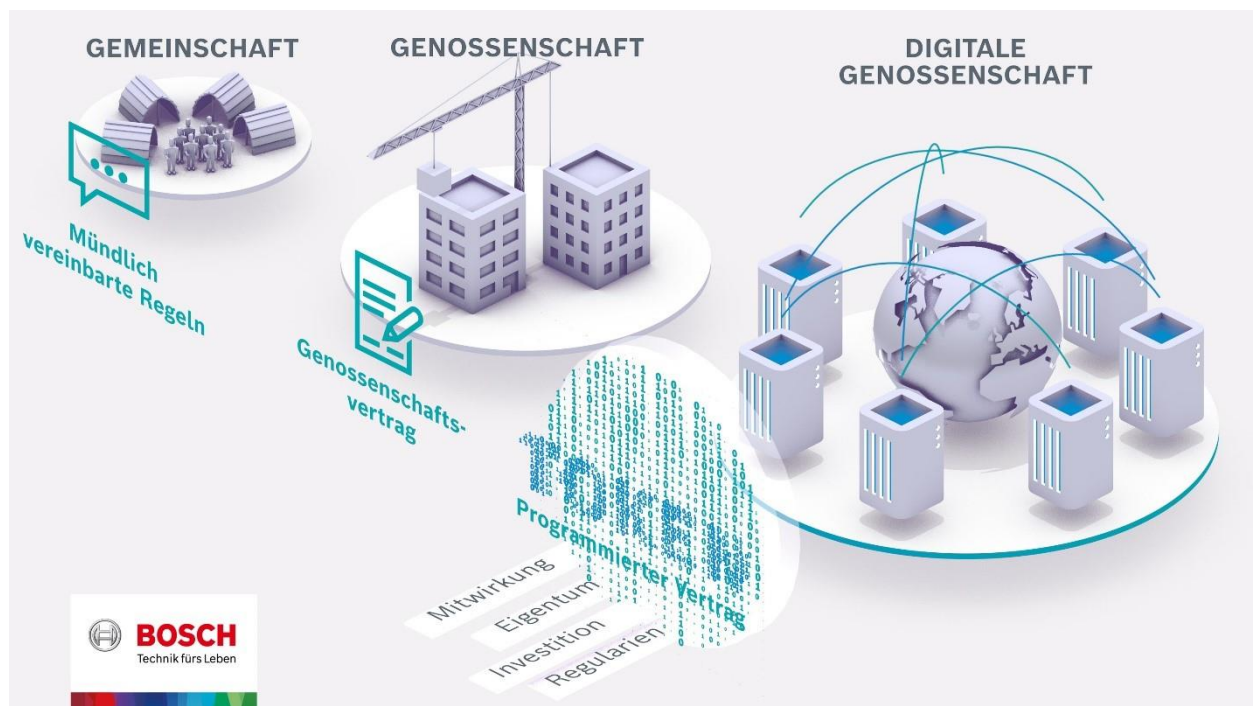


Abbildung 7 Wichtige Merkmale des Bausteins Organisationsstrukturen und Anreizsysteme

Wie bereits in der Einleitung beschrieben, können Märkte ohne Regulierung und Anreize nicht ihr volles sozioökonomisches Potenzial ausschöpfen. Aus diesem Grund beschäftigt sich Baustein 4 mit neuen Zusammenarbeitsmodellen für digitale Ökosysteme.

Die Koordination und zielgerichtete Steuerung der Teilnehmer erfordert Anreizmechanismen sowie Regeln und Prozesse, die im Folgenden unter dem Begriff „Governance“ zusammengefasst werden. Governance ist ein altbekanntes angewandtes gesellschaftliches Problem und bezieht sich im Allgemeinen auf den Prozess der Erzielung eines gesellschaftlichen Konsenses, um ein gemeinsames Ziel möglichst effizient zu erreichen.

Um eine Unternehmung zum Ziel zu bringen, bedienen sich konventionelle Zusammenarbeitsmodelle an Hilfsmitteln wie einer gemeinsamen Sprache, Prozessbeschreibungen, Verträgen und Dokumentation. Diese manuell zu interpretierenden Werkzeuge zur Zusammenarbeit entstammen der analogen Welt, aus der wir kommen. Im digitalen Zeitalter müssen Governance-Werkzeuge einen höheren Grad an Automatisierung und Integrität entwickeln, um den Anforderungen einer internationalen Unternehmung mit einer Vielzahl an Teilnehmern in einem digitalen Ökosystem gerecht zu werden und dieses so zu orchestrieren, dass es wettbewerbsfähig bleibt.

Intransparente Organisationsstrukturen und analoge Prozesse sind anfällig dafür, dass Individuen Entscheidungen treffen, die nicht im Sinne des Gemeinwohls liegen. Werden wiederum alle an den unzureichend automatisierten Entscheidungsprozessen beteiligt, leiden darunter die Effizienz und Skalierbarkeit – und die Organisation wird bei wachsender Anzahl der Teilnehmer regelrecht lahmgelegt. Es besteht also eine Spannung zwischen der Skalierbarkeit, d.h. der Anzahl der Entscheidungen, die ein Kollektiv in einem bestimmten Zeitraum treffen kann, und der Belastbarkeit, d.h. der Unbestechlichkeit dieser Entscheidungen. Der Erfolg von nicht gewinnorientierten Organisationen, die das Ziel haben, ein Gemeingut zu entwickeln, scheitert aber vor allem aufgrund von fehlenden Anreizmechanismen, die Teilnehmer und Investoren motivieren, die Weiterentwicklung nachhaltig mit finanziellen und Entwicklungsbeiträgen anzukurbeln.

2.4.2 LÖSUNGSANSATZ: DIGITALISIERUNG DER ÖKOSYSTEM-GOVERNANCE UND ANREIZMECHANISMEN

Wie in der Ausgangssituation beschrieben, kommt der Umsetzung eines digitalen Entscheidungs- und Konfliktbewältigungsprozesses sowie der Bereitstellung ausreichender Anreizmechanismen eine immer stärkere Dringlichkeit zu. Analoge Geschäftspraktiken und Entscheidungsprozesse verhindern eine effiziente Ausgestaltung einer digitalen Kooperative.

Im Kontext der digitalen Ökosysteme möchten wir ein Governance-Rahmenwerk schaffen, bei dem die Teilnehmer zum einen durch automatisierte, effektive und faire Entscheidungsprozesse handlungsfähig und unabhängig bleiben, sowie durch Anreize motiviert sind, sich am Aufbau und der Weiterentwicklung zu beteiligen. Unerwünschtes Verhalten sollte hingegen ökonomisch uninteressant sein.

Unter Einsatz von maschinenlesbaren, rechtskonformen Verträgen sowie moderner Technologie wie DLT und digital abgebildeten Rechten und Anreizen in Form von digitalen Token, lässt sich das Teilnehmerverhalten so steuern, dass die Maxime des anreizbasierten Ökosystems erreicht werden kann.

Token dienen dabei als zentrales digitales Anreizinstrument und sind der Schlüssel zu einer nachhaltigen Finanzierung sowie den effizienten Betrieb von nicht gewinnorientierten Ökosystemen. Die digitalen Anreizinstrumente basieren auf Kryptographie sowie ökonomischer Spieltheorie und ermöglichen digitalen Netzwerken sich ökonomisch effizient entlang gewünschter Eigenschaften und Ziele zu evolvieren [10] [11].

Anreize steuern das menschliche Verhalten. Das Verständnis von Anreizen ist der Schlüssel zum Verständnis der Sozioökonomie. Anreizmechanismen können als Spielregeln für Personengruppen beschrieben werden, die so gestaltet sind, dass bestimmte Ziele erreicht werden, wenn die Gruppenmitglieder im Rahmen dieser Regeln rational und zu ihrem eigenen Nutzen handeln. Digitale Anreizmechanismen dienen dazu, das

vorgegebene soziale Ziel durch ein nicht-kooperatives Gleichgewicht umzusetzen, auch in Abwesenheit eines zentralen Intermediärs. Anreize können entweder sein:

- **Negative Anreize:** Erhöht die Bereitschaft, das erwünschte Verhalten zu zeigen, indem das unerwünschte Gegenüber sanktioniert wird.
- **Positive Anreize:** Ermöglicht und erhöht die Bereitschaft, das erwünschte Verhalten zu zeigen, indem es belohnt wird.

Anreizmechanismen sind ein wichtiges Instrument der Wirtschafts- und Spieltheorie. Sie werden für ökonomische Analysen in verschiedenen Bereichen der Wirtschaftswissenschaften eingesetzt, z.B. für Anreizmechanismen in der Besteuerung der Industrieökonomik, der Allokation von Gütern, Ressourcen und Risiken oder der Ökonomie des öffentlichen Sektors. Anreize können jede Art von Belohnung oder Bestrafung sein, die von lohnenden bis hin zu rein moralischen oder Reputationsaspekten reichen.

Zudem können mittels DLT Entscheidungs- sowie Konfliktbewältigungsprozesse transparent über mehrere Parteien abgebildet werden, ohne dass hierzu Individuen überproportional an Macht gewinnen. Das schafft Vertrauen unter den Teilnehmern und ist der Nährboden für ein nachhaltiges Wachstum des Ökosystems.

Konkrete Lösungsansätze demonstrieren sogenannte dezentrale autonome Organisationen (DAO). Diese Implementierung der Kooperation lebt autonom im virtuellen Raum. Sie nutzt dazu Distributed Ledger Technologie (DLT) als Kollaborationswerkzeug bzw. gemeinsames Handelsregister. Die Organisationsstruktur und Prozesse zur Entscheidungsfindung werden digital abgebildet. Vertrauen wird über offenen Quellcode in Software und transparente Prozesse erzeugt. Zielgerichtete Entwicklungsbeiträge sowie gutes Verhalten werden durch tokenbasierte Anreizmechanismen gefördert. DAOs werfen momentan durchaus noch rechtliche und technische Fragen auf⁶, geben aber einen Ausblick darauf, wie sich Verträge und Kooperationsprozesse schrittweise in den digitalen Raum überführen lassen. Um die Bausteine 1 bis 3 zum Erfolg zu bringen, ist ein Governance-Rahmenwerk zu entwickeln, das sowohl widerstandsfähig gegen böswilliges Verhalten, als auch effizient und skalierbar ist.

3 ZUSAMMENFASSUNG

Durch die Etablierung von auf europäischen Werten basierenden, geeignet organisierten Marktplätzen, Bezahlssystemen und Anreizsystemen, wird die Vielfaltigkeit und Individualität Europas als Stärke genutzt, um eine effiziente und international wettbewerbsfähige Basis für eine europäische, digitale Sozioökonomie zu schaffen.

Um ein Gegengewicht zu drohenden, mit europäischen Grundsätzen inkompatiblen Ansätzen zu etablieren, ist es angezeigt, die oben genannten Bausteine für die digitale europäische Wirtschaft der Zukunft zügig zu erarbeiten.

⁶ Markus Büch (2019), <https://www.btc-echo.de/die-idee-der-dao-von-missverstaendnissen-und-potentialen/>

4 AUTOREN



Nik Scharmann ist promovierter Wirtschaftsingenieur und leitet die Forschungsaktivitäten von Bosch im Bereich „Economy of Things“ (EoT) seit deren Beginn 2017 als Projektdirektor. Zuvor war er unter anderem in der Anwendungsentwicklung im Bereich Energietechnik bei Bosch Rexroth tätig, wo er seine berufliche Laufbahn 2002 als Trainee startete.



Alexander Poddey promovierte im Jahr 2008 in theoretischer Physik an der TU Clausthal und begann ein Jahr später als Experte für Machine Learning bei Bosch. Im EoT-Projekt bei Bosch Research ist er der leitende Forscher und verbindet in seinen Arbeiten die Themen digitale Sozioökonomie, Kryptologie und künstliche Intelligenz.



Ricky Lamberty forscht und promoviert seit 2019 an der Universität Basel zum Schwerpunktthema „Cryptoeconomic Primitives“. Seit dem vergangenen Jahr bringt er sein Wissen auch im strategischen Vorausbau-Projekt „Economy of Things“ (EoT) bei Bosch Research als Experte für Tokenomics und digital Payment ein.



Denis Kramer studierte Informatik an der Universität Bielefeld und kam 2016 zu Bosch. Dort arbeitete er von Anfang an an IoT-Themen rund um digitale Marktplätze und Interoperabilität. Im strategischen Vorausbau-Projekt „Economy of Things“ (EoT) bei Bosch Research ist er Experte für Multi-Party Computation und Industriemarktplätze.



Danny de Waard studierte Medieninformatik in Stuttgart und arbeitet seit 2005 bei Bosch als Netzwerkingenieur. Dieses Wissen wendet er seit 2016 als Systemberater für die Entwicklung von DLT im Projekt „Economy of Things“ (EoT) an. Er hat sich zudem auf die Mechanismen der Governance für neutrale Informationsökosysteme spezialisiert.

5 BIBLIOGRAFIE

- [1] A. Poddey und N. Scharmann, „On the importance of system-view centric validation for the design and operation of a crypto-based digital economy,“ 2019.
- [2] B. Herd, N. Scharmann und S. Phelps, „Towards the Model-Based Analysis and Design of Decentralised Economies of Things,“ *King's Research Portal*, 2018.
- [3] T. Kölbel und D. Kunz, „Mechanisms of intermediary platforms,“ *arXiv preprint arXiv:2005.02111*, 2020.
- [4] C. Finley, *Nest's Hub Shutdown Proves You're Crazy to Buy Into the Internet of Things*: <http://www.wired.com/2016/04/nests-hub-shutdown-proves-youre-crazy-buy-internet-things/>, WIRED, Hrsg., 2016.
- [5] Ecorys, P. Bas, O. Batura, A. Yagafarova und N. Gorp, Business-to-Business relations in the online platform environment: FWC ENTR/300/PP/2013/FC-WIFO : final report, Brussels: European Commission, 2017.
- [6] B. Martens, „An economic policy perspective on online platforms,“ *Bertin Martens (2016) An Economic Policy Perspective on Online Platforms. Institute for Prospective Technological Studies Digital Economy Working Paper*, Bd. 5, 2016.
- [7] S. Nakamoto, „Bitcoin: A peer-to-peer electronic cash system,“ 2009.
- [8] S. Voshmgir, *Token Economy*, Blockchain Hub Berlin, 2019.
- [9] K. Polanyi, „The Great Transformation: The Political And Economic Origins Of Our Time Author: Karl Polanyi, Publisher: Beacon Press,“ 2001.
- [10] G. Akerlof, „The market for Lemons: Quality uncertainty and the market mechanism,“ *Quarterly Journal of Economics*, Bd. 84, pp. 488-500, 1970.
- [11] A. Smith, „The Theory of Moral Sentiments,“ *McMaster University Archive for the History of Economic Thought*, 1759.
- [12] J. Stiglitz, „There is no invisible hand,“ *The Guardian Comment. London: Guardian Media Group.*, 2002.
- [13] D. Altman, „Q & Answers with Joseph E. Stiglitz.,“ *Managing Globalization (blog) The International Herald Tribune*, 2006.
- [14] R. Lamberty und A. Poddey, „Regulation conform DLT-operable payment adapter based on trustless - justified trust combined generalized state channels,“ <https://arxiv.org/abs/2007.01605>, 2020.
- [15] F. Bundesministerium der Finanzen, „Der digitale, programmierbare Euro,“ *Stellungnahme Januar*, 2020.
- [16] R. Lamberty, D. Waard und A. Poddey, „Leading Digital Socio-Economy to Efficiency,“ p. 9.
- [17] Libra, „Whitepaper, Libra Association, <https://libra.org/de-DE/white-paper>“.
- [18] F. M. Finance, „Joint Statement on Libra,“ 17 9 2019. [Online]. Available: https://www.bundesfinanzministerium.de/Content/EN/Standardartikel/Topics/Financial_markets/Articles/2019-09-17-Libra.html.
- [19] M. Waters, „Open Letter to Mark Zuckerberg, CEO Facebook,“ *Chairwomen U.S. House of Representatives Committee on Financial Services*, 2019.

- [20] Y. Mersch, „Money and private currencies: reflections on Libra, Speech at the ECB Legal Conference, Frankfurt am Main, 2 September 2019,“ 2019. [Online]. Available: https://www.ecb.europa.eu/press/key/date/2019/html/ecb.sp190902_aedded9219.en.html.
- [21] U. Bindseil, „Tiered CBDC and the financial system,“ p. 42.
- [22] D. Bundesbank, „Krypto- Token im Zahlungsverkehr und in der Wertpapierabwicklung,“ *Monatsbericht* - 39 - Juli, 2019.
- [23] S. Dziembowski, S. Faust und K. Hostáková, „General state channel networks,“ in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, 2018.
- [24] J. Coleman, L. Horne und L. Xuanji, *Counterfactual: Generalized state channels*, 2018.
- [25] J. Poon und T. Dryja, *The bitcoin lightning network: Scalable off-chain instant payments*, 2016.
- [26] A. Miller, I. Bentov, S. Bakshi, R. Kumaresan und P. McCorry, „Sprites and state channels: Payment networks that go faster than lightning,“ in *International Conference on Financial Cryptography and Data Security*, 2019.
- [27] T. Close und A. Stewart, „ForceMove: an n-party state channel protocol,“ 2018.
- [28] S. Dziembowski, L. Eckey, S. Faust und D. Malinowski, „Perun: Virtual payment hubs over cryptocurrencies,“ in *2019 IEEE Symposium on Security and Privacy (SP)*, 2019.
- [29] H. Foundation, „Hyperledger Labs Project Perun,“ 2020. [Online]. Available: <https://github.com/hyperledger-labs/hyperledger-labs.github.io/blob/master/labs/perun.md>.
- [30] Q. Stokkink und J. Pouwelse, „Deployment of a Blockchain-Based Self-Sovereign Identity,“ in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 2018.
- [31] W. D. I. D. W. Group, „Decentralized Identifiers (DIDs),“ 19 8 2020. [Online]. Available: <https://www.w3.org/TR/did-core/>.
- [32] B. Wirtschaft und Energie, „Self Sovereign Identity für Deutschland,“ 19 8 2020. [Online]. Available: https://www.digitale-technologien.de/DT/Redaktion/DE/Standardartikel/SchaufensterSichereDigIdentProjekte/sdi-projekt_ssi.html.
- [33] „EMIL - eIDAS ökosysteme Identity self-sovereign,“ [Online]. Available: https://www.digitale-technologien.de/DT/Redaktion/DE/Standardartikel/SchaufensterSichereDigIdentProjekte/sdi-projekt_emil.html.