

Studienergebnisse 2018/19

Meilenstein 3 für das Projekt

PABlo

Potenziale und Anwendungen der Blockchain Technologie für kleine und mittlere Unternehmen

gefördert vom IFAF Berlin e.V.

koordiniert vom Kompetenzzentrum Angewandte Informatik

Projektlaufzeit: 01.04.2018 bis 31.03.2020

Projektleitung: Prof. Dr. Hölzner

Prof. Dr. Heike M. Hölzner



**Hochschule für Technik
und Wirtschaft Berlin**

University of Applied Sciences

Prof. Dr. Stefan Edlich



BEUTH HOCHSCHULE
FÜR TECHNIK
BERLIN

University of Applied Sciences

Beteiligte Projektpartner:

Emerald Risk Consulting GmbH
Manfred-von-Richthofen-Str. 9
12101 Berlin

Sirius Minds GmbH
Französische Straße 12
10117 Berlin

Bitkom e.V.
Albrechtstraße 10
10117 Berlin

Inhaltsverzeichnis

1. Technologieradar.....	5
1.1 Einleitung	5
1.2 Blockchain-Ökosysteme und Unternehmensanwendungen	5
1.3 Grundlagenforschung, Consensus Algorithmen und Proof of (*)-Strategien	7
1.2 Skalierbarkeit	9
1.3 Mobile Blockchain, Wallets	10
1.4 Blockchain Bridges	10
1.5 Security / Encryption	11
1.6 Web Frameworks / JS support	12
1.7 Blockchain as a Service (BaaS)	13
1.8 Abschließende Bemerkungen	14
2. Technologieszenarien	16
2.1 Decentralized Autonomous Organizations (DAOs)	16
2.2 Self-Sovereign Identity (SSI)	17
2.3 Blockchain as a Service (BaaS)	18
2.4 Stärkerer Bereich zwischen Datenbanken und Blockchain	18
2.5 Blockchain und Data Science	19
2.6 Zusammenfassung weiterer Szenarien	20

EINLEITUNG

Stand 17.09.2019

Eine frühe Identifizierung und Adaption technologischer Neuentwicklungen kann für Unternehmen zu einem starken Marktvorteil gegenüber Wettbewerbern werden. Das Verpassen eines technologischen Fortschritts auf der anderen Seite, kann die Existenz eines Unternehmens bedrohen. Das zeigt das Beispiel Kodak und die Digitalfotografie. Um Potenziale und Risiken zu erkennen, ist ein gewisses Vorstellungsvermögen und die aktive, wie auch systematische Analyse der aktuellen technologischen Entwicklung unabdingbar.

Technologischer Fortschritt verläuft meist nicht linear, sondern exponentiell. Im Bereich der Blockchain-Technologie wird dies anhand der täglich neuerscheinenden Entwicklungen besonders evident. Hieraus ergibt sich das Risiko einer informationstechnologischen Überforderung seitens der Unternehmen, bei gleichzeitiger Relevanz für das eigene Geschäftsmodell.

Die Technologiepotenzialanalyse des Fraunhofer-Instituts für Arbeitswirtschaft und Organisation dient der fachlichen Unterstützung von Produkt- und Dienstleistungsentwicklungen. Sie soll die Erschließung von Potentialen neuer Technologien, sowie ihrer möglichen Anwendungsbereiche systematisch ermöglichen. Unternehmen können so spezielle Technologien analysieren und identifizieren, ob und wie sie diese in ihrem Geschäftsmodell verwenden können und ob die untersuchten Technologien zur Erschließung eines neuen Marktsegments dienen können. Um diese Analyse erschöpfend abzuschließen und die Relevanz der Blockchain-Technologie adäquat einzuordnen, werden im Kapitel 3.1 Technologieanalyse auch signifikante Konkurrenztechnologien vorgestellt, sowie die Felder, in denen bisher das größte Marktinteresse vorzufinden ist. Zu beachten ist, dass das aktive Interesse an der Technologie bisher primär von Start-Ups, Forschungseinrichtungen, sowie großen Unternehmensberatungen ausgeht und KMU noch ausloten müssen, wie sie die Technologie für sich beanspruchen können.

Im darauffolgenden Kapitel Geschäftsmodellmuster werden die gesammelten Erkenntnisse der Kapitel 1-3 auf konkrete Geschäftsmodelle übertragen, um Mechanismen freizulegen, die für KMU von Relevanz sein können.

TEIL 1

TECHNOLOGIERADAR

Stand 17.09.2019

1. Technologieradar

1.1 Einleitung

Ziel des Technologieradars ist es, aufbauend auf Fachpublikationen¹ und eigenen Recherchen, die wichtigsten Bereiche zu identifizieren, in denen sowohl weltweit, als auch in Berlin Forschung und Entwicklung zum Thema Blockchain betrieben wird. Es geht darum, nicht nur Kryptowährungen oder Frameworks aufzulisten, sondern ein möglichst breites Spektrum an Produkten, Dienstleistungen, Einsatzgebieten und Möglichkeiten zu erfassen und gegebenenfalls zu bewerten. Fokus sind hier vor allem Technologien und Entwicklungen, die für kleine und mittelständische Unternehmen von Bedeutung sein können.

1.2 Blockchain-Ökosysteme und Unternehmensanwendungen

Obwohl viele Wirtschaftsmedien und Analysten wie Gartner² oder McKinsey³ Anfang des Jahres das Ende vieler Blockchain-Technologien vorhergesagt haben, wächst seither die Anzahl der Anwendungen, die das Blockchain-Ökosystem weiter stärken. Eine gute Übersicht über den Stand der Ökosysteme (Stand 2018) ist in der folgenden Übersicht zu finden: "The Blockchain ecosystem v3: six months after the hype"⁴. Eine Zusammenfassung über firmenrelevante Blockchains hier⁵.

Ein wichtiges Signal für die Entwicklung der Branche sind auch erfolgreiche Start-ups, die auf etablierten Blockchain-Lösungen aufsetzen. Eines dieser Start-ups ist beispielsweise parity.io. Als erster Dienst kam zu dem Ethereum-Inhouse-Produkt "Geth Client" der "Parity Client" hinzu. Die Anwendungen „Geth Client“ und „Parity Client“ stellen unterschiedliche Client-Software dar, die die Verbindung zu anderen Ethereum Clients bereitstellen können. Doch die Palette der Dienste hat sich stark erweitert und zeigt typisch an, welche Dienste am Markt benötigt werden:

- Client Miner für das Bitcoin Netzwerk
- Eine Plattform für die Konnektivität von Blockchains (Polkadot, Bridge)

¹ "Technology Radar | An opinionated guide" <https://www.thoughtworks.com/radar>. Aufgerufen am 9 Mai. 2019.

² "Blockchain-Hype geht vorbei: Viele Projekte sterben bald ... - WinFuture." 9 Mai. 2019, https://winfuture.de/news_108839.html. Aufgerufen am 13 Mai. 2019.

³ Vgl. Matt Higginson, Marie-Claude Nadeau, and Kausik Rajgopal (2019)., Letzter Zugriff 22.07.2019

⁴ "The Blockchain ecosystem v3: six months after the hype - Blackmoon." 28 Juni. 2018, <https://news.blackmooncrypto.com/the-blockchain-ecosystem-v3-six-months-after-the-hype-ca14e9879001>. Aufgerufen am 13 Mai. 2019.

⁵ "Blockchain für Unternehmen: Ethereum vs. R3 Corda vs. Hyperledger Fabric vs. Quasar (Stellar)" - BTC-Echo." 7 Mai. 2019, <https://www.btc-echo.de/blockchain-fuer-unternehmen-ethereum-vs-r3-corda-vs-hyperledger-fabric-vs-quasar-stellar/>. Aufgerufen am 16 Mai. 2019.

- Custom Blockchain Building Frameworks (Substrate) mit interessanten Eigenschaften für permissions, security, mobile, IoT, networking, etc.
- Ethereum Wallets (Fether & Signer)
- Sichere Verschlüsselung von Informationen via Smart Contract oder direkt auf öffentlichen Blockchains (Secret Store)
- Cross-Platform Tech Stacks (Wasm)
- Proof of Authority Testing für dApps und Smart Contracts (Kovan)
- Java Script Frameworks (light.js)

Auch der Markt für Unternehmensanwendungen wächst stärker, als es Analysten noch Ende 2018 prognostizierten. Erfolgreiche Blockchain-Anwendungen werden in den folgenden Bereichen angewendet:

1. im Bereich der Finanzinstitute oder als Finanzinstrumente⁶
2. im Bereich der Nahrungs- und Genussmittelindustrie⁷
3. im Waste Management ⁸

Eine Übersicht verschiedenster Anwendungsfelder und weiterer Beispiele finden sich u.a. in "Blockchain Success Stories Show Valuable Opportunities"⁹ und "The 10 Most Successful Blockchain Technology Companies In The World"¹⁰

Forbes listet 2018¹¹ bereits über 100 Unternehmen, die in Blockchain investieren und Lösungen aufbauen. Geschätzt würden dafür 2,9 Milliarden US\$ in 2019 und 12,4 Milliarden US\$ in für 2022 gelistet. Dabei geben über 50% der Unternehmen an, auf die öffentliche Blockchain Ethereum zu setzen. Bitcoin hingegen wird unter den Blockchain-Anwendungen als reine Währungs- bzw. Transaktionsmaschine für Geld gesehen. Andere Lösungen sind teilweise nicht quelloffen oder setzen zu sehr auf private oder zentralisierte Anwendungen. Ethereum geht mit der dApp-Programmierbarkeit einen Mittelweg, der zu seiner breiten Adaption beiträgt.¹²

⁶ "Blockchain-Netzwerk wächst um Landesbanken – Helaba ... - BTC-Echo." 26 Apr.. 2019, <https://www.btc-echo.de/blockchain-netzwerk-waechst-um-landesbanken-helaba-und-bayernlb-treten-marco-polo-bei/>. Aufgerufen am 13 Mai. 2019.

⁷ "Im Kampf gegen Schwarzmarkt-Zigaretten: Tabakriese ... - BTC-Echo." 26 Apr.. 2019, <https://www.btc-echo.de/im-kampf-gegen-schwarzmarkt-zigaretten-tabakriese-phillip-morris-setzt-auf-blockchain-loesungen/>. Aufgerufen am 13 Mai. 2019.

⁸ "Smart Waste Management And BlockChain Technology – Hacker Noon." 10 Feb.. 2019, <https://hackernoon.com/smart-waste-management-and-blockchain-technology-887a8a185357>. Aufgerufen am 13 Mai. 2019.

⁹ "Blockchain Success Stories Show Valuable Opportunities - ReadWrite." 5 Feb.. 2019, <https://readwrite.com/2019/02/05/blockchain-success-stories-show-valuable-opportunities/>. Aufgerufen am 13 Mai. 2019.

¹⁰ "The 10 Most Successful Blockchain Technology Companies In The" 27 Dez.. 2018, <https://www.msn.com/en-sg/money/topstories/the-10-most-successful-blockchain-technology-companies-in-the-world/ar-BBRtx1W>. Aufgerufen am 13 Mai. 2019.

¹¹ "Forbes Releases 'Top 50 Billion-Dollar Companies Exploring' 17 Apr.. 2019, <https://media.consensys.net/forbes-releases-top-50-billion-dollar-companies-exploring-blockchain-over-half-are-working-with-d4f9e44f144d>. Aufgerufen am 13 Mai. 2019.

¹² "The State of the Ethereum Network – ConsenSys Media." 1 Juni. 2018, <https://media.consensys.net/the-state-of-the-ethereum-network-949332cb6895>. Aufgerufen am 13 Mai. 2019.

Viele große Konzerne wie beispielsweise Facebook¹³, Adidas¹⁴ etc. planen zudem, eigene Währungen aufzusetzen. Die Anzahl der Start-Ups im Bereich Blockchain und deren Finanzierungsrunden (beispiel Ubirch¹⁵) steigen ebenfalls.

Der Verlauf der Technologiediffusion im Bereich Blockchain ist vergleichbar mit anderen Technologiebereichen, wie z.B. NoSQL, und verläuft unserer Ansicht nach insgesamt typisch für eine Grundlagentechnologie. Obwohl einige Bereiche der Technologie wieder sterben, bleiben Investition in die Entwicklung erfolgreicher Protokolle und Frameworks hoch und der Gesamtfortschritt ist positiv.

1.3 Grundlagenforschung, Consensus Algorithmen und Proof of (*)-Strategien

Grundlagenforschung für Blockchain findet auf vielen Ebenen statt. Eines der größten Probleme von Blockchain-Technologien ist ihre Performance. Anwender schreiben Transaktionen, welche gesammelt werden und dann via Heartbeat in gültige Blöcke verwandelt werden. Bei unzureichender Hardware, Netzwerkleistung oder fehlerhafter Konfiguration in einem Ethereum Client, können selbst einfache Transaktionen via API oder Shell, Minuten dauern. Eines der größten Probleme - wie generell in verteilten Systemen - ist hier der Consensus Algorithmus¹⁶.

Um die Herausforderungen einordnen zu können, sind verschiedene Ebenen zu betrachten. Beispielsweise die grundlegenden Algorithmen, mit denen die in der Blockchain verteilten Partner den gleichen Datenbestand sehen, der in einen Block geschrieben w. Wie bei standverteilten Systemen wird hier auf Algorithmen wie Paxos oder Raft gesetzt¹⁷. Hier gibt es Grundlagenforschung (z.B. Universität Oxford¹⁸), die versucht, zu generalisieren und die Algorithmen durch Differenzierung der Voraussetzungen zu verbessern. Sowohl auf der Softwareseite¹⁹, als auch auf der Hardwareseite - Stichwort Google Spanner²⁰ mit Atomuhren und GPS-Zeit - sind Verbesserungen vorgeschlagen worden. Hier wird es auch von Seiten der Rechenzentren bzw. im Cloud Computing weitere Verbesserungen geben. Auf der

¹³ "Neuromarketing: Mehr Umsatz mit dem richtigen Duft | W&V." 9 März. 2015, https://www.wuv.de/marketing/neuromarketing_mehr_umsatz_mit_dem_richtigen_duft. Aufgerufen am 13 Mai. 2019.

¹⁴ "Adidas Using SAP's Leonardo To Improve Business Processes." <https://blockchainflashnews.com/adidas-blockchain-sap-leonardo/>. Aufgerufen am 13 Mai. 2019.

¹⁵ "ubirch – The Blockchain for Things." <https://ubirch.de/>. Aufgerufen am 13 Mai. 2019.

¹⁶ "Consensus in the Age of Blockchains." 10 Nov.. 2017, <https://arxiv.org/abs/1711.03936>. Aufgerufen am 13 Mai. 2019.

¹⁷ "Paxos & Raft Consensus Protocols: Complete ... - Blockonomi." 14 Nov.. 2018, <https://blockonomi.com/paxos-raft-consensus-protocols/>. Aufgerufen am 9 Mai. 2019.

¹⁸ "Distributed consensus revised - Cambridge Computer Laboratory." <https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-935.pdf>. Aufgerufen am 9 Mai. 2019.

¹⁹ "Managing Critical State: Distributed Consensus for Reliability - Google." <https://landing.google.com/sre/sre-book/chapters/managing-critical-state/> . Aufgerufen am 9 Mai. 2019.

²⁰ "Spanner (database) - Wikipedia." [https://en.wikipedia.org/wiki/Spanner_\(database\)](https://en.wikipedia.org/wiki/Spanner_(database)). Aufgerufen am 9 Mai. 2019.

anderen Seite müssen die Proof of (*) -Verfahren betrachtet werden, was im folgenden Teil geschieht.

Schon früh wurde das Proof of Work-Dilemma offensichtlich. Der Proof of Work-Mechanismus bietet momentan immer noch den sichersten Weg, eine Blockchain unveränderlich zu machen. So scheint es derzeit viel mehr erfolgreiche Angriffe auf private Keys und deren Server zu geben als auf etablierte, Proof of Work-gesicherte Blockchains wie Bitcoin oder Ethereum^{21,22}. Dennoch existieren immer noch genügend 51%-Angriffe²³. Die Sicherheit des Proof of Work-Verfahrens bedingt jedoch einen hohen Energieverbrauch. Das Bitcoin-Netzwerk verbraucht jährlich fast so viel Energie wie die Schweiz²⁴. Der Proof of Work-Mechanismus wird deshalb ab einem gewissen Reife- und Sicherheitsgrad zu einem starken Energiekonsumenten.

Vor diesem Hintergrund wächst der Druck auf viele wichtige Blockchains wie - beispielsweise Ethereum - sich mit dem Basiskonsensus von Proof of Work abzuwenden. Ethereum erprobt daher für die Version 2.0 andere Konsensmechanismen und plant, diese optional einzuführen²⁵. Hier soll beispielsweise eine spezielle Proof of Stake-Architektur aufgebaut werden, die von der Main Chain andere Chains (Beacon & Shard) ableitet, um vertrauliche Execution Engines einzurichten, welche die Blöcke validieren sollen. Dies kann bereits getestet werden, wozu man 3,2 Ether aus dem Görli-Testnet aufwenden muss. Auch hier sieht man, dass Deutschland und insbesondere Berlin eine wichtige Rolle dabei spielen (Beispiel Görli²⁶), Ethereum-basierte Technologien voranzutreiben.

Viele der Proof of-Varianten opfern die Sicherheit durch Rechenzeit daher in abgeschlossenen Netzen mit standard-kryptographischer Sicherheit (z.B. Proof of Authority) oder mehr Zentralisierung (private / permissioned). Auch hier stellt sich zukünftig die Frage, ob beispielsweise Cloud Provider wie Amazon oder andere Institutionen als vertrauenswürdige Ledger auftreten können, um einen Proof of Stake zu vereinfachen. Die Webseite "Bitcoin-Echo" hat einen umfangreichen Überblick über alternative Verfahren erstellt²⁷. Auffallend ist hier die hohe Anzahl der Varianten, die zentralisiert arbeiten oder auf private Netze setzen. Neuere Varianten unterscheiden sich radikal von Proof of Work oder privaten / zentralisierten Varianten:

- DAGs (Directed Acyclic Graphs)

²¹ "10 Blockchain and New Age Security Attacks You Should Know" 22 Jan.. 2019, <https://blogs.arubanetworks.com/solutions/10-blockchain-and-new-age-security-attacks-you-should-know/>. Aufgerufen am 21 Mai. 2019.

²² "Blockchain Attack Vectors: Vulnerabilities of the Most Secure ... - Apriorit." 1 Nov.. 2018, <https://www.apriorit.com/dev-blog/578-blockchain-attack-vectors>. Aufgerufen am 21 Mai. 2019.

²³ "Once hailed as unhackable, blockchains are now getting hacked - MIT" 19 Feb.. 2019, <https://www.technologyreview.com/s/612974/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/>. Aufgerufen am 9 Mai. 2019.

²⁴ "Bitcoin Energy Consumption Index" <https://digiconomist.net/bitcoin-energy-consumption>. Aufgerufen am 9 Mai. 2019.

²⁵ "Ethereum 2.0: Proof of Stake wird im Testnet erprobt | BTC-ECHO." 9 Mai. 2019, <https://www.btc-echo.de/ethereum-2-0-proof-of-stake-wird-im-testnet-erprobt/>. Aufgerufen am 9 Mai. 2019.

²⁶ "Görli Testnet." <https://goerli.net/>. Aufgerufen am 9 Mai. 2019.

²⁷ "ConsensusPedia: An Encyclopedia of 30+ Consensus Algorithms." 2 Juli. 2018, <https://hackernoon.com/consensuspedia-an-encyclopedia-of-29-consensus-algorithms-e9c4b4b7d08f>. Aufgerufen am 9 Mai. 2019.

- Tangle
- HashGraph
- Holochain
- BlockLattice
- Spectre
- ByteBall

Einige von diesen sind bereits weit verbreitet, wie beispielsweise Tangle in IOTA. Andere müssen erst evaluiert und weiter ausgebaut werden. Jedoch ist in diesem Bereich - insbesondere graphbasierte Lösungen - weitere Forschung und Entwicklung zu erwarten.

1.2 Skalierbarkeit

Die Bereiche Verteiltheit / Konsistenz und Sicherheit sind, wie beschrieben, Gründe für die bisher mangelhafte Skalierbarkeit von Blockchain-basierten Lösungen. Paypal selbst schafft 193 Transaktionen und VISA 1667 Transaktionen pro Sekunde. Ethereum bewältigt 20 und Bitcoin gar nur 20 Transaktionen pro Sekunde²⁸ (theoretisch sind alle Protokolle in der Lage, eine größere Menge an Transaktionen durchzuführen). Selbst mit einer großen Blockgröße von mehreren Megabytes und vielen gebündelten Finanztransaktionen ist dies immer noch zu gering. Der limitierende Faktor ist hier die Zeit, um ein Ereignis in einen Block zu schreiben und die Zeit, den Konsensus zu erreichen. Daher ist der Aspekt der Skalierbarkeit für die Industrie, für Start-Ups, aber ebenso für Frameworks und neue Lösungen ein weites Forschungs- und Marktfeld.

Mit ProvenDB²⁹ gibt es beispielsweise eine große Zahl an quasi Blockchain-basierten Lösungen. Diese gehen von etablierten, verteilten Datenbanken aus, und fügen nachträglich Unveränderlichkeit, Verschlüsselung, Beweisbarkeit, Merkle Trees und ähnliches hinzu. Da hier kein Proof of Work-Konsensalgorithmus angewendet wird und MongoDB als schnelle Cache-Datenbank von Anfang an performant konzipiert wurde, kann diese Lösung für Teilbereiche interessant sein. Gleichzeitig gibt es neue Datenbanken wie BigChainDB³⁰, welche versuchen, Blockchain-Funktionalität auf bekannte, skalierbare NoSQL-Datenbanken anzubinden. Hier beginnen einige Firmen und Forschungsansätze, die Grenze zwischen Datenbanken und Blockchain zu verwischen³¹.

Blockchaingeeks³² listen einige Bereiche auf, in denen Verbesserungen möglich sind:

1. Unnötige Daten / Redundanzen entfernen (Segwit)
2. Blockgröße erhöhen

²⁸ "Blockchain Scalability: When, Where, How? - Blockgeeks."
<https://blockgeeks.com/guides/blockchain-scalability/>. Aufgerufen am 13 Mai. 2019.

²⁹ "ProvenDB." <https://provendb.com/>. Aufgerufen am 13 Mai. 2019.

³⁰ "BigchainDB •• The blockchain database.." 16 Mai. 2018, <https://www.bigchaindb.com/>. Aufgerufen am 13 Mai. 2019.

³¹ "Blurring the Lines between Blockchains and Database Systems: the" <https://bigdata.uni-saarland.de/publications/mod485-sharma.pdf>. Aufgerufen am 14 Mai. 2019.

³² <https://blockgeeks.com/guides/blockchain-scalability/> "Blockchain Scalability: When, Where, How? - Blockgeeks."

3. Sharding: Jeder Knoten muss nicht mehr den Gesamtbestand der Daten halten (verringerte Sicherheit). Forschungsbeispiele sind hier zu finden^{33 34}.
4. Andere Proof of (*) -Methoden (Stake)
5. Schnellere Kommunikationskanäle (lightning channel)
6. Layer über Ethereum, der Last von Ethereum auslagert und Ethereum selbst nur noch als Verifikationsmaschine betrachtet (Plasma)

Dies sind Bereiche, in denen ein praktischer Performancegewinn durch Konfiguration, Einschränkungen oder Auslagerung etc. erreicht wird. Dies wird ergänzt durch Basisforschung an Konsensusprotokollen, schnelleren Datenbanken oder Netzwerken.

1.3 Mobile Blockchain, Wallets

Börsen wie Bitcoin.de³⁵ unterscheiden im Bereich Wallets in Desktop-, Hardware-, Mobil- und Web-Wallets.

Besonders interessant ist der mobile Markt. Hier sind die ersten Hardware-/Phone Hersteller aufgesprungen. HTC hat mit dem Exodus³⁶ bereits die zweite Generation an Mobiltelefonen vorgestellt, welche Built-In-Funktionen für Blockchains beinhalten. Konkret handelt es sich um *secure enclaves*, welche nicht von Android aus verwaltet werden können. Interessant ist hier die Möglichkeit, beim Verlust des Gerätes den Masterkey aus Teilkeys von Vertrauenspersonen wieder zusammensetzen zu können.

Wallets auf Mobiltelefonen zu haben, wird zukünftig ein einfacher und vermutlich fester Bestandteil der Standard-Hardware. Wallet-Hardware wie Sticks, die momentan noch den Standard³⁷ darstellen, werden künftig in weitere Geräte und Anwendungen integriert werden.

1.4 Blockchain Bridges

Ein wichtiger Technologiebereich sind die Blockchain-Bridges. Im Wesentlichen sollen hiermit Assets sicher von einer Chain in eine andere übertragen werden. In Zukunft müssen, vor dem Hintergrund des Internet der Dinge und der fortschreitenden Digitalisierung der Industrie, immer mehr Geräte und Datenbanken durch Brücken

³³ "RapidChain: scaling blockchain via full sharding | the morning paper." 7 Dez.. 2018, <https://blog.acolyer.org/2018/12/07/rapidchain-scaling-blockchain-via-full-sharding/>. Aufgerufen am 13 Mai. 2019.

³⁴ "Towards Scaling Blockchain Systems via Sharding - NUS Computing." <https://www.comp.nus.edu.sg/~hungdang/papers/sharding.pdf>. Aufgerufen am 14 Mai. 2019.

³⁵ "Wählen Sie Ihre Wallet - Bitcoin.org." <https://bitcoin.org/de/waehlen-sie-ihre-wallet>. Aufgerufen am 13 Mai. 2019.

³⁶ "Exodus 2: HTC entwickelt neues Blockchain-Smartphone" 4 Mai. 2019, <https://www.notebookcheck.com/Exodus-2-HTC-entwickelt-neues-Blockchain-Smartphone.420108.0.html>. Aufgerufen am 13 Mai. 2019.

³⁷ "Wallets - Buy Bitcoin Worldwide." <https://www.buybitcoinworldwide.com/de/bitcoin-wallets/>. Aufgerufen am 13 Mai. 2019.

verbunden werden. Teils wird bereits vom "the Internet of Blockchains"³⁸ gesprochen. Mit der Parity Bridge wurde bereits eine solche Technologie vorgestellt. Weitere Aktivitäten sind im Gange, dies nicht nur via Software zu lösen, sondern auch Standardisierungen vorzuschlagen.³⁹ Papers zu diesem Bereich wurden z.B. von Adrian Colyer vorgestellt⁴⁰.

1.5 Security / Encryption

Blockchain-Sicherheit ist ein wichtiger Forschungsbereich. Dies zeigt die Vielzahl der Hacks von Coins im vergangenen Jahr. Jedoch spielt Blockchain-Sicherheit auch auf anderen Ebenen eine Rolle. In einem Forschungsbericht von Mazutt et. al⁴¹ wurde gezeigt, dass über 1600 falsche, illegale oder vertrauliche Inhalte auf Bitcoin zu finden sind. Dies sind:

- Allgemeine problematische Inhalte
- Copyright Violations
- Malware
- Privacy Violations (z.B. im Kontext von Erpressungen, aber auch diverse private Keys)
- Politisch bedenkliche Inhalte
- Illegale Inhalte

Die wichtigste Forschung findet jedoch im Bereich der Security von Smart Contracts statt. In der Regel werden hier Ethereum Smart Contracts untersucht. Zankov et al⁴², Marvidou & Laszka⁴³, Kalra et al.⁴⁴ und Demolino et al.⁴⁵ sind hier wichtige Publikationen in dem Bereich, die aufzeigen, wohin die Forschung tendiert. Ein zentraler Bereich ist die formale Verifikation von Smart Contracts.

³⁸ "Cross-Chain Bridges: Paving the Way to Internet of Blockchains." 15 Nov.. 2017, <https://medium.com/poa-network/cross-chain-bridges-paving-the-way-to-internet-of-blockchains-422ac94bc2e5>. Aufgerufen am 13 Mai. 2019.

³⁹ "Blockchain Interoperability Alliance (BIA) - Defining ... - Cryptovest." 11 Feb.. 2018, <https://cryptovest.com/features/blockchain-interoperability-alliance-bia---defining-blockchain-30/>. Aufgerufen am 13 Mai. 2019.

⁴⁰ "Towards a design philosophy for interoperable blockchain systems" 30 Mai. 2018, <https://blog.acolyer.org/2018/05/30/towards-a-design-philosophy-for-interoperable-blockchain-systems/>. Aufgerufen am 13 Mai. 2019.

⁴¹ "A Quantitative Analysis of the Impact of Arbitrary Blockchain Content" <https://fc18.ifca.ai/preproceedings/6.pdf>. Aufgerufen am 13 Mai. 2019.

⁴² "Securify: Practical Security Analysis of Smart Contracts - arXiv." <https://arxiv.org/pdf/1806.01143>. Aufgerufen am 13 Mai. 2019.

⁴³ "Designing secure Ethereum smart contracts: a finite state machine" 20 März. 2018, <https://blog.acolyer.org/2018/03/20/designing-secure-ethereum-smart-contracts-a-finite-state-machine-approach/>. Aufgerufen am 13 Mai. 2019.

⁴⁴ "Zeus: Analyzing safety of smart contracts | the morning paper." 8 März. 2018, <https://blog.acolyer.org/2018/03/08/zeus-analyzing-safety-of-smart-contracts/>. Aufgerufen am 13 Mai. 2019.

⁴⁵ "Step by Step Towards Creating a Safe Smart Contract: Lessons and" 17 Mai. 2015, <https://eprint.iacr.org/2015/460.pdf>. Aufgerufen am 13 Mai. 2019.

Eine Übersicht über alle gelisteten Sicherheitspublikationen im Bereich Bitcoin sind bei Conti et al.⁴⁶ zu finden.

1.6 Web Frameworks / JS support

Bedienbarkeit ist noch immer eine Diffusionshürde der Blockchain. Für die Entwicklung auf Anwenderseite stehen einerseits Ethereum-basierte Lösungen in vorderster Reihe. Und andererseits Basistechnologien wie:

- **geth** als client auch für das Minen und den Transfer von Tokens, die Erstellung von Smart Contracts oder das inspizieren der Block history
- **Mist** Wallet für Smart Contracts und Tokens
- **Solc / Remix** als Compiler für Solidity
- etc.

Für die Web-Client-Entwicklung sind - besonders auch unter JavaScript - die folgenden Technologien / Bibliotheken⁴⁷ *state of the art*:

- **Ganache CLI**: als Blockchain Emulator NodeJS package.
- **Metamask**⁴⁸: Verwaltung von ETH Assets und DApp-Interaktion via Browser Extension.
- **ether.js**⁴⁹, **web3**⁵⁰ **light.js**⁵¹: Ethereum API, Key Management, Wallets, etc. (light.js von parity)
- **truffle**⁵², **embark**⁵³: Entwicklungsumgebung, Pipelines, DApp-Support, Deployment etc.

Eine weitere, interessante Entwicklung ist, Solidity Smart Contracts über einfachere Interfaces zur Verfügung zu stellen. An dieser Stelle werden im Folgenden zwei Ansätze genannt:

1. **iOLite**⁵⁴: Als umfassende Plattform für Nichtprogrammierer mit graphischer Unterstützung / Re-Use von Code und Machine Learning-Unterstützung.
2. **EtherScripter**⁵⁵: Als graphische Oberfläche mit farblichen Codeblöcken.

⁴⁶ "A Survey on Security and Privacy Issues of Bitcoin." 3 Juni. 2017, <https://arxiv.org/abs/1706.00916>. Aufgerufen am 13 Mai. 2019.

⁴⁷ "Popular JavaScript blockchain Projects - Libraries.io."

<https://libraries.io/search?keywords=blockchain&languages=JavaScript>. Aufgerufen am 13 Mai. 2019.

⁴⁸ "MetaMask." <https://metamask.io/>. Aufgerufen am 13 Mai. 2019.

⁴⁹ "GitHub - ethers-io/ethers.js: Complete Ethereum wallet implementation"

<https://github.com/ethers-io/ethers.js/>. Aufgerufen am 13 Mai. 2019.

⁵⁰ "Web3.js - GitHub." <https://github.com/ethereum/web3.js/>. Aufgerufen am 13 Mai. 2019.

⁵¹ "@parity/light.js | Read the Docs." <https://readthedocs.org/projects/paritylightjs/>. Aufgerufen am 13 Mai. 2019.

⁵² "Truffle Suite | Ganache - Truffle Framework." <https://truffleframework.com/ganache>. Aufgerufen am 13 Mai. 2019.

⁵³ "Embark into the Ether. | Embark." <https://embark.status.im/>. Aufgerufen am 13 Mai. 2019.

⁵⁴ "iOLite.io." <https://iolite.io/>. Aufgerufen am 13 Mai. 2019.

⁵⁵ "EtherScripter - Visual smart-contract builder for Ethereum." <https://etherscripter.com/>. Aufgerufen am 13 Mai. 2019.

1.7 Blockchain as a Service (BaaS)

Das Aufsetzen einer privaten Blockchain oder einer Chain mit Konsortialmitgliedern ist nicht trivial. Lösungen wie Ethereum, Lisk, ASCH or RISE sind durchaus schwer zu installieren, einzurichten und zu administrieren. Vor diesem Hintergrund steigt die Anzahl der Dienstleister, die Blockchain as a Service (BaaS) anbieten. Dazu gehören u.a.:

- Amazon AWS
- IBM (Hyperledger) as a Service
- Microsoft Azure Blockchain Workbench
- Hewlett Packard Enterprise R3 (Corda)
- SAP Cloud Platform Blockchain "Leonardo"
- Oracle
- R3 Financial Consortium behind Corda
- BitSE VeChain
- Blocko (South Korea)
- Blockstream
- PayStand
- PeerLedger
- Deloitte Rubix Core
- und viele weitere Lösungen, die noch nicht ausgereift sind: Google Storj, LedgerX, Veen, etc.

Besonders interessant in Bezug auf Marktpräsenz und Zuverlässigkeit sind Amazon AWS Blockchain und kaleido.io.

Amazon ist seit 2018 als Player auf dem Markt und bietet verschiedene Blockchain-Templates an. Alle basieren auf Ethereum und Hyperledger Fabric. Andere Lösungen wie Hyperledger Sawtooth und Corda sollen folgen. Der Anspruch war hier - wie auch bei Kaleido, Blockchain-Lösungen mit folgendem Ansatz in wenigen Minuten aufsetzen zu können: Dies geschieht durch einfaches auswählen von Templates, selektion der Plattform, aufbau des Netzwerkes und anschließend dem deployment der Dapps mit Stat der Knoten.

AWS hat bereits einige bedeutende Kunden wie T-Mobile, Guidewire, AT&T, Nestle oder SGX gewinnen können. Amazon selbst nennt als wesentliche Use-Cases: *supply-chains*, *financial transactions*, *identity and compliance*, *ensurance* und *health management*. Ein entscheidender Vorteil des Amazon-Netzes soll die weitreichende Verteilung sein, welche kleine Latenzzeiten auch weltweit zur Folge hat. AWS bietet hier ebenfalls interessante Partnerservices an. Die "Managed Blockchain" wurde Ende April für produktionsreif erklärt⁵⁶. Microsoft hat mittlerweile nachgezogen⁵⁷.

⁵⁶ "Blockchain für alle: Amazons Managed-Blockchain-Dienst verfügbar ..." 2 Mai. 2019, <https://www.heise.de/developer/meldung/Blockchain-fuer-alle-Amazons-Managed-Blockchain-Dienst-verfuegbar-4411321.html>. Aufgerufen am 13 Mai. 2019.

⁵⁷ "Microsoft launches a fully managed blockchain service | TechCrunch." 2 Mai. 2019, <https://techcrunch.com/2019/05/02/microsoft-launches-a-fully-managed-blockchain-service/>. Aufgerufen am 14 Mai. 2019.

Kaleido.io bietet eine ähnliche Fullstack-Lösung an. Diese kann auf AWS oder der Microsoft Cloud gehostet werden. Es werden weiterhin eine Reihe von eigenen Diensten angeboten wie HD-Wallets, Registries, eth-connect, Ethereum mainnet tether und auch viele nützliche Services von Drittanbietern.

1.8 Abschließende Bemerkungen

Es gibt eine weitere Vielzahl an wichtigen Bereichen, die in einem Technologieradar beobachtet werden müssen, jedoch hier nur am Rande erwähnt werden können:

- **Blockchain und Data Science/Machine Learning:** Hier sind interessante Protokolle in der Entstehung, wie z.B. das Ocean Protocol⁵⁸, welches nachhaltig dazu beitragen könnte dass Anbieter und Vermittler von Daten sicher kommunizieren und Assets austauschen können.
- **Blockchain und IoT:** Obwohl hier bei der ersten Betrachtung die Skalierbarkeit im Wege steht, sind einige Start-Ups erfolgreich am Markt tätig und beeinflussen diesen Bereich radikal. Mit IOTA steht ein Unternehmen am Markt, das bereits von vielen großen Konzernen unterstützt wird. Andere Firmen wie Ubirch wurden in diesem Bericht bereits erwähnt.
- **Blockchain DAOs:** Einer der interessantesten Bereiche sind Decentralized Autonomous Organizations (DAOs). Dabei handelt es sich um organisationsähnliche Gebilde, die in der Gesellschaft und im Staat agieren können. Dies können beispielsweise Firmen, staatliche Organisationsstrukturen oder sogar ganze Staaten sein, die mit Hilfe von Smart Contracts arbeiten und mit dezidierten Schnittstellen mit der Außenwelt kommunizieren⁵⁹ Hier wird es weiterhin interessant sein zu beobachten, wie derartige Gebilde in unsere Welt Einzug halten und wie Start-Ups dies aufgreifen werden, um neue Strukturen zu erschaffen.

⁵⁸ "Ocean Protocol — A Decentralized Data Exchange Protocol to Unlock"
<https://oceanprotocol.com/>. Aufgerufen am 13 Mai. 2019.

⁵⁹ "What is DAO - Decentralized Autonomous Organizations." <https://blockchainhub.net/dao-decentralized-autonomous-organization/>. Aufgerufen am 13 Mai. 2019. "Was ist eine DAO (Dezentrale Autonome ... - Blockchainwelt." 21 Nov.. 2018, <https://blockchainwelt.de/dao-dezentrale-autonome-organisation-was-ist-das/>. Aufgerufen am 13 Mai. 2019.

TEIL 2

TECHNOLOGIESZENARIEN

Stand: 17.09.2019

2. Technologieszenarien

Mit der Szenariotechnik sollen potenzielle zukünftige Entwicklungen antizipiert und daraus Handlungsmöglichkeiten abgeleitet werden. Dabei können je nach Ausgangsfragestellung unterschiedliche Betrachtungsebenen festgelegt werden, die entsprechende Zukunftsbilder von Märkten und Branchen, Unternehmen oder einzelnen Produkten abbilden. Konkret wird versucht, folgende Fragestellungen zu beantworten:

1. Wo sind Durchbrüche oder Auswirkungen im Bereich Blockchain zu erwarten?
2. Wie werden diese aussehen?

Aufgrund der Tatsache, dass sich die Blockchain noch immer in einem sehr frühen Entwicklungsstadium befindet, sind Vorhersagen zur Zukunft von Technologien jedoch mit hoher Unsicherheit verbunden. Im Folgenden findet eine Zusammenfassung und Bewertung einschlägiger Expertenmeinungen, darunter Autoren, Unternehmen und Analysten vor dem Hintergrund der Relevanz für KMU statt.^{60,61,62,63,64}

2.1 Decentralized Autonomous Organizations (DAOs)

DAOs stehen für Dezentralisierte Autonome Organisationen, die i.d.R. auf Blockchain-Basis konzipiert wurden. Mike Hearn, einer der Bitcoin-Pioniere, hat diese Idee früh formuliert und darauf hingewiesen, dass führungslose Organisationen quasi wie Lebewesen agieren und handeln können. Wenn Bitcoin vermittelnde Einheiten wie Banken, Notare, etc. ausschalten könne, dann können ganze Unternehmen oder Staaten von einem hierarchielosen DAO-System profitieren. Dies hat gleichzeitig Sicherheitsbedenken hervorgebracht, da diese neuen Systeme jedoch nicht mehr so einfach gestoppt werden können.

Interessanterweise sind viele dieser Prinzipien in Entwicklungs- und Schwellenländern einfacher und sinnvoller zu implementieren als in Industrieländern, da das Vertrauen in IT und Algorithmen dort höher sein kann, als in lokale Mittelsmänner.

⁶⁰ "Blockchain for Good - The Hague Security Delta."

https://www.thehaguesecuritydelta.com/media/com_hsd/report/220/document/Visiedocument-brochure-Blockchain-For-Good-A4-ENGELS-WEB-031218.pdf. Aufgerufen am 7 Juni. 2019.

⁶¹ "Infographic: How the Blockchain is Powering Our Future." 6 Sept.. 2018,

<https://www.visualcapitalist.com/blockchain-powering-future/>. Aufgerufen am 7 Juni. 2019.

⁶² "The Future of Blockchain Technology: Top Five ... - Blockchain Expo." 11 Okt. 2018,

<https://www.blockchain-expo.com/2018/10/blockchain/future-of-blockchain-technology/>.

Aufgerufen am 7 Juni. 2019.

⁶³ "The Future of Blockchain Technology: Top Five ... - Blockchain Expo." 11 Okt. 2018,

<https://www.blockchain-expo.com/2018/10/blockchain/future-of-blockchain-technology/>.

Aufgerufen am 7 Juni. 2019.

⁶⁴ "The 4 Phases of the Gartner Blockchain Spectrum - Smarter With Gartner." 22 Jan. 2019,

<https://www.gartner.com/smarterwithgartner/the-4-phases-of-the-gartner-blockchain-spectrum/>.

Aufgerufen am 7 Juni. 2019.

Dass aber auch Staaten mit ausgeprägter Digitalisierungskompetenz von der Idee der DAO's profitieren können, zeigt beispielsweise das *Estonia Virtual Citizenship*⁶⁵. Estland bietet eine e-residency⁶⁶ an, die es in Minuten erlaubt, ein estonia e-Bürger zu werden und die Vorteile dieses Programms zu nutzen.

Auch Firmen können die Vorteile von Kryptowährungen nutzen, um transparentere, sichere und günstige Organisationsprozesse, interne- und externe, sowie Interaktions- und Handelsprozesse zu gestalten.

2.2 Self-Sovereign Identity (SSI)

Definition: *"Self-Sovereign Identity (SSI) - A self-sovereign identity (SSI) is the driving force for a supple interaction in the online economy with a direct impact on the physical world."*⁶⁷

Der Begriff "Self-Sovereign Identity (SSI) geht auf ein Manifest von Christopher Allen⁶⁸ aus dem Jahr 2016 zurück. Zentraler Aspekt einer SSI ist die Kontrolle über die eigene digitale Identität und Verwaltung von persönlichen Daten. Dies ist zwar auch ohne eine Blockchain möglich, jedoch bietet die Technologie hier einige Vorteile ⁶⁹.

Kernidee ist das Speichern von öffentlichen Schlüsseln in Blockchains, die über einen URL-ähnlichen Identifier (DID) auffindbar sind. Jeder, der diese URL-ähnliche DID besitzt, kann damit Dokumente signieren und andere können dies verifizieren. Hier sind bereits Standards in Arbeit, wie beispielsweise die von der *Decentralized Identity Foundation* (DIF), die DIDs (Decentralized Identifier), DKMS (Decentralized Key Management System), DID Auth und Verifiable Credentials (W3C Working Group). Dazu passend existieren verschiedene Proof of (*) -Konzepte, die den Einsatz dieser SSI-Systeme untersuchen, wie z.B. das VON-Projekt, Trust-Net, Alastria, Illinois Blockchain Initiative, Blockchain on the Move, oder auch eine schweizer Lösung mit dem eID-System in der Stadt Zug.

SSI's können als Treiber für zahlreiche Geschäftsmodellinnovationen betrachtet werden. Sobald es möglich sein wird, sicher und dennoch anonym Services zu nutzen, entstehen z.a. im Bereich der Sharing-Economy neue Anwendungsfelder. Jedoch sind in diesem Bereich in naher Zukunft keine sprunghaften Durchbrüche und auch kein Ersatz staatlicher oder privater Identitätsverfahren (siehe PostIdent) zu erwarten. Möglich ist, dass sich, wie bei DAOs durchaus Parallelwelten in Form von Dienst Anbietern oder freien Plattformen entwickeln werden, die als Konkurrenz zu den etablierten Playern stehen. Es bleibt dann den Nutzern selbst überlassen, zu welchem Grade sie welcher SSI-Plattform

⁶⁵ "What is e-Residency | How to Start an EU Company Online." <https://e-resident.gov.ee/>. Aufgerufen am 7 Juni. 2019.

⁶⁶ "e-Residency of Estonia - Wikipedia." https://en.wikipedia.org/wiki/E-Residency_of_Estonia. Aufgerufen am 7 Juni. 2019.

⁶⁷ "Self-Sovereign Identity (SSI) - Dutch Blockchain Coalition." 6 Dez.. 2018, <https://dutchblockchaincoalition.org/en/usecases/self-sovereign-identity-ssi>. Aufgerufen am 21 Juni. 2019.

⁶⁸ "The Path to Self-Sovereign Identity - Life With Alacrity." 25 Apr.. 2016, <http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html>. Aufgerufen am 7 Juni. 2019.

⁶⁹ "Self-sovereign Identity - Jolocom." 23 Okt.. 2018, <https://jolocom.io/wp-content/uploads/2018/10/Self-sovereign-Identity--Blockchain-Bundesverband-2018.pdf>. Aufgerufen am 7 Juni. 2019.

vertrauen und diese einbinden. Hier sind ebenfalls Start-Ups gefordert, an Lösungen zu arbeiten und Unternehmen aufgerufen, das Ökosystem zu beobachten und gegebenenfalls zu integrieren.

2.3 Blockchain as a Service (BaaS)

Der Bereich Blockchain as a Service für Unternehmensanwendungen wird weiterhin an Fahrt gewinnen und in den nächsten 5 Jahren etwa 20 globale Player hervorbringen, die man als produktionsbereit bezeichnen kann. Gemeint sind hier programmierbare Anwendungslösungen, wie sie für Konsortialchains benötigt werden und keine Payment Lösungen wie Blockstream, die noch zahlreicher sind.

Neben den großen Playern wie Amazon AWS (auf Ethereum und Hyperledger), IBM, Microsoft Azure und SAP Leonardo (und evtl. auch Intel, HP, Oracle und RedHat) wird es weitere kleine Anbieter geben, die produktionsreife Lösungen haben. Hinzukommen werden Anbieter wie beispielsweise:

- R3 Corda-Anbieter
- Kaleido.io (Zusammenarbeit mit Microsoft)
- Deloitte Rubix.core
- Blockapps

Viele von diesen haben noch keine Produktionsreife (Stand Anfang 2019). Bis 2023 sind jedoch zwanzig produktionsreife BaaS-Dienste zu erwarten.

2.4 Stärkerer Bereich zwischen Datenbanken und Blockchain

In dem Bereich zwischen Datenbanken und Blockchain werden neue Lösungen entstehen, welche sich auf folgende Aspekte beziehen:

1. die Eigenschaften der Datenbank
2. neue Ansätze für Blockchain Performance auf Datenbanken

Ein treffendes Beispiel für den ersten Bereich ist Amazons Quantum Ledger Database (QLDB)⁷⁰. Diese Datenbank spiegelt ein unveränderliches Zeitprotokoll aller gespeicherten Daten ab (ähnlich wie Event Sourcing) und basiert auf einer vertrauenswürdigen Instanz, die die Historie der Änderungen protokolliert. Dies lässt sich alles ebenfalls in relationalen Datenbanken nachimplementieren, ist meist jedoch aufwändiger. Von dieser Klasse von Datenbanken werden in einigen Jahren noch mehrere entstehen, die ebenfalls autoscaling realisieren. Dieser Bereich ist vor allen für Firmen interessant, die eine hohe Dokumentationspflicht haben (wie z.B. CMS-Anbieter) und bisher auf CD-ROM Anbieter setzen mussten; bei denen aber gleichzeitig die Hürde für Blockchain entweder zu aufwändig war oder diese rechtlich noch nicht zulässig war. Wenn es hier neben Amazon auch regionale Anbieter geben wird, können rechtliche und

⁷⁰ "Amazon QLDB - Amazon Web Services." <https://aws.amazon.com/de/qldb/>. Aufgerufen am 12 Juni. 2019.

staatliche Hürden angepasst werden und dieser Bereich kann von mehr Firmen genutzt werden.

Der zweite Bereich versucht die klassische, schnelle Datenbanktechnologie um NoSQL und NewSQL zu nutzen. Das Ziel ist hierbei einige klassische Merkmale der Blockchain wie PoW, Sicherheitsaspekte oder Verteilung zu opfern, um performantere Blockchains zu entwickeln. Beispiele finden sich bei zksystems.io, ProvenDB und BigchainDB. Weitere werden folgen.

2.5 Blockchain und Data Science

Der Bereich Blockchain und Data Science wird immer interessanter, zudem hier auch Unternehmen aus Berlin aktiv sind. An bekanntesten ist das Ocean Protokoll⁷¹, welches eine dezentrale Plattform zum Austausch von Daten ist, die auf Blockchain basiert und eine unterliegende Währung hat⁷². Die Roadmap⁷³ sieht wie folgt aus:

- April 2019 V1 Beta (Tethys), Project Manta Ray (a data science workflow powered by OP)
- V2 (2019 later or 2020) - Proof of Authority Network, Initial PoA network governance enabling contract update prioritization and upgrades and network optimization, Token migration from ETH Mainnet to Ocean PoA.
- V3 (TBD) - Verification and Validation of conditions and service, Web3.0 integration
- V4 (TBD) - Bounties on-chain, Clan governance (enable marketplace specific governance)
- V5 (TBD) - Fully permission-less Ocean Protocol

Interessant ist hier, dass die Ocean selbst noch einen tragenden Leuchtturm Use-Case benötigt und die Verwendung von Ocean Endpoints, Storage und die Ocean Nutzung so effizient und einfach sein wird, wie es Jupyter Notebooks bereits sind.

Ein Beispiel dessen ist das genannte Projekt Manta Ray. Entwickler können aus ihren skalierbaren Jupyter Notebooks heraus direkt und einfach das Ocean Protocol nutzen, um auf alle Daten zuzugreifen, auf die sie Zugriff haben⁷⁴.

Dies hat weitreichende Auswirkungen auf die Datenhoheit. In einigen Jahren könnten dann Unternehmen schon in der Lage zu sein, Ihre Daten nicht mehr lokal zu halten, sondern in den Datenspeichern, die mit dem Ocean Protokoll verknüpft sind / erreichbar sind. Dies würde es ermöglichen, dynamisch zu entscheiden, welche Daten monetarisiert werden sollen und welche nur vom Unternehmen genutzt werden. Dies

⁷¹ "Ocean Protocol — A Decentralized Data Exchange Protocol to Unlock"
<https://oceanprotocol.com/>. Aufgerufen am 12 Juni. 2019.

⁷² "Ocean Protocol (OCEAN) price, marketcap, chart, and ... - CoinGecko."
<https://www.coingecko.com/en/coins/ocean-protocol>. Aufgerufen am 12 Juni. 2019.

⁷³ "The Ocean Protocol — Ocean Protocol." <https://oceanprotocol.com/protocol/>. Aufgerufen am 12 Juni. 2019.

⁷⁴ "Project Manta Ray — Data Science powered by Ocean Protocol." 19 Dez.. 2018,
<https://blog.oceanprotocol.com/project-manta-ray-data-science-powered-by-ocean-protocol-535c54089b0f>. Aufgerufen am 12 Juni. 2019.

kann auch als Angriff auf zentrale Datenmarktplätze verstanden werden, welche dabei helfen, Daten zu monetarisieren.

Das bedeutet im Umkehrschluss jedoch nicht, dass Nischen-Marktplätze wie IOTA, Data Market oder Datapace ihre Bedeutung verlieren, sondern Datensilos ihre Bedeutung verlieren.

2.6 Zusammenfassung weiterer Szenarien

- Die **programmierbare Blockchain** wird im Bereich der Business-Anwendungen und des "nicht"-Krypto-Bereiches weiter dominieren. Anwendungslogik in, oder nahe an die Blockchain zu verlagern, wie es bei Ethereum / Solidity nötig ist, wird weiter und noch stärker die Basis für Blockchain Apps / DAOs bilden.
- **Wallets** werden in 5 Jahren allgegenwärtig sein und genutzt werden und einen weiteren Schub für Parallelwährungen und Coins / Tokens für Großunternehmen aller Art werden. Entsprechende Großkonzerne wie Facebook, Adidas, Netflix und Tron werden davon profitieren. Die meisten Smartphones werden sichere Wallets "on board" haben und eine Vielzahl von Währungen unterstützen, so wie dies jetzt bereits schon bei einigen HTC Produkten oder dem Samsung Galaxy S10 der Fall ist.
- Die Zahl der **spezialisierten Blockchains** und Kryptochains wird weiter zunehmen und sich in Bereichen etablieren, wie dies jetzt schon im IoT- Bereich sichtbar ist. Wir sehen hier die Bereiche Digital Identity, Healthcare, Music/TV/Film und Automobil als einige Beispiele, die hier Vorreiter sein werden.
- Der Bereich **Proof of Work** wird bei den großen Playern hoffentlich aus Umweltschutzgründen an Bedeutung verlieren, sich aber nicht ausschalten lassen. Daher verbleibt es den Nutzern zu entscheiden, ob auf die relativ sichere Methode des Konsensalgorithmus mit PoW oder klimaverträglichere Varianten gesetzt wird.
- Im Bereich **Blockchain-Ausbildung** ist ebenfalls viel Bewegung zu erwarten. Wo sich heute fast ausschließlich private Unternehmen um die Blockchain- Ausbildung mit Kursen kümmern oder Blockchain-MOOCs⁷⁵ verfügbar sind, werden auch staatliche Anbieter langsam aufspringen und Bachelor- und Masterstudiengänge anbieten. Bisher ist in Deutschland lediglich die Hochschule Mittweida Vorreiter und bietet den Studiengang "Blockchain & Distributed Ledger Technologies" an⁷⁶. Andere Universitäten verpacken Blockchain in allgemeineren Studiengängen wie Business Management. Da der Bedarf an Ingenieuren in dem Bereich aber hoch ist und die

⁷⁵ "Blockchain Courses | Coursera." <https://www.coursera.org/courses?query=blockchain>. Aufgerufen am 12 Juni. 2019.

⁷⁶ "Blockchain & Distributed Ledger Technologies (DLT) - Fakultät" <https://www.cb.hs-mittweida.de/studienangebote-der-fakultaet/blockchain-distributed-ledger-technologies-dlt.html>. Aufgerufen am 12 Juni. 2019.

Anforderungen bekannt sind⁷⁷, rechnen wir in den nächsten 5 Jahren mit zahlreichen neuen Studiengängen.

Weitere Use Case Referenzen, die in die Zukunft weisen

1. AdTech - To minimize Ad fraud. (Example: Toyota [partnered](#) with the blockchain startup [Lucidity](#) to minimize the ad fraud.)
2. 20 Blockchain Use Cases for 2018 You Should Know [[hackernoon](#)]
3. Inside the Jordan refugee camp that runs on blockchain [[techreview](#)]
4. Food Safety - Testing blockchain for food products [[ripe.io](#)]
5. Automated Device - Automated drone delivery on the blockchain [[coindesk](#)]
6. Bosch Nexo Case Study - Blockchain Powered Nutrunner [[medium](#)]
7. Bosch Rexroth CytroBox Case Study: Machine-as-a-Service [[medium](#)]
8. Dutch Blockchain for Good - the vision and mission [[PDF Report](#)]

⁷⁷ "What Skills Do You Need to Become a Blockchain Engineer? - Dataflog." 6 Juni. 2019, <https://dataflog.com/read/skills-need-become-blockchain-engineer/6456>. Aufgerufen am 12 Juni. 2019.