dena
Deutsche Energie-Agentur

Future Energy Lab

ANALYSE

Quantentechnologien für die Energiewende

Welche Chancen und Potenziale ergeben sich für die Energiewirtschaft?

Impressum

Herausgeber
Deutsche Energie-Agentur GmbH (dena)
Chausseestraße 128 a
10115 Berlin
Tel.: +49 (0)30 66 777-0
Fax: +49 (0)30 66 777-699
E-Mail: info@dena.de
Internet: www.dena.de

Autorinnen und Autoren:
Mathias Böswetter, dena
Malena Eder, dena
Jasmin Wagner, dena

Stand:
11/2022

Bitte zitieren als:

Deutsche Energie-Agentur (Hrsg.) (dena, 2022): Quantentechnologien für die Energiewende: Welche Chancen und Potenziale ergeben sich für die Energiewirtschaft?

Bundesministerium für Wirtschaft und Klimaschutz

Die Veröffentlichung dieser Publikation erfolgt im Auftrag des Bundesministeriums für Wirtschaft und Klimaschutz. Die Deutsche Energie-Agentur GmbH (dena) unterstützt die Bundesregierung in verschiedenen Projekten zur Umsetzung der energie- und klimapolitischen Ziele im Rahmen der Energiewende.

Inhalt

Zusammenfassung

Quantentechnologien werden einen großen Einfluss darauf haben, wie wir in Zukunft komplexe Systeme verwalten und schützen werden. Diese von der Deutschen Energie-Agentur (dena) im Auftrag des Ministeriums für Wirtschaft und Klimaschutz verfasste Analyse bietet einen ersten Ansatz, die Auswirkungen der Quantentechnologien auf die Energiewende und kritische Energieinfrastrukturen abzuschätzen und einzuordnen.

Mittel- bis langfristig gesehen haben Quantencomputing und Quantenkommunikation das Potenzial, bestimmte Bereiche und Anwendungsfälle im Energiesektor grundlegend zu verändern. Diese reichen von der Modellierung und Planung der Integration von Millionen neuer Anlagen mithilfe von Quantencomputing bis hin zur abhörsicheren Kommunikation für hochkritische Energieinfrastrukturen über Quantenkommunikation.

Allerdings werden Quantentechnologien die konventionellen Ansätze für die Datenverarbeitung und Kommunikation nicht in kurzer Zeit ersetzen. **Statt eines disruptiven und plötzlichen Paradigmenwechsels ist es wahrscheinlicher, dass Quantentechnologien parallel zu Nicht-Quantentechnologien eingesetzt werden** und sogar die Weiterentwicklung von Nicht-Quantenlösungen wie Algorithmen für konventionelles Rechnen beeinflussen und fördern.

Eine inkrementelle und hybride Umsetzung von Quantentechnologien könnte insbesondere im Energiesektor wahrscheinlich sein. Im Falle Deutschlands ist dies auf den stark regulierten und kleinteiligen Energiesektor und die langen Amortisationszeiten für IKT-Investitionen zurückzuführen. Wichtig ist somit, bereits bei aktuellen Projekten auf die Möglichkeit von Schnittstellen zwischen den Technologien zu achten.

Kurzfristig gesehen sollte die Post-Quanten-Kryptografie bereits ein wichtiges Anliegen des Energiesektors und der Regulierungsbehörden sein. Denn einerseits könnten Daten bereits jetzt abgefangen und erst später entschlüsselt werden, wenn die erforderliche Technologie verfügbar ist. Andererseits könnten geopolitische und wirtschaftliche Vorteile durch das Erreichen einer Vorreiterrolle im Bereich der **kryptografischen Verfahren** erzielt werden.

Im Zuge der obigen Ausführungen sollten in Zukunft folgende Schwerpunkte zur weiteren Forschung, Erprobung und Implementierung der Quantentechnologien in der Energiewirtschaft verfolgt werden:

- Förderung des Dialogs und der Zusammenarbeit auf dem Gebiet der Quantentechnologien für die Energiewende unter Einbeziehung aller relevanten Akteure
- Schärfung des Bewusstseins für die Bedeutung der Post-Quanten-Kryptografie im Energiesektor und entsprechende Anpassung der kryptografischen Regulierung in der mittelfristigen Perspektive
- Entwicklung und Unterstützung von Projekten zum Quantencomputing und zur Quantenkommunikation mit Fokus auf die Energiewende und die Anforderungen des Energiesektors

1 Innovative Impulse für die Energiebranche

1.1 Zielsetzung

Ziel dieser Analyse ist es, Entwicklungen und Trends im Bereich der Quantentechnologie so darzustellen und einzuordnen, dass ihre Folgen für die Energiewende und die Energiewirtschaft schon jetzt absehbar werden. Dabei sollen keine wesentlichen Entwicklungssprünge der Technologien durch diese Analyse antizipiert werden und in ihre Argumentation einfließen. Erstens sind viele Anwendungen noch so marktfern, dass die spekulative Natur solcher Annahmen den prognostischen Wert der Betrachtung in Bezug auf energiewirtschaftliche Anwendungen schwächen würde. Zweitens sind die Quantentechnologien noch so jung, dass unerwartete Entwicklungssprünge jederzeit möglich scheinen (BSI, 2018).

Deshalb geht das Papier einerseits von konservativen Annahmen über die Leistungsentwicklung von Quantencomputern in den kommenden Jahren aus, ohne aber andererseits dadurch die tatsächlich schon jetzt gebotene Dringlichkeit der Diskussion in Frage zu stellen, denn wir können jederzeit von erheblichen Quantendurchbrüchen überrascht werden (BSI, 2018). Die Dringlichkeit der Diskussion dieser Technologien durch die Energiewirtschaft begründet sich aber auch schon aus dem Stand der Technik und der Forschung im Bereich der Quantentechnologie selbst, und dies in doppelter Weise.

Erstens wissen wir für einige Bereiche schon jetzt, welche Folgen ein überraschender Quantendurchbruch im Bereich des Quantencomputing haben kann. Insbesondere im Bereich der Kryptografie wurde bereits 1994 von Peter Shor ein entsprechender Quantenalgorithmus beschrieben (Shor, 1994), wodurch mögliche, daraus resultierende Folgen für die Sicherheit von Daten diskutiert wurden. Der Einsatz solcher Algorithmen hängt somit „lediglich“ von den für ihre technische Realisierbarkeit erforderlichen technologischen Durchbrüchen bei Quantencomputern ab. Das würde auch die Energiewirtschaft mit ihren hohen Anforderungen an Datenschutz und Datensicherheit sowie für den Betrieb kritischer Infrastrukturen betreffen.

Zweitens bedeutet die bereits erwähnte Marktferne der Quantentechnologien keineswegs, dass einzelne Technologien im Einzelfall nicht schon im Einsatz sind oder bald zum Einsatz kommen werden. Insbesondere staatliche Akteure sind nicht auf marktorientierte Lösungen angewiesen. Wenn ein ausreichend großes politisches Interesse besteht, tritt bei der Technologieentwicklung die Frage nach der Wirtschaftlichkeit in den Hintergrund. Es kommt dann oftmals zu einer Entkopplung des technischen Reifegrades einer Technologie von einer möglichen Marktreife.

1.2 Industriepolitischer und geopolitischer Kontext

Sogenannte **Moonshots**, in denen bahnbrechende und strategisch wichtige Technologien mit ungewisser Amortisationsperspektive entwickelt werden, erfolgen bei ausreichend nationalen Interessen auch unter Ausschluss der Öffentlichkeit, um daraus weitere strategische Vorteile zu ziehen.

Moonshots haben zudem eine große industriepolitische Bedeutung. Sie können technologische Abhängigkeiten bei Schlüsseltechnologien schaffen, die als geopolitischer Hebel genutzt werden können. **Insofern stellt die Förderung von innovativen Technologien auch einen wesentlichen Aspekt für die Sicherung der technologischen Unabhängigkeit und digitalen Souveränität eines Staates dar.**

Wo im Einzelfall eine Unabhängigkeit nicht gewährleistet werden kann – etwa, weil ganze quantentechnologische Anwendungsbereiche oder Basistechnologien auf Importe oder Lizenzierungen angewiesen sind –, ist abzuwägen, wie und ob der Einsatz dieser betroffenen Technologien im Zusammenhang mit kritischen Infrastrukturen erfolgen sollte. **Umgekehrt muss immer dort, wo eine führende Rolle in der Entwicklung technologischer Innovationen eingenommen wird, im Rahmen der Ausfuhrkontrolle genau geprüft werden, unter welcher Voraussetzung der Export dieser quantentechnologischen Lösungen oder Basistechnologien erfolgen darf**. Schließlich kann ein solcher Technologietransfer auch zu einem Verlust der Vorreiterrolle auf dem Weltmarkt oder zu (noch nicht veröffentlichten) Quantendurchbrüchen anderer Länder beitragen (Berger, 2021).

Vor diesem Hintergrund werden die einzelnen Quantentechnologien entsprechend ihrem Entwicklungsstand und ihrer möglichen Relevanz für das Energiesystem in dieser Analyse eingeordnet und priorisierte Anwendungsfelder herausgestellt. Darüber hinaus erfolgt die Priorisierung auch dahingehend, ob bezüglich einzelner quantentechnologischer Anwendungsfelder ein akuter, mittelfristiger oder langfristiger Handlungsbedarf in der Energiewirtschaft, der Verwaltung oder der Politik besteht. Abschließend werden erste Handlungsempfehlungen abgeleitet.

Auf diese Weise trägt die Analyse dazu bei, die Erwartungen an das energiewirtschaftliche Potenzial der Quantentechnologien auf realistische Fluchtpunkte für die weitere Diskussion einzustellen.

1.3 Das Future Energy Lab als Plattform

Initiativen wie das Future Energy Lab als Wissens- und Projektstandort ermöglichen der Energiewirtschaft, zu den Early Adoptern dieser digitalen Zukunftstechnologie zu gehören. Voraussetzung dafür war und ist aber, dass neue digitale Technologien durch Demonstrations- und Pilotierungsprojekte im engen Austausch mit der Energiewirtschaft und der Digitalwirtschaft erprobt werden. Der dadurch erreichte Brückenschlag zwischen Energie- und Digitalwirtschaft ist im Rahmen des Projekts „Blockchain Machine Identity Ledger“ (BMIL) für die Blockchain-Technologie vorbildlich gelungen und sollte auch Vorbild für die energiewirtschaftliche Erschließung neuer digitaler Technologien wie der Quantentechnologien sein. Dabei sollte es vor allem zu einer frühzeitigen Vernetzung aller einschlägigen Akteure kommen.

Erstens sollten dadurch frühzeitig geeignete energiewirtschaftliche Anwendungsfälle für die Forschung identifiziert werden, um dieser eine stärkere Anwendungsorientierung zu geben (Agenda Quantensysteme 2030, 2021[1]). Trotz eines umfangreichen Rahmenprogramms für die Forschung besteht in diesem Bereich gegenwärtig noch ein hoher Ausbaubedarf.

Zweitens sollte sich dadurch die „Anwender-Branche“ Energiewirtschaft schon früh mit den Quantentechnologien auseinandersetzen. Das hat zunächst mit den oben beschriebenen Folgen für die Sicherheit energiewirtschaftlicher Daten zu tun. Darüber hinaus werden neben Quantentechnologien aber auch lang-

[1] Leitlinien für ein gemeinsames Handeln von Wirtschaft, Politik und Wissenschaft, entwickelt durch eine Fachcommunity für Quantentechnologien aus Wissenschaft und Wirtschaft.

fristig konventionelle Informations- und Kommunikationstechnik-Lösungen (IKT) bestehen bleiben. Ein frühzeitiges Verständnis kann dabei helfen, bestehende und geplante Infrastrukturen sinnvoll durch quantentechnologische Lösungen zu ergänzen, ohne sie zu ersetzen. Auch hierfür muss der Blick für die möglichen Anwendungsfälle früh genug geschärft werden.

Hybridisierung von quantentechnologischen und konventionellen Lösungen bei der Datenverarbeitung oder Datenübertragung, nicht aber disruptive Verdrängung wird daher auch langfristig die Energiewirtschaft prägen.

2 Energiewirtschaftliche Relevanz und Anwendungsfelder von Quantentechnologien

Quantentechnologien stellen eine Schlüsseltechnologie von überragender strategischer Bedeutung für Wirtschaft und Sicherheit dar. Dies hat auch die Bundesregierung erkannt und fördert diese Technologien mit insgesamt über 2 Milliarden Euro (FAZ, 2021). Damit steht das Förderprogramm der Bundesregierung, wie es Abbildung *2.1* zu entnehmen ist, im internationalen Vergleich, nach der Volksrepublik China, erfolgreich an zweiter Stelle. Für die Forschungs- und Förderpolitik der Bundesrepublik ist das Rahmenprogramm „Quantentechnologien – von den Grundlagen zum Markt“ maßgeblich, das vom Bundesministerium für Bildung und Forschung (BMBF), vom Bundesministerium für Wirtschaft und Klimaschutz (BMWK), vom Bundesministerium des Innern, für Bau und Heimat (BMI) und vom Bundesministerium der Verteidigung (BMVg) erarbeitet wurde (BMBF, 2022). Im Zusammenhang damit hat sich eine breite Projektlandschaft entwickelt, die Anwendungsbereiche eines Quantencomputers über die Quantenkommunikation bis hin zur Quantensensorik umfasst. Darüber hinaus besteht mit dem Quantum Flagship der Europäischen Union ein 2018 ins Leben gerufenes und auf zehn Jahre angelegtes Programm mit einem Volumen von 1 Milliarde Euro (Europäische Kommission, 2018). Diese positive Entwicklung muss über die nächsten Jahre beibehalten werden.

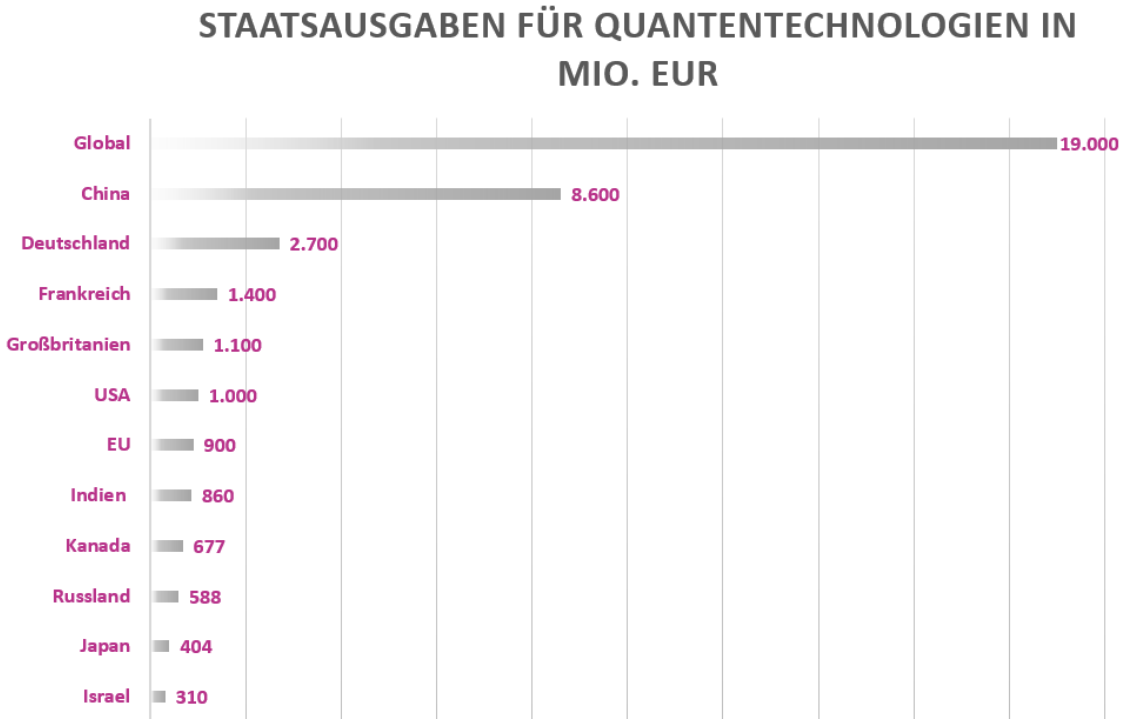

Abbildung 2.1 : Staatsausgaben für Quantencomputing in Millionen Euro (Quelle: Berger, 2021)

Insbesondere für kritische Infrastrukturen und komplexe Systeme können die Quantentechnologien langfristig zum „Game Changer“ werden. Das in der Transformation begriffene Energiesystem kann von diesem Paradigmenwechsel in doppelter Weise betroffen sein: einerseits beim Schutz kritischer Energieinfrastrukturen und andererseits bei der Bewältigung der Energiewende sowie dem dafür antizipierten Ausbau der Elektromobilität.

2.1 Quantentechnologien für kritische Energieinfrastrukturen

Das Energiesystem stellt die grundlegende kritische Infrastruktur für das wirtschaftliche und gesellschaftliche Leben eines modernen Industrielandes dar. Das Energiesystem ist damit als Infrastruktur für die Infrastrukturen zu verstehen: Von ihm hängt neben allen Lebensbereichen auch das Funktionieren anderer kritischer Infrastrukturen ab. Die Digitalisierung als technische Voraussetzung für die Energiewende vermehrt jedoch durch die steigende Anzahl an Akteuren und Technologien sowie die Vernetzung komplexer Prozesse mögliche Einfallstore für Cyberangriffe in das System. Dem Schutz der kritischen Infrastruktur Energiesystem kommt damit eine übergeordnete Bedeutung zu.

Quantentechnologien können, bei ausreichender Robustheit durch sichere Quantenkommunikation und von ihnen abgeleitete kryptografische Verfahren, einen zukunftssicheren Beitrag zum Schutz kritischer Infrastrukturen leisten. Allerdings ergibt sich damit im Umkehrschluss schon jetzt bei allen Betreibern kritischer Energieinfrastrukturen ein akuter Handlungsbedarf: Daten, die in Zukunft durch Quantenkryptografie sicherer verschlüsselt werden können, lassen sich durch quantenkryptografische Verfahren dann auch schneller entschlüsseln. Auch wenn die dafür notwendigen technologischen Durchbrüche noch auf sich warten lassen, sollten daher schon jetzt energiewirtschaftliche Daten durch Verfahren der **Post-Quanten-Kryptografie** gesichert werden. Post-Quanten-Kryptografie erlaubt die quantensichere Verschlüsselung von Daten, ohne dabei auf die Verfügbarkeit einzelner Quantentechnologien angewiesen zu sein.

Der Handlungsdruck für die Energiewirtschaft ergibt sich dabei aus zwei Faktoren. Zunächst können nach dem **Prinzip „Harvest now, decrypt later“** sensible Daten zunächst durch Angreifer abgefangen und gespeichert werden, um sie dann bei Vorliegen der entsprechenden quantenkryptografischen Verfahren später zu entschlüsseln.

Die Sinnhaftigkeit eines Angriffs, der dem Prinzip „Harvest now, decrypt later“ folgt, hängt dabei auch von der „Halbwertszeit“ der Daten selbst ab: Damit sich dieses Vorgehen lohnt, müssen die Daten auch über einen längeren Zeitraum hinweg einen Wert besitzen. Davon sind vor allem energiewirtschaftliche Stammdaten betroffen, die über Jahre aktuell bleiben können.

Zum anderen nimmt die Wahrscheinlichkeit von (inoffiziellen) Quantendurchbrüchen stetig zu, besonders durch den starken Anreiz einer dadurch erreichbaren geopolitischen respektive wirtschaftlichen Pionierrolle. Deshalb sollten sensible energiewirtschaftliche Daten bereits zum jetzigen Zeitpunkt durch Verfahren der Post-Quanten-Kryptografie gesichert werden.

2.2 Quantentechnologien für die Energiewende

Schließlich können Quantentechnologien eine große Bedeutung für die Digitalisierung der Energiewende haben. Quantencomputing, Quantensimulationen oder quantengestützte künstliche Intelligenz (KI) können in Zukunft bei der Planung und im Betrieb helfen, um die zunehmende Komplexität des Energiesystems beherrschbar und effizient umzusetzen. Insbesondere der Ausbau der Elektromobilität und der dezentralen Erzeugung wird von der Energiewirtschaft schon jetzt als ein wichtiger Anwendungsbereich angesehen. Im Rahmen des Projekts Vehicle to Grid (V2G) arbeitet E.ON zusammen mit IBM daran, den Einsatz von Quantencomputing für ein intelligentes und dynamisches Lastmanagement für Millionen von Elektrofahrzeugen zu erproben (E.ON, 2021). Mit EnerQuant gibt es ferner ein deutsches Forschungsprojekt zum energiewirtschaftlichen Einsatz von Quantensimulationen für die Berechnung komplexer Energiemarktmodelle (EnerQuant, 2022).

2.3 Hybride Lösungen statt disruptive Marktverdrängung

Neben den gegenwärtig noch hohen Kosten für Quantencomputing hängt der wirtschaftliche Einsatz auch von der sogenannten Quantenüberlegenheit ab. Unter Quantenüberlegenheit wird die leistungsbezogene Überlegenheit der Quantencomputertechnologie gegenüber der konventionellen Computertechnologie verstanden. Erst bei Vorliegen von Quantenüberlegenheit kann es auch zu einer genauen Kosten-Nutzen-Analyse darüber kommen, ob der Einsatz von Quantencomputing für einen konkreten Anwendungsfall tatsächlich wirtschaftlich ist. Es kann davon ausgegangen werden, dass sich deshalb auch hybride Lösungen am Markt etablieren werden. Somit ist von wechselseitigen Lern- und Anpassungsprozessen zwischen konventionellen und quantentechnologischen Lösungen auszugehen, beispielsweise durch Rückübertragung von Erkenntnissen und Verfahren auf konventionelle Lösungen, um diese etwa im Bereich von Algorithmen weiterzuentwickeln.

Für den Schutz kritischer Energieinfrastrukturen und die Bewältigung der Energiewende ist ebenfalls mit einer allmählichen und ergänzenden Marktdurchdringung quantentechnologischer Anwendungen der Energiewirtschaft zu rechnen. Eine schlagartige Ablösung der bisherigen Technik ist aufgrund der Heterogenität bestehender IKT-Paradigmen und -Technologien in diesem Bereich dagegen nicht zu erwarten. Auch ist die deutsche Energiewirtschaft eher zurückhaltend, wenn es um die Implementierung neuer digitaler Technologien geht. Denn strenge regulatorische Vorgaben, hohe Anforderungen an die Robustheit (Schwarzstartfähigkeit[2]) von Systemen, langwierige Standardisierungsprozesse und lange Abschreibungszeiten von Investitionen führen zu aufwendigen und langwierigen Umsetzungsprozessen. Schließlich ist die Energiewirtschaft in Deutschland sehr kleinteilig und heterogen aufgestellt. **Dies wird auch eine „Ungleichzeitigkeit" von Implementierungspfaden für quantentechnologische Lösungen zur Folge haben**. IKT-Investitionen folgen oftmals noch den Abschreibungszyklen der Operational Technology (OT) von 25 Jahren. Auch deshalb ist bei den vielen kleinen Akteuren der Energiewirtschaft davon auszugehen, dass die Investitionsbereitschaft bei Quantentechnologien im Vergleich zu den großen Early Adoptern der Branche erst mit einer Verzögerung von einer Dekade vorhanden sein wird. Es bleibt daher abzuwarten, ob große energiewirtschaftliche oder digitalwirtschaftliche Akteure eine marktbeherrschende Rolle im Bereich des Quantencomputings beispielsweise durch „Quantencomputing-as-a-Service" einnehmen werden. Etwa bei den Anbietern von Cloud-Services ist davon auszugehen, dass sie zu den frühen Adoptern von Quantentechnologien gehören werden: Dadurch können die kleinen energiewirtschaftlichen Akteure indirekt von diesen Technologien profitieren. Dies bedeutet im Umkehrschluss jedoch, dass im Sinne der Diskriminierungsfreiheit der Energiewirtschaft bei allen Technologieentwicklungen und der Etablierung neuer Software-Lösungen gleichzeitig auf **Schnittstellen zwischen der neuen und der bisherigen Technologie** geachtet werden muss – vor allem da die Kosten für die neue Technologie eine erhebliche Markteintrittsbarriere darstellen können und somit besonders KMUs belasten würden.

Auch bei der Post-Quanten-Kryptografie sollten konventionelle Lösungen schrittweise implementiert und ergänzt werden. Denn gegenwärtig sind zwar Verfahren der Post-Quanten-Kryptografie beschrieben und umfangreich getestet worden; ihr breiter Einsatz steht aber noch aus. Insofern existiert auch noch kein Wissen über mögliche Folgen und Wechselwirkungen ihres Einsatzes innerhalb konkreter Anwendungsfälle und komplexer Systeme. **Daher sollten die über Jahrzehnte erprobten kryptografischen Verfahren als Fallback-Lösungen weiterhin im Einsatz bleiben, um einen „Status-quo-Grundschutz" weiterhin gewährleisten zu können**.

[2] Hochfahren eines Kraftwerks(blocks) vom abgeschalteten Zustand unabhängig vom Stromnetz.

3 Quantentechnologien im Überblick und ihre energiewirtschaftliche Relevanz

Der Abschnitt *Quantentechnologien im Überblick und ihre energiewirtschaftliche Relevanz* konzentriert sich auf die Anwendungsbereiche Quantencomputer und Quantenkommunikation. Zum besseren Verständnis dient die folgende Abbildung *3.1*, die, ausgehend von den grundlegenden Quantenprinzipien, einen Überblick über die verschiedenen Quantentechnologien und ihre Anwendungsbereiche sowie die sich daraus ableitbare Relevanz für die Energiewirtschaft gibt.

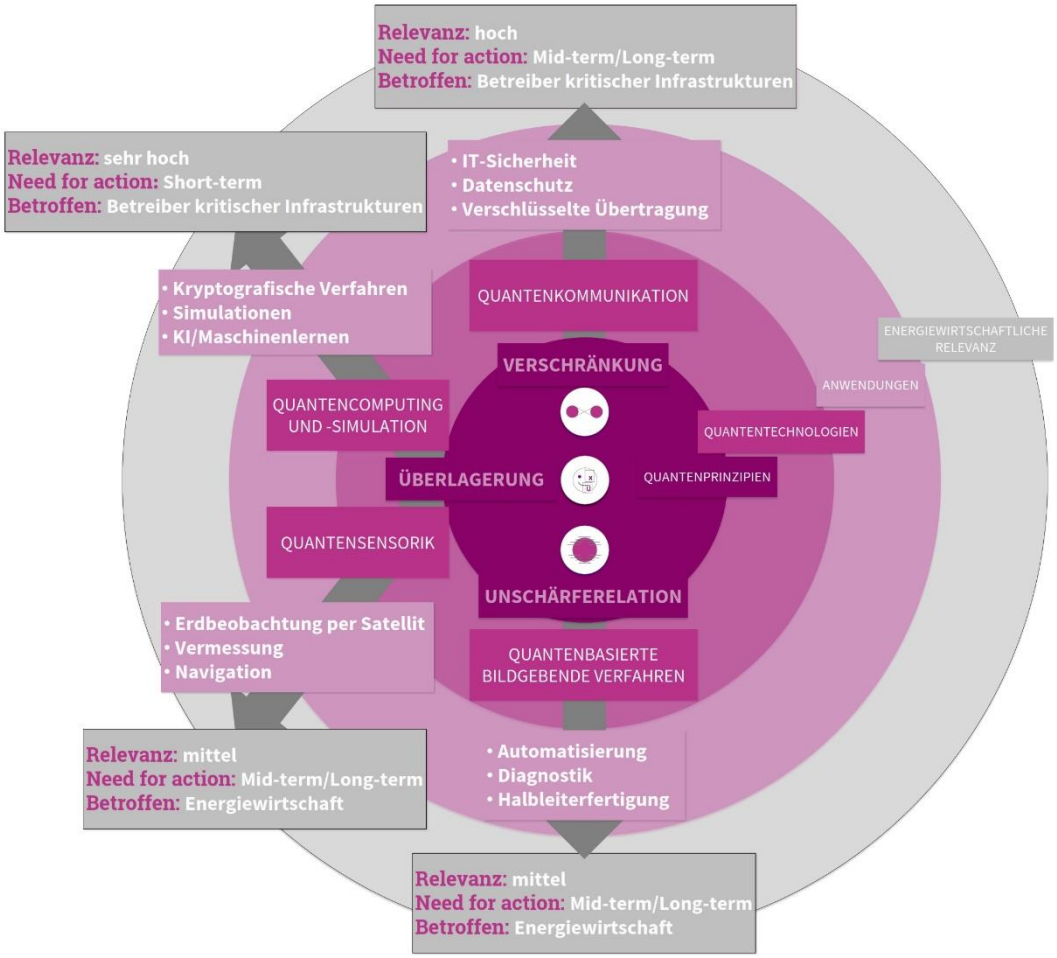

Abbildung 3.1: Quantentechnologien und ihre energiewirtschaftliche Relevanz.

Auf die Anwendungsbereiche Quantensensorik oder quantengestützte KI wird in diesem Abschnitt nicht gesondert eingegangen, da der Anwendungsbereich der **Quantensensorik** eine Basistechnologie für Quantencomputer und Quantenkommunikation darstellt. Die Verfügbarkeit von Quantensensorik wird hier als notwendig vorausgesetzt und ihre Funktionsweise ist mit den unten beschriebenen Funktionsweisen von Quantencomputern und Quantenkommunikation eng verknüpft. Es sei hier aber angemerkt, dass es über

den Charakter der Basis- und Enabler-Technologien für Computing und Kommunikation hinaus ein breites Spektrum möglicher Anwendungen von Quantensensorik in Industrie oder Medizin gibt, bei denen es für Fertigungsverfahren bei Halbleitern oder Krebsdiagnostik auf immer genauere Messverfahren ankommt (Universität Stuttgart, 2020). Inwiefern sich aber daraus schon jetzt mögliche Anwendungsszenarien für die Energiewirtschaft ergeben, ist schwer zu sagen. Die bestehende Messtechnik auf allen Netzebenen sowie im Wärmebereich ist gegenwärtig auch den Anforderungen eines immer komplexeren, kleinteiligeren und sich sektorübergreifend integrierenden Energiesystems gewachsen. Die von Quantensensorik versprochenen Messgenauigkeiten und Messgeschwindigkeiten scheinen daher noch keinen Mehrwert zu bieten, der einen kurz- bis mittelfristigen Einsatz von Quantensensorik in der Energiewirtschaft rechtfertigen könnte. **Mittelfristig** könnten **Quanten-Magnetometer**[3] aber zum Beispiel dabei helfen, die Energiedichte, Lebensdauer und Sicherheit von Batterien durch ein besseres Verständnis der **Leistungsfähigkeit von Batterien** zu erhöhen. Hier gibt es schon jetzt vielversprechende Projekte (UK Quantum Technology Hub, 2021). **Langfristig** ließen sich etwa durch sogenannte **Quantenuhren**, die eine sehr genaue Zeitmessung über die Schwingungsmessung von Atomen ermöglichen, **komplexe und extensive Energieinfrastrukturen wie das europäische Verbundnetz synchronisieren**.

3.1 Quantencomputer

3.1.1 Funktionsweise

Die Funktionsweise von Quantencomputern unterscheidet sich fundamental von der eines konventionellen Computers: Arbeiten Letztere mit Bits, die nur zwei Zustände erlauben, so operieren Quantencomputer mit sogenannten Qubits (Quanten-Bits) als kleinstmögliche Speichereinheit, die erheblich mehr Zustände abbilden können. Dabei machen sich Quantencomputer zwei quantenmechanische Phänomene zunutze: Überlagerung und Verschränkung.

Bei der **Überlagerung (Superposition)** liegen Quantenteilchen wie Elektronen oder Photonen in mehreren Zuständen gleichzeitig vor. Ferner liegen diese Quantenteilchen auch in einer bestimmten Wahrscheinlichkeit vor. Der Pionier der Quantenmechanik Erwin Schrödinger hat gezeigt, dass die Zustandsmessung diese Überlagerung aufhebt: Das Quantenteilchen hat im Ausgang der Messung stets nur einen einzigen Zustand und die Summe aller Quantenwahrscheinlichkeiten bestimmter Zustände liegt bei 1 (also 100 Prozent). Gleichwohl erlaubt die Quantenmechanik die Veränderung und das Auslesen der Wahrscheinlichkeiten von Quantenteilchen. Daraus ergibt sich schließlich auch die Möglichkeit, mit ihnen große Zahlen darstellen und Berechnungen durchführen zu können. Im Gegensatz zu Bits erlauben Qubits auf diese Weise die Darstellung nahezu beliebig großer Zahlen. Allerdings hängt dies auch davon ab, wie genau die einzelnen Wahrscheinlichkeiten von Zuständen gemessen werden können (LBBW, 2022).

Bei der **Verschränkung** können Qubits miteinander so verschaltet werden, dass sich die Anzahl der Zustände der verschränkten Qubits mit jedem weiteren Qubit verdoppelt. Allerdings müssen die Wahrscheinlichkeiten jedes einzelnen Qubits bekannt sein. Das stellt hohe Anforderungen an die Messung und Auswertung, da Messfehler bei einem Qubit auf das Gesamtergebnis der Operation durchschlagen (LBBW, 2022).

[3] Als Magnetometer bezeichnet man eine sensorische Einrichtung zur Messung magnetischer Flussdichten.

Deshalb kommt der **Fehlerkorrektur** eine große Bedeutung zu. Dabei kommt ein Verfahren zum Einsatz, das auch bei konventionellen Rechnern verwendet wird: Es werden Qubits dazu abgestellt, die Ergebnisse anderer Qubits zu prüfen. Derartig fehlerkorrigierte Qubits werden als **logische Qubits** bezeichnet, die dafür benötigten Qubits als **physikalische Qubits**. Das Verhältnis von fehlerkorrigierten logischen Qubits zu fehlerkorrigierenden physischen Qubits kann bis zu 1:10.000 betragen (BSI, 2018).

Das langfristige Ziel ist es daher, die Fehlerrate deutlich zu verringern und die Anzahl der Qubits deutlich zu erhöhen. Ein universell fehlertoleranter Quantencomputer verlangt dabei allerdings erhebliche Verbesserungen der Hardware, die Systemgrößen von bis zu einer Million physikalischen Qubits ermöglichen kann. Gegenwärtig wird von 20 bis 30 Jahren bis zum Erreichen dieser Schwelle ausgegangen (Agenda Quantensysteme 2030, 2021).

3.1.2 Entwicklungsstand

Ziel der gegenwärtigen Entwicklungen im Bereich der Quantencomputer ist es, sogenannte **Quantum Supremacy** bzw. **Quantenüberlegenheit** zu erreichen. Unter Quantenüberlegenheit wird die Eigenschaft von Quantencomputern verstanden, Aufgabenklassen zu lösen, die konventionelle Rechner nicht lösen können.

Allerdings besteht Uneinigkeit darüber, wann die Schwelle zur Quantenüberlegenheit erreicht ist. 2019 beanspruchte Google für sich, diese Schwelle mit seinem 53-Qubit-Quantencomputer überschritten zu haben – laut Google hätten die vorgenommenen Berechnungen auf einem konventionellen Rechner 10.000 Jahre gedauert (The Economist, 2019). IBM attestierte dem Setup von Google daraufhin allerdings lediglich einen sogenannten Quantenvorteil, das heißt einen nicht wesentlichen Geschwindigkeitsvorteil, weil die gleichen Berechnungen auf einem konventionellen Rechner innerhalb von zweieinhalb Tagen möglich gewesen wären (Edwin et al., 2019).

Im Oktober 2021 zeigten zwei Forscherteams der University of Science and Technology of China in zwei unabhängig veröffentlichen Studien (H.-S. Zhong et al., 2021, und Y. Wu et al., 2021) erhebliche Fortschritte im Bereich photonischer Systeme und supraleiterbasierter Systeme, die als entscheidende Schritte Richtung Quantenüberlegenheit zu betrachten sind.

Im November 2021 gab IBM bekannt, einen Quantenprozessor entwickelt zu haben, der die 100-Qubit-Grenze überschritten hat (IBM, 2021). Mit dem 127-Qubit-Prozessor konnte IBM die Zeitplanung der eigenen Quantum Roadmap einhalten und will 2023 einen 1.000 Qubit großen Rechner vorstellen.

3.1.3 Relevanz für die Energiewirtschaft

Ab dem Zeitpunkt der erreichten Quantenüberlegenheit wird sich Quantencomputing weiträumig etablieren. Eine hohe Relevanz für die Energiewirtschaft ergibt sich besonders für **die Entwicklung von Ausbauszenarien und Prognoseberechnungen**, die für die Umsetzung des flächendeckenden Ausbaus erneuerbarer Energien zum Erreichen der Klimaziele benötigt werden. Durch die umfassenden und schnelleren Berechnungen ergeben sich zudem Vorteile für die Kraftwerkseinsatzplanung und speziell für ein optimiertes Engpassmanagement.

Neben diesen Optimierungsansätzen besteht für Quantencomputer eine erhöhte Relevanz aufgrund ihrer Fähigkeit zur **Entschlüsselung sensibler Daten**. Durch kurzfristige und nicht publik gemachte Quantendurchbrüche sowie das in Abschnitt *2.1* beschriebene Prinzip „Harvest now, decrypt later" besteht die Gefahr, dass sensible energiewirtschaftliche Daten mittel- bis langfristig entschlüsselt und unsachgemäß verwendet werden könnten.

Die Fähigkeit von Quantencomputern, eine Verschlüsselung zu brechen, hängt von dem verwendeten Verschlüsselungsverfahren ab. Im Zusammenhang mit kryptografischen Verfahren muss dabei gegenwärtig zwischen **symmetrischen** und **asymmetrischen Verfahren** unterschieden werden.

Symmetrische Verfahren nutzen sowohl zur Verschlüsselung als auch zur Entschlüsselung denselben geheimen Schlüssel. Dabei ist der Advanced Encryption Standard (AES) quasi-post-quanten-sicher, weil er variable Verschlüsselungen erlaubt. Gegenwärtig ist der sogenannte Grover-Algorithmus der einzige bekannte Quantenalgorithmus, der die Entschlüsselung einer durch AES-verschlüsselten Nachricht quadratisch beschleunigen kann. Die Möglichkeit für eine exponentielle Beschleunigung durch Quantencomputer besteht allerdings gegenwärtig nicht. Demnach ist die Verwendung entsprechend längerer Schlüssel hinreichend, um die Wirksamkeit der AES-Verschlüsselung trotz Quantencomputern zu gewährleisten (BSI, 2022).

Im Gegensatz zu symmetrischen Verfahren kommen in der **asymmetrischen Kryptografie** zwei verschiedene Schlüssel für Verschlüsselung und Entschlüsselung zum Einsatz. Ein privater Schlüssel (Private Key), der ausschließlich einer Partei bekannt ist, wird genutzt, um einen öffentlichen Schlüssel (Public Key) abzuleiten, der an alle potenziellen Kommunikationspartner und sonstige Parteien verteilt werden kann. Basierend auf diesem Prinzip lassen sich sowohl Verschlüsselung als auch Authentifizierung realisieren. Ein typisches Verfahren zur Authentifizierung von Nachrichten ist, dass eine Prüfsumme der Nachricht mit dem Private Key der sendenden Partei verschlüsselt wird und zusammen mit der eigentlichen Nachricht als digitale Signatur zur empfangenden Partei gesandt wird. Diese kann die verschlüsselte Prüfsumme mithilfe des entsprechenden Public Key entschlüsseln und gegen die Nachricht verifizieren. Stimmt die Prüfsumme überein, kann die empfangende Partei sicher sein, dass die Prüfsumme durch den Besitzer des Private Key verschlüsselt und dass die Nachricht bei der Übermittlung nicht manipuliert wurde (BSI, 2022).

Asymmetrische Verfahren gelten nur so lange als sicher, wie die ihnen zugrundeliegende mathematische Funktion nicht durch den Einsatz von Computern umgekehrt werden kann. Peter Shor hat schon 1994 gezeigt, wie ein dafür geeigneter Algorithmus aussehen könnte.

Aus dessen Arbeit und weiteren Arbeiten (etwa von Grover) ergibt sich, dass alle gebräuchlichen Verfahren zur asymmetrischen Verschlüsselung durch hinreichend performante Quantencomputer kompromittiert werden könnten. Dazu zählen:

- RSA
- Elliptic Curve Cryptography (ECDSA)
- Diffie-Hellman key exchange
- Finite Field Cryptography (DSA)

Von der Kompromittierung dieser Verfahren wären folgende auch für die Energiewirtschaft essenzielle Anwendungsbereiche betroffen:

- Austausch symmetrischer Schlüssel (etwa im Rahmen der SM-PKI)

- Digitale Signaturen und Zertifikate (etwa im Rahmen der SM-PKI)
- GWA in der SM-PKI und im Backend
- OT, IoT und SMGW (Firmware-Updates oftmals schwierig oder gar unmöglich)
- SmartCards und Hardwaresicherheitsmodule
- Netzwerkverkehr (Problematik „Harvest now, decrypt later")

Aus der Sorge heraus, dass Quantencomputer mittel- bis langfristig dazu imstande sein werden, den Shor-Algorithmus effektiv ausführen zu können, entstand die **Post-Quanten-Kryptografie (PQK)**. Die Annahme der PQK ist dabei, dass die Sicherheit von PQK auf der Schwierigkeit mathematischer Probleme basiert, von denen derzeit angenommen wird, dass sie auch mit Quantencomputern, die performant genug für den Shor- oder Grover-Algorithmus sind, nicht effizient lösbar sein werden.

Vor diesem Hintergrund hat das BSI schon 2020 Handlungsempfehlungen zur Migration von Prä-Quanten- hin zu Post-Quanten-Verfahren veröffentlicht (BSI, 2020). Diese Handlungsempfehlungen hat das BSI Ende 2021 aktualisiert und in der Publikation „Kryptographie quantensicher gestalten – Grundlagen, Entwicklungen, Empfehlungen“ (BSI, 2021) erweitert. **Dabei empfiehlt das BSI auch die Hybridisierung von Prä-Quanten- und Post-Quanten-Verfahren**. Denn nur durch die Kombination aus bewährter symmetrischer Kryptografie mit hinreichend großer Schlüssellänge und den vorgestellten quantensicheren Schlüsseleinigungs- und Signaturverfahren kann auch ein sogenannter **Fallback-Grundschutz gegeben sein, wenn sich die PQK-Verfahren im Einsatz aus unvorhergesehenen Gründen nicht als geeignet und praxisfähig (auch im konventionellen und von Quantencomputern losgelösten Einsatz) zeigen**.

Schließlich hat das BSI 2018 parallel zu den Standardisierungsbemühungen des amerikanischen National Institute of Standards (NIST) im Bereich PQK die Studie „Status of quantum computer development“ erarbeitet und 2019 und 2020 aktualisiert (BSI, 2018).

Im Zuge des NIST-Standardisierungsverfahren wurden in einem Auswahlverfahren von November 2016 – Juli 2022 insgesamt vier PQK-Algorithmen für die weitere Standardisierung ausgewählt. Die finalen Standards werden aber nicht vor 2024 zur Verfügung stehen.

- **Algorithmus für Public-Key-Verschlüsselung/Schlüsselaustausch:** CRYSTALS–KYBER
- **Algorithmen für digitale Signaturen:** CRYSTALS–Dilithium (soll primärer Standard werden), FALCON, SPHINCS+
- **Alternative Algorithmen (Schlüsselaustausch):** BIKE, Classic McEliece, HQC, und Sike (wurde im August 2022 gebrochen)

Die Migration auf quantensichere Kryptografie wird einige Zeit in Anspruch nehmen. Das BSI empfiehlt schon heute beispielsweise in der BSI-TR-02101-1 hashbasierte Signaturen sowie digitale signaturverfahren in der BSI-TR-03140 03140 im Rahmen des Satellitendatensicherheitsgesetzes (SatDSiG).

Wie lange die Umstellungszeit für die Migration auf quantensichere Kryptographie dauern wird, hängt nach dem sogenannten Theorem von Mosca drei Faktoren ab (Mosca, 2015):

1. Wie lange sollen Daten sicher bleiben? (X Jahre)
2. Wie lange dauert die Umstellung der Systeme auf quantensichere Kryptographie? (Y Jahre)
3. Wie lange wird es dauern, bis leistungsstarke Quantencomputer zur Verfügung stehen? (Z Jahre)

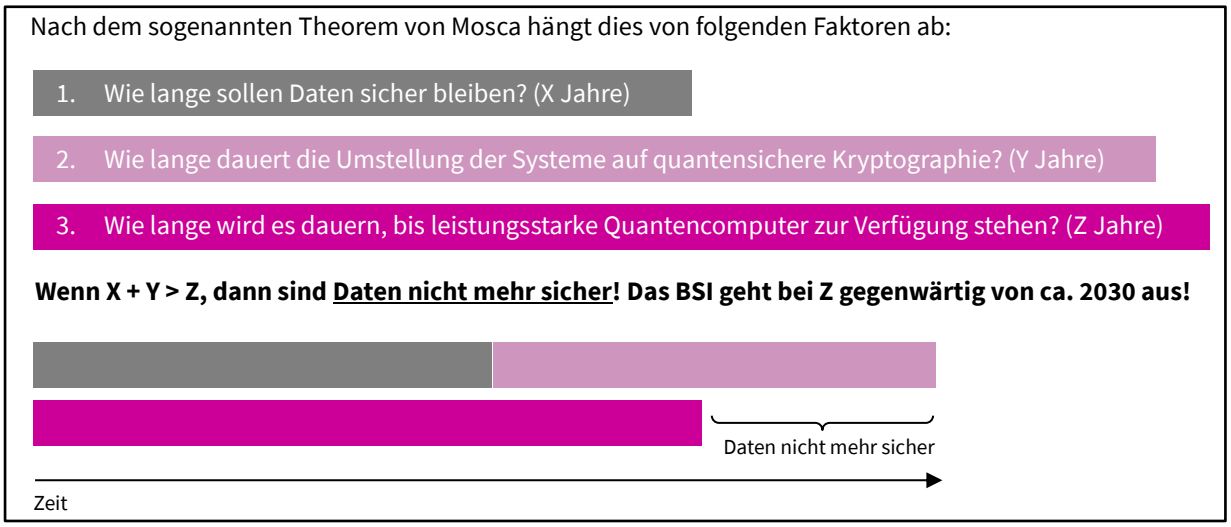

Abbildung 3.2: Theorem von Michele Mosca (Quelle: Mosca, 2015).

Die Daten gelten dann als sicher, wenn die Dauer in der die Daten ihre Vertraulichkeit behalten müssen und die Umstellung für die Migration auf PQK kürzer ist als der Zeitraum, in dem performante Quantencomputer entwickelt werden.

Hinsichtlich des Zeitraums, in dem Daten ihre Vertraulichkeit behalten müssen, lässt sich feststellen, dass viele Daten aus dem Bereich der Netzüberwachung eine geringe Halbwertszeit haben. Sie sind deshalb auch kaum von Interesse für „Harvest now, decrypt later"-Angriffe. Allerdings gibt es auch Anwendungsbereiche, in denen die Vertraulichkeit von Daten aufgrund geschäftlicher, juristischer oder auch technischer Voraussetzungen über einen langen Zeitraum hinweg gewährleistet bleiben muss, wie beispielsweise:

- „Hart-verdrahtete" Passwörter OT und IoT
- Wurzelzertifikate
- Generalschlüssel
- Geschäfts- oder Vertragsgeheimnisse

Die Vertraulichkeit muss bei „hart-verdrahteten" Passwörtern oder Generalschlüsseln aber auch deshalb sichergestellt werden, weil sonst auch der Zugang zu den betroffenen Systemen kompromittiert werden kann und damit auch die Integrität und Verfügbarkeit der Daten verloren gehen kann. Vor diesem Hintergrund kann die sektorspezifische Beantwortung der Frage nach der Dauer, in der Daten vertraulich bleiben müssen, nicht allein an der Prozesskritikalität der Daten entschieden werden. Vielmehr zeigen die oben genannten Beispiele, dass in der Energiewirtschaft die Vertraulichkeit vieler Daten in anderen kritischen Bereichen ohne „Ablaufdatum" gewährleistet werden muss.

Bezogen auf die Dauer des Umstellungszeitraumes lässt sich grob sagen, je komplexer und heterogener die IT-/OT-/IoT-Landschaft, desto langwieriger und aufwendiger ist die Migration auf PQK. Zusätzlich ist zu berücksichtigen, dass proprietäre Lösungen und Legacy-Systeme oftmals nur in einem sehr geringem Maße upgradable sind.

3.2 Quantenkommunikation

3.2.1 Funktionsweise

Quantenkommunikation verspricht eine abhörsichere Kommunikation, was sowohl die sichere Datenverschlüsselung als auch die Datenintegrität umfasst. Diese Eigenschaft hängt unmittelbar mit dem quantenphysikalischen Prinzip dieses Anwendungsfelds zusammen: Denn der Zustand eines Quantenobjekts, wie etwa eines Photons, kann nicht gemessen werden, ohne zugleich seinen Zustand zu verändern. Verfahren, die dabei Superposition und Verschränkung von quantenmechanischen Zuständen ausnutzen, können zur **Verteilung von Quantenschlüsseln** und zum **Transfer von Quantenzuständen** genutzt werden (Fraunhofer-Gesellschaft, 2022).

Bei der **Verteilung von Quantenschlüsseln** wird durch optische Fasernetze oder durch den Einsatz von lasergestützter Satellitenkommunikation ein gemeinsamer geheimer Schlüssel für beide Übertragungsparteien erzeugt. Dabei kommen entweder Verschränkung (Ekert-Protokoll) oder einzelne und polarisierte Photonen (BB84-Protokoll) zum Einsatz (BMBF, 2022).

Beim **Transfer von Quantenzuständen** werden, im Gegensatz zur Verteilung von Quantenschlüsseln, die konkreten Zustände von Quantenobjekten durch die Verschränkung von Photonen oder anderen Quantenobjekten transferiert. Zwar muss für die Herstellung der Verschränkung die Information über den Quantenzustand, in dem die Photonen verschränkt werden sollen, ausgetauscht werden. Doch sobald diese Verschränkung gelungen ist, muss keine weitere Information zwischen Sender und Empfänger als direktes Signal ausgetauscht werden, um diesen Zustand aufrechtzuerhalten. Durch die Verschränkung wird schließlich das Zustandsverhalten der Photonen synchronisiert. Dadurch ließe sich bei entsprechender Skalierung der Transferrate eine völlig neue Form der Kommunikation und der Datenverarbeitung ermöglichen, in der ein paralleles und synchrones Quantencomputing an verschiedenen Standorten ohne Latenz möglich wird. Allerdings können beim Transfer von Quantenzuständen herkömmliche Verfahren der Signalverstärkung nicht zum Einsatz kommen. Da die Signalstärke zur Übertragung von Quantenzuständen sehr gering ist, müssen daher neue quantentechnologische Signalverstärkungsverfahren erforscht und entwickelt werden, bis ein Einsatz über praxisrelevante Entfernungen möglich wird (BMBF, 2022).

3.2.2 Entwicklungsstand

Im Zusammenhang mit der Verteilung von Quantenschlüsseln gibt es erste wesentliche Erfolge, die zum Teil schon den Einsatz im operativen Wirkbetrieb erlauben. Nachdem in den letzten Jahren die Übertragungsreichweite von Dutzenden Zentimetern auf Hunderte Kilometer vergrößert wurde, beschreibt ein Artikel (Yu-Ao Chen et al., 2021) aus Januar 2021 ein chinesisches Quantenkommunikationsnetzwerk, das durch die Kombination aus Glasfaserverbindungen und Satellitenkommunikation eine Übertragungsreichweite von bis zu 4.600 Kilometern erreicht.

Dabei wurden verschiedene Netzwerktopologien auch für dezentralere Anwendungsszenarien erprobt. Vier sogenannte Small-scale Quantum Metropolitan-Area Networks (Beijing, Jinan, Shanghai und Hefei) sind dabei an das zentrale Netzwerk von 2.000 Kilometern angeschlossen. Darüber hinaus verfügt das Netzwerk über zwei Bodenstationen für die Satellitenkommunikation (Xinglong und Nanshan). Das chinesische Quantenkommunikationsnetzwerk hat dadurch gezeigt, dass nicht nur eine durch Quantenverschlüsselung gehärtete Punkt-zu-Punkt-Kommunikation über große Entfernungen möglich ist, sondern auch dezentralere

Netzwerke nach dem heutigen Stand der Technik realisiert werden können. Dadurch wird auch eine quantenkommunikative Vernetzung von komplexen Infrastrukturen wie dem Energiesystem möglich. Schließlich hat sich das chinesische Quantenkommunikationsnetzwerk auch gegenüber den gegenwärtig bekannten Störungen und Angriffsverfahren (z. B. Jamming-[4] oder Denial-of-Service-Angriffe (DoS)[5]) als robust und sicher gezeigt.

Aufgrund der hohen Relevanz, die Quantenkommunikation für die sichere Kommunikation in Zukunft haben wird, hat die Bundesregierung die QuNET-Initiative[6] gestartet, die eine zunehmende aktive Industriebeteiligung zum Ziel hat und schließlich einen breiten Rollout von Quantenkommunikationsinfrastruktur in der zweiten Hälfte der Zwanzigerjahre anstrebt.

Ein solcher Rollout ist dabei aber auch von den infrastrukturellen Voraussetzungen im Bereich Glasfaser abhängig: Er sollte nicht nur im Sinne des Koalitionsvertrags schnell und flächendeckend erfolgen, sondern auch berücksichtigen, dass die Glasfasernetze auch für Quantenkommunikation genutzt werden können.

3.2.3 Relevanz für die Energiewirtschaft

Eine hohe Relevanz der Quantenkommunikation ergibt sich schon durch § 11 Abs. 1a EnWG, der „einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Netzbetrieb notwendig sind“, zu den Pflichten der Netzbetreiber zählt.[7] Sicherheitsstandards müssen somit stetig an die neuen technischen Möglichkeiten digitaler Innovationen angepasst werden, wodurch **sich voraussichtlich ein erhöhter Handlungsbedarf für die Netzbetreiber** ableiten lässt.

Quantenkommunikation kann durch den mit der Technologie verbundenen hohen Sicherheitsstandard hierzu einen wertvollen Beitrag leisten. Dabei ist schon heute auf die Bereitstellung dafür notwendiger technischer Voraussetzungen, wie beispielsweise den Ausbau von Glasfasernetzen, zu achten. Schon heute sind Anlagen in der Hoch- und Höchstspannung teilweise über Glasfasernetze kommunikativ angebunden. **Hierfür könnte mittel- bis langfristig eine quantenkommunikative Ertüchtigung in Erwägung gezogen werden, zum Beispiel, wenn Erzeugungsanlagen zur Bereitstellung von Primärregelleistung dienen oder als Schwarzstartanlagen kontrahiert sind**. Zudem sollte neu installierte Kommunikationstechnik in kritischen Bereichen direkt unter Berücksichtigung einer quantenkommunikativen Anbindung ausgelegt werden.

Die Einführung der Quantenkommunikation bringt dabei einige Herausforderungen für die energiewirtschaftlichen Akteure mit sich. Zum einen **ist eine flächendeckende quantenkommunikative Anbindung von Millionen dezentralen Erzeugungsanlagen mittel- bis langfristig nicht sinnvoll**, daher muss dezidiert ermittelt werden, für welche Systembereiche dieser Aufwand notwendig ist. Für die weiteren Bereiche sollten zum anderen die **Anforderungen quantenkryptografischer Verfahren berücksichtigt werden.**

Darüber hinaus ist für die Implementierung der Quantenkommunikation die Erarbeitung von Standards und Zertifizierungsvorgaben wichtig, da nur auf diese Weise eine umfassende Umsetzung und somit

[4] Jamming beschreibt die gezielte Nutzung von Störsendern, um anderen das Benutzen der Frequenz oder eines ganzen Bandes zu erschweren.
[5] Bei einem DoS-Angriff werden die für den externen Datenaustausch zuständigen Netzwerkverbindungen eines IT-Systems gezielt mit einer Unzahl an Anfragen überlastet, das System verlangsamt sich dadurch oder bricht ganz zusammen.
[6] Mehr Informationen: https://www.qunet-initiative.de/
[7] Energiewirtschaftsgesetz vom 7. Juli 2005 (BGBl. I S. 1970, 3621), das zuletzt durch Artikel 5 des Gesetzes vom 20. Juli 2022 (BGBl. I S. 1325) geändert worden ist.

Verwendung der Technologie stattfinden kann. Im Sinne der Planungssicherheit und in Anbetracht der Kosten, die mit jeder Implementierung von IKT verbunden sind, müssen klare Standards zur Orientierung gesetzt werden.

4 Herausforderungen

Quantentechnologien werden weitreichende Anwendungsgebiete der Energiewirtschaft betreffen. Aus diesem Grund ist es sinnvoll, gezielte Maßnahmen zu erarbeiten und diese in Abstimmung mit allen Stakeholdern sukzessive umzusetzen.

4.1 Nächste Schritte

Die Anwendungsmöglichkeiten von Quantentechnologien werden in den jeweiligen Branchen unterschiedlich stark diskutiert. Eine branchenübergreifende Zusammenarbeit findet bisher kaum statt. Hierfür sollte das Thema kurzfristig im Rahmen von Veranstaltungen und Themenformaten weiter beleuchtet und diskutiert werden, um Aufmerksamkeit zu generieren und alle Akteure zu sensibilisieren. Die **Vernetzung wesentlicher Akteure** aus Forschung, Photonik-Branche, IT-Branche, Start-ups und Energiewirtschaft ist dabei grundlegende Voraussetzung.

Neben der Aufmerksamkeit für die Technologien und ihre Anwendungen besteht eine Herausforderung auch darin, die Umsetzbarkeit und die dafür **notwendigen Rahmenbedingungen** in den Fokus der Zusammenarbeit rücken, um **ausreichend Anreize** zu bieten und somit gleichzeitig den **Wirtschaftsstandort Deutschland** zu stärken.

Durch den „Harvest now, decrypt later“-Ansatz ergibt sich zudem die dringliche Herausforderung, die Informationsbereitstellung und die nachhaltige **Verankerung der Post-Quanten-Kryptografie in der Energiewirtschaft** zu verfolgen. Dazu muss die Berücksichtigung der Post-Quanten-Kryptografie in entsprechende Regularien, zum Beispiel die Technischen Richtlinien des BSI, überführt und es müssen klare Zertifizierungsstandards erarbeitet werden. Eine explizite Kosten-Nutzen-Kommunikation und die Bereitstellung von Leitfäden für entsprechende Netzbetreiber und energiewirtschaftliche KMUs sollten dabei **Orientierung und Sicherheit** geben.

4.2 Ausblick

Um die Bewältigung dieser Herausforderungen zu unterstützen, ist langfristig besonders die Erarbeitung von Zertifizierungen und Standards voranzubringen, um Planungssicherheit für alle Akteure zu gewährleisten. Dabei sollte auch auf Schnittstellen zwischen den etablierten Technologien und neu einzuführenden Quantentechnologien geachtet werden, um einen störungsfreien Rollout zu gewährleisten und keine Marktbarrieren sowie unnötige Mehrkosten zu schaffen.

Nach dem aktuellen Entwicklungsstand der Technologien ist auch die weitere Forschungsförderung mit Pilot- und Demonstrationsprojekten mit den Schwerpunkten „Quantencomputing für die Energiewende“ und „Quantenkommunikation für die Energiewende“ wesentlich.

Weiterhin sollten KMUs und Netzbetreiber besonders bei der Implementierung der Quantentechnologien in Form von Analysen und Leitfäden unterstützt werden, um eine effiziente Umsetzung zu gewährleisten. Auch ist auf die Abstimmung des ganzheitlichen Energiesystems und die Verankerung der abgeleiteten Maßnah-

men in entsprechenden Regularien zu achten. Dies bedeutet ebenfalls, dass besonders kritische Energieinfrastrukturen (zukünftige Gas- und Wasserstofferzeugungsanlagen) bereits unter den Vorgaben einer quantenkommunikativen Anbindung geplant und realisiert werden sollten.

Literaturverzeichnis

Agenda Quantensysteme 2030 (2021): Agenda Quantensysteme 2030, https://www.quantentechnologien.de/fileadmin/public/Redaktion/Dokumente/PDF/Publikationen/Agenda_Quantensysteme_2030_web_C1.pdf [Zugriff: 21.09.2022].

Berger, Roland (2021): Quantentechnologie – Die nächste Disruption, https://www.rolandberger.com/de/Insights/Publications/Quantentechnologie-die-n%C3%A4chste-Disruption.html [Zugriff: 21.09.2022].

BMBF (2022): Quantentechnologien, https://www.quantentechnologien.de/index.html [Letzter Zugriff: 21.09.2022].

BSI (2018): Quantencomputer, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Quantencomputer/P283_QC_Studie-V_1_2.pdf?__blob=publicationFile&v=19 [Zugriff: 21.09.2022].

BSI (2020): Post-Quanten-Kryptografie, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Post-Quanten-Kryptografie.pdf?__blob=publicationFile&v=1 [Zugriff: 21.09.2022].

BSI (2021): Kryptografie quantensicher gestalten, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Kryptografie-quantensicher-gestalten.pdf;jsessionid=40CBD7271259EEA13D9342B2AEE9FB92.internet462?__blob=publicationFile&v=4 [Zugriff: 21.09.2022].

BSI (2022): Arten der Verschlüsselung, https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/Verschluesselt-kommunizieren/Arten-der-Verschluesselung/arten-der-verschluesselung_node.html [Zugriff: 21.09.2022].

Edwin et al. (2019): Leveraging Secondary Storage to Simulate Deep 54-qubit Sycamore Circuits (IBM T.J. Watson Research Center, 19.10.2019).

EnerQuant, 2022: Enerquant Quantencomputing Enrgiewirtschaft, https://www.itwm.fraunhofer.de/de/abteilungen/fm/flexible-lasten-energie/enerquant-quantencomputing-energiewirtschaft.html [Zugriff: 21.09.2022].

E.ON (2021): Eon allies with IBM Quantum, https://www.eon.com/en/about-us/media/press-release/2021/2021-09-02-eon-allies-with-ibm-quantum.html [Zugriff: 21.09.2022].

Europäische Kommission (2018): Quantum Technologies Flagship, https://digital-strategy.ec.europa.eu/en/policies/quantum-technologies-flagship [Zugriff: 02.08.2022].

FAZ (2021): Zwei Milliarden Euro für die Quantentechnologie, https://www.faz.net/aktuell/wirtschaft/bundesregierung-foerdert-quantentechnologie-mit-fast-zwei-milliarden-euro-17336539.html [Zugriff: 21.09.2022].

Fraunhofer-Gesellschaft (2022): Quantenkommunikation, https://www.fraunhofer.de/de/forschung/aktuelles-aus-der-forschung/quantentechnologien/quantenkommunikation.html [Zugriff: 21.09.2022].

IBM (2021): 127 Qubit Quantum Prosessor Eagle, https://research.ibm.com/blog/127-qubit-quantum-processor-eagle [Zugriff: 21.09.2022].

LBBW (2022): Quantencomputer – eine Innovation, die die Welt verändern kann, https://www.lbbw.de/konzern/research/2022/studien/20220110-lbbw-blickpunkt-corporates-quantencomputer_aehmi5wjsf_m.pdf [Zugriff: 21.09.2022].

Lee, Robert M, Assante, MJ, und Conway, T (2017): Crashoverride: Analysis of the threat to electric grid operations. Dragos Inc., März, 2017.

Mosca, Michele (2015): Session 8: Cybersecurity in a Quantum World: will we be ready?, https://csrc.nist.gov/csrc/media/events/workshop-on-cybersecurity-in-a-post-quantum-world/documents/presentations/session8-mosca-michele.pdf [Zugriff: 21.09.2022].

Shor, P.W. (1994): Algorithms for quantum computation: discrete logarithms and factoring. Proceedings 35th Annual Symposium on Foundations of Computer Science. IEEE Comput. Soc. Press: 124–134.

The Economist (2019): Google Claims to have demonstrated ‘quantum supremacy’, https://www.economist.com/leaders/2019/09/28/google-claims-to-have-demonstrated-quantum-supremacy [Zugriff: 21.09.2022].

UK Quantum Technology Hub (2021): Battery camera developed using quantum technology launches in key milestone for transport electrification, https://quantumsensors.org/news/2021/09/22/battery-camera-developed-using-quantum-technology-launches-in-key-milestone-for-transport-electrification [Zugriff: 21.09.2022].

Universität Stuttgart (2020): Quantensensoren: neue Möglichkeiten für Medizin, Alltag und Industrie, https://www.uni-stuttgart.de/universitaet/aktuelles/meldungen/quantensensoren/ [Zugriff: 21.09.2022].

Yu-Ao Chen et al. (2021): An integrated space-to-ground quantum communication network over 4,600 kilometres, https://www.nature.com/articles/s41586-020-03093-8 [Zugriff: 21.09.2022].

Y. Wu et al. (2021): Strong quantum computational advantage using a superconducting quantum processor, https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.127.180501 [Zugriff: 21.09.2022].

Zhong, H.-S., et al. (2021): Phase-programmable Gaussian boson sampling using stimulated squeezed light, https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.127.180502 [Zugriff: 21.09.2022].

Abkürzungen

AES	Advanced Encryption Standard
BMBF	Bundesministerium für Bildung und Forschung
BMI	Bundesministerium des Innern, für Bau und Heimat
BMIL	Blockchain Machine Identity Ledger
BMVg	Bundesministerium der Verteidigung
BMWK	Bundesministerium für Wirtschaft und Klimaschutz
DoS	Denial of Service
EnWG	Energiewirtschaftsgesetz
FHE	Fully Homomorphic Encryption (Homomorphe Verschlüsselung)
IKT	Informations- und Kommunikationstechnik
KI	Künstliche Intelligenz
KMU	Kleine und mittlere Unternehmen
NIST	National Institute of Standards
OT	Operational Technology
PQK	Post-Quanten-Kryptografie
Qubit	Quanten-Bit
RSA	Rivest-Shamir-Adleman
V2G	Vehicle to Grid

www.dena.de

dena
Deutsche Energie-Agentur