# iBlockchain Policy Paper: Empfehlungen und Erkenntnisse für die Politik


**In diesem Artikel werden aus der Arbeit des iBlockchain-Projektes hervorgegangene technologische und regulatorische Erkenntnisse und Anforderungen zum Thema Blockchain und DLT im Industrie-Kontext zusammengefasst.**

Die Blockchain- oder auch Distributed-Ledger-Technologie (DLT) eröffnet ein enormes Potential an neuen und innovativen Anwendungen für Industrie und Wirtschaft. Vertrauen und Kontrolle (im Sinne einer fälschungssicheren Dokumentation) werden durch die Technologie selbst geschaffen. Das ermöglicht Anwendungen, die bisher nur unter Zuhilfenahme vertrauenswürdiger Intermediäre möglich waren. Zusätzlich können Unternehmen durch die inhärent dezentrale Struktur an innovativen Entwicklungen anderer partizipieren. So können beispielsweise KMU von Sicherheitslösungen profitieren, die vormals aus Kostengründen nur Großunternehmen vorbehalten waren.

Durch Kombination der Blockchain mit selbst ausführenden, an festgelegte Bedingungen geknüpften Programmen – sogenannten Smart Contracts und darauf aufbauenden Second-Layer-Anwendungen – entsteht ein technologisches System, das es ermöglicht ganze Geschäftsprozesse vollautomatisch und autonom direkt Machine-to-Machine (M2M) abzuwickeln. Das ist in der Industrie 4.0 (I4.0) oder dem Internet der Dinge (IoT) von besonderer Bedeutung.

Um das volle Potential der Blockchain-Technologie ausschöpfen zu können, gilt es einige Hürden zu überwinden. Für viele technologische Vorbehalte stehen bereits Lösungen aus der Forschung bereit oder werden intensiv erforscht (beispielsweise Effizienz, Skalierbarkeit, sichere Einbindung von Maschinen und Sensoren). Allerdings herrscht auf regulatorischer Seite teils Unsicherheit. Beispielsweise ist unklar, welche Token und Token-Arten auf der

Blockchain als Finanzinstrumente gelten. Solche Unklarheiten schaffen Unsicherheit bei Investitionen und stellen eine Hürde für eine Vielzahl von Unternehmen, insbesondere KMU, dar und bremsen Markteintritt und Innovationen. Hier besteht die Notwendigkeit auf institutioneller Ebene in den verschiedenen Bereichen für Klarheit zu sorgen und Rechtssicherheit zu schaffen. Im Folgenden werden aus der Arbeit des iBlockchain-Projektes hervorgegangene technologische und regulatorische Erkenntnisse und Anforderungen zusammengefasst.

# Regulatorische und institutionelle Anforderungen für erfolgreiche DLT-basierte Innovationen

## Identität auf der Blockchain

Für die Ausgestaltung eines Identitätssystems auf der Blockchain sind klare und erreichbare **Richtlinien und Anforderungen** aufzustellen. Dies betrifft erstens die Vereinbarkeit von auf der Blockchain gespeicherten Identitätsdaten mit dem **GDPR** (s.a. Datenschutz), und zweitens die Vereinbarkeit und Integration mit dem **eIDAS Framework**. Bezüglich eIDAS sind einerseits die **Konformität und Kompatibilität der verwendeten Identitäten** zu prüfen und entsprechend regulatorisch zu verankern, wie beispielsweise die Verwendung von im Rahmen von eIDAS ausgestellten und verifizierten Credentials in SSI (Self Sovereign Identity)-Lösungen und DIDs (Decentralized Identifiers). Andererseits ist zu klären, inwiefern die in Blockchains verankerten **Zeitinformationen als Zeitstempel** und das **Verankern von Transaktionen** selbst aufgrund deren Unveränderlichkeit **als Signaturen** im Sinne von eIDAS betrachtet werden können. Bei Signaturen liegt ein besonderer Schwerpunkt auf dem **qualifizierten Status**, um die gleiche Rechtssicherheit wie bei handschriftlichen Signaturen zu erlangen. Drittens sollte der rechtliche Status von "Dingen" bzw. die **Verbindung zwischen "Dingen" und natürlichen oder juristischen Personen** aus Haftungsgründen definiert werden. Die Relevanz für das iBlockchain-Projekt ist begründet durch die **notwendige Identifizierung von Firmen zugehörigen Unterinstanzen**, Institutionen und Individuen auf der von uns vorgeschlagenen Marktplattform für IoT-Services und Produkte. Diese soll Informationsasymmetrien vermeiden, die durch große Plattformen (wie beispielsweise Amazon) entstehen.

## Machine-to-Machine Payments

Um dezentrale Machine-2-Machine (M2M) Payments in Smart Factories implementieren und vor allem skalieren zu können, braucht es Payment-Channel-Netzwerke. In Payment-Channel-Netzwerken kann jede Maschine Zahlungen senden, empfangen und weiterleiten. Sobald eine Maschine Zahlungen weiterleitet, wird sie zum *M2M-Payment-Hub*. Um für die produzierenden Unternehmen für Rechtssicherheit zu sorgen, gilt es offene Fragen zu beantworten. Zum Thema **Wertpapieraufsicht** muss klargestellt werden, welche Token oder Token-Arten als **"Finanzinstrumente" nach WpHG und MiFiD II** gelten. Im Bereich der **Bankenaufsicht** gelten laut BaFin derzeit die meisten Token als **Rechnungseinheiten** und daher als Finanzinstrument nach KWG. Es muss definiert werden, welche Konsequenzen dies für Unternehmen hat, die M2M-Payment-Hubs als

technische Infrastruktur betreiben. Des Weiteren muss geklärt werden, inwieweit diese Unternehmen beim Betrieb der Hubs vom Thema **Geldwäschebekämpfung** betroffen sind.

## Second-Layer-Lösungen und Off-Chain-Kanäle

Als Second-Layer-Lösungen werden im allgemeinen Lösungen bezeichnet, die auf bestehenden Blockainsystemen aufsetzen und deren Funktionalität erweitern, wie beispielsweise Off-Chain-Kanäle zur Lösung der Skalierbarkeitsproblematik (s.u.). Allerdings gehen diese Methoden Umwege, deren rechtliche Validität gesichert sein sollte. Eine **rechtliche Einordnung von Off-Chain-Protokollen**, sowie der Exekution von Smart Contracts in diesen sollte nicht aus der Regulierung von Blockchain- und DLT-Systemen ausgeklammert werden. Somit können bereits beim Design solcher Second-Layer-Lösungen rechtliche Anforderungen Berücksichtigung finden.

## Datenschutz

Blockchain-Technologie bietet verschiedene Techniken, um Pseudonymität zu erreichen. Um beurteilen zu können, welcher rechtliche Rahmen für die Datenverarbeitung anwendbar ist, wird eine **technische Anonymisierungsschwelle benötigt**, um zwischen persönlichen und nicht-persönlichen Daten unterscheiden zu können. Hierfür wäre eine technische Definition hilfreich. Zweitens widerspricht die Architektur von Blockchains in der Regel dem Datenschutz-Grundprinzip der **Änderbarkeit und Löschung von Daten**. Es besteht Klärungsbedarf, auf welche Weise (oder ob) die Löschung durchgeführt werden muss, um beispielsweise mit dem GDPR (entspricht der DSGVO) konform zu sein. Außerdem gehen diese Gesetze davon aus, dass jeder personenbezogene Datenpunkt mindestens mit einer natürlichen oder juristischen Person verbunden ist, was sicherstellt, dass die Betroffenen ihre jeweiligen Rechte nach dem EU-Datenschutzrecht durchsetzen können. Da Blockchain-basierte Lösungen in der Regel einem dezentralen Ansatz folgen, ist die **Identifizierung eines Verantwortlichen (Datenschutzbeauftragter)** unter den Betreibern von Nodes und damit die Zuordnung von Verantwortung für die Nutzer in einem solchen Netzwerk **kaum möglich**. Für Unternehmen, die Privatpersonen Zugang zu Blockchain-Lösungen geben besteht eine Unsicherheit inwieweit sie für die Daten auf der Blockchain verantwortlich sind, auf die sie keinen oder nur sehr begrenzten Zugriff haben.

## Digitaler Euro als einheitliche Währungslösung

Ein Blockchain-basierter digitaler Euro kann **Euro-notierte Smart Contracts** ermöglichen, sodass Maschinen, Autos, Sensoren, etc. direkt Pay-per-Use, Leasing, Factoring und vieles mehr anbieten können. Auch der Kauf und Verkauf von Vermögenswerten, wie Immobilien oder Kunstgegenständen, und Wertpapieren wird durch einen digitalen Euro wesentlich effizienter. Im Einzelnen ist ein **digitaler Euro das präferierte Finanzinstrument europäischer Firmen**. Der digitale Euro kann innovative Projekte legitimieren, da ein beliebtes, weit verbreitetes Zahlungsmittel verwendet werden kann und kein Token mit begrenzter Akzeptanz genutzt werden muss. Ebenso kann bei geeigneter technischer Implementierung in der Industrie ein **Konversionsschritt zwischen digitaler Währung und verfügbarer Liquidität gespart** werden.

Mit der Aufnahme der Vision eines solchen digitalen Euro in die Blockchain-Strategie der

Bundesregierung und der Förderung eines digitalen Euro durch den Bundesverband deutscher Banken (BdB) ist dieses Thema in die breite Öffentlichkeit gelangt. **Es können nun rechtliche Rahmenrichtlinien definiert werden, die die Reichweite der Nutzung eines digitalen Euros beschreiben, sodass eine Einführung von digitalem Zentralbankgeld (CBDC) auf europäischer Ebene eingeleitet werden kann.**

## Blockchain als Beweis vor Gericht

Der Einsatz eines Blockchain-Systems kann die **Arbeitsbelastung der Justizsysteme verringern**, indem es harte und neutrale Beweise liefert. In Deutschland kann dies bereits angewendet werden, durch beispielsweise Berufung auf die Definition eines Kryptowertpapierregisters (Abschnitt 3, §16 (1), eWpG) oder durch gute Argumentation eines technisch bewanderten Anwalts. Der Rechtsapparat ist also theoretisch bereits in der Lage, dieses Instrument zu nutzen. Um sich vor jedem Richter durchsetzen zu können, kann die Politik jedoch dazu beitragen, **dass das technische Verständnis des Justizsystems geschult wird und die Beweisfähigkeit einer Blockchain akzeptiert**.

# Technologische Herausforderungen und Lösungen

Im Folgenden werden aktuelle technische Herausforderungen und eine kurze Antwort aus Forschungsergebnissen bereitgestellt.

## Skalierbarkeit und Nachhaltigkeit

Die größten technologischen Herausforderungen und ebenso die Hauptkritikpunkte, die regelmäßig ins Feld geführt werden, sind die **schlechte Skalierbarkeit und der enorme Energieverbrauch** der Blockchain-Technologie. So verbrauchen derzeitige Blockchain-Systeme wie Ethereum und Bitcoin Unmengen an Energie (das Bitcoin Netzwerk hat einen Energieverbrauch vergleichbar mit Tschechien) und ihre Transaktionsdurchsatz und Verarbeitungsgeschwindigkeit ist beschränkt auf wenige Transaktionen pro Sekunde.

Die Probleme der Skalierbarkeit und Nachhaltigkeit werden im Projekt iBlockchain unter **Einsatz von Off-Chain-Technologien** adressiert. Dadurch kann die **große Menge an Transaktionen** außerhalb der Blockchain in einem Second-Layer-Netzwerk verarbeitet werden, wodurch die Effizienz der **Transaktionsverarbeitung drastisch gesteigert** werden kann. Im iBlockchain-Projekt werden unter anderem die **Perun und Raiden** Off-Chain-Technologien entwickelt und eingesetzt. Ein dazu komplementärer Ansatz sind **Proof-of-Stake-Systeme**. Diese ersetzen das kostspielige „Proof-of-Work“ Verfahren aus klassischen Kryptowährungen wie Bitcoin und Ethereum und können den Energieverbrauch in Blockchain-Systemen signifikant reduzieren. Ein weiterer Ansatz, der insbesondere im Industrieumfeld zum Einsatz kommt, sind **permissioned Blockchains**. Diese verzichten vollständig auf Proof-of-Works und bieten nachhaltige Lösungen im Industrieumfeld an.

## Sicherheit

Die Sicherheit von Blockchain-basierten Anwendungen ist von zentraler Bedeutung. Bisherige Erfahrungen mit der Technologie haben gezeigt, dass **kleinste Fehler** in der Konzeption **großen Schaden verursachen** können. Die **hohe Komplexität und die Vielzahl der Angriffsvektoren** wie etwa die eingesetzte Hardware, die zugrundeliegende

Blockchain-Infrastruktur, oder darauf aufbauenden Walletsysteme und Second-Layer-Anwendungen stellen dabei eine besondere Herausforderung dar. Die vollautomatische und autonome Ausführung ganzer Geschäftsprozesse mittels Smart Contracts rückt insbesondere auch die Sicherheit selbiger in den Vordergrund.

Im iBlockchain-Projekt wird dieser Herausforderung mit einer **kritischen und transparenten wissenschaftlichen Sicherheitsanalyse** begegnet. Die eingesetzten und im Projekt entwickelten kryptographischen Bausteine, Protokolle, Anwendungen und eingebundenen Hardwarekomponenten werden nach gängigen **wissenschaftlichen Methoden evaluiert und deren Sicherheit analysiert**. Um der hohen Komplexität von Smart Contracts gerecht zu werden, kommen für deren Sicherheitsanalyse **spezialisierten Analysetools** zum Einsatz, die selbst im Projekt entwickelt werden. Gleichzeitig erfordert die fortschreitende Entwicklung der Blockchain-Technologie eine kontinuierliche Weiterentwicklung und Verfeinerung der zur Verfügung stehenden Analysemethoden und Tools.

## Sichere Anbindung und Identifizierung/Legitimierung von Maschinen

Im I4.0 Umfeld ist die sichere Anbindung von Maschinen und Sensoren und damit die **Verknüpfung von Geräten und Informationen mit den virtuellen Blockchain-Anwendungen** eine Grundvoraussetzung für die autonome Ausführung von Geschäftsprozessen. Dazu kommt die Herausforderung, die **eingebundenen Komponenten zu identifizieren und legitimieren**.

Im iBlockchain-Projekt wird dieser Aspekt mit der Entwicklung und Einbindung von **Hardware basierten Smart Oracles** adressiert. Im Projekt werden die notwendigen **Schnittstellen und Protokolle** mit besonderem Schwerpunkt auf die IT-Sicherheit entwickelt und die technische Machbarkeit demonstriert. Die Identifizierung von Maschinen wird über die Erstellung einer **Identität für eine Firma** realisiert, die in der Lage ist, **ihren Flotten Sub-Identitäten zu verleihen**, die automatisch durch sie legitimiert sind, sodass der Prozess der Identitätsvergabe effizient bleibt. Folglich ist eine Rückverfolgung einer Maschine im Streitfall zu bewerkstelligen. Die angenommene Praktik sollte, abhängig vom genauen Mechanismus der Identitätsvergabe rechtlich beleuchtet und abgesichert sein.

## Datenschutz und Transparenz

Eine der Stärken von Blockchain-Technologien ist die Transparenz, die diese bieten. So lassen sich sämtliche Transaktionen, die auf einer Blockchain durchgeführt werden, lückenlos nachvollziehen. Dies steht jedoch im Widerspruch zum Ziel des Datenschutzes. **Um den jeweiligen Datenschutzanforderungen gerecht werden zu können, muss dieser Widerspruch technologisch gelöst werden.**

Im iBlockchain-Projekt werden hierfür kryptographische Methoden wie **Zero Knowledge Proofs** untersucht und eingesetzt. Damit kann Konsens über einen Transaktion erzeugt werden, ohne deren Inhalt preis zu geben, was deren Privatheit schützt.

# Fazit

Die Wechselwirkung zwischen regulatorischer Klarheit und technischer Innovationsfähigkeit bestimmt den Fortschritt aufstrebender Technologien. Im Fall der Blockchain-Technologie ist die Gesetzgebung nun gefragt, weiteren Fortschritt in Deutschland als starken Forschungsstandort zu ermöglichen. In dem vorgelegten Artikel schildern die Mitglieder des iBlockchain-Konsortiums regulatorische Hürden für eine breite Anwendung von Blockchain-Technologie und räumen mit technischen Herausforderungen auf, die durch Forschungsergebnisse nachhaltig gelöst werden können.

# Bemerkungen

Dieses Forschungs- und Entwicklungsprojekt wurde vom **Bundesministerium für Bildung und Forschung (BMBF)** unter dem Förderkennzeichen **16KIS0906** gefördert. Für den Inhalt dieser Publikation sind die Autoren (in diesem Fall das gesamte Konsortium) verantwortlich.

Wenn Ihnen dieser Artikel gefällt, würden wir uns freuen, wenn Sie ihn an Ihre Kollegen weiterleiten oder in sozialen Netzwerken weitergeben. Weitere Informationen über iBlockchain finden Sie hier. Über diese Homepage können Sie auch Kontakt zu uns aufnehmen.