
LAND
OBERÖSTERREICH
KRYPTO-
GESELLSCHAFT
SICHERHEIT IN DER
DIGITALEN WELT
OBERÖSTERREICHISCHE
ZUKUNFTS
AKADEMIE

Impressum
Medieninhaber und Herausgeber:
Amt der Oö. Landesregierung
Direktion Präsidium, Oö. Zukunftsakademie
Kärntnerstraße 10-12, 4021 Linz
Tel.: +43 732 7720 14402
E-Mail: zak.post@ooe.gv.at
www.ooe-zukunftsakademie.at
Auflage: Mai 2019

Informationen zum Datenschutz finden Sie unter:
https://www.land-oberoesterreich.gv.at/datenschutz

Titelfoto: Nmedia/Retusche – stock.adobe.com

Redaktionsteam:
Mag.[a] Dr.[in] Reingard Peyrl, MSc (Projektleitung)
DI Dr. Klaus Bernhard
Mag.[a] Simone Hüttmeir
Monika Pleiner

Inhaltsverzeichnis

Zusammenfassung auf einen Blick

Der Megatrend Digitalisierung führt zur Generierung von Unmengen an Daten, die gespeichert, verarbeitet und ausgewertet werden. Jeder Mensch ist in unterschiedlicher Weise mit digitalen Vorgängen konfrontiert, vom digitalen Fernsehen und Digital-Telefonie über Computerdateien, Internet und E-Mail bis hin zu Bankomatzahlungen und Online-Käufen. Wir leben in zunehmendem Maße in einer **Kryptogesellschaft** (altgriech. „krypto“ = verborgen, versteckt), in der die Bedeutung der Informationssicherheit und Verschlüsselungssysteme größer und größer wird. Dieser Trendreport legt den Fokus auf folgende besonders relevante Bereiche:

- **Sichere Zugänge:** Die richtige Auswahl und der richtige Umgang mit Passwörtern können maßgeblich zur Sicherheit vor unbefugten Zugriffen und Manipulationen beitragen. Bedeutung kommt speziell der Authentifizierung mit mehreren Faktoren, insbesondere biometrischen Merkmalen, zu.
- **Sichere Bearbeitung und Prozesse:** Mit Blockchain-Technologien können Prozesse und Transaktionen ohne zentrale (überwachende) Stelle ablaufen. Besonders interessant für den Einsatz sind Finanzanwendungen, das Führen von Registern und lückenlosen Dokumentationen sowie Mikrotransaktionen im Internet der Dinge.
- **Sichere Datenübertragung:** Für eine sichere Datenübertragung sind drei Schritte nötig: Verschlüsselung, Übertragung und Entschlüsselung. Beim Verschlüsselungsverfahren wird ein sog. Schlüssel mit Geheiminformationen (z.B. ein Passwort, eine Geheimnummer oder auch eine Folge von Bits) verwendet.
- **Sichere Speicherung:** Mit der fortschreitenden Datafizierung unserer Gesellschaft nimmt auch die Notwendigkeit einer möglichst sicheren, aber trotzdem finanziell erschwinglichen Datenspeicherung über Jahrzehnte hinweg zu.

Unsere wachsende Kryptogesellschaft hat **positive, aber auch negative Auswirkungen auf viele unterschiedliche Bereiche**, wie zum Beispiel auf unser Gesundheitswesen, auf die Arbeitswelt und die Wirtschaft, auf die Verwaltung und unser Rechtssystem ebenso wie auf unsere Mobilität und die Umwelt.

Oberösterreich mit seinen Forschungsschwerpunkten in Bereichen der Informationstechnologien und Hardwareentwicklung, aber auch mit den vielen innovativen Technologie-Unternehmen und -Netzwerken bietet beste Voraussetzungen, um Herausforderungen der zunehmend digitalisierten Welt zukunftsorientiert zu begegnen.

Einleitung

Durch die zunehmende Digitalisierung werden immer mehr Daten gespeichert. Waren es vor wenigen Jahren noch hauptsächlich Informationen, die wir selbst z.B. zum Tätigen eines Einkaufes eingegeben haben, sind es nunmehr automatisch generierte Datensätze, die immense Mengen ausmachen. Im Jahr 2018 betrug die **globale Datenmenge** 33 Zettabyte. Ein Zettabyte sind 10^{21} Bytes (=1.000.000.000.000.000.000.000). Eine unvorstellbar große Datenflut, die vor unerlaubten Zugriffen oder Auswertungen geschützt werden muss. Innerhalb der weltweiten digitalen Vernetzung eine schier unmögliche Herausforderung: Hackerangriffe, unerlaubte Datenweitergabe, Wahlmanipulationen, Verschärfungen der Datenschutzgesetze etc. zeigen die gegenwärtige Brisanz. Für das Jahr 2025 prognostizieren das Analystenhaus IDC und Seagate einen Anstieg der Datenmenge auf 175 Zettabytes, d.h. eine Verfünffachung innerhalb der nächsten sieben Jahre. Das Internet der Dinge (IoT), selbstfahrende Fahrzeuge, virtuelle Assistenten – die digitale Smartness der kommenden Jahre vergrößert die digital vernetzte Welt mit vielfältigen Sensoren und Aktoren in einem unglaublichen Ausmaß.

Die seit Mai 2018 EU-weit anzuwendende Datenschutz-Grundverordnung (DSGVO) hat Sicherheitsbedenken und Datenschutz vermehrt in das Bewusstsein der Öffentlichkeit gerückt. Restriktive gesetzliche Rahmenbedingungen sollten jedoch die großen Zukunftschancen durch die zunehmende Digitalisierung zugleich nicht einengen. Beispielsweise sind smarte Systeme und Künstliche Intelligenz ohne digitale Daten unmöglich und etwa auch im medizinischen Bereich werden durch Big Data-Analysen große Fortschritte erwartet.

Die Gesellschaft der Zukunft mit ihrem starken **digitalen Fußabdruck** ist von Verschlüsselungsmechanismen abhängig, denn nicht alle Informationen sollten für jeden Menschen durch das World Wide Web zugänglich sein. Datenschutz beginnt im Kleinen, bei den eigenen Accounts, die durch Passwörter geschützt werden, bei den PCs und Smartphones, die mit Firewalls gegen Außenangriffe abgesichert sind, um unerlaubten Zugriff auf private Daten zu verwehren. Geht über in den Schutz von personen- und unternehmensbezogenen Daten, von Gesundheitsdaten, Bankverbindungen, Betriebsgeheimnissen und –prozessen, Forschungsergebnissen und endet im Großen: bei Informationen zur Staatssicherheit.

Wo können Daten und Informationen gestohlen bzw. „abgehört“ werden?

- am Gerät selbst, das Daten speichert oder überträgt (Netzkomponenten, Dateien)
- am Übertragungsmedium (Kupferkabel, Glasfaserkabel; bei drahtloser Datenübertragung z.B. elektromagnetische Wellen oder Laser, Satellit)
- in Computernetzen (z.B. Telefon, LAN, DSL, Mobilfunk) und
- im Internet (z.B. Router, IP-Manipulation).

Die so entstehende **Kryptogesellschaft** (altgriech. „krypto“ = verborgen, versteckt) steht vor der Herausforderung positive zukünftige Entwicklungen durch die Digitalisierung zu nützen, ohne jegliche Privatsphäre und Freiheit zu verlieren. Der vorliegende Trendreport ist in vier Teilbereiche untergliedert, die den Weg der Daten vom sicheren Zugang über Bearbeitung und Übertragung bis zur Speicherung verfolgen:

- Sichere Zugänge
- Sichere Bearbeitung und Prozesse
- Sichere Datenübertragung
- Sichere Speicherung

Im zusammenführenden Ausblick stehen Anwendungsfelder und Chancenfelder in Oberösterreich im Mittelpunkt.

1. Sichere Zugänge

Sichere Zugänge sichern schützenswerte Daten. Die richtige Auswahl und der richtige Umgang mit Passwörtern können maßgeblich zur Sicherheit vor unbefugten Zugriffen und Manipulationen beitragen. Bedeutung kommt speziell der Authentifizierung mit mehreren Faktoren, insbesondere biometrischen Merkmalen, zu.

1.1. Auswahl und Umgang mit Passwörtern

Um sensible Daten wie Bankverbindungen, aber auch andere personenbezogene Daten und private Bilder gegen potenzielle Angriffe zu schützen, kommt der **Passwort-Sicherheit** ein immer höherer Stellenwert zu.

Doch bei der Wahl eines Passwortes sind viele Personen nachlässig. Auch weiterhin lassen die beliebtesten Eingaben die nötige Passwortstärke vermissen. Nach einer Erhebung des Hasso-Platter-Instituts für Softwaresystemtechnik zeigt sich, dass 2018 das beliebteste Passwort in Deutschland 123456 war.

> TIPP #1
> Gehe sorgsam mit deinen (persönlichen) Daten um!

Laut IMAS Report (02/2018) ist der Umgang der Österreicher/innen mit eigenen Passwörtern von Sparbüchern, Social Media Accounts oder Kundenportalen mehrheitlich relativ sorglos. Nur jeder Fünfte hat ein eigenes Passwort für jeden Bereich, jeder Zweite nutzt bei beinahe jedem bzw. manchen Bereichen den gleichen digitalen Einstiegscode. Somit setzen genau genommen 51 Prozent der Bevölkerung in der Verwendung ihrer Passwörter häufig auf idente Begriffe, Namen oder Zahlenkombinationen. Nur jede/r Fünfte unterscheidet die Passwörter nach Plattform oder Account. Hierbei fällt auf, dass jüngere Personen und Menschen mit höherer Bildung differenzierter umgehen und häufiger verschiedene Passwörter verwenden. Knapp zwei Drittel der Österreicher/innen mit einem digitalen Postfach oder Social Media Zugang wechseln das Passwort nur alle zwei bis drei Jahre bzw. seltener oder nie.

Empfehlungen für die Auswahl sicherer Passwörter und den verantwortungsvollen Umgang mit Passwörtern

Auswahl sicherer Passwörter

- Ein Passwort sollte aus Großbuchstaben, Kleinbuchstaben, Ziffern und/oder Sonderzeichen (Satzzeichen, Währungssymbole etc.) bestehen. Sonderzeichen nicht an Buchstabenabfolgen anhängen sondern in das Passwort integrieren.
- Passwörter können dazu auf einem persönlichen Merksatz oder auf komplett unreflektierten Zeichenreihen beruhen. Man kreiert einen einprägsamen Satz. Aus den Anfangsbuchstaben jedes Wortes setzt man das Passwort zusammen. Einzelne Bestandteile werden durch ähnliche Sonderzeichen ersetzt.
  Beispiel: Mein Auto steht seit Januar 2019 in der Garage = MAs$01/19@dG (= kryptisches Passwort)
- Das Passwort soll mindestens acht Zeichen lang sein, für Benutzerkonten mit besonderen Rechten (Administratoren) sollte ein längeres Passwort gewählt werden. Je länger und komplexer das Passwort, desto besser.
- Namen (auch von Haustieren und Familienangehörigen), Zahlenkombinationen aus Geburtsdaten, Telefonnummern und KFZ-Kennzeichen sollten unbedingt vermieden werden. Auch sind Begriffe, die in einem Wörterbuch nachschlagbar sind, unsichere Passwörter.
- Trivialpasswörter, Tastaturabfolgen und Umlaute (aaaaaa, qwertz, asdf, 123456, 08/15, etc.) vermeiden.

Umgang mit Passwörtern

- für jede Registrierung ein neues, sicheres unterschiedliches Passwort verwenden
- sämtliche Passwörter auswendig kennen und nicht an andere Personen weitergeben
- Passwörter regelmäßig ändern
- Passwörter nicht auf elektronischen Geräten frei zugänglich ablegen oder per Mail versenden
- falls schriftliche Absicherung gewünscht, diese sicher (zB im Tresor) aufbewahren

Quelle: A-SIT – Zentrum für Sichere Informationstechnologie Austria, datenschutz.org

Ein **Passwort-Manager** ist ein Programm, das Passwörter wie eine Liste in einem Safe verwaltet. Der Vorteil eines Passwort-Managers ist es, sich einzelne Passwörter nicht mehr merken zu müssen. Somit können diese auch länger und komplizierter sein, was sie auch sicherer macht. In der Folge müssen Nutzerinnen und Nutzer nur das sogenannte **Master-Passwort** kennen, um Zugriff auf diesen Safe zu bekommen. Das Master-Passwort muss daher ganz besonders stark sein, da es Zugriff auf alle anderen Passwörter gewährt. Passwort-Manager sind meist kostenpflichtig. Zu den bekanntesten Anbietern zählen 1Password, Dashlane, LastPass oder Keypass. Nicht alle Passwort-Manager sind mit sämtlichen Geräten und Betriebssystemen kompatibel. Am sinnvollsten ist es, den Passwortmanager auf allen Geräten, die man verwendet, zu installieren.

1.2. Mehrfaktor-Authentifizierung

Eine neuere und sicherere Methode zur Anmeldung ist die Mehrfaktor-Authentifizierung. Sie folgt folgendem Prinzip: Sie erweitert Anmeldungen, die Benutzernamen (Identifizierung) und Passwort (Authentifizierung) benötigen, um einen zusätzlichen Authentifizierungsschritt. Das Entscheidende daran ist, dass dafür ein gesonderter Übertragungskanal verwendet wird.
Grundsätzlich gibt es drei unterschiedliche Möglichkeiten, um sich auszuweisen:

- durch Wissen, etwas das man weiß (z. B. Passwort)
- durch Besitz, etwas das man hat (z. B. Bankomatkarte, Token oder Tokengenerator)
- durch biometrische Merkmale (z. B. Fingerabdruck, Venen-Scan, Iris-Scan, Gesichtserkennung)

Diese mehrfache Absicherung reduziert das Risiko, dass Dritte unautorisierten Zugriff auf sensible Daten erlangen. Dazu muss die Webseite oder der Internet-Dienst eine solche Mehrfaktor-Authentifizierung aber auch anbieten. Große Internet-Dienste wie Google, Facebook, PayPal und andere setzen derartige Verfahren schon seit geraumer Zeit ein. Eine in Österreich verbreitete Lösung ist die bei Behörden eingesetzte Handy-Signatur bzw. Bürgerkarte.

Eine **bekannte Zwei-Faktor-Authentifizierung** ist das Zusammenspiel von Bankomatkarte (Besitz) und der zugehörigen PIN (Wissen). Um Bargeld beheben zu können, werden beide Bestandteile benötigt. Das Gleiche gilt für Online-Überweisungen, bei denen die Anmeldedaten (Wissen) und zur Freigabe einer Überweisung die TAN (Besitz) vorliegen müssen.

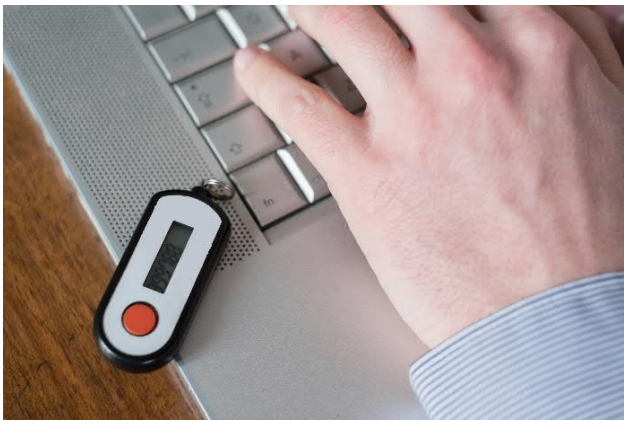

Foto: Paolese – stock.adobe.com
Zwei-Faktor-Authentifizierung mit Token

Eine neue Zwei-Faktor-Authentifizierung nutzt **Token bzw. Tokengeneratoren**: Die Benutzer/innen müssen ein Passwort kennen und in Besitz eines Tokens bzw. eines Tokengenerators sein. Der Tokengenerator generiert jede Minute einen neuen Sicherheitstoken in Form einer 6- bis 8-stelligen Zahl. Dieser Code wird nach einer Anmeldung mit Name oder Passwort an einem Terminal abgefragt und dann mit dem im Server für diesen speziellen User nach gleichen Kriterien erzeugten Code verglichen. Stimmen die Codes überein,

wird der Zugang gewährt. Der Tokengenerator kann in Form eines Hardware-Tokens zum Beispiel als Schlüsselanhänger, im Kreditkarten-Format oder Schlüssel mit oder ohne USB-Schnittstelle existieren sowie als Softwaretoken.

1.3. Authentifizierung mit biometrischen Erkennungsverfahren

Biometrie ist eine Authentifizierungsmethode, die zur Personen-Identifikation biologische Merkmale wie Fingerabdruck, Augeniris oder Stimme verwendet. Ein biometrischer Scanner liest diese Merkmale und wandelt das Ergebnis in digitale Informationen um, so dass ein Computer diese interpretieren und verifizieren kann.

Im Vergleich zu anderen Systemen wie Passwörtern bieten biometrische Systeme ein Mehr an Sicherheit. Denn PINs und Passwörter erfassen lediglich personenbezogene Merkmale, die sich problemlos an andere Personen weitergeben lassen und vergessen oder gestohlen werden können. Bei biologischen Eigenschaften ist das schwieriger möglich. Biometrische Merkmale, wie der im Ausweis verwendete Fingerabdruck, aber auch die Iris beinhalten Eigenschaften, die einen Menschen eindeutig charakterisieren. Dieses biometrische Muster hat nur ein Mensch. Biometrische Eigenschaften sind **personengebunden**.

Grob unterscheidet man biometrische Merkmale in physiologiebasierte und verhaltensbasierte Charakteristika. **Physiologiebasierte** Charakteristika beziehen sich auf dauerhafte äußere Merkmale einer Person und sind passiv. Dazu gehört die Gesichts-, Venen- und Iriserkennung und der Fingerabdruck. Diese Attribute sind statisch-unveränderlich und bleiben das ganze Leben erhalten. Die **verhaltensbasierten** Charakteristika richten sich hingegen auf das aktive Handeln, welches Änderungen unterliegt. Zu den verhaltensbezogenen Charakteristika gehören die Stimme, die Unterschrift oder der Anschlagsrhythmus der Tastatur. Diese Merkmale sind aktiv und dynamisch, also veränderlich. Da sie von der Physiologie und den Emotionen beeinflusst werden, unterliegen sie natürlichen Schwankungen.

Der **Fingerprint** ist das älteste und derzeit am weitesten verbreitete biometrische Verfahren. Sensoren eines Lesegerätes scannen in wenigen Sekunden Linienverläufe, Wirbel, Schlingen und Verzweigungen des Fingerabdrucks. Als Zugangsidentifikation für Computersysteme und Mobilgeräte wie Notebooks, Tablets, Smartphones sowie für Autos ist der Fingerabdruck-Scan bereits weit verbreitet.

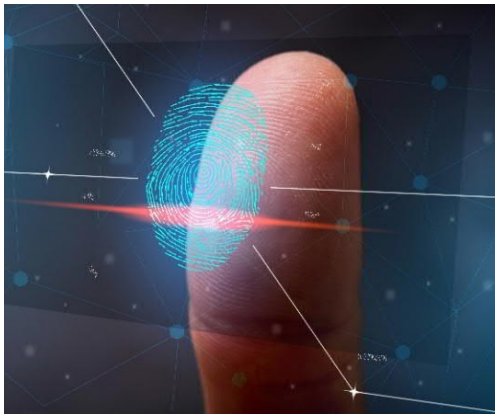

Foto: Artem - stock.adobe.com
Authentifizierung durch Fingerprint

Iris-Scanning gilt als besonders genaue Identifizierungstechnologie, da sich die Merkmale der Iris (= Regenbogenhaut) im Verlauf des Lebens eines Menschen nicht verändern. Zudem weist die Iris mehrere hundert messbare Variablen auf. Iris-Scanning ist ein schnelles Verfahren, das nicht länger als ein bis zwei Sekunden dauert. Mit einem speziellen Scan-Mechanismus werden individuelle optische Eigenschaften des farbigen Bereichs um die Pupille herum aufgenommen. Ein durch Infrarotlicht unterstütztes Kamerasystem kann das Muster der Iris auch bei erschwerten Lichtverhältnissen erkennen.

Foto: Sergey Nivens - stock.adobe.com
Authentifizierung durch Iris-Scanning

Die **Venenerkennung** gilt als sicheres biometrisches Verfahren zur Identifizierung von Menschen. Venen sind schwierig auszulesen, da sie sich im Körperinneren befinden. Die Hand wird vor einen Sensor gehalten, der das Venenmuster der Handfläche oder eines Fingers berührungslos erfasst. Dies gelingt mit Hilfe einer Infrarotstrahlung, die vom sauerstoffarmen venösen Blut absorbiert wird. Das daraus erstellte Bild wird mit der Datenbank abgeglichen und das System erkennt zutrittsberechtigte Personen. Der Venenscan wird als Zutrittsschutz zu Hochsicherheitsbereichen z.B. in Atomkraftwerken, Bank- oder Regierungsgebäuden angewendet.

Gesichtserkennung bezeichnet die Analyse der Ausprägung sichtbarer Merkmale im Bereich des frontalen Kopfes gegeben durch die geometrische Anordnung von Augen, Nase, Mund und Kinn und Textureigenschaften. Bei der zwei-dimensionalen geometrischen Vermessung werden die Position, der Abstand und die Lage zueinander von Augen, Nase, Mund bestimmt. Das deutlich sicherere 3D-Verfahren tastet hingegen beispielsweise durch Streifenprojektion oder mit einem komplexen Kamerasystem das Gesicht dreidimensional ab. Es werden ein 3D-Tiefenmodell und ein Referenzfoto erzeugt. Dieses Referenzfoto wird mit späteren Fotos der Anwendenden verglichen.

Sprach- oder Stimmerkennung ist die einzige biometrische Technologie, die nichtvisuelle Eigenschaften des menschlichen Körpers vermisst. Bei der Stimmerkennung werden die Tonvibrationen in der Stimme einer Person gemessen und mit bestehenden Mustern verglichen. Normalerweise muss dazu die zu identifizierende Person ein bestimmtes Erkennungswort oder einen ganzen Erkennungssatz aussprechen. Stimmerkennungs-systeme werden oft am Telefon und im Telebanking eingesetzt.

Eine weitere biometrische Option ist ein **Authentifizierungssystem zum Tippverhalten**. Diese Technologie misst die Art und Geschwindigkeit des Tastendrucks eines Users – getippte Wörter pro Minute, häufige Fehler und Buchstabenfolgen. Die Informationen werden in einem Systemverzeichnis gespeichert und können in der Folge verwendet werden, um einen User zu authentifizieren.

2. Sichere Bearbeitung und Prozesse

Im Jahr 2008 als Antwort auf riskante Geschäfte und „faule“ Kredite, die in eine weltweite Finanz- und Wirtschaftskrise führten, wurde unter dem Pseudonym Satoshi Nakamoto ein Whitepaper für eine dezentrale Währung, den Bitcoin, verfasst – eine erste Anleitung für die Blockchain-Technologie als open source.[1] Der Boom um die Währung, rasante Aufstiege und Preisverfälle, Hacker-Angriffe, aber auch Unzufriedenheiten mit zentralisierten Systemen sicherten der Blockchain-Technologie ungeahntes Forschungsinteresse und rückten sie immer mehr in den Fokus der Öffentlichkeit. Wie können die Vorteile einer Dezentralisierung in einer immer stärker digitalisierten Welt genutzt werden? Wie können Datensätze und Transaktionen sicher dokumentiert werden? Wie gelingen automatisierte Prozesse schneller?

2.1. Blockchain-Technologien

Die Blockchain-Technologie beruht auf dem **Peer-to-Peer-Prinzip** und schaltet damit eine zentralisierte (überwachende) Stelle aus. Bei Finanztransaktionen sind das beispielsweise die Banken. In immer mehr anderen Anwendungsfeldern kommen Blockchains zum Einsatz. Notare zur Beurkundung könnten zukünftig überflüssig werden und auch Wirtschaftsprüfungen würden in einem effizienten großen Blockchain-Netzwerk unnötig. Auch für öffentliche Einrichtungen, die die Aufgabe haben öffentliche Register zu führen oder die als Zertifizierungsstelle dienen, hat die Blockchain-Technologie revolutionierendes Potenzial.

Eine Blockchain funktioniert wie ein Notizbuch, das auf **viele verschiedene Rechner** verteilt ist. Jeder Netzwerk-Knoten verfügt über eine vollständige Kopie. Eine einzige zentrale Speicherung wie es gegenwärtig meistens der Fall ist, z.B. lokal am PC, auf den Firmenservern oder in der Cloud, gibt es nicht mehr. Soll nun ein neuer Eintrag ins Notizbuch erfolgen, gibt es keine autorisierende Stelle mehr, sondern die Durchführung (= Transaktion) wird per **Mehrheits-Konsens** auf ihre Richtigkeit überprüft und abgespeichert. Mehrere Transaktionen werden in einen Block zusammengeführt und an den vorherigen angereiht (= Kette, daher der Name Blockchain). Dieses System ist gegenüber Manipulationen vergleichsweise sicher, da

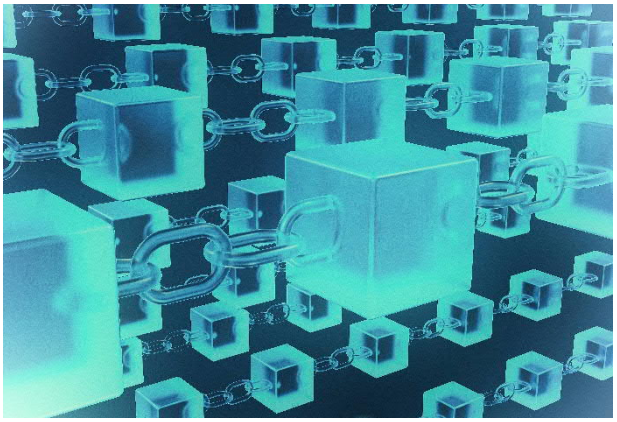

Foto: kugelwolf – stock.adobe.com
Verbildlichte Darstellung einer Blockchain

[1] siehe auch: https://www.ooe-zukunftsakademie.at/Zukunftsthema_digitaleWaehrung_2015.pdf

jede Veränderung zeitgleich an vielen dezentralen Knotenpunkten erfolgen müsste, um unbemerkt in die Blockchain zu gelangen. Durch die Dezentralisierung ist das System auch sehr robust gegenüber dem Ausfall einzelner Knotenpunkte.

Mittlerweile gibt es neben den öffentlichen Blockchains wie Bitcoin oder Ethereum auch private Blockchains und Konsortium-Blockchains, die nur einem bestimmten Teilnehmendenkreis zugänglich sind. Auch müssen nicht alle Teilnehmer/innen in einer Blockchain über sämtliche Lese- und Eintragungsrechte verfügen, was die Transparenz als einen der großen Vorteile der Blockchain-Technologie etwas einschränkt („relative Anonymität“).

Die Konsensfindung zur Verifizierung und Eintragung einer neuen Transaktion benötigt etwa durch zu lösende kryptografische Rätsel **enorme Rechenleistungen**, was mit hohem Energieverbrauch und Verzögerungen in der Transaktionsabwicklung einhergeht, denn der langsamste Knoten bestimmt die Performance des Systems. Für das Lösen des Rätsels werden die Teilnehmenden mit einem Anteil (z.B. Bitcoins) belohnt. Man spricht vom sogenannten „Mining“.

Dies zeigt nun auch schon einige Schwachstellen der Blockchain-Technologie auf, weshalb der derzeitige Hype um Blockchain-Anwendungen nur schwer einzuschätzen ist. Viele Unternehmen treten an Blockchain-Dienstleister heran, um sichere und effiziente Lösungen für ihre Geschäftsfälle und –prozesse zu realisieren (**BaaS = Blockchain as a Service**). Oftmals geschieht dies ohne die entsprechenden Voraussetzungen und Standards mitzubringen, weshalb herkömmliche Applikationen z.B. eine zentral gespeicherte Datenbank effektiver, schneller und billiger wären. Um bestmögliche Ergebnisse zu erzielen, wird im Unternehmensbereich auch mit neuen Architekturen gearbeitet. Die Blockchain wird als Data Layer mit der kleinstmöglichen, notwendigen Logik verwendet. Komplexere Business-Strukturen liegen jedoch in einem eigenen Layer („Kryplet-Technologie“).

TIPP #2
Blockchain-Technologien sind nicht für alle Anwendungen geeignet. Wäge Kosten und Nutzen ab bzw. lasse dich von einem Profi beraten!

Als weitere Herausforderung für alle Anwendungen, die wie die Blockchain auf vernetzte Knotenpunkte verteilt sind, werden ältere Einträge zwar mit jedem weiteren verifizierten Eintrag sicherer und unveränderbar gespeichert, jedoch muss der Inhalt der verifizierten Transaktion nicht zwangsläufig auch der Wahrheit entsprechen. Ein Beispiel ist etwa die Anwendung bei Lieferketten in der Logistik. Soll nun z.B. die Biozertifizierung eines Produktes unveränderbar hinterlegt werden, kann das ein/e Netzwerkteilnehmende/r beantragen, ohne dass etwa eine unabhängige Stelle dies vorher auch tatsächlich geprüft hat. Hier muss es im Vorfeld einen Konsens über automatisierte Abläufe und Kriterien geben. Zur Überprüfung der

Einhaltung vertraglicher Regeln gibt es sogenannte **Smart Contracts**. Sie sind nicht als herkömmliche Verträge anzusehen, sondern sind vielmehr automatisch ausführbare Programme. Wenn eine Transaktion alle vorher definierten Kriterien erfüllt, wird sie automatisch eingetragen, was die Transaktionskosten senkt.

Neben der Blockchain wird an weiteren sicheren Verfahren zur Verarbeitung von Daten und Abwicklung von Prozessen gearbeitet. Die Blockgenerierung braucht nicht nur, wie bereits erwähnt, hohe Rechenleistungen, sie braucht auch viel Zeit und sehr viel Bandbreite. Vor allem für Anwendungen im Bereich der Maschine-Maschine-Kommunikation in einem Internet der Dinge, in dem viele unterschiedliche Komponenten miteinander vernetzt sind, ist eine echtzeitnahe Transaktionsabwicklung unabdingbar. So ist beispielsweise **Tangle** zwar grundsätzlich einer Blockchain nicht unähnlich, hat aber kein Miningsystem. Für eine Transaktion müssen die Teilnehmer/innen zwei andere Transaktionen verifizieren. Die dazu nötigen kryptografischen Verfahren brauchen wenig Rechenleistung und können rasch durchgeführt werden, was bei einer Netzwerkgröße von mehreren Tausend Knotenpunkten bereits rund 1000 Transaktionen pro Sekunde ermöglicht. Das ist vielversprechend für Mikrotransaktionen smarter Technologien, wie etwa bei der Übertragung von einzelnen Sensorwerten.

2.2. Digitale Signatur und elektronischer Identitätsnachweis

Um in großen Netzwerken mit vielen verbundenen Clients sichere Transaktionen durchführen zu können, werden digitale Signaturen verwendet. D.h. ein individueller zuordenbarer Schlüssel wird einer Datei beigefügt, die den/die Urheber/in sicher identifiziert. Bei einer Manipulation der signierten Transaktion würde der Schlüssel mit der Datei nicht mehr zusammenpassen und einer Prüfung nicht standhalten.

Die österreichische Handy-Signatur und die Bürgerkarte sollen in ein neues EU-weites e-ID-System überführt werden. Schrittweise sollen alle EU-Bürger/innen mit einem elektronischen Identitätsnachweis (e-ID) ausgestattet werden. Damit sollen digitale Prozesse besonders auch im Bereich des e-Governments rascher und sicherer abgewickelt werden können. Die Identifizierung bei Behörden und das rechtsgültige elektronische Unterfertigen von Dokumenten ist ein nicht zu unterschätzender Benefit der e-ID und wird neue Modelle im Bürger/innen-Service ermöglichen. Der elektronische Identitätsnachweis führt aber auch in allen anderen

> TIPP #3
> Ab voraussichtlich 2020 wird die einheitliche europäische e-ID in Österreich eingeführt. Sie gibt dir mehr Sicherheit in allen Bereichen des digitalen Lebens durch eindeutige Identifizierung und ist EU-weit gültig!

Bereichen des digitalen Lebens zu mehr Sicherheit durch eindeutige Identifizierung. Online-Einkäufe und Bankgeschäfte sind nur die naheliegendsten Anwendungen. Grundsätzlich könnten alle Anwendungen, die die Angabe eines Benutzernamens und Passworts benötigen, über die e-ID zugänglich gemacht werden. In einem Ausbauschritt der e-ID ist die Hinterlegung von weiteren personenbezogenen Merkmalen angedacht, auch einzelne Befugnisse (z.B. Führerschein) können vermerkt werden. Besondere Herausforderung ist dabei einmal mehr der Datenschutz.

3. Sichere Datenübertragung

Digitale Daten durchdringen immer mehr unseren Alltag – von der Handytelefonie über PIN-Nummern-Eingaben bis zur Online-Bestellung. Dabei ist es essenziell, dass Informationen sicher und nicht für alle zugänglich gespeichert und übermittelt werden. Sichere Datenübertragung kann nicht für sich alleine betrachtet werden, sie besteht aus den Schritten Verschlüsselung – Datenübertragung – Entschlüsselung. Die **Kryptografie**, die Lehre von der Verschlüsselung von Daten, beschäftigt sich mit Methoden, die die Daten durch Verschlüsselung und verwandte Verfahren vor unbefugtem Zugriff schützen. Im Gegensatz zur Kryptografie befasst sich die **Kryptoanalyse** mit der unbefugten Entschlüsselung von verschlüsselten Daten. Beides gemeinsam wird unter dem Begriff **Kryptologie** zusammengefasst.

3.1. Grundlegende Verschlüsselungsverfahren

Beim Verschlüsselungsverfahren, auch **Verschlüsselungsalgorithmus oder Chiffre** genannt, wird ein sog. Schlüssel mit Geheiminformationen verwendet. Dieser Schlüssel kann je nach Verfahren z.B. ein Passwort, eine Geheimnummer oder auch eine einfache Folge von Bits sein.

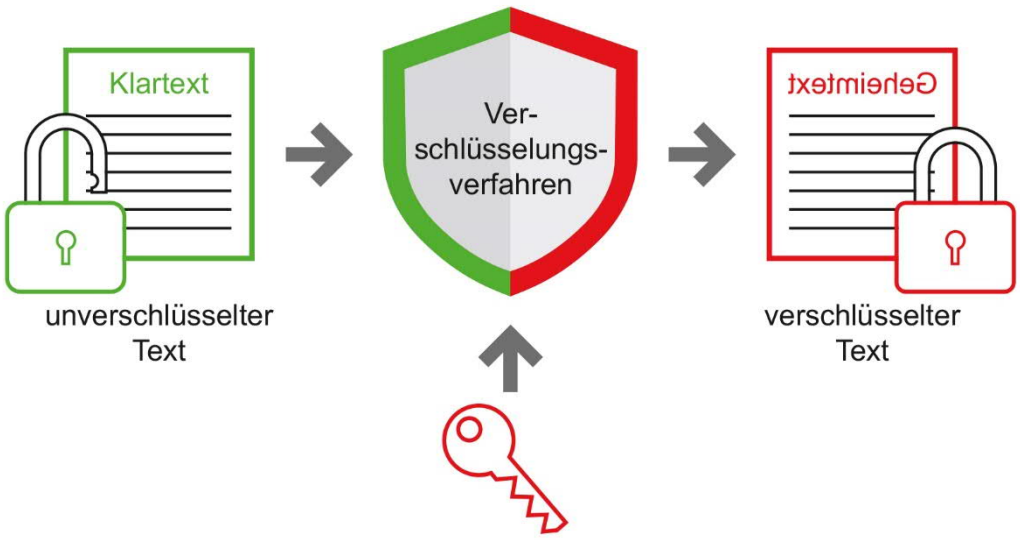

Abb.1.: Ablauf eines Verschlüsselungsverfahrens (Quelle: Schmeh 2016, eigene Darstellung)

Die Basis von Verschlüsselungsverfahren liegt in der Unterscheidung private Schlüssel und öffentliche Schlüssel.

In der sog. **Symmetrischen Verschlüsselung**, auch Secret-Key-Verfahren genannt, liegen die Anfänge der Kryptografie. Dabei gibt es nur einen geheimen bzw. privaten Schlüssel: der Text wird auf die gleiche Weise ver- und entschlüsselt. Das heißt, alle Beteiligten müssen den Schlüssel kennen. Wichtig dabei ist natürlich die sichere Weitergabe des geheimen Schlüssels an den/die Empfänger/in, denn sobald Unbefugte den Schlüssel in Händen haben, ist die Verschlüsselung wertlos. Früher wurde er meist persönlich, z.B. mittels Boten, weitergegeben.

Abb.2.: Symmetrische Verschlüsselung (eigene Darstellung)

Heute bedient man sich der **Asymmetrischen Verschlüsselung** oder dem Public-Key-Verfahren, v.a. um Probleme bei der Schlüsselweitergabe zu vermeiden. Dabei gibt es zwei Schlüssel: die Daten werden mit einem öffentlich zugänglichen Schlüssel chiffriert und mit einem privaten Schlüssel dechiffriert, den nur der/die Empfänger/in besitzt. Das bedeutet, quasi jede/r Beteiligte kann Daten mittels bekanntem Schlüssel verschlüsseln, aber für die Entschlüsselung gibt es nur einen – geheimen – Schlüssel pro Person.

Abb.3.: Asymmetrische Verschlüsselung (eigene Darstellung)

Die **Hybride Verschlüsselung** oder PGP (Pretty Good Privacy) ist eine kombinierte Chiffrier-Methode, bei der die Datenübertragung mittels symmetrischer Verschlüsselung erfolgt, der Schlüssel selbst jedoch zuvor mittels asymmetrischer Verschlüsselung codiert und so übertragen wird. Dieses Verfahren läuft zumeist auch auf unseren Rechnern, denn die Kombination mit symmetrischer Verschlüsselung bedeutet weniger Rechenaufwand und somit schnelleres Codieren.

Das Alphabet war lange Zeit die Basis für Verschlüsselung, heute ist es das **Binärsystem** mit binären Codes. Die Zahlen 0 und 1 bilden Bits und Bytes und sind zentral bei der Codierung in der modernen Kryptografie des Computerzeitalters.

Mathematisch funktioniert das Ver- und Entschlüsseln vereinfacht gesagt über Berechnungen, die in eine Richtung sehr leicht, in die andere hingegen schwierig zu lösen sind. Dabei wird heute mit der Multiplikation von großen und sehr großen **Primzahlen** gearbeitet. Der öffentliche Schlüssel ist das Ergebnis der Multiplikation zweier Primzahlen. Um die Daten zu entschlüsseln, braucht man die beiden Ausgangsprimzahlen. Diese sind der private Schlüssel.

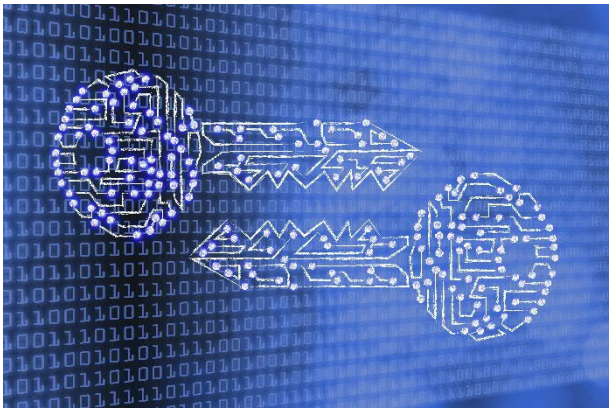

Foto: faithie – stock.adobe.com
Verschlüsselung

3.2. Verschlüsselung für Datenübertragung in der Anwendung

E-Mail – Messenger-Dienste – digitales Bezahlen – elektronische Ausweise – Online-Ein- und Verkauf – digitale Wahlen – Blockchain. Wir kommunizieren, arbeiten, kaufen, lesen etc. heute digital und kaum ein Informationsfluss läuft noch ungesichert ab. Viele verschiedene Methoden der Verschlüsselung und Codierung finden dabei Anwendung bei der Datenübermittlung. Einige Beispiele:

- **Ende-zu-Ende-Verschlüsselung**. Im Alltag kennen wir diesen Begriff vor allem von Messenger-Diensten wie WhatsApp. Dabei werden die Daten bei den Sendenden verschlüsselt und erst bei der empfangenden Person wieder entschlüsselt. Unterwegs können sie ohne Schlüssel nicht gelesen werden. Das heißt, auch ein Anbieter, auf dessen Server solche Daten liegen, kennt den Schlüssel nicht und kann mit den darin enthaltenen Informationen nichts anfangen.

> TIPP #4
> Sollen Daten besonders sicher übertragen werden, ist die Ende-zu-Ende-Verschlüsselung eine gute Wahl!

- **Punkt-zu-Punkt-Verschlüsselung oder Transportverschlüsselung**. Im Gegensatz zur obigen Methode sind bei dieser Art der Codierung Daten nur verschlüsselt, solange sie unterwegs sind, also z.B. zwischen zwei Geräten in einem Rechnernetz. Um beim Beispiel Messenger-Dienst zu bleiben heißt das, dass Nachrichten unverschlüsselt am Server eines Anbieters liegen.

- **Hash-Funktionen**. Die digitale Kommunikation und Information lässt heute jedem Menschen Informationen aus unzähligen Quellen zukommen. Daher wird es immer wichtiger, den Ursprung einer Nachricht bzw. die Authentizität von Sender/in oder der Sendeadresse erkennen zu können. Hash-Funktionen dienen dieser Authentifizierung von Nachrichten und Schlüsseln. Das Signieren einer Nachricht erfolgt i.d.R. über mathematische Ressourcen – die sog. Hash-Funktionen: Algorithmen erzeugen aus der Originalnachricht eine einfache Bit-Kette, den sog. Hash. Breite Anwendung finden Hash-Funktionen heute z.B. in der Blockchain-Technologie.

- **Fehlerkorrigierende Codes**. Bei der digitalen Datenübertragung wird eine Nachricht, nachdem sie erzeugt wurde, in einem Binärsystem verschlüsselt und gelangt in den Kommunikationskanal. Dieser besteht aus den Computern von Sender/in und Empfänger/in und aus der eigentlichen Verbindung (z.B. Kabel, Funkwellen, Infrarot). Auf diesem Weg kann es zu Störungen, dem sog. Rauschen kommen – beispielsweise durch physikalische Einflüsse oder durch eine Vermischung mit anderen Signalen. Fehlerkorrigierende Codes können Probleme bei der digitalen Datenübertragung erkennen und Fehler gegebenenfalls korrigieren.

- **Code Signing** ist eine Methode zur Erkennung bzw. Bekämpfung von Schadsoftware, die wir beim Runterladen von Software auf unseren Rechner nutzen können. Die Software wird von seinem/r Urheber/in digital signiert. Will man eine Datei ausführen, überprüft man zuvor diese Signatur: ein positives Ergebnis bestätigt, dass die Software vom/von der angegebenen Hersteller/in stammt. Dies garantiert freilich nicht, dass das Programm nicht schädlich ist, lässt es aber bei vertrauenswürdigen Urhebern/innen annehmen.

3.3. Quanten- und Post-Quanten-Kryptografie

Die sog. **Quantenkryptografie** basiert auf einer völlig neuen Technologie der Verschlüsselung – sie arbeitet mit dem Licht. An ihrer Entwicklung arbeiten weltweite Forschungsprojekte seit einigen Jahren intensiv. Der österreichische Quantenphysiker Anton Zeilinger erklärt:
„Wir nutzen hier die Teilchen des Lichts, Photonen genannt. Für diese gelten Quantengesetze. Das Zentrale für die Verschlüsselung ist, zwei Teilchen miteinander zu verschränken. Das bedeutet: Sie bleiben über große Entfernungen miteinander in Verbindung, obwohl eigentlich keine direkte Verbindung zwischen ihnen besteht. Was immer man mit einem Teilchen tut, beeinflusst scheinbar augenblicklich auch den Zustand des anderen Teilchens. Messe ich also ein Photon an einem Ort und ein weiteres an einem anderen, dann geben beide eine zufällige Antwort. Die allerdings stimmt überein. Das ist der Schlüssel.“ (ZEIT ONLINE 2016)

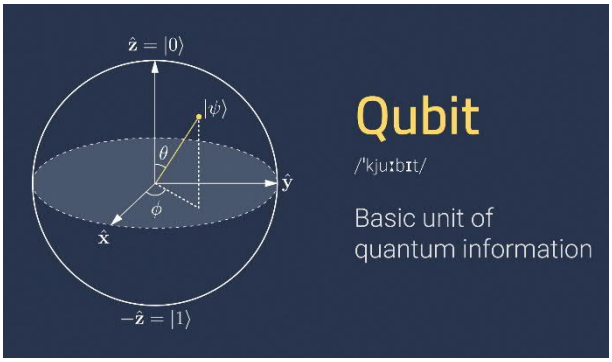

Foto: Astibuag – stock.adobe.com
Qubit – Maß für die Quanteninformation

Das sog. **Qubit** übernimmt dabei die gleiche Rolle wie das Bit beim klassischen Computer.
Das Qubit ist die kleinstmögliche Speichereinheit und definiert gleichzeitig das Maß für die Quanteninformation. Im Unterschied zu den Bits können Qubits aber unendlich viele Mischzustände zwischen 0 und 1 annehmen. Außerdem können sich mehrere Qubits in einem verschränkten Zustand befinden.

Da ein Quantenschlüssel durch echten Zufall entsteht und nicht durch einen Computer erstellt wird, kann er auch von Hochleistungsrechnern heutiger Bauart nicht geknackt werden. Zapft jemand einen Quantenstrom an, verändert er die Eigenschaften der Photonen und der Hacker fliegt sofort auf. Der/die Sender/in kann dann die Übertragung einfach stoppen und es mit einem neuen Schlüssel auf einer anderen Leitung versuchen. Ein internationales Datennetzwerk, das sog. Quanteninternet, ist Voraussetzung für diese Art der Kommunikation im Alltag. Die Entwicklung dorthin verläuft rasant.

Auch die Forschung rund um Quantencomputer pulsiert. Diese nutzen als Rechen- und Speichereinheiten ebenfalls Qubits. Quantencomputer werden heute schon als Megacomputer bezeichnet, denn sie werden komplexe Optimierungsaufgaben lösen, große Datenmengen analysieren oder etablierte und weitverbreitete Verschlüsselungsmethoden knacken können. Und: in ihnen steckt jedenfalls das Potenzial, auch Quantenschlüssel zu knacken.

Post-Quanten-Kryptografie. Unter diesem Begriff werden all jene asymmetrischen Krypto-Verfahren zusammengefasst, die von einem Quantencomputer nicht geknackt werden können. Denn Experten/innen, z.B. die NASA, empfehlen den Einsatz von sog. Post-Quantum-Algorithmen gegen zukünftige Superhacker.

Hier bewegen wir uns – noch – auf Zukunftsterrain, aktive Forschungen gibt es aber auch zu diesem Themenfeld schon. Inzwischen intensiviert u.a. die EU in das Forschungsgebiet der Post-Quanten-Kryptografie. Das 2015 gestartete Projekt PQCRYPTO (Post-Quantum Cryptography) fördert die EU-Kommission mit 3,9 Millionen Euro. Beteiligt sind Universitäten und Unternehmen aus elf Ländern.

4. Sichere Speicherung

Mit der fortschreitenden Digitalisierung unserer Gesellschaft nimmt nicht nur die anfallende Datenmenge exponentiell zu, sondern auch die Notwendigkeit einer möglichst sicheren, aber trotzdem finanziell erschwinglichen Datenspeicherung über Jahrzehnte hinweg.

4.1. Digitale Speichersysteme im Wandel der Zeit

Wie schnell die Entwicklung von Datenspeichersystemen voranschreitet, zeigt das Beispiel der klassischen 3,5 Zoll **Floppy Disk**. Während in den achtziger und frühen neunziger Jahren diese Form der Datenspeicherung sowohl im geschäftlichen als auch im privaten Umfeld weit verbreitet war, kennen viele junge Menschen dieses Medium gar nicht mehr.

Foto: sierra21 – stock.adobe.com
Speichermedium der Vergangenheit: 3,5 Zoll Diskette

Mittlerweise befinden sich auch die darauf folgenden optischen Datenträger **CD** und **DVD** auf dem Rückzug. Aufgrund der sehr hohen Speicherkapazität sind **Blu-ray Disks** weiterhin besonders als Medium für Filme, Video- und Computerspiele beliebt.

Die Lebensdauer dieser Speicher konnte kontinuierlich verbessert werden: Während Floppy Disks häufig schon nach 5-10 Jahren defekt wurden, wird die maximale Lebensdauer von CDs und DVDs mit bis zu 30 Jahren, bei Blue-Rays sogar mit bis zu 100 Jahren angegeben.

Zu den derzeit am häufigsten verwendeten Speichermedien gehören **Festplattenlaufwerke** (hard-disk-drive, HDD), bei welchen Daten auf die Oberfläche rotierender magnetisierbarer Scheiben geschrieben werden. Ohne bewegliche Teile kommen **SSD Speicher** (solid-state drives) aus. Solid-state drives basieren auf der Speicherung von Informationen in Form von elektrischen Ladungen in winzigen Speicherzellen. Auf dieser Technologie beruhende Beispiele sind **SSD Festplatten** oder die bekannten **USB-**

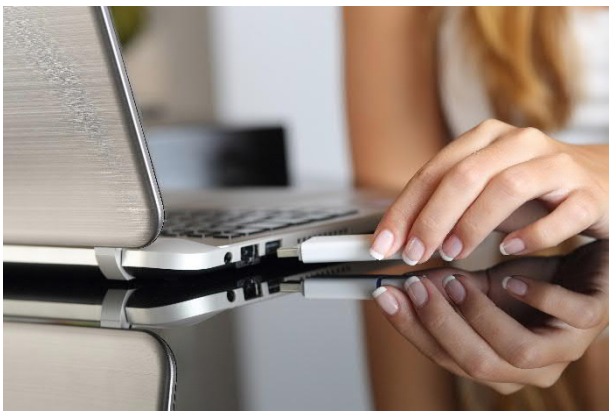

Foto: Antonioguillem – stock.adobe.com
Speichermedium der Gegenwart: USB-Sticks

Sticks. Während SSD Platten derzeit noch etwas geringere Speicherkapazitäten als die HDD aufweisen, sind aber die Zugriffszeiten deutlich geringer. Auch das Fehlen mechanischer Teile erhöht die Zuverlässigkeit sowie Robustheit im Vergleich zu HDD Speichern.

Um die Zuverlässigkeit von klassischen Speichern zu erhöhen, dienen sogenannte **RAID-Systeme**, also „redundant arrays of independent disks“, (=„redundante Anordnung unabhängiger Festplatten“). Für einen Schutz vor unerwünschten Zugriffen werden insbesondere für portable Datenspeicher wie externe Festplatten immer bessere Varianten der Verschlüsselung ersonnen, wie eine Hardwareverschlüsselung, die die Eingabe eines Kennwortes erfordert („**Data Locker**“).

Eine Alternative zur Speicherung von Daten auf eigenen Computersystemen bieten zunehmend **Cloudlösungen** an, wobei aber Restrisiken der Datensicherheit (technisches Gebrechen oder Konkurs der Cloudanbieter, missbräuchliche Zugriffe durch Hacker etc.) verbleiben.

TIPP #5
Lokale Speichermedien können kaputt gehen. Lege Backups an verschiedenen Orten an oder verwende sichere Cloudspeicher!

4.2. Datenspeicher in Entwicklung

Bei allen gebräuchlichen Systemen nehmen die maximalen Speicherkapazitäten weiter kontinuierlich zu, wahrscheinlich existieren aber physikalische Grenzen, die z.B. bei magnetischen Speichern künftig nicht mehr überschritten werden können. In Hinblick auf die wachsenden Datenmengen und eine möglichst hohe Zuverlässigkeit aber auch in Hinblick auf einen möglichst geringen Stromverbrauch wird weltweit an alternativen Lösungen geforscht, von denen im Folgenden einige vorgestellt werden:

Forschende der Universität Southampton (UK) entwickelten einen „ewigen“ Datenspeicher, der Daten solange speichern soll, wie unser Universum bereits existiert (13,8 Milliarden Jahre bei 190°C). Ein Femtosekundenlaser beschreibt hierzu eine nanostrukturierte **Glas-Disk**, wobei unter Verwendung der Polarisationseigenschaften von Nanopartikeln Informationen in fünf Dimensionen abgespeichert und somit eine Kapazität von 360 TB erreicht wird. Mit einer thermischen Stabilität bis zu 1.000 °C könnte die Disk sogar manche Brände überstehen.

Eine aus der Bionik abgeschaute Möglichkeit zur dauerhaften Speicherung großer Datenmengen benützt eine künstlich hergestellte **DNA**. Schon seit Jahren können einerseits DNA Stränge mit biochemischen Verfahren künstlich hergestellt werden und andererseits mit kommerziell verfügbaren Sequenzierautomaten wieder ausgelesen werden. Im Vergleich zu anderen Methoden ist mit deutlich längeren Zugriffszeiten zu rechnen. Vorteil der von einer

Bioinformatikergruppe an der Columbia University in New York erstmals praktisch mit einem speziellen Algorithmus umgesetzten Methode ist die theoretisch enorm hohe Speicherdichte von 215.000 Terabyte pro Gramm. Forscher/innen arbeiten auch an der Speicherung von Informationen in organischen Molekülen. Eine Kodierung mit diesen sogenannten **„MolBits“** soll wenig Energie benötigen und schneller als die DNA Speicherung sein.

Foto: Korn V. – stock.adobe.com
Künftiges mögliches Speichermedium DNA

Eine weitere mögliche Variante zur Speicherung großer Datenmengen, mit der einige Zukunftshoffnungen verbunden werden, ist die sogenannte Racetrack (deutsch „Rennstrecke“) Technologie, die beispielsweise am Max-Planck-Institut für Mikrostrukturphysik in Halle (D) erforscht wird. **Racetrack-Speicher** legen die Information in winzigen Abschnitten eines magnetisierbaren Nanodrahts ab. Die Informationen lassen sich mit kleinen Stromstößen im Draht vor- und zurückschieben, sodass sie einfach zum Schreib- und Lesekopf des Datenspeichers manövriert werden können. Auch Racetrack-Speicher benötigen somit keine beweglichen Teile mehr, was die Vorteile von HDD und SSD Speichern kombinieren könnte. Der Energieverbrauch ist sehr gering, was bei der steigenden Anzahl elektronischer Geräte weltweit immer mehr Bedeutung erlangen wird.

Auf Grund der sehr schnellen technologischen Fortschritte herkömmlicher Geräte sind einige als durchaus innovativ einzustufenden Entwicklungen von Prototypen nicht zur Marktreife entwickelt worden. Allerding ist nicht auszuschließen, dass künftig die eine oder andere dieser „im Sand verlaufenen“ Entwicklungen wieder einmal aufgegriffen und auf eine andere Art und Weise realisiert werden.

Foto: videodoctor – stock.adobe.com
Künftige Datenspeicherung als Hologramm?

Zwei derartige Beispiele sind die **Protein coated Disk** und der **holografische Speicher**, die um das Jahr 2007 großes Interesse hervorriefen. Während bei der Protein coated Disk das Medium eine mit Eiweißen beschichtete Diskette war, sollte die holografische Speicherung in speziellen Kristallen als dreidimensionales Hologramm erfolgen. Neben den erwähnten schnellen Fortschritten der klassischen Speicher trugen auch die hohen Kosten (Holografie) sowie technische Schwierigkeiten (Haltbarkeit der Eiweißbeschich-

tung bei Protein-coated disks) zum vorläufigen großtechnischen Aus bei.

Trotz aller technologischen Fortschritte befürchten manche Wissenschaftler/innen, dass es auf Grund der z.B. im Vergleich zu Büchern oder Briefen vergänglichen digitalen Informationen zu einem „dunklen digitalen Zeitalter“ kommen könnte, über das in ferner Zukunft nur mehr wenige Informationen vorliegen werden. Dieser durchaus nicht unwahrscheinlichen Entwicklung vorzubeugen haben sich Organisationen wie das „**Memory of Mankind**“ verschrieben.

Informationen werden mittels Jahrtausende haltbarer keramischer Farben bzw. keramischer Mikrofilme aufgezeichnet. Die Einlagerung dieser Keramiktafeln im **Salzberg von Hallstatt** soll sogar das Überdauern von Eiszeiten sichern. Dadurch könnten auch Menschen in einer fernen Zukunft - ähnlich wie bei alten Höhleninschriften oder dem berühmten Stein von Rosetta - Informationen über unser Leben erhalten, unabhängig davon, ob es noch digitale Speicher und Lesegeräte bzw. eine weltumspannende dauerhafte Cloud gibt oder nicht.

Übersicht über einige verschiedene Speichersysteme:
(Angaben teilweise grobe Schätzungen, ohne Gewähr)

Speicherart	Max. Kapazität (MB)	Lebensdauer (Jahre)	Anmerkungen
3,5 Zoll Floppy Disk	3	5-10	veraltet
CD	700	30	noch gebräuchlich
DVD	4.700	30	aktuell
Blue Ray	25.000	100	aktuell
USB Stick	2.000.000	10-30	aktuell
Solid-state drive	2.000.000	10-30	aktuell
Hard-disk drive	8.000.000	10	aktuell
Glas-Disk	360.000.000	10 Milliarden	Versuchsstadium
DNA Speicher	215.000.000.000	Jahrhunderte	Versuchsstadium

Wie in diesem Kapitel dargelegt wird, können Datenspeicher theoretisch aus verschiedensten Materialien (von DNA bis zu Glas) gestaltet sein, was unter Umständen auch für weitere disruptive Ideen Raum bieten würde. Dies könnte beispielsweise auch eine Chance für heimische Forschungseinrichtungen darstellen.

5. Auswirkungen und Chancenfelder in Oberösterreich

Es ist zukünftig darauf zu achten, die richtigen Anwendungen mit angepasstem Digitalisierungsgrad zu versehen und sicher abzuwickeln. Überspitzt formuliert: Nicht jedes Urlaubsfoto muss mit neuester Quantenverschlüsselung gesichert oder auf einem DNA-Speicher für die Ewigkeit aufbewahrt werden. Bewusstseinsbildung durch aufbereitete Informationen zur Sensibilisierung und zum Aufbau der nötigen digitalen Kompetenz ist unabdingbar.

Unsere wachsende Kryptogesellschaft hat **positive, aber auch negative Auswirkungen auf viele unterschiedliche Bereiche**, was nicht alle möglichen Anwendungsfälle auch sinnvoll erscheinen lässt. Einen Überblick geben wir nachstehend.

Oberösterreich mit seinen Forschungsschwerpunkten in Bereichen der Informationstechnologien und Hardwareentwicklung, aber auch mit den vielen innovativen Technologie-Unternehmen und -Netzwerken bietet beste Voraussetzungen, um Herausforderungen der zunehmend digitalisierten Welt zukunftsorientiert zu begegnen. Eine Auswahl an oberösterreichischen Aktivitäten und Impulsen für die Zukunft findet sich bei den jeweiligen Themenfeldern.

5.1. Finanzwesen

Die ersten größeren Umwälzungen durch neue Kryptoverfahren und Blockchain-Technologien sind in der Finanzwelt bereits angekommen. Das Geschäftsmodell der Banken verändert sich, was in starken Umstrukturierungen sichtbar wird: Bankstellen werden geschlossen, Online-Banking nimmt stark zu. Die Möglichkeiten mit Blockchains sichere Transaktionen durchzuführen, lässt die Banken ihre Systeme einerseits umstellen, andererseits könnte die Bank als Mittler zukünftig gar nicht mehr nötig sein.

Foto: escapejaja – stock.adobe.com
Bezahlen mit der Kryptowährung Bitcoin

In Österreich ist Bargeld nach wie vor sehr beliebt, doch nehmen Kartenzahlungen vor allem bei größeren Beträgen zu. In anderen Ländern wie etwa Schweden oder

Dänemark wird eine Abschaffung des Bargelds angestrebt. Die Regierungen versprechen sich **Kosteneinsparungen und weniger Kriminalität**. Profite sieht auch der Bankensektor durch die steigende Anzahl von Transaktionen und nicht zuletzt würden Banküberfälle der Vergangenheit angehören. Insgesamt sind die Auswirkungen noch schwer abschätzbar, da auch die sprießenden Kryptowährungen das grundsätzliche Potenzial für weitreichende Umbrüche in sich tragen.

> TIPP #6
> Investiere in Kryptowährungen nicht unüberlegt!

5.2. Gesundheit

Wie auch den öffentlichen Diskussionen zu entnehmen ist, sind Gesundheitsdaten ein sehr sensibler Bereich, bei dem der Datenschutz im Sinne der Rechte der Patientinnen und Patienten eine besonders Bedeutung hat. Gesundheitsbezogene elektronische Daten fallen in einer rasch steigenden Menge an, z.B. in der bildgebenden Diagnostik, bei der Telemedizin, bei roboterunterstützten Operationen („Surgical Robots“) oder in der medizinischen Forschung.

Das Spannungsfeld einer möglichst sicheren und datenschutzkonformen Speicherung und Verarbeitung einerseits und neuartiger Möglichkeiten durch **künstliche Intelligenz und Big Data Analysen** Krankheiten besser zuerkennen und behandeln andererseits eröffnet heimischen Unternehmen und Forschungseinrichtungen vielfältige neue Chancen. Dies trifft gerade in der heutigen Zeit zu, in der überregionale Netzwerke für medizinische Daten zur bestmöglichen Behandlung aufgebaut werden, und bei denen Kryptografie und Blockchain wesentliche Bestandteile sein werden. Oberösterreich ist durch die Stärken in der Medizin- sowie IT-Technik prädestiniert, Vorreiter in diesem Zukunftsbereich zu bleiben bzw. zu werden.

> TIPP #7
> Mit der Zustimmung zu einer datenschutzkonformen Verarbeitung deiner Gesundheitsdaten hilfst du Krankheiten heilen!

5.3. Know-how und Wissenszugänge

Digitale Prozesse, Übertragungsverfahren und Sicherheitszertifizierungen ermöglichen das **Überdenken von alten Strukturen** – sowohl in der Ausbildung selbst kommt es zu massiven Änderungen, als auch in der späteren Berufs- und Arbeitswelt. Interdisziplinäre

und digitale Kompetenzen werden zukünftig in allen Branchen an Bedeutung gewinnen. D.h. nicht, dass jede/r Auszubildende selbst Algorithmen und Blockchains programmieren können muss, sondern vielmehr, dass ein Verständnis für die grundlegenden Funktionsweisen vorhanden sein sollte.

Der **Bedarf an IT-Beratungen** steigt, was aktuelle Zahlen der Wirtschaftskammer Österreich belegen. Seit 2008 verzeichnet der Fachverband Unternehmensberatung, Buchhaltung und Informationstechnologie stark steigende Umsatzzahlen. Als derzeit dynamischste Wirtschaftsbranche ist IT-Know-how aus Österreich auch im Ausland gefragt. Die WKO-Statistik weist für Oberösterreich 3.588 IT-Dienstleister aus (Stand 31.12.2018). Wird per UBIT-Onlineabfrage[2] gezielt nach „Cloud“ gefiltert, verringert sich die Zahl auf 42 Treffer, bei „Blockchain“ werden nur drei Unternehmen angeführt.

Weiterbildung und flexible Anpassungen an Kundenwünsche ist in Digitalbranchen unumgänglich. Die Zukunft ist gekennzeichnet durch eine **rasche Veränderung der Berufsbilder, Entstehen neuer Berufe und Wegfallen von Arbeiten**. Oberösterreichs Bildungseinrichtungen müssen diese Flexibilität widerspiegeln, um Ausbildungen und Berufe zu synchronisieren. Oö. Schwerpunkte im Bereich Künstlicher Intelligenz, die Verknüpfung von Psychologie und Informationstechnologien an der Johannes Kepler Universität oder neue FH-Studiengänge in Automotive Computing, Data Science oder Business Intelligence zeigen die Innovationskraft und sollten weiter unterstützt werden.

TIPP #8
In Oberösterreich stehen dir viele verschiedene MINT-Ausbildungen (Mathematik, Informatik, Naturwissenschaften, Technik) zur Verfügung!

5.4. Mobilität

Die Zukunftsprognosen im Bereich Mobilität sind von **autonomen Fahrzeugen** unterschiedlicher Ausprägungen gekennzeichnet – von Lieferdrohnen über selbstfahrende Autos bis zu Flugtaxis. Autonome Bewegungen sind in unserer komplexen Welt nur mit einer Vielzahl von Sensoren möglich, die riesige Datenmengen in Echtzeit übertragen, verarbeiten und auswerten. Die **sichere Verschlüsselung** ist ein zentrales Element, um die Zukunft digitaler Mobilität möglich zu machen. Nicht auszudenken, wenn durch einen Hacker-

TIPP #9
Mit einem teil- bzw. zukünftig vollautonomen Fahrzeug kannst du dein Unfallrisiko senken!

[2] https://firmen.wko.at/Web/SearchPartner.aspx?CID=74f292eb-6893-45f8-975c-3869150022c2

angriff Millionen von autonomen Fahrzeugen beeinflusst werden könnten. Um dies zu verhindern, sind verstärkte Anstrengungen in die Entwicklung redundanter, d.h. von einander unabhängiger Systeme zu setzen, um die Ausfallsrate des Gesamtsystems zu minimieren.

Ungeklärt sind rechtliche Fragen der Datenverwaltung und –übertragung. Was darf mit generierten Mobilitätsdaten passieren? Gerade im Bereich Internet of Things ist die unverschlüsselte Datenweiterleitung an die Hersteller/innen weit verbreitet und sollte schnellstmöglich EU-weit geregelt werden. Daten aus digital vernetzten Fahrzeugen können insbesondere sehr sensibel sein, weil sowohl Bewegungs- als auch Verhaltensmuster abgeleitet und missbräuchlich verwendet werden könnten.

Im Projekt „DigiTrans“ des Automobil-Clusters wird Oberösterreich von 2018 bis 2023 zur Testregion für automatisiertes und vernetztes Fahren im multimodalen Güterverkehr. Vom automatisierten Be- und Entladen inkl. Rangieren im Betriebsgelände über LKW-Platooning (automatisiertes Fahren im LKW-Konvoi mit minimalem Sicherheitsabstand) auf Autobahnen bis hin zur City Logistik (Zustell- und kommunale Dienste) sollen unterschiedlichste Bereiche auf ihre Umsetzbarkeit geprüft werden. Dabei spielen Datenerfassung, -übertragung und -auswertung eine zentrale Rolle.

5.5. Rechtssystem

Unsere Kryptogesellschaft ist eine noch nie dagewesene Herausforderung für unser Rechtssystem. Einerseits entwickeln sich in der digitalen Welt in raschem Tempo neue Anwendungen, die die Arbeit der Juristen/innen grundlegend verändert. Andererseits verschwinden nationale Grenzen.

Beispielsweise könnte die Beurkundung von Verträgen durch öffentliche Notare künftig nicht mehr notwendig sein. In Ghana werden Verträge über Landkauf mittlerweile bereits per Blockchain vollzogen. Geokoordinaten stehen mit der Signatur in der Blockchain. Ein/e Notar/in, der/die in Ghana häufig mehrere Autostunden entfernt ist, muss nicht mehr beigezogen werden. Was früher Tage oder gar Wochen dauerte und hohe Kosten mit sich brachte, erfolgt mit der Blockchain-Technologie nun umgehend und ohne großen Aufwand.

In einer Technologieumfrage der International Legal Technology Association wurden drei Digitalisierungsbereiche identifiziert, die aktuell besonders viel juristisches Know-how binden:

- **Daten- und Cybersicherheit:** Durch die Datenschutzgrundverordnung (anzuwenden seit Mai 2018) wurde ein EU-weites Zeichen gesetzt, das bei vielen Unternehmen, Institutionen und Vereinen zu großen Unsicherheiten führte.

- **Cloud Computing:** Mit der Benützung von Speicherplatz, Rechenleistung oder Software, die nicht lokal verfügbar ist, gibt es insbesondere Klärungsbedarf im Hinblick auf anzuwendendes Recht (z.B. bei grenzüberschreitenden Dienstleistungen), Urheberrecht und Datenschutz.
- **Datenanalyse:** Die Beschaffung und Auswertung großer digital vorhandender Datenmengen ist datenschutzrechtlich heikel.

> TIPP #10
> Mittlerweile gibt es Juristen/innen, die auf Digitalisierungs- und Datenschutzfragen spezialisiert sind!

Sichere Verschlüsselungen und eindeutige Authentifizierungen sind für die Abwicklung von rechtsgültigen digitalen Geschäften oder Behördenwegen essentiell. Rechtliche Standards, sichere Transaktionsmöglichkeiten und im Bedarfsfalle auch rechtliche Handhabe sind umfassend zu regeln. Am LIT Law Lab der Johannes Kepler Universität steht die interdisziplinäre Behandlung von rechtlichen Fragen im Zusammenhang mit der digitalen Transformation im Vordergrund.

5.6. Sicherheit

IT-Security ist in Oberösterreich ein Schwerpunktthema, das verschiedene Organisationen, Institute und Unternehmen erfolgreich sichtbar machen. Der Softwarepark in Hagenberg soll als Zentrum für IT-Security international etabliert werden. Partner sind neben der FH Hagenberg und der Johannes Kepler Universität das Software Competence Center, die Business Upper Austria und auch einzelne Unternehmen. In Hagenberg angesiedelt soll das Zentrum Teil des digitalen Wirtschaftsnetzwerkes Oberösterreich mit besten Kontakten zu internationalen Experten/innen sein. Kryptografie, Blockchain und Quantencomputing sind Teilbereiche, die durch solche Netzwerke auch in Oberösterreich z.B. durch Zusammenarbeiten mit Fachleuten aus Tirol oder Wien stärker positioniert werden könnten.

Die wissenschaftliche **Auseinandersetzung mit Informationstechnologien und Sicherheit** sollte durch einen niederschwelligeren Zugang für die oberösterreichische Bevölkerung ergänzt werden. Wie bin ich selbst bei Sicherheitslücken betroffen? Wie kann jeder Mensch zu mehr digitaler Sicherheit im persönlichen Umfeld beitragen? Effektiv sind z.B. Veranstaltungen, die zeigen, wie leicht etwa ein verschlüsseltes Word-Dokument gehackt werden kann oder wie Phising-Seiten funktionieren. Bewusstseinsbildung könnte auch über eine Medienkooperation erfolgen.

> TIPP #11
> Entscheide zwischen dem richtigen Grad an Digitalisierung, Freiheit und Sicherheit!

Nicht zuletzt sollte die **Einführung neuer IT-Strukturen** wie das 5G-Netz einer intensiven sicherheitstechnischen Überprüfung unterzogen werden. Wie kann in einem Störfall, oder gar im Zuge einer absichtlichen Sabotage (im Sinne eines **Cyber Wars**) die immer wichtiger werdende elektronische Kommunikation aufrechterhalten werden? Ein wichtiger Bestandteil einer sicheren Datenübertragung im Einsatzfall war bereits die Einführung des (abhörsicheren) **Digitalfunks** in Oberösterreich im Jahr 2018.[3]

5.7. Umwelt

Die Verifizierung von Transaktionen in Blockchains, sichere Verschlüsselungen, mehrstufige Zugangssysteme und dauerhafte Speicher sind mit enormen Rechnerleistungen und damit **hohen Energieverbräuchen** verbunden. Die stark steigenden Datenflüsse brauchen überdies robuste Infrastrukturen und Hardwarekomponenten. Die Umweltauswirkungen sind vielfältig und reichen vom **Flächenverbrauch** für Verteiler- und Datenverarbeitungszentren bis hin zu **benötigten Rohstoffen**, deren Abbau oftmals in Ländern mit geringen Umweltstandards erfolgt bzw. auch eine hochgradige Import-Abhängigkeit mit sich ziehen (z.B. Seltenerdmetalle).

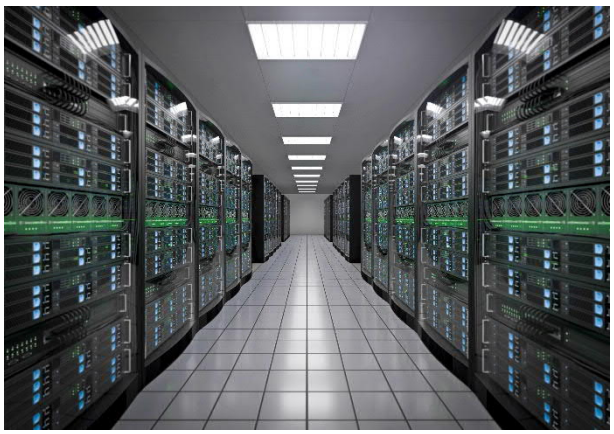

Foto: fotomek – stock.adobe.com
Serverraum eines Datenverarbeitungszentrums

Durch Digitalisierung von Abläufen kann andererseits aber auch Energie gespart werden. Ein Beispiel sind Smart Grids und dezentrale Energieversorger, die zukünftig mittels Blockchain-Technologien die Energieverteilung abwickeln können.

> TIPP #12
> Auch Speicherplatz benötigt Ressourcen. Überlege dir, welche Dokumente, Bilder und Videos du für längere Zeit aufheben willst!

In der oberösterreichischen Gemeinde Kronstorf zeigt der Internet-Gigant Google Interesse an der Errichtung eines Datenverarbeitungszentrums. Die Vorteile für die internationale Sichtbarkeit als Wirtschafts- und Innovationsstandort und die Schaffung von Arbeitsplätzen in der Gemeinde sind augenscheinlich. Das Land Oberösterreich ist bestrebt die negativen Auswirkungen möglichst gering zu halten

[3] http://www.fireworld.at/berichte/details/news/digitalfunk-fuer-die-einsatzkraefte-soll-2018-in-oberoesterreich-flaechendeckend-sein/

bzw. so weit als möglich auszugleichen. Beispielsweise wurde bereits vor tatsächlichem Baubeginn ein Mischwald als ökologischer Ausgleich angepflanzt.

5.8. Verwaltung

Ein wesentlicher Teil einer modernen, zukunftsorientierten Verwaltung liegt in der elektronischen Datenverwaltung: **Elektronische Akte** (ELAK, im Land Oö. „ELVIS“) müssen nicht mehr zwischen Behörden hin- und her geschickt werden, sondern der Arbeitsprozess ist völlig transparent und Recherchen werden vom Arbeitsplatz gemacht. Die Verwaltung arbeitet kontinuierlich an der Weiterentwicklung des ELAKs, um sich an immer neue Anforderungen anzupassen.

> TIPP #13
> Verwende den digitalen Weg, wenn er von einer Behörde angeboten wird!

Weitere künftige Anforderungen werden etwa in einer stärkeren Vernetzung von verschiedenen Verwaltungen oder zwischen Verwaltung und Kunden/innen (z.B. automatische Übermittlung von umweltrelevanten Daten von Firmen) liegen. Auch bedingt durch technologische Entwicklungen wie das möglichen „Knacken“ von herkömmlichen Passwörtern durch künftige Quantencomputer werden in Zukunft neuartige Methoden wie die Quantenverschlüsselung wahrscheinlich an Bedeutung gewinnen.

Durch die Blockchain-Technologie könnte beispielsweise das zentrale Verwalten von öffentlichen Verzeichnissen durch verschiedene Behörden eine Veränderung erfahren.

5.9. Wirtschaft

Eine immer stärker globalisierte Wirtschaft verbunden mit steigenden Qualitätsanforderungen führt zu neuen Herausforderungen für zahlreiche Logistikketten wie Gefahrguttransporte, Medikamententransporte, Kühlketten, (zertifizierte) Biolebensmittel, Automobilteile und vieles mehr.

Werden vorab definierte Kriterien erfüllt, werden **Smart Contracts** automatisch ausgeführt. Sinkt beispielsweise auf einer Großbaustelle die Menge an einem bestimmte Baustoff unter die vorab definierte Grenze, erfolgt die Bestellung beim Zulieferer automatisch. Diese smarten Verträge verändern derzeitige Logistikketten massiv und tragen dazu bei, Transaktionskosten zu senken.

In Analogie zum Internet der Dinge ist zukünftig durch die Verwendung von Verschlüsselungen und Blockchain-Technologien eine **Ökonomie der Dinge** möglich. D.h. Maschinen können nicht nur abgestimmt miteinander arbeiten und just-in-time-Bestellungen aufgeben, sondern Waren oder Leistungen auch gleich verrechnen.

> TIPP #14
> Zunehmende Digitalisierung in der Wirtschaft kann Geschäfte sicherer und schneller machen!

Insbesondere für komplexe Güter stellt ein sogenannter **digitaler Zwilling**, der Wertschöpfungsketten über den gesamten Lebenszyklus (Design, Erstellung, Betrieb und Wiederverwertung) abbildet, eine Lösung dar. Für die technische Umsetzung könnten Blockchain-Technologien sowie neue Verschlüsselungstechnologien steigende Bedeutung erlangen: Dies stellt eine Chance für eine Forschungskooperation im Bereich Wirtschaft mit IT und Physik dar. Im Projekt „Digi-Twin“ unterstützt der Mechatronik-Cluster die Implementierung von digitalen Zwillingen in oö. Unternehmen, um Effiziensteigerungen über den gesamten Wertschöpfungsprozess zu erzielen.

5.10. Schlussbemerkung

Auf Grund der vielfältigen möglichen Auswirkungen auf unterschiedliche Lebensbereiche besitzt die Krypto- bzw. die Blockchain-Technologie das längerfristige **Potenzial zu massiven Umwälzungen in der Informationstechnologie**, ähnlich wie das Smartphone die Kommunikation sowie die gesamte Gesellschaft tiefgreifend revolutioniert hat.

Gerade in einer Zeit der breiten Etablierung dieser Technologie ergeben sich besonders viele Möglichkeiten für den Forschungs- und Wirtschaftsstandort Oberösterreich, die Chancen auf eine dauerhafte Präsenz auf diesem Wachstumsmarkt eröffnen, wobei besonders interdisziplinäre Ansätze erfolgversprechend erscheinen. Neben wirtschaftlichen Vorteilen wird auch jede/r einzelne Oberösterreicher/in von den neuen Technologien z.B. durch eine verbesserte Sicherheit persönlicher Daten profitieren.

Mit Blick auf die abzusehende „Flut“ von Daten, die es zu verwalten und schützen gilt, und die vielfältigen Anwendungsmöglichkeiten von Krypto-Technologien muss ihr achtsamer und verantwortungsvoller Einsatz zum Wohle des Einzelnen und der Gesellschaft zentraler Auftrag bleiben.

6. Quellen- und Literaturverzeichnis

A-SIT Zentrum für sichere Informationstechnologie Austria: Passwort-Auswahl
https://www.onlinesicherheit.gv.at/praevention/konten_und_passwoerter/passwort-auswahl/249589.html

#Blockchainwelt, 2018: Distributed Ledger Technologie (DLT) ist mehr als Blockchain
https://blockchainwelt.de/dlt-distributed-ledger-technologie-ist-mehr-als-blockchain/

BGBl. I Nr. 10/2004 in der geltenden Fassung: e-Government-Gesetz
https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20003230

Business Upper Austria, 2019: Projekt „DigiTrans"
https://www.testregion-digitrans.at/

Business Upper Austria, 2019: Projekt „Digi-Twin"
https://www.mechatronik-cluster.at/themenschwerpunkte/entwicklung-mechatronischer-systeme/digitwin/

CIO, 2017: Falscher Hype um Blockchain
https://www.cio.de/a/falscher-hype-um-blockchain,3330977,2

Der Standard, 2018: Schwedens Bemühungen zu bargeldloser Gesellschaft führen zu Protesten
https://derstandard.at/2000092084046/Schwedens-Bemuehungen-zu-bargeldloser-Gesellschaft-fuehren-zu-Protesten

Der Standard, 2008: Holografischer Speicher bald erhältlich
https://derstandard.at/3309153/Holografischer-Speicher-bald-erhaeltlich

Der Stern, 2007: Die Eiweiß-Scheibe
https://www.stern.de/digital/technik/speichermedien-die-eiweiss-scheibe-3274286.html
https://www.fraunhofer.de/content/dam/zv/de/forschung/artikel/2017/Fraunhofer-Positionspapier_Blockchain-und-Smart-Contracts_v151.pdf

Die Presse, 2010: Kronstorf: Wie Google eine Gemeinde verändert
https://diepresse.com/home/wirtschaft/economist/568607/Kronstorf_Wie-Google-eine-Gemeinde-veraendert

Finance Business, 2018: Von der Automatisierung über das Internet der Dinge bis zum vernetzten Ecosystem
https://www.financebusiness.afb.de/2018/03/13/vom-internet-der-dinge-zum-ecosystem/

Frauenhofer SIT, Hrsg., 2018: Eberbacher Gespräch on „Next Generation Crypto“. Eberbacher Gespräche 01/2018.
https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Eberbach-crypto-download.pdf?_=1530524662

Gómez, Juan, 2017: Geheimsprachen und Decodierung. Mathematiker, Spione und Hacker. Verlag Librero IBP.

ICD, 2018: Data Age 2015 – The Digitation of the World. From Edge to Core.- IDC White Paper, sponsored by Seagate
https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf

IMAS International, 2018: Datenschutz im Zeitalter der Datenflut - Der Umgang der Österreicher mit dem Passwort. IMAS® Report 02/2018
http://www.imas.at/index.php/en/86-produkte/imas-report-de/aktuelle-reports/984-datenschutz-im-zeitalter-der-datenflut-der-umgang-der-oesterreicher-mit-dem-passwort

ITA et al., 2018: Foresight und Technikfolgenabschätzung: Monitoring von Zukunftsthemen für das Österreichische Parlament
https://www.parlament.gv.at/ZUSD/PDF/FTA-Monitoring_November2018_fin.pdf

Legal Tech Blog, 2018: ILTA-Umfrage identifiziert Herausforderungen für Kanzleitechnologen
https://legal-tech-blog.de/ilta-umfrage-identifiziert-herausforderungen-fuer-kanzleitechnologen

LIT Law Lab, 2019:
https://www.jku.at/linz-institute-of-technology/forschung/research-labs/law-lab/

Löfken, Jan Oliver, 2017: Festplatten aus DNA speichern mehr als jeder Chip. In: ZEIT ONLINE.
https://www.zeit.de/wissen/2017-03/dna-datenspeicher-erbgut

Manhart, Klaus, 2019: Biometrische Authentifizierung: Methoden, Systeme und praktische Umsetzung

https://www.searchsecurity.de/tipp/Biometrische-Authentifizierung-Methoden-Systeme-und-praktische-Umsetzung

Max-Planck-Gesellschaft, 2017: Exotische Inseln für magnetische Festplatten
https://www.mpg.de/11469506/antiskyrmion-racetrack-festplattenspeicher

Memory of Mankind, 2019: Aufbewahrung für die Ewigkeit
https://www.memory-of-mankind.com/de/

Müller, Stefan, 2017: Die Geschichte der Kryptografie – Von Cäsar bis zum Quantencomputer. Brickscience TV. Folge 3.
https://fastforwardscience.de/preistraeger/brickscience-tv-kryptographie/
http://stemue-web.de/stemue/brickfilm.html

Oö. Nachrichten, 2019: Neues Konzept: Wer IT-Sicherheit googelt, soll Hagenberg finden
https://www.nachrichten.at/nachrichten/wirtschaft/wirtschaftsraumooe/neues-konzept-wer-it-sicherheit-googelt-soll-hagenberg-finden;art467,3101939

Oö. Zukunftsakademie, Hrsg., 2018: Zukunftstechnologie Photonik. Licht als Innovator.
https://www.ooe-zukunftsakademie.at/Photonik_Zukunftsthema_2018.pdf

ORF, 2019: Stabil und sparsam: Chemische Datenspeicher
https://science.orf.at/stories/2979277/

Österreich Journal, 2019: Fit for Future. Oberösterreich 2030
http://www.oe-journal.at/index_up.htm?http://www.oe-journal.at/Aktuelles/!2019/0319/W2/21503ooeAchleitner.htm

Schadwinkel, Alina, 2016: Quantenkryptografie. „Und dann laden wir Menschen ein, die Daten zu hacken“ Interview mit Anton Zeilinger. In: ZEIT ONLINE
https://www.zeit.de/wissen/2016-08/quantenkryptografie-satellit-china-kommunikation

Schasche, Stefan, 2018: Haltbarkeit von Speichermedien. In: PC-Magazin
https://www.pc-magazin.de/ratgeber/speichermedien-lebensdauer-dvd-festplatte-usb-stick-floppy-disk-1485976.html

Schmeh, Klaus, 2016: Kryptografie – Verfahren, Protokolle, Infrastrukturen. dpunkt.verlag

Security Insider, 2018: Blockchain-Alternativen für das Internet der Dinge
https://www.security-insider.de/blockchain-alternativen-fuer-das-internet-der-dinge-a-724903/

Security Insider, 2017: Definition Token – Was ist ein Security-Token?
https://www.security-insider.de/was-ist-ein-security-token-a-613250/

Stern, Nicole, 2019: Wie man sich vor Passwort-Dieben schützt. In: Die Presse vom 25. Feb. 2019

T-Systems Austria GmbH, 2018: Ein Quäntchen Hoffnung
https://www.t-systems.com/at/de/newsroom/blickwinkel/security/ict/post-quantum-kryptographie-790328

University of Southampton, 2016: Eternal 5D data storage could record the history of humankind. In: Phys.org, Science X network
https://phys.org/news/2016-02-eternal-5d-storage-history-humankind.html

VFR Verlag für Rechtsjournalismus GmbH Berlin, 2019
https://www.datenschutz.org/sicheres-passwort/

Voshmgir, Shermin, 2016: Blockchain, Smart Contracts und das dezentrale Web
https://www.technologiestiftung-berlin.de/fileadmin/daten/media/publikationen/170130_BlockchainStudie.pdf

Wirtschaftskammer Österreich, 2019: WKO Statistik Österreich
http://wko.at/statistik/BranchenFV/B_704.pdf

Wirtschaftskammer Österreich, 2018: Rekordumsatz für hochqualifizierte IT- und Unternehmensberatung in Österreich: 13 Prozent Plus für Fachverband UBIT-Betriebe
https://news.wko.at/news/oesterreich/Rekordumsatz-fuer-hochqualifizierte-IT--und-Unternehmensb.html

Wolfangel, Eva, 2016: Zehn Schlüsselfragen zur Kryptografie. In: Spektrum.de
https://www.spektrum.de/wissen/zehn-schluesselfragen-der-kryptografie/1407523