Anatol **BADACH**
Erwin **HOFFMANN**

Zukunft der IP-NETZE

Virtualisierte, software-definierte, intelligente Systemlösungen und -anwendungen

HANSER

Badach/Hoffmann

Zukunft der IP-Netze

Anatol Badach
Erwin Hoffmann

Zukunft der IP-Netze

Virtualisierte, software-definierte, intelligente System-lösungen und -anwendungen

HANSER

Print-ISBN: 978-3-446-47756-8
E-Book-ISBN: 978-3-446-47921-0

Die allgemein verwendeten Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

Bibliografische Information der Deutschen Nationalbibliothek:
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet unter http://dnb.d-nb.de abrufbar.

Vilshofener Straße 10 | 81679 München | info@hanser.de
www.hanser-fachbuch.de
Lektorat: Sylvia Hasselbach
Copy editing: Jürgen Dubau, Freiburg/Elbe
Herstellung: Grazyna Lada
Coverkonzept: Marc Müller-Bremer, *www.rebranding.de*, München
Covergestaltung: Thomas West
Titelmotiv: © Adobestock/AllistairBot/Peopleimages - AI
Satz: le-tex publishing services GmbH, Leipzig
Druck: Elanders Waiblingen GmbH, Waiblingen
Printed in Germany

Inhalt

Vorwort ..... **XV**

1 Digitalisierung, Virtualisierung, Künstliche Intelligenz und die Quantenwelt **1**

1.1 Die Digitalisierung der Welt 2

1.1.1 Die erste Digitalisierung 3

1.1.2 Die zweite Digitalisierung 8

1.1.3 Die dritte Digitalisierung 11

1.1.4 Vor und nach dem Internet-Zeitalter 13

1.1.5 Objekte im digitalen Raum (Cyberspace) 15

1.1.6 Interaktion des digitalen Raums mit der Wirklichkeit 18

1.1.7 Unternehmens- und Geschäftsprozesse im digitalen Raum 19

1.2 Die Virtualisierung der Welt 22

1.2.1 Virtuelle Welten im digitalen Raum 22

1.2.2 Interaktion mit der virtuellen Welt 24

1.2.3 Anreicherung der realen Welt durch Informationen aus dem digitalen Raum: Augmented Reality 25

1.2.4 Besitztum an digitalen Objekten: Cybercurrency und Non-Fungible Token (NFT) 28

1.3 Die Sache mit der „künstlichen Intelligenz“ 35

1.3.1 Vereinfachtes Funktionsmodell von KI-Systemen 36

1.3.2 Entwicklung der KI-Systeme 39

1.3.3 Siri, das Fräulein vom Amt – ist heute unpässlich 44
1.3.4 Die virtuelle Welt träumt 45
1.3.5 Usability: KI-Agenten 47
1.3.6 Die Beherrscher der digitalen Welt 49
1.4 Die Eroberung der digitalen Welt durch Quantencomputer 51
1.4.1 Quantenmechanik und Quantenprozesse 53
1.4.2 Quantencomputer 58
1.4.3 Quanteninformationstheorie 63
1.5 Schlussbemerkungen 66

Teil 1 Die neuen Netzwerkprotokolle 71

2 VPLS – Virtual Private LAN Service 73
2.1 Grundlegende Idee von VPLS 74
2.2 Logisches Modell von MPLS 76
2.2.1 Ethernet over MPLS (EoMPLS) 78
2.2.2 VPLS erbracht durch Vollvermaschung von VSIs 81
2.3 Basisfunktionen von VSIs 82
2.3.1 VPLS-Modell im Hinblick auf die VSI-Vernetzung 83
2.3.2 Information im PE über bereitgestellte VPLSs 85
2.3.3 Learning von MAC-Adressen aus Broadcast Frames 89
2.3.4 Learning von MAC-Adressen aus Unicast Frames 90
2.4 Skalierbarkeit des VPLS 91
2.4.1 Auto Discovery und VPLS Signaling 92
2.4.2 Bekanntgabe von Informationen über PW Labels 93
2.5 Hierarchical VPLS als Multi-Tenant VPLS 94
2.5.1 H-VPLS und VLANs – Bedeutung von VLAN Stacking 96
2.5.2 H-VPLS als Multi-Tenant-VPLS 97
2.6 Schlussbemerkungen 97

3 Network Functions Virtualisation 99
3.1 Die grundlegende Idee von NFV 100
3.1.1 Verteilte NFVI 102

3.1.2 Tunneling zwischen vSwitches nach NVGRE 104
3.1.3 Weg zur Verwirklichung von NFV 106
3.2 Systemkomponenten der NFV-Referenzarchitektur 107
3.2.1 Bedeutung der Orchestrierung 109
3.2.2 Network Services und Unternehmensprozesse 110
3.2.3 Bedeutung von NFV-MANO 111
3.3 Beispiele für Vernetzungen von VSIs 114
3.3.1 Arten der Vernetzung von VNFs 115
3.4 Orchestration und Management von VNFs 118
3.4.1 Network Service Lifecycle Management 120
3.5 Schlussbemerkungen 121

4 SFC – Service Function Chaining 123
4.1 Die Idee von SFC 124
4.1.1 Funktionelle Komponenten und Architektur von SFC 127
4.1.2 Grundlegende Aufgabe von SF Forwarding 128
4.2 Virtualisierung von Rechnern – die erste Säule von SFC 130
4.2.1 SF Forwarding innerhalb einer Virtualisierungsplattform 131
4.2.2 Virtual Overlay Networks – die zweite Säule von SFC 133
4.2.3 SF Forwarding zwischen Virtualisierungsplattformen 134
4.2.4 Tunneling-Konzepte für die Bildung von VONs mit SFs 135
4.2.5 Beispiel für den Einsatz von SFC 138
4.3 Network Service Header (NSH) – Struktur und Bedeutung 140
4.3.1 Network Service Header (NSH) mit `MD-Type=0x1` 142
4.3.2 Network Service Header (NSH) mit `MD-Type=0x2` 142
4.3.3 Network Service Header (NSH) – Wer macht was? 143
4.4 SFC-Topologie als SF-Graph 143
4.4.1 Raum mit den Koordinaten „Network Service“ und „Service Function“ 144
4.4.2 Ermittlung der Lokation von SFs und der Transportart 145
4.5 NFV, SFC und SDN – ihre Gemeinsamkeiten 146
4.5.1 Umsetzung von SFC in der Praxis – ein mögliches Szenario 149
4.6 Schlussbemerkungen 149

5 SRv6 – IPv6 Segment Routing 151
5.1 Multiplane-Struktur von Netzen mit SRv6 152
5.1.1 Hierarchie der Funktionen in IPv6-Netzen mit SRv6 153
5.1.2 Bedeutung von SDN bei SRv6 154
5.1.3 Analogie zwischen SRv6 und MPLS 155
5.2 Grundlegende Eigenschaften des SRv6 156
5.2.1 Arten von SRv6-Domains 158
5.2.2 Operationen entlang eines SRv6-Path 160
5.2.3 SRH im IPv6-Paket 161
5.2.4 Übermittlung über einen SRv6-Path 164
5.2.5 Verlauf der SRH-Analyse 165
5.3 SRv6 Network Programming 167
5.3.1 Struktur von SID bei SRv6-NP 168
5.3.2 Remote Network Function Call bei SRv6-NP 169
5.4 Kategorien von SRv6 Network Functions 171
5.4.1 Nutzung von `T.Insert` und `T.Encaps` 173
5.4.2 Nutzung von `End` und `End.X` 175
5.4.3 Spezifikation einiger Endfunktionen 176
5.4.4 Einsatz von `End.DX4` und `End.DX6` 178
5.5 Schlussbemerkungen 179

Teil 2 Software Defined Networking 181

6 SDN – Software Defined Networking 183
6.1 Quelle und Architektur von SDN 185
6.1.1 Voraussetzung für Realisierung 187
6.1.2 Allgemeine logische Architektur des SDN 188
6.1.3 SDN-Architektur ohne Virtualisierung von Netzwerkressourcen 189
6.1.4 SDN-Architektur mit Virtualisierung von Netzwerkressourcen 191
6.1.5 SDN-Architektur der ONF 193
6.2 Einsatz von SDN 194
6.2.1 SDN in Datacentern 195
6.2.2 Hierarchische SDN-Architektur 198
6.2.3 Hierarchische Strukturen von SDN beim IoT 199
6.2.4 Rekursiv-hierarchische SDN im IoT 200

6.3 Software Defined Optical Networking 203
6.3.1 OpenFlow-Switche und das OpenFlow Protocol 205
6.3.2 Aufbau und Funktionsweise eines OF-Switch 207
6.3.3 OF-Switch mit beispielhaftem Flow-Table Einsatz 208
6.3.4 OF-Switch-Funktionen bei einer einzigen Flow Table 212
6.4 SDN bei MPLS, GMPLS und SPB 217
6.4.1 Link Aggregation, Multiplexing und Multipathing beim SDN 219
6.4.2 Beispiele für Group-Table-basierte Funktionen 222
6.5 SDN, NFV und SR6 Network Programming 223
6.5.1 SDN und SRv6 Network Programming 224
6.5.2 Symbiose von SDN mit NFV und SRv6-NP 225
6.5.3 Die Idee von vSDN 226
6.5.4 Bedeutung von SRv6-NP für vSDN 228
6.5.5 Fernaufrufe von VNFs bei SRv6-NP 229
6.5.6 Multi-Tenancy-Architektur von SDN 232
6.6 Software Defined Anything Networking 233
6.7 Schlussbemerkung 237

7 SD-IoT – Software Defined Internet of Things 239
7.1 Symbiose von IoT mit NFV und SDN 240
7.2 Funktionale Architektur von IoT 242
7.2.1 IoT-Definition aus funktionaler Sicht 243
7.2.2 Allgemeines Multilayer-Modell des IoT 243
7.2.3 Hierarchische SDN-Architektur beim IoT 245
7.3 Grundlegende Idee von SD-IoT 246
7.3.1 SD-IoT-Devices als virtuelle Rechner 246
7.3.2 Modelle zur Bereitstellung von SD-IoT-Services 247
7.3.3 Definition von SD-IoT 247
7.3.4 Grundlegende Reichweiten von SD-IoT 247
7.3.5 Control & Orchestration Level 248
7.3.6 Reichweiten von Systemlösungen für SD-IoT 248
7.3.7 Anschauliche Interpretation der Reichweite von SD-IoT 249
7.3.8 Controller in Edge und Fog Sublayers 249
7.3.9 Controller auf Fog und Clouds Sublayers 251

7.4 Entwicklung von SD-IoT-Systemen ... 253
7.4.1 Software Defined Smart Home ... 253
7.4.2 Software Defined City Park System ... 255
7.4.3 Proxy-basierte IoT-Services ... 257
7.4.4 Bedeutung des Network Hypervisor im IoT-Proxy-System ... 258
7.4.5 Proxy-basierte SD-IoT-Architektur ... 259
7.4.6 Besonderheiten von SDSHs ... 261
7.4.7 Proxy-basierte SDSH City Service ... 261
7.4.8 vSD-IoT versus Server mit VMs ... 263
7.5 Entwicklungsstadien des IoT ... 265
7.6 Schlussbemerkungen ... 266

8 SD-WAN – Software Defined Wide Area Network ... 267
8.1 Funktionale Anforderungen an ein WAN ... 268
8.1.1 Klassische Systemlösung für WAN-Dienste ... 270
8.1.2 Funktionale Bedeutung des SD-WAN ... 272
8.1.3 SD-WAN als Data Plane in logischer SDN-Architektur ... 274
8.1.4 Logische Struktur von SD-WANs ... 274
8.2 Vom Internet über LISP zum SD-WAN ... 276
8.2.1 DNS als Control Plane im herkömmlichen Internet ... 277
8.2.2 Definition von SD-WAN aus technischer Sicht ... 279
8.3 Grundgedanke von LISP ... 279
8.3.1 Logische Struktur des Internets mit LISP ... 280
8.3.2 Kommunikationsvarianten mit LISP ... 281
8.3.3 LISP-spezifische Kommunikation über ein SD-WAN ... 281
8.3.4 Übermittlung von IP-Paketen bei LISP ... 282
8.3.5 Bedeutung von RLOC und EID in Kurzfassung ... 284
8.3.6 LISP als Muster für das SD-WAN ... 284
8.3.7 Adressierung der IP-Pakete bei LISP als Schritt zum SD-WAN ... 286
8.3.8 Hybrides ERM-System in Kurzfassung ... 287
8.4 ERM-System als Vorbild für die Control Plane im SD-WAN ... 288
8.4.1 Einsatz von IPsec im SD-WAN ... 288
8.4.2 Datenübermittlung über das SD-WAN ... 291
8.5 Schlussbemerkungen ... 293

Teil 3 Das „Internet der Dinge“ ... 295

9 6TiSCH-Netzwerke für Industrial IoT ... 297

9.1 6TiSCH-Netzwerke ... 298
9.2 Idee von TSCH ... 300
9.2.1 TSCH Schedule Matrix (TSM) ... 302
9.2.2 Multilayer-Protokollarchitektur ... 304
9.2.3 Spezifikation von Tracks ... 307
9.2.4 Funktionen von 6P ... 310
9.3 Kommunikation über TSCH Data Link ... 311
9.3.1 Struktur der 6P MAC-Frames ... 312
9.3.2 6P-Nachrichten ... 315
9.4 6P-Transactions ... 317
9.4.1 Hinzufügen von Zellen ... 318
9.4.2 Duplikate und abweichende Nachrichtenfolgen ... 322
9.5 Schlussbemerkungen ... 324

10 Digital Twins in IoT ... 327

10.1 Bedeutung digitaler Zwillinge ... 328
10.1.1 Services mit digitalen Zwillingen ... 330
10.1.2 Wissensbasis für digitale Zwillinge ... 333
10.1.3 Einsatz im Gesundheitswesen ... 333
10.2 Logisches Modell von Services mit DTs ... 335
10.2.1 Allgemeines Multilayer-Modell des IoT ... 337
10.2.2 Modell für den Einsatz von DTs im IoT ... 339
10.3 Virtuelle Sensoren und Aktuatoren ... 341
10.3.1 Überwachung der Gebäudesicherheit ... 341
10.3.2 Services in Smart Cities ... 343
10.3.3 Smartphone als Gesundheitsassistent ... 344
10.4 Digital Twin Federation ... 346
10.4.1 Verbund Ökosystem-relevanter Funktionen ... 347
10.4.2 Einsatzmöglichkeiten digitaler Zwillinge ... 348
10.5 Schlussbemerkungen ... 353

11 IIoT – Intelligent IoT 355
11.1 Allgemeine logische IoT-Architektur 357
11.1.1 Funktionelle Bereiche im IoT 359
11.2 Quellen der Intelligenz im IoT 361
11.2.1 Menschliche Kognition als Ideenquelle 363
11.2.2 Context-Aware Thinking/Computing 365
11.2.3 Modell der künstlichen Kognition 367
11.2.4 Kognitive Prozesse 368
11.3 Logische Multilayer-Architektur 370
11.3.1 Arten von Computing und Intelligenz 371
11.3.2 Support Computing for Distinguished Content Aware Computing (DCAC) 374
11.3.3 Support Computing for IoT 375
11.4 Dew Computing (DC) 377
11.4.1 Idee von Dew Computing 378
11.4.2 Dew Computing beim autonomen Fahren 378
11.5 Big Data im IoT 379
11.5.1 Big Data Attributes 380
11.5.2 ML-Techniken 381
11.6 Schwarmintelligenz im IIoT 382
11.6.1 Typische IIoT-Applikationen 383
11.7 Schlussbemerkung 384

12 Sicherer Einsatz und Betrieb des IoT 385
12.1 IoT-Hardware und IoT-Kommunikation 387
12.1.1 IoT-Kommunikationsprotokolle 389
12.1.2 Übertragung der IoT-Daten 391
12.1.3 RIOT als Betriebssystem 393
12.2 Sichere Datenübertragung bei CoAP 396
12.2.1 Das Arbeitsmodell von CoAP 397
12.2.2 Transportverschlüsselung bei CoAP mit DTLS 403
12.2.3 OSCORE für CoAP 411

12.3 Operationalisierung des IoT 421
12.3.1 ToFU: Trust on First Use 423
12.3.2 Bootstrapping Remote Secure Key Infrastructure 424
12.3.3 SUIT – Software Update für das IoT 426
12.3.4 Nummer 5 lebt! 430
12.4 Correctness – Die Mutter aller Sicherheit 433
12.4.1 Code Correctness 435
12.4.2 Data Correctness 438
12.4.3 Verifiable Data Structures 440
12.5 Post-quantum Kryptographie beim IoT 444
12.5.1 Klassische, pre-quantum Kryptographie 445
12.5.2 Implementierungen der post-quantum Kryptographie 447
12.5.3 Hybride Verfahren 449
12.6 Schlussbemerkungen 451

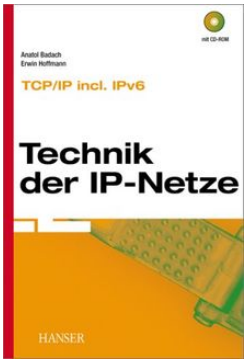
Abkürzungsverzeichnis 455

Abbildungsverzeichnis 461

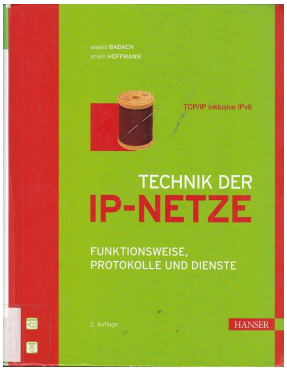
Tabellenverzeichnis 469

Literaturverzeichnis 471

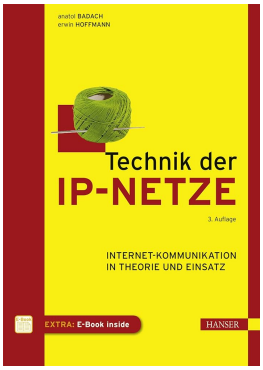
Stichwortverzeichnis 477



1. Auflage: 2000



2. Auflage: 2007



3. Auflage: 2015

4. Auflage: 2019

5. Auflage: 2023

Weiterführung mit neuem Stoff

1. Auflage: 2026

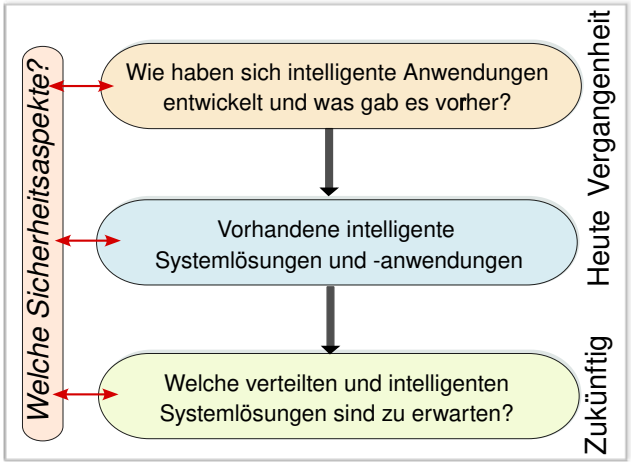
Vorwort

„Zukunft der IP-Netze“ schließt an unser Buch „Technik der IP-Netze“ [16] an und versucht, die Themen aufzugreifen, die hierin nicht behandelt werden konnten.

Scope des Buchs

Im Grunde beschreibt „Technik der IP-Netze“ die Welt bis zum Jahr 2020, während „Zukunft der IP-Netze“ den Blick weitet und die Perspektiven der Computernetze und den Einfluss für unsere Gesellschaft zu vermitteln versucht. In diesem Buch wollen wir den Blick auf die Zukunft richten und unter Kenntnis der bisherigen Entwicklungen folgende Fragen aufwerfen:

- Wie verlief die Menschheitsentwicklung und ihre technisch-wissenschaftliche Kultur, sodass es zu den heutigen IT-Technologien kommen konnte?
- Was sind die heute gebräuchlichen Systemlösungen für verteilte und intelligente Komponenten?
- Welche denkbaren Entwicklungen werden bereits heute konzipiert, die unser Leben von morgen bestimmen werden?



Und natürlich: Welche Gefahren sind hiermit verbunden bzw. welche Maßnahmen und Schritte sind zu unternehmen, sodass Sicherheitsrisiken vermieden oder zumindest minimiert werden können?

Hintergrund

Die Entwicklung der IP-Netze hat in den 2000er-Jahren enorm an Momentum gewonnen. Während wir die „Materialisierung" dieser Technologie quasi in unseren Händen halten, treten damit aber nicht nur neue Perspektiven, sondern auch Gefahren auf. Die Politik (in Europa und speziell Deutschland) sieht sich Gefahren aus dem „Cyberspace" ausgesetzt, die Politiker nur von ihren Beratern und aus Zukunftsromanen kennen.

Die Zukunft ist heute

Bereits 1942 hatte der bekannte Science-Fiction-Autor *Isaac Asimov* die drei Robotergesetze in seiner Kurzgeschichte „*Runaround*"[1] so formuliert:

Die drei Robotergesetze

1. Ein Roboter darf kein menschliches Wesen verletzen oder durch Untätigkeit zulassen, dass einem menschlichen Wesen Schaden zugefügt wird.
2. Ein Roboter muss den ihm von einem Menschen gegebenen Befehlen gehorchen – außer solche Befehle stünden im Widerspruch zu Regel eins.
3. Ein Roboter muss seine Existenz beschützen, solange dieser Schutz nicht mit Regel eins oder zwei kollidiert.

Roboter begegnen uns heute bereits in Supermärkten und werden in naher Zukunft auch als Bestandteile von Fahrzeugen – in Form von autonomem Fahren – für uns selbstverständlich sein.

Ein weiterer Science-Fiction-Autor – *Arthur C. Clark* – hat 1973 darüber hinaus folgende Ansicht postuliert[2]:

«Jede hinreichend fortschrittliche Technologie ist von Magie nicht zu unterscheiden.»

Dies trifft für viele Menschen zu, die täglich ihr Smartphone benutzen und glauben, dass sie Beherrscher dieses Gerätes sind.

Die oben genannten Thesen können letztlich zurückgeführt werden auf *Alan Turing* – einer der Gründerväter der Informatik –, der 1949 in einem Interview mit der Zeitschrift *Times* sagte:

«This is only a foretaste of what is to come, and only the shadow of what is going to be.»

1 Darin soll ein Roboter einem Menschen helfen, gerät hierbei aber in Konflikt mit seiner eigenen „Existenz".

2 *Essay Hazards of Prophecy: The Failure of Imagination*

Dieser Satz ist mehr als weitsichtig: Er antizipiert die (ab diesem Zeitpunkt 1949) zu erwartenden bahnbrechenden Entwicklungen der Informatik als Wissenschaft und des Computers als Werkzeug sowie der Computernetze als deren Verbindungen, was zu diesem Zeitpunkt noch nicht erahnt werden konnte und auf den grundlegenden Arbeiten zur Kommunikationstheorie von *Claude Shannon* [77] aufbaut.

Selbst Fachleuten erscheint die Entwicklung *virtueller Welten*, der *künstlichen Intelligenz* (KI) und des *Quantencomputers* (QC) kaum mehr nachvollziehbar. Seit dem Jahr 2024 ist zudem die Möglichkeit vorhanden, Forschungsergebnisse in diesen Bereichen durch KI so aufzubereiten und zu fälschen, dass diese kaum mehr von realen Forschungen zu unterscheiden sind. In diesem Zusammenhang ist man fast geneigt zu glauben, dass wir in einer *post-faktischen Zeit* leben.

Ziel und Entstehung des Buchs

Ziel des Buchs

Wie auch in unserem Buch „Technik der IP-Netze“ wollen wir den Versuch wagen, die komplexen technischen Sachverhalte soweit herunterzubrechen, dass sie für den Leser nachvollziehbar sind. Dies verlangt allerdings teilweise Vorkenntnisse, die wir in „Technik der IP-Netze“ vermittelt haben, aber auch einige Kenntnisse der Mathematik und Physik, ohne die die aktuellen Entwicklungen nicht vermittelbar sind.

Wir hoffen allerdings, einen geeigneten Mittelweg gefunden zu haben, der die Rezeption dieses Buches auch für interessierte Leser, Studenten der Naturwissenschaften und der Informatik sowie das Fachpublikum ermöglicht und mit dem vermittelten Erkenntnisgewinn belohnt.

Zur Entstehung des Buchs

„Zukunft der IP-Netze“ versteht sich als Fortsetzung unseres Standardwerks „Technik der IP-Netze“ und spannt den Rahmen bewusst weiter. Ausgehend von den Entwicklungen, die sich im Netzwerkbereich seit etwa 2010 vollzogen haben, kamen wir nicht umhin, auch die neuesten Entwicklungen im Bereich der IT aufzunehmen, die zunehmend Gestalt annehmen.

Ausgehend von Prof. Badachs Forschungsunterlagen, die sich auf *Researchgate* finden lassen, wurden die zentralen Teile des Buchs erstellt und bieten somit eine aktuelle Zusammenfassung und Weiterführung dieser Ergebnisse.

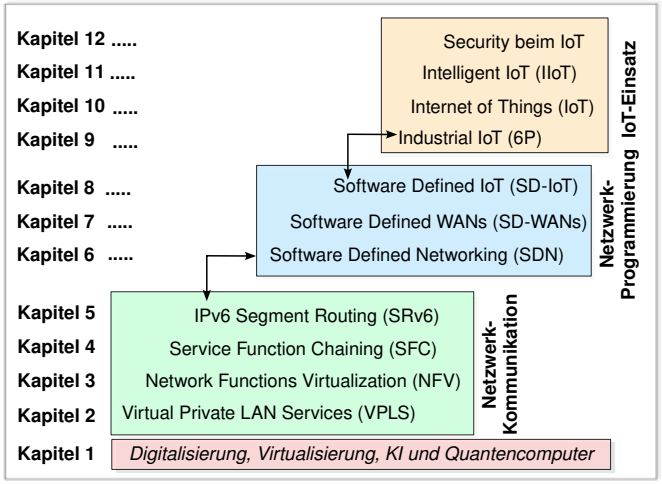
Basierend auf Vorlesungsmaterialien für die Informatik an der *Frankfurt University of Applied Sciences* und der Wirtschaftsinformatik an der *Provadis Hochschule*, wurde Kapitel 1 und Kapitel 12 zeitnah erstellt (2025). Sie präsentieren hier also einen „Snapshot“ der Diskussion über die Themen *Künstliche Intelligenz*, *Quantencomputer* und Kryptographie im Zeitalter der „*Post Quantum Cryptography*“. Kapitel 1 unterschiedet sich von den weiteren Kapiteln dadurch, dass die Abbildungen in deutscher Sprache verfasst sind, während in den weiteren Kapiteln hierfür durchgängig Englisch genutzt wird. Wir hoffen damit, dem Leser die Hürden für die Rezeption des Stoffs nicht zusätzlich anzuheben. Hingegen haben wir es vorgezogen, die „Technitizität“ der folgenden Kapitel nicht durch die „Eindeutschung“ vom vorliegenden Quellmaterial zu verwässern.

Zur Erstellung des Buchs wurde natürlich wieder LaTeX eingesetzt, wobei die Abbildungen diesmal mittels *InkScape* in die finale Form gebracht wurden und daher auch im SVG-Format vorliegen. Diese können bei Bedarf separat bereitgestellt werden.

Zum Aufbau des Buchs

Das erste Kapitel stellt zunächst die allgemeinen Prinzipien der Digitalisierung, die der Virtualisierung sowie der der Einordnung der „Künstlichen Intelligenz“ vor. Ergänzt wird dies abschließend mit einer Vorstellung der Grundlagen von Quantencomputern.

Die nachfolgenden drei Abschnitte besitzen die im Folgenden dargestellten Schwerpunktthemen:



- Die neuen Protokolle zur Netzwerkkommunikation — Teil 1
- Die sich hiermit öffnenden Möglichkeiten der Software Defined Netzwerk-Programmierung — Teil 2
- Deren Umsetzung in Form des „Internet of Things“ — Teil 3

Nutzung and Adressaten des Buchs

Neben den üblichen Referenzen schließen die meisten Kapitel mit Verweisen auf relevante Internet-Adressen ab, die als Start für weitere Recherchen genutzt werden können. Häufig verweisen wir auch auf *Wikipedia*-Quellen. Im webbasierten Internet sind Quellen häufig *volatil*, d. h. die Adresse (URL) ändert sich oder das Quellmaterial wird nicht mehr referenziert. Dies ist ein Fluch, von dem auch wir uns nicht befreien können.

Die Nutzer und Adressaten des Buchs sind aufgefordert, uns Korrekturen und ggf. alternative Quellen und Ergänzungen mitzuteilen. Diese werden über die Webadresse *https://www.fehcom.de/pub/zipn.html* bekanntgegeben. Über diese URL sind auch Korrekturen und Ergänzungen zu finden.

Die Autoren

Prof. Dr.-Ing. Anatol Badach
Über 40 Jahre war er auf den Gebieten Informatik und Telekommunikation tätig; Promotion (1975), Habilitation (1983). Von Dezember 1985 bis August 2012 war er Professor im Fachbereich Angewandte Informatik an der Hochschule Fulda. Seine Schwerpunkte in Lehre und Forschung waren: Rechnerkommunikation, Netzwerktechnologien, VoIP und Next Generation Networking. Er war 1983 bei der Konzeption der Anbindung des Deutschen Forschungsnetzes an das *Computer Science Network* maßgeblich beteiligt. Über diesen Verbund wurde die erste Internet-E-Mail in Deutschland am 3.8.1984 empfangen, womit die Internet-Ära in Deutschland begann. Er ist Verfasser und Mitverfasser von über 20 Fachbüchern.

https://www.researchgate.net/profile/Anatol-Badach

Prof. Dr. rer. nat. Erwin Hoffmann
Jahrgang 1958, Studium der Physik und Astrophysik an der Universität Bonn und 1989 Promotion an der TU München (Max-Planck-Institut für Physik und Astrophysik). Durch seine Tätigkeit in der experimentellen Teilchenphysik am CERN und Fermilab verschaffte er sich Kenntnisse über unterschiedlichste Rechnerbetriebssysteme. Bis 2025 war er Professor für Informatik an der Frankfurt University of Applied Science. Seit 1998 ist er an der Weiterentwicklung der Software von D.J. Bernstein involviert und veröffentlicht diese als *Public Domain*.

https://www.fehcom.de

Danksagung

An dieser Stelle sei allen Dank ausgesprochen, die mit ihren Bemühungen und ihrem Einsatz das föderative Internet aufrecht erhalten und so zu der Kommunikationsplattform des 21. Jahrhundert werden ließ, die unser tägliches Leben begleitet.

Um dies auch „mundgerecht“ zu gestalten hat der Hanser-Verlag uns dankenswerterweise ein qualifiziertes Lektorat zur Verfügung gestellt, wobei unser besonderes Dankeschön Herrn Jürgen Dubau gilt.

1
Digitalisierung, Virtualisierung, Künstliche Intelligenz und die Quantenwelt

Für viele Angehörige der *Generation „Z“* (GenZ), also für diejenigen, die um das Jahr 2000 geboren sind, ist die Digitalisierung ihrer Alltagswelt zur Selbstverständlichkeit geworden. Vertreter früherer Generationen schütteln hierüber gerne mal die Köpfe und haben Schwierigkeiten, hier mitzuhalten.

Grundlage hierfür ist ein Technologiebruch, der sich ab 1970 erst schrittweise, nach 2000 dann aber massiv vollzogen hat: das Internet und seine Möglichkeiten.

In diesem Buch versuchen wir, den Bogen zu schlagen zwischen den Grundlagen der sich entwickelnden Internet-Technologien und ihren Auswirkungen. Hierbei erscheint es uns wichtig, zunächst die Begriffe „Digitalisierung“ und „Virtualisierung“ – die in aller Munde sind – genauer einzugrenzen. Wir werden sehen, dass speziell die „Digitalisierung“ eine Grundlage der menschlichen Zivilisation ist und sich nicht nur auf das Internet-Zeitalter beschränkt. Die Nutzung dieser jeweiligen „Digitalisierung“ brachte in vielen Fällen revolutionäre Umbrüche mit sich, von denen wir nun selbst zu Zeitzeugen werden.

Die „Virtualisierung“ ist hingegen nur auf Grundlage leistungsfähiger Computertechnologien zu verstehen: Elemente der „realen Welt“ werden in die „digitale Welt“ abgebildet und somit „virtualisiert“. Die Interaktion dieser beiden Welten ist nicht nur „faszinierend“, sondern prägt auch die moderne Nutzung der Internet-Technologie, die wir hier näher beschreiben.

In Kapitel 1 wollen wir den Leser mit folgenden Themen vertraut machen:

- Die „erste Digitalisierung“ der realen Welt ist eng verbunden mit der Entwicklung der menschlichen Zivilisation, Wissen und Technik, sowie Ökonomie. Sie reicht zu den Anfängen der Menschheit zurück und hat zu Systembrüchen maßgeblich beigetragen.
- Als „zweite Digitalisierung“ der technischen Welt wollen wir die Entwicklung der Computer- und später Internet-Technologie bezeichnen, die auf der Grundlage der

Elektronik, genauer des Einzugs von modernen Halbleitertechnologien (insbesondere des Transistors) fußt. Diese zweite Welle führte über mehrere Zeitdekaden zu den sehr bedeutsamen technischen Entwicklungen insbesondere von Computern (60er-Jahre), dem Betriebssystem Unix (70er-Jahre) und dem Internet (ab 1980).

- Die „dritte Digitalisierung“ kann um das Jahr 1995 (*E-Commerce*) verortet werden, was schließlich mit der Entwicklung von Smartphones um ca. 2005 zu der heutigen „digitalen Welt“ mit ihren Virtualisierungsmöglichkeiten geführt hat.
- Neben der von Politikern geforderten „digitalen Souveränität“ – die ohne Kenntnis der technischen Hintergründe aussichtslos ist – wollen wir kurz einen kleinen Blick auf das aktuelle Thema AI (*Artificial Intelligence*) und die *Large Language Models* (LLM) werfen.
- Noch herausfordernder ist der Blick auf zukünftige Entwicklungen: dem *Quantencomputer*, dessen erste Ideen sich auf Anfang der 1990er-Jahre zurückdatieren lassen, und den sich hieraus entwickelnden Möglichkeiten, einschließlich der Erfordernissen der *Post Quantum Cryptography* (PQC).

1.1 Die Digitalisierung der Welt

Wenn wir an Digitalisierung denken, assoziieren wir in der Regel *Nerds*, die hinter großen Computern sitzen [Bild 1.1-4]. Tatsächlich könnte kaum ein Bild falscher sein als dieses. Da Sie – lieber Leser – Ihre Augen auf diese Zeile richten, dürfen wir Ihnen verraten, dass diese Zeilen Gegenstand einer (ersten) Digitalisierung sind: *Buchstaben*.

Buchstaben: Das Alphabet als Code

Buchstaben und speziell auch Zahlen sind der Ausdruck eines Codes. Ein Code ist eine Abbildung eines (fiktiven) Gegenstands in ein Symbol, was allgemeinverbindlich mitgeteilt und anerkannt ist. In der Schule lernen wir die Buchstaben „A“ bis „Z“ und „a“ bis „z“ kennen und verstehen, was deren Aussprache und Bedeutung ist. Manchmal macht das uns Schwierigkeiten, wenn es um Buchstaben wie „Y“ geht. Wozu wird das gebraucht? Wenn Fremdsprachen auf dem Lehrplan stehen, verrät uns der Lehrer (oder die Lehrerin), dass das Deutsche „sch“ in Englisch „sh“ geschrieben wird: „Die Leute von der Shiloh Ranch“.

Zahlen als Code

Bei den Zahlen ist es vergleichbar: Die „1“ zählt ein Finger, die „2“ zwei, und wenn wir beide Hände benutzen, symbolisiert das die „10“, also die Grundlage des Dezimalsystems. Andere Zählweisen beziehen sich auf die Knochen im Finger: Hieraus können wir ein *Hexagesimalsystem* konstruieren.

Dies alles sind Konventionen, die von Generation zu Generation übermittelt werden, und sie bilden das Grundgerüst der menschlichen Zivilisation:

- Wir benötigen *Zahlen* (in beliebiger Darstellung), um unser Hab und Gut *quantitativ* zu erfassen.

- Wir benötigen *Symbole* (Buchstaben und Wörter), um die Gegenstände zu beschreiben – und somit *semantisch* zu erfassen –, derer wir habhaft sind.

Cyberspace

Diese generellen Anforderungen gelten unverändert auch für die moderne Welt. Mittlerweile haben wir Maschinen (*Computer*), die rechnen können und eigenständig in der Lage sind, Texte zu verfassen: Sie agieren im Cyberspace.

Bei der ersten Digitalisierung bestand die Aufgabe darin, die reale Welt in eine Zahlenwelt zu überführen. Die zweite – aktuelle – Digitalisierung führt dazu, dass die digitale Welt die reale Welt beeinflusst. Wie dies im technischen Sinne „auf der Netzwerkwelt" passiert, wird in den nächsten Kapiteln ausführlich vorgestellt. Welche Konsequenzen hiermit verknüpft sind, soll in diesem Kapitel erläutert werden. Hierzu wollen wir einen historischen Exkurs vornehmen, der allerdings vornehmlich aus westlicher Sichtweise geprägt ist.

1.1.1 Die erste Digitalisierung

Die Fähigkeit des Rechnens und Schreibens besitzt die Menschheit seit mindestens 7000 Jahren. Sie stellt die Grundlage der modernen Gesellschaften dar. Die zivilisatorischen und technischen Leistungen der frühen Babylonier, der Ägypter, Griechen, Römer, aber auch Chinesen, Azteken, Mayas und Inkas (um nur einige zu nennen) haben sich in das Gedächtnis der Menschheit eingebrannt, wofür die *Sieben Weltwunder der Alten Welt* Zeugnis sind.

Die Erfindung von Zahlen und Symbolen

Die Erfindung von Zahlen und Symbolen ist die erste Digitalisierung: Gegenstände der Realwelt werden durch definierte, unterscheidbare Symbole beschrieben und gekennzeichnet, die allgemein anerkannt und in ihrer Bedeutung gleichbleibend sind. Hiermit lässt sich ein Wirtschaftssystem (*Ökonomie*) aufbauen:

1. Die Menge und Art von Gütern kann *protokolliert* werden.
2. Ein *Datenträger* wird benötigt, der die eindeutigen Bezeichnungen festhält und der nach seiner Erstellung über eine gewisse Zeit gelesen werden kann.
3. Der Wert eines Gutes kann durch Zahlen ausgedrückt (*bepreist*) werden – so wurde „*Geld*" erfunden.

Die Zahlenwelt – Grundlage der ersten Digitalisierung

Einfache Operationen mit Zahlen

Von besonderer Bedeutung sind zunächst die Zahlen: damit kann man die Anzahl an Besitzgütern festhalten, wozu die Operation „Addition" gebraucht wird[1)]. Werden Güter entfernt, benötigen wir die Umkehroperation: Subtraktion[2)]. Allerdings können nie mehr Einheiten entfernt werden, als vorhanden sind. Negative Größen werden somit

1 Dies wird als *Inkrement* – also Zuwachs um eine (u. U. komplexe) Einheit – bezeichnet.
2 Also die *Dekrement*-Operation.

zunächst nicht gebraucht; auch die „0“ ist nur fiktiv und fand erst im 6. Jahrhundert – aus Indien kommend – in unser Zahlensystem Einzug [74].

Die „negativen“ Zahlen

Wie sieht es nun aus, wenn einer Person Güter überlassen werden, die diese nicht besitzt? Hierzu wurde historisch ein *Kerbholz* [Bild 1.1-1] herangezogen. „Etwas auf dem Kerbholz haben“ heißt sinngemäß, etwas zu schulden (engl: debt); sondern schlicht etwas „schuldig sein“, also eine Verbindlichkeit „besitzen“. Das Kerbholz war im einfachsten Fall ein „Stock“, und so wundert es auch nicht, dass die Börse im Englischen *Stock Exchange* genannt wird: *Verbindlichkeiten* (Schuldscheine) können hier ausgetauscht werden.

Die erste Virtualisierung: Bepreisung

Besitzanteile an den Verbindlichkeiten werden nun im Grunde genommen *virtualisiert*, in dem hierfür ein eigener *Markt* geschaffen wird: Der virtuelle Wert bezieht sich somit

- auf die potenzielle *Nützlichkeit* des erworbenen Gegenstandes oder der Leistung und eben
- nicht auf die *Wiederbeschaffungsaufwände* für das Produkt (Material und Herstellung) oder die Mühsal der Leistung (Regenerierung des Körpers).

Durch die *Bepreisung* haben sich Produkt bzw. Leistung und der Wert (ausgedrückt durch eine einfache quantitative Größe) entkoppelt. Hierdurch ergibt sich eine neue Dynamik im Wirtschaftssystem, was letztlich die Grundlage für unsere heutige Zivilisation ist.

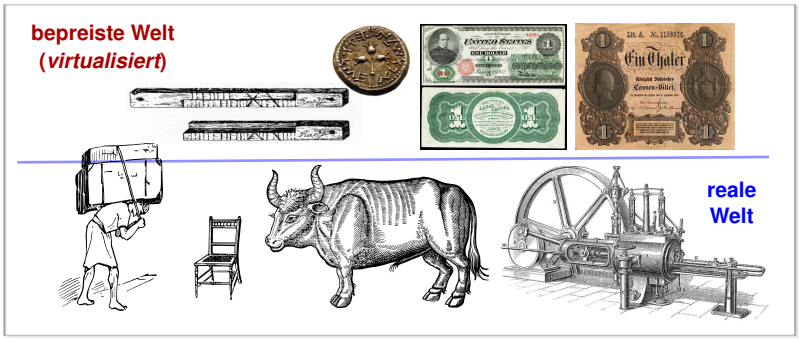


Bild 1.1-1 Entwicklung der Zahlungssysteme (oben: Kerbholz, Münzen, Banknoten) zur Bepreisung der realen Welt (unten: Menschen und Arbeitskraft, Produkte, Tiere und Maschinen)

Kataster und Buchhaltung – Erfassung von Gütern und Besitztümern

Erweiterte Operationen mit Zahlen

Im alten Ägypten war es notwendig, ein *Kataster* für die Felder anzulegen, die regelmäßig vom Nil überschwemmt wurden und somit zur Ernte beitrugen. Die Größe eines rechteckigen Feldes entspricht bekanntermaßen Länge mal Breite. Andere Formen können auftreten (Dreiecke). Zur korrekten Beschreibung benötigen wir Multi-

plikation (aber auch die Division) und Ansätze der Trigonometrie, die uns aus der Schulmathematik durch den „Satz des Pythagoras“ noch in Erinnerung sind.

Zuvor muss aber noch das Problem des „Überlaufs“ gelöst werden. Falls bei der Addition (oder Multiplikation) Zahlen vorkommen, die außerhalb des darstellbaren Bereichs auftreten, müssen wir eine Buchhaltung vornehmen und ein System einführen, das uns mitteilt, dass die folgende Zahl um die „Basis“ zu vergrößern ist.

Die Nützlichkeit des „richtigen“ Zahlensystems und seine Schreibweise

Basis der Zahlensysteme

Diese „Basis“ ist bei uns die Zahl 10, weshalb wir von einem *Dezimalsystem* sprechen. Die „Zehn“ ist aber keine günstige Wahl für das „Teilen“, weil hierdurch selbst einfache Berechnungen schwierig werden. Sinnvoll ist eine Zahl zu wählen, die sehr viele Teiler besitzt:

- 2, 3, 5, 6, 8, 10, 12, 15, 20, 30 … und das ist die Zahl 60. Diese bildete für Jahrtausende die Grundlage des Rechnens und der Mathematik. Das Dutzend macht hier Sinn, und wir sind hier beim *Hexagesimalsystem* gelandet.
- Zudem ist $60/19 \simeq 3.1579$ nur 0.5 % vom wahren Wert der Kreiszahl π entfernt.
- Für die *Eulersche Zahl* gilt, dass `60/22` $\simeq$ `2.727` „e“ auf eine Genauigkeit von 0.3 % approximiert.
- Auch der Wert für den „*Goldenen Schnitt*“ $\Phi = \frac{1+\sqrt{5}}{2} \simeq 1.6180$ wird mit $60/37 = 1.62162162162$ erstaunlich genau getroffen.

Arabische Ziffern

Die Darstellung der Zahlen ist darüber hinaus von besonderer praktischer Bedeutung: Rechneten die Römer mit *lateinischen Ziffern* (`I`, `II`, `V`, `IX`, `X`, `L`, `C` … `MCMLXX`, also 1970), bedienen wir uns heute der arabischen Schreibweise, bei der im Dezimalsystem jeder Ziffernwert durch genau ein Symbol dargestellt wird, was das praktische Rechnen ungemein vereinfacht (vgl. Bild 1.1-2a). Nun können wir – bei einem Überlauf – das nächste Zeichen der „Basis“ einfach durch eine *führende* weitere Ziffer ausdrücken. Diese Umstellung erfolgte in Europa im 15. Jahrhundert und war ein Meilenstein für die Weiterentwicklung der Algebra. Diese war zuvor in der arabischen Kultur deutlich weiter fortgeschritten [82]. Ausgehend von *Fibonacci* (Leonardo von Pisa) verbreiteten sich die arabischen Ziffern in Europa ab dem Jahr 1202, was dann ein Jahrhundert dauerte.

Von der Arithmetik über die Algebra zur Differentialrechnung

Rationale und „reelle“ Zahlen

Damit verlassen wir den Bereich der natürlichen und ganzen Zahlen und haben nach einem Ausflug zu den rationalen Zahlen (*Brüche*) die Welt der reellen Zahlen betreten, die bei der Operation „*Wurzelziehen*“ auftreten können. Das ist naturgemäß sehr unangenehm. Im gleichen Schritt sind auch andere Probleme der Trigonometrie zu lösen: Winkelfunktionen wie *Sinus*, *Kosinus* und *Tangens*.

Infinitesimalrechnung → „Kalkül“

Die notwendige Mathematik bildet zu diesem Zeitpunkt die reale Welt ab: Zahlen können beliebig klein werden („Infinitesimal“). Diese Eigenschaft war bereits bei den Griechen (*Archimedes*) bekannt, aber erst in der Neuzeit durch *Newton* und *Leibniz* im Rahmen des *Kalküls* systematisch erforscht und axiomatisiert worden. Der Leser weiß nun, woher die irrationalen und transzendenten Zahlen wie „e“ und „π“ stammen.

In der physikalischen Welt werden deren Objekte durch *reelle Zahlen* abgebildet; erst mit der Quantenmechanik finden beim Drehimpuls wieder ganze und halbe („gequantelte“) Zustände bzw. Zahlen Verwendung.

Abschluss der ersten Digitalisierung

In Europa war die erste Digitalisierung Mitte des 19. Jahrhunderts weitgehend abgeschlossen:

- Die *Französische Revolution* lag nun einige Jahrzehnte zurück und brachte auch für Deutschland einen merklichen Modernisierungsschub mit sich, in dessen Folge das metrische *Einheitensystem* Einzug fand.
- Die *Mathematik* war soweit entwickelt, die Welt (ohne *Quantenmechanik*) mit *Differentialgleichungen* bis hin zu stochastischen Prozessen zu beschreiben.
- In England vollzog sich die erste Industrialisierung mit der *Dampfmaschine* [Bild 1.1-1] unter Einsatz dieses Wissens (*Carnot’scher Kreislauf*).
- Die *allgemeine Schulpflicht* hatte sich durchgesetzt: Die Menschen hatten die Grundlagen des Rechnens, Lesens und Schreibens vermittelt bekommen. Somit konnte nun jeder volljährige Mensch – und nicht nur die Mitglieder der herrschenden Klassen und des Klerus – als vollumfängliches *Geschäftssubjekt* fungieren: Der *Kapitalismus* war geboren.

Blick zurück in die Medienwelt

Buchdruckkunst

Ursächlich für die Realisierung einer allgemeinen Schulpflicht war eine Erfindung, die einige Jahrhunderte zuvor stattgefunden hatte: die *Buchdruckkunst*.

Damit war eine Technologie erfunden worden, die das schnelle und verlustfreie Duplizieren von Daten und Informationen ermöglichte. Die Einführung von Papier in Europa datiert auf das 12. Jahrhundert, und in seinem Zuge wurden Bücher im *Skriptorium* (von wenigen qualifizierten Menschen) mühsam kopiert. Mit dem Aufkommen des Holzschnitts und des Kupferstichs (*Albrecht Dürer* und *Lucas Cranach*) und kurz danach durch die Erfindung des Buchdrucks durch *Johannes Gutenberg* – bei dem bewegliche und wiederverwendbare *Lettern* genutzt wurden – ergab sich im Mittelalter ein bahnbrechender Medienbruch (vgl. Bild 1.1-2b) und der Aufbruch zur Neuzeit.

Cranach’s Kupferstiche für die Luther-Propaganda

Die Folge war eine nie dagewesene Medien- und Informationsflut (in Form von antiklerikalen Kupferstichen), die mit als Auslöser des 30-jährigen Krieges gelten kann. War es zunächst das gedruckte Bild, mit dem *Martin Luther* und *Lucas Cranach* (der Ältere) den Protestantismus einläutete, so war es in darauf folgenden Jahrhunderten möglich,

Bücher günstig auch für das profane Volk verfügbar zu machen und somit Wissen zu verbreiten: Der Medienbruch wurde zu einer politisch-sozialen Zäsur[3].

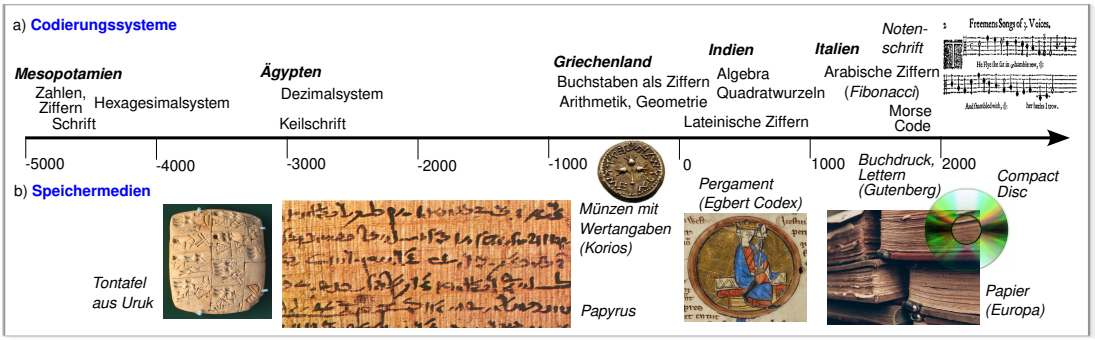


Bild 1.1-2 Entwicklung von a) Codierung von Zahlen, Schrift sowie Noten und b) Datenträgermedien über die Jahrtausende

Papier wird zum Informationsträger und zu Geld

Mit Banknoten zur Geldwirtschaft

Zwei Jahrhunderte später führten diese Umbrüche auch dazu, dass die Zahlungssysteme *digitalisiert* wurden: Statt Münzen zu stanzen, wurden nun Geldscheine gedruckt [Bild 1.1-1]. Der US-amerikanische *Dollarbill* und der in Deutschland ab 1864 eingeführte *Thalerschein* sind Zeugen hierfür, nachdem schon ein Jahrhundert zuvor der papierene *Livre*[4] in Frankreich als Zahlungsmittel eingesetzt und nach seinem Kollaps 1795 durch den *Franc* ersetzt wurde.

Etwa zur gleichen Zeit machten sich *Karl Marx* und (später auch) *Friedrich Engels* auf den Weg, die hierdurch sich umfangreich ändernden ökonomischen Strukturen in *Das Kapital* zu beschreiben [51]. Dies allerdings, ohne die Konsequenzen für die sich hierdurch bedingten radikalen Auswirkungen auf die Geldwirtschaft und die Gesamtökonomie bereits im Voraus antizipieren zu können: Für die Wirtschaft (und die westliche Gesellschaft) hatte sich ab diesem Zeitpunkt die *Geldwirtschaft* von der *Realwirtschaft* entkoppelt. Diese Konsequenz wird uns in der zweiten und dritten Digitalisierung ein weiteres Mal begegnen.

---

3 Dies begleitet uns seit dieser Zeit durch das *Digital Rights Management* (DRM) – als Auswirkung der Rechte der englischen *Buchdruckergilde*. Das Monopol auf das gedruckte Werk wurde im 19. Jahrhundert in den deutschen Ländern unterlaufen, und die Popularisierung des nun günstigen Buchs erfolgte postwendend und erreicht dadurch auch „bildungsferne“ Bevölkerungsschichten.

4 franz. *Blatt*; abgeleitet von lateinisch *libra*; ital. *Lire*.

1.1.2 Die zweite Digitalisierung

Geburt des Computers

Die zweite Digitalisierung startete etwa zur gleichen Zeit, zu der die erste Digitalisierung Vollzug meldete:

- Um das Jahr 1820 stellte *Charles Babbage* in England eine digitale Rechenmaschine vor: die *Difference Engine*. Zwar gab es schon zuvor sowohl „digitale“ (*Abakus*) als auch „analoge“ Rechengeräte (*Rechenschieber*).
- Das Neuartige an dieser Maschine war aber ihre *Programmierbarkeit* und die Durchführung automatischer Berechnungen.
- Auch wenn hierbei nicht von *Binärzahlen*, sondern von *Dezimalzahlen* Gebrauch gemacht wurde, ist die *Difference Engine* doch durch ihr *Rechenwerk* der Vorläufer aller modernen Computer.

Digitale Logik: Boole'sche Algebra

Während *David Hilbert* auf dem 23. „Weltkongress der Mathematik“ in Paris im Jahr 1900 die „Probleme der Mathematik des 20. Jahrhunderts“ umriss, trugen die Jahrzehnte zuvor erfolgten Arbeiten von *George Boole* zur mathematischen Logik maßgeblich zum Verständnis *binärer* – also mit zwei Zuständen – arbeitenden Rechenmaschinen bei.

Lochkarte als Symbol der Datenverarbeitung mit dem Computer

Für die in dieser frühen Phase noch jungen Industrialisierung war eine schnelle und konsistente Datenverarbeitung notwendig. *Lochkarten* gab es schon länger zur Steuerung mechanischer Webstühle. Die bis in die 70er-Jahre des letzten Jahrhunderts verwendeten Lochkarten (*punch cards*) basierten nun auf dem Codierungsschema des Wieners *Hermann Hollerith* und wurden zunächst für Tabellierungsmaschinen eingesetzt.

Erfinder der Informatik: Alan Turing

Bedingt durch die Umwälzungen Anfang des 20. Jahrhunderts besonders im Bereich der Physik (*Albert Einstein*, *Nils Bohr*, *Werner Heisenberg* und *Erwin Schrödinger*) und die beiden verheerenden Weltkriege, erfolgte die Weiterentwicklung der Computertechnik erst wieder in den 40er-Jahren des 20. Jahrhunderts. Sie mündete in den ersten lauffähigen Computern, die vor allem im militärischen Bereich genutzt wurden. So auch in England am *Bletchley Park*, wo ein Team um *Alan Turing* und weiteren polnischen Kryptoanalytikern beschäftigt war, damit die mittels der *Enigma*-Maschine verschlüsselten Funksprüchen der deutschen Wehrmacht zu entziffern.

Von da an war die Computertechnologie in aller Munde, und in den 50er- und 60er-Jahren entwickelte sich die Informatik als eigenständige Wissenschaft rapide.

Rechnen mit binären Zahlenwerten

Neben dem Militär und den Regierungen waren aber auch die großen Firmen daran interessiert Computer einzusetzen. Die nun verfügbaren Computer arbeiteten aber im Binär- bzw. Dualsystem und nutzen für die Berechnung folglich nur die „0“ und die „1“. Dies wird auf der elektronischen Ebene durch zwei Spannungszustände abgebildet; in der Regel 0 Volt für die „0“ sowie +5 Volt für die „1“ [Bild 1.1-3]. Für den seit Mitte der 50er-Jahre verfügbaren Transistor sind dies die idealen Spannungswerte und erlauben die Abbildung der logischen Axiome von *George Boole* in einfachen Schaltungen und zur Durchführung von arithmetischen und logischen Berechnungen.

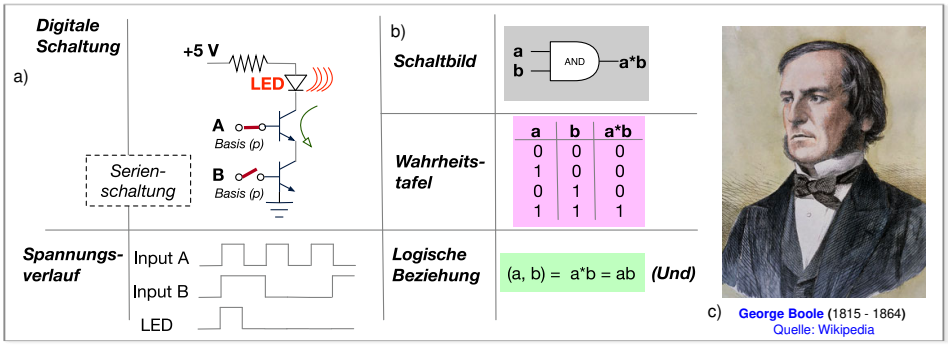


Bild 1.1-3 a) Einfache digitale Transistorschaltung b) mit einer UND-Verknüpfung nach den Grundlagen von c) George Boole (Quelle: Wikipedia)

Hierbei kommt man allerdings schnell an Grenzen, will man einen „Universalcomputer“ bauen:

Aufgaben eines Universalcomputers

1. Obwohl nur auf „0“ und „1“ aufgebaut, mit denen sich die natürlichen Zahlen im Binärsystem elementar darstellen lassen, muss der Computer noch mit negativen Zahlen (ganze Zahlen) und reellen Zahlen (Fließkommazahlen) umgehen können.
2. Der Computer sollte auch eine *Textverarbeitung* durchführen können, also Texte (Buchstaben) lesen, schreiben und manipulieren können.
3. Zudem braucht der Computer ein *Interface*, über das er mit Menschen kommunizieren kann.

In der Phase der „zweiten Digitalisierung“ wurden diese Probleme dann wie folgt angegangen (und gelöst):

- Die einzelnen „0“en und „1“en – nun als Bit (*Binary Digit*) bezeichnet – werden in einer Struktur angeordnet, die Byte genannt wird (1956). Die Länge eines Bytes, d. h. wie viele Stellen es besitzt, war zunächst unklar. Aufgrund der digitalen Arbeitsweise von Computern bietet es sich aber an, dieses als Zweierpotenz darzustellen: 1 Byte = 8 Bit ($2^8 - 1$ als größtem darstellbaren Wert). Zahlen im Binärsystem
- Damit auch negative Zahlen abgebildet werden können, wird für das „Minuszeichen“ ein zusätzliches Bit benötigt, das aus dem Byte entnommen wird. Negative Zahlen werden sodann als „Zweierkomplement“ aufgefasst.
- Will man, dass der Computer auch mit Texten klar kommt, müssen diese auf Zahlen abgebildet (codiert) werden. Beispielsweise könnte der Buchstabe „a“ als Zahl 1, „b“ als Zahl „2“ etc. umgesetzt werden; der Computer muss dann wissen, dass er bei der Ausgabe statt der Zahl „1“ ein „a“ zu schreiben hat. Ein besonders einfaches Schema wurde 1963 als ASCII-Code veröffentlicht (Tab. 1.1-1), wobei die Buchstaben durch ein Byte (unter Auslassung des Vorzeichenbits) codiert werden. ASCII-Alphabet

Tabelle 1.1-1 Die ASCII-Tabelle für die Abbildung von Buchstaben, Ziffern sowie Sonderzeichen in korrespondierende Hexadezimalwerte „00“ bis „FF“ [RFC 20 (!)].

Hex	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	NUL	SOH	STX	ETX	EOT	ENQ	ACK	BEL	BS	HT	LF	VT	FF	CR	SO	SI
1	DLE	DC1	DC2	DC3	DC4	NAK	SYN	ETB	CAN	EM	SUB	ESC	FS	GS	RS	US
2	SP	!	"	#	$	%	&	’	(	)	*	+	,	-	.	/
3	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
4	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
5	P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	_
6	‘	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
7	p	q	r	s	t	u	v	w	x	y	z	{	|	}	~	DEL

Die ersten 32 Zeichen dienen zur Steuerung, von denen heute nur noch das NUL (Terminierung einer Zeichenkette), HT (Horizontal Tabulator), CR (Carriage Return für Zeichenumbruch) sowie LF (Line Feed für Ende einer Zeile) relevant sind. Auch das Zeichen DEL wird nicht mehr benutzt

IEEE 754 Fließkommazahlen

- Besonders kniffelig wird es mit der Umsetzung nicht-ganzer Zahlen (reelle Zahlen): Diese müssen speziell codiert werden: Entweder mit einer festen Anzahl oder aber einer variablen Zahl von Nachkommastellen (Festkomma- bzw. Fließkommazahlen). Bis vor Kurzem war die 1985 eingeführte Norm IEEE 754 der unangefochtene Standard hierfür. Allerdings handelt man sich damit einige prinzipielle Schwierigkeiten ein:
  1. Die Rechengenauigkeit ist beschränkt und hängt von der Anzahl der Bit bzw. Bytes ab. Normalgenauigkeit liegt mit 32 Bit vor, hohe Genauigkeit verlangt 64 (oder 128) Bit.
  2. Bei der Verarbeitung von Fließkommazahlen ist deren Reihenfolge entscheidend: $(a + b + c)$ ist nicht dasselbe wie $(c + b + a)$. Das Assoziativ- und das Distributivgesetz gelten hier prinzipiell nicht. Um Berechnungen mit Fließkommazahlen effizient durchführen zu können, werden diese Operationen in der Regel von einem speziellen *Arithmetic CoProcessor* (ACPU) durchgeführt (vgl. Bild 1.1-6a ohne ACPU).
- Zur Steuerung des Computers braucht es eine Sprache, die sowohl der Computer als auch der Mensch verstehen kann: eine *Programmiersprache*. Zudem wird ein Kommunikationsinterface benötigt, mit denen Befehle an den Rechner übergeben werden können als auch Ergebnisse mitgeteilt werden. Dies wird als *Betriebssystem* verstanden und realisiert die Computer/Mensch-Schnittstelle.

In Bild 1.1-4 sehen wir die beiden „Nerds“ *Ken Thompson* und *Dennis Ritchie*, wie sie an einem der ersten Unix-Systeme arbeiten, das auf der DEC PDP-11 lief. Eingabesystem ist die Tastatur; Ausgabesystem ist der Drucker. Das sind die „Peripherals“, die bis heute die Unix-Welt begleiten und in abstrakter Form in das Betriebssystem konzeptionell eingeflossen sind.

Bild 1.1-4 Dennis Ritchie (links) und Ken Thompson 1972 am Bedienerpult einer PDP-11 unter Unix

Quelle: *https://www.nokia.com/bell-labs/about/dennis-m-ritchie/picture.html* (public domain)

Das Betriebssystem, das die beiden Herren hier nutzen, läuft bis heute (in etwas angepasster Form) auf unserem Smartphone, der Smartwatch, in unseren Autos, aber auch auf Computern in den Raketen von *Elon Musk* oder *Jeff Bezos*.

Die digitale Welt hat die Menschheit in ihrer zweiten Ausprägung praktisch vollständig erfasst, ohne dass die meisten verstanden haben, welch einen „Faustkeil“ sie da in den Händen halten.

1.1.3 Die dritte Digitalisierung

Nachdem wir uns bereits mit dem Zahlensystem beschäftigt haben, benötigt die dritte Digitalisierung nun einen Ausflug in die Algebra, die sich seit etwa 1990 schrittweise in die Computerwelt eingeschlichen hat:

Was ist die Antwort auf alle Fragen[5)]? 42! Die Zahl 42 ist eigentlich nichts Besonderes. Schreiben wir sie im Binärsystem hin, ergibt sich:

5 Douglas Adams: *Per Anhalter durch die Galaxis*

- 101010 – dem entspricht: $1 * 2^5 + 0 * 2^4 + 1 * 2^3 + 0 * 2^2 + 1 * 2^1 + 0 * 2^0 = 42$, oder
- 010101 – in der Darstellung: $0 * 2^0 + 1 * 2^1 + 0 * 2^2 + 1 * 2^3 * 0 * 2^4 + 1 * 2^5 = 42$,

MSB und LSB

je nachdem, ob wir die binäre Zeichenkette von links nach rechts oder von rechts nach links interpretieren, wobei wir davon ausgehen, dass die Bitwertigkeit monoton aufsteigend oder absteigend ist. Wir interpretieren dies als:

- *Most Significant Bit* (first)
- *Least Significant Bit* (first)

Die Wertigkeit einer Bitfolge (Byte) ist eine Konvention! In der arabischen Sprache wird von rechts nach links geschrieben, in den meisten westlichen Sprachen von links nach rechts. Das spielt für die Verarbeitung kaum eine Rolle, ist jedoch für die zeitliche Übertragung von Signalen ausschlaggebend: Hier wird eine *Synchronisation* erwartet. Wird im LSB-Fall das erste ankommende Bit falsch interpretiert, hat dies (für seinen numerischen Wert) wesentlich geringere Auswirkungen als im MSB-Fall.

Algebraische Interpretation einer Bitfolge

Die Übertragung des Bitmaterials kann aber nicht nur zahlentheoretisch, sondern auch *algebraisch* interpretiert werden. Hierbei nutzen wir die Tatsache, dass die Zahl 2 eine Primzahl ist, und wir interpretieren ein Byte als Galois-Feld über der Primzahl $p = 2$ unter Angabe des Rangs des jeweiligen Bit mit n, sodass sich p^n ergibt. Dies entspricht dem *Galois-Feld* $GF(p^n)$ mit der allgemeinen Repräsentierung (für $GF(2^8)$):

$$b(x) = b_7 \cdot x^7 + b_6 \cdot x^6 + b_5 \cdot x^5 + b_4 \cdot x^4 + b_3 \cdot x^3 + b_2 \cdot x^2 + b_1 \cdot x^1 + b_0$$

Rechnen mit Polynomen

Dies ist nun ein Polynom, und die Koeffizienten b_i fassen wir hierbei als die *Bit* in einem *Byte* auf, was für die Informatik auf binären Rechensystemen eine günstige Wahl darstellt. Damit kann die Darstellung von Dezimalzahlen einfach vorgenommen werden: $53 \rightarrow x^5 + x^4 + x^2 + x^0$ bzw. für $42 \rightarrow x^5 + x^3 + x^1$.

Mittels dieser Polynom-Darstellung der Bit bzw. Bytes lassen sich die elementaren Berechnungen sehr einfach durchführen, und durch die Erweiterung des Verständnis der Bitstruktur auf eine algebraische Struktur fallen uns zentrale Aussagen und Beispiele der Zahlentheorie quasi in den Schoß. Hierzu zählen z. B.

- der *Reed-Solomon-Code*, mit dem sich Bitfehler, die in der Übertragung auftreten können, sehr effizient erkannt und korrigiert werden können,
- das sog. irreduzible *Rijndael*-[6)] Polynom: $m(x) = x^8 + x^4 + x^3 + x + 1$ als Grundlage für die AES-Verschlüsselung,
- und natürlich die gesamte modulare Arithmetik, die zentraler Baustein für die *Public Key Cryptography* ist.

Auch wenn wir es nicht auf Anhieb merken: Beim Empfang eines verschlüsselten Fernsehsignals über unsere Satellitenschüssel oder beim Streamen eines *YouTube*-Videos

6 Benannt nach ihren Erfindern *Joan Daemen* und *Vincent Rijmen*

auf unserem Smartphone spielen diese drei Aspekte eine tragende Rolle: Die *dritte Digitalisierung* ist im täglichen Leben angekommen.

Es ist diese neue Art der Mathematik – also algebraische Strukturen –, die unsere Computerprogramme so leistungsfähig macht. Die Algorithmen werden hierbei durch spezielle Bausteine in der CPU abgebildet und dadurch für Programme, die diese nutzen, sehr schnell gemacht.

1.1.4 Vor und nach dem Internet-Zeitalter

Die zweite Digitalisierung verlief ab den 50er-Jahren des letzten Jahrhunderts zunächst nur in den Köpfen der beteiligten Wissenschaftler und Ingenieure. Da Computer unglaublich groß und teuer waren, spielte deren Einsatz für den Normalbürger zunächst kaum eine Rolle.

20. Jahrhundert = analoges Medienzeitalter

Im Gegenteil, im zweiten Drittel des 20. Jahrhunderts und dann verstärkt im dritten Drittel ergab sich durch die Verbreitung des Mediums *Radio* sowie *Film* und *Fernsehen* eine starke Fokussierung auf analoge Medien: Die Informationsdichte beim Lesen eines Buches ist deutlich niedriger als beim Zuhören bzw. Konsum eines Films.

Während das Gehirn die Reize über die Stäbchen und Zäpfchen des Auges, die über den Sehnerv weitergeleitet werden, umfangreich filtern muss, um hieraus eine „Szene“ zu ermitteln, bedingt das Lesen eines Buches genau das Gegenteil: Informationen müssen aus dem Code synthetisiert werden. Da die Filter in unserem Gehirn quasi automatisch angelegt und genutzt werden, stellt die *Synthetisierung* von Informationen aus dem vorliegenden Material einen bewussten Akt dar, der intellektuelle, angelernte Fähigkeiten erfordert.

Allerdings gilt es auch den umgekehrten Weg zu beachten: Durch die Entwicklung elektronischer Geräte (wie Radio, Telefon und Fernsehen) für die breite Masse fielen die Preise hierfür rapide, und die nun verfügbare Technologie konnte auch für den Bau von Computern genutzt werden.

Inkubator: Xerox PARC

Für die meisten Anwender ist es daher erforderlich, dass der Computer mit ihnen „spricht“ und Bilder präsentiert [Bild 1.1-5a]. Diese Technologie wurde in den 70er-Jahren am *Xerox PARC*[7)] entwickelt und vollzog sich praktisch zeitgleich mit der Entwicklung des Unix-Betriebssystems (nachdem *Multics* gescheitert war) und der Vernetzung von Rechnern [Bild 1.1-5b]. Diese fand zunächst „on-premises“ statt und wurde anschließend über das *DARPA-Projekt* quasi ins „Internet“ verlegt.

7 PARC: Palo Alto Research Center

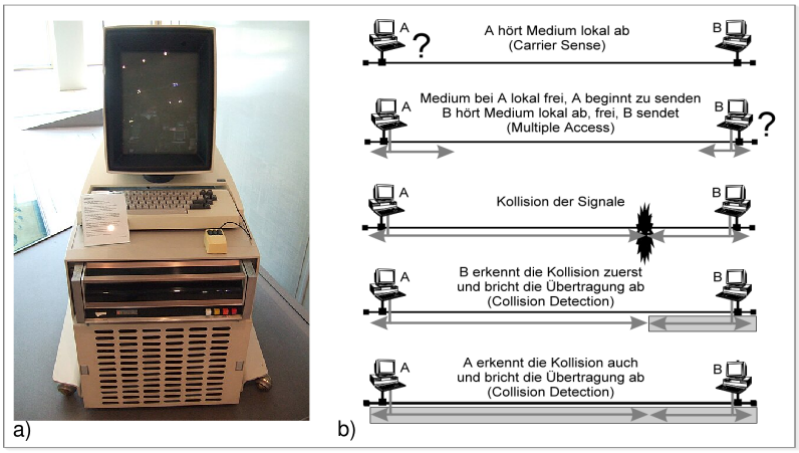


Bild 1.1-5 Zwei grundlegende Erfindungen am Xerox PARC: a) die interaktive Workstation Xerox Alto von 1973 mit Maus (Quelle: Wikipedia), b) das Ethernet LAN als Carrier Sense Multiple Access/Collision Detection (CSMA/CD) Netzwerk

World Wide Web

Die Zusammenführung dieser drei Entwicklungen erfolgte Anfang der 80er-Jahre über das *World Wide Web* (WWW), das zunächst als Prototyp (zur Informationsvernetzung) am CERN von *Tim Berners-Lee* konzipiert und entwickelt wurde. Zusammen mit dem nun verfügbaren, preisgünstigen *Personal Computer* erfolgte schrittweise die Nutzung des Internets zunächst für (ingenieur-)wissenschaftliche Zwecke und mit Aufkommen der SSL-Verschlüsselungstechnologie auch für Geschäftsprozesse.

CD → MP3

Zugleich wurden die Erkenntnisse aus der dritten digitalen Revolution in Consumer-Geräte eingebaut: Mit dem Einzug der *Compact Disc* Anfang der 80er-Jahre begann der Wandel von der Analog- in die Digitalzeit, da hier bereits nicht nur von der Digitalisierung analoger Signale, sondern auch von einer ausgeprägten Fehlerkorrektur auf Bit- und Frame-Ebene Gebrauch gemacht wurde.

Smartphones mit Internetzugang

Mit dem Aufkommen des Smartphones, speziell des *iPhones* im Jahr 2007, schaffte es diese Technologie dann bis in jede Hand und verbindet den Benutzer mit dem Internet bzw. den Applikationen, die anschließend dort zur Verfügung standen. Die Technologie ist somit für die meisten Menschen konsumerabel geworden, ohne dass notwendigerweise ein Verständnis über die hintergründigen Abläufe hierfür vorhanden sein muss bzw. vorausgesetzt wird.

Diesen Umstand machen sich die großen (wie auch kleinen) Konzerne zunutze und bilden nun ihr Angebot im Internet ab, um dieses rund um die Uhr für die Kunden verfügbar zu machen. Hierzu werden nicht nur die eigentlichen Geschäftsprozesse, sondern auch die Unternehmensprozesse soweit als möglich *digitalisiert*, um der nun vorhandenen Volatilität zu entsprechen.

1.1.5 Objekte im digitalen Raum (Cyberspace)

Mitte der 80er-Jahre schuf der Autor *William Gibson* in seinem Roman „Neuromancer“ den Begriff *Cyberspace* und damit ein geflügeltes Synonym für das sich nun entwickelnde Internet, verband es doch den Begriff „Cyber“ (also Kybernetik) mit dem Weltraum („Space“) im Rahmen seiner Science-Fiction-Reihe, die später das Etikett „Cyberpunk“ erhalten sollte. Etwa zur gleichen Zeit erstellte der Autor dieser Zeilen auf einem vom legendären *Seymour Cray* konzipierten Computer der *Control Data Corporation* CDC-7600 („Cyber“) Datenbänder für ein Experiment am CERN.

Bit → Bytes → Datenworte

Wir erinnern uns daran, dass ein Computer in der Regel Bit verarbeitet, die als Bytes zusammenfasst werden. Genauer gesagt müssen diese Bit vom Schaltwerk des Rechners – das aus mehreren elektronischen Bausteinen wie Transistoren besteht – in einem gemeinsamen Schritt angefasst werden. Wie schnell die Abfolge vorgenommen wird, bestimmt die Schaltfrequenz bzw. Taktrate des Rechners. Wie viele Bit oder Bytes gleichzeitig verarbeitet werden können, wird durch die sog. Wortbreite festgelegt und als *Datenwort* bezeichnet. Hierin sind eine oder mehrere Instruktionen untergebracht – oder alternativ die Daten. Diese Wortbreite beträgt heutzutage bei den meisten „größeren“ Computern in der Regel 64 Bit.

Damit ein Computer überhaupt arbeiten kann, müssen zwei prinzipiell unterschiedliche Arten von Informationen vorliegen:

1. Die *Daten*, mit denen es zu rechnen gilt, und
2. die *Instruktionen*, mit denen mitgeteilt wird, wie die Daten zu verarbeiten sind, wobei der Computer hier zwischen arithmetischen und logischen Operationen unterscheidet.

Arithmetische Operationen werden für Zahlen eingesetzt. Bei der Textverarbeitung hingegen erfolgt deren Verarbeitung über logische Verknüpfungen (Vergleiche). Bei der vorgestellten ASCII-Tabelle wurde der Trick angewendet, dass einige Operationen auf Buchstaben sich arithmetisch darstellen lassen[8)].

Gemeinsamer Speicher für Instruktionen und Daten

Nach dem *von-Neumann-Prinzip* [Bild 1.1-6d] liegen Daten und Instruktionen gemeinsam im Hauptspeicher des Rechners; aber an getrennten Stellen. Das Schaltwerk überführt die aufbereiteten Instruktionen an die CPU. Die Daten werden an die Register weitergereicht und nach der Berechnung dort abgeholt.

Informationsobjekte

Die „Objekte“ im Cyberspace liegen als strukturierte Informationen (Bitfolgen) vor, die nach einem Schema dekodiert und anschließend entweder als Instruktionen genutzt oder als Daten verarbeitet werden. Das ist genau das gleiche Prinzip, mit dem auch die Sätze in diesem Buch aufgebaut sind:

- Entweder wissen wir, wo der Datenstrom beginnt (bei uns links oben auf der Seite, im Arabischen rechts oben), oder

8 Zum Beispiel: $a \rightarrow b = a + 1; A \rightarrow a = A + 32$.

- wir identifizieren Sequenzen (Sätze) durch ihre Struktur: Der Satz fängt mit einem Großbuchstaben an und endet mit einem *Terminal-Symbol* (z. B. der Punkt „.“).

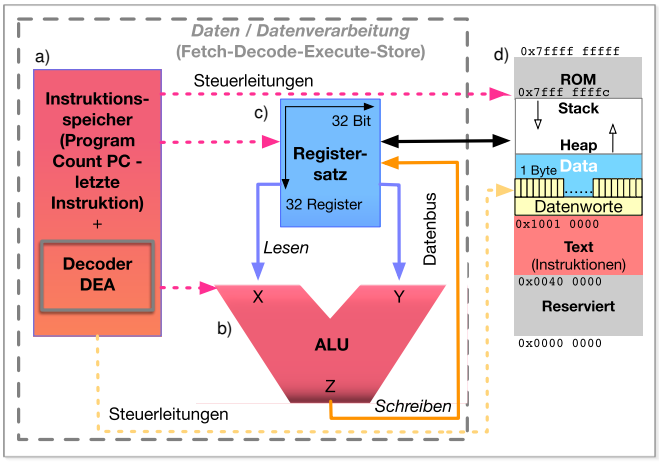


Bild 1.1-6 Zentrale Komponenten eines 32-Bit-Computers mit Instruktionszyklus (Fetch/Decode/Execute/Store) und Datenverarbeitung; a) Instruction-Decoding-Einheit (Schaltwerk), b) Arithmetic Logic Unit (ALU), c) Registersatz, d) Hauptspeicher (Random Access Memory, RAM)

DEA: Deterministischer Endlicher Automat, ROM: Read-Only Memory. Hauptspeicheradressen werden mit mit hexadezimalen Werten dargestellt, die mit „0x“ beginnen.

Grammatiken von Computersprachen

Während wir aber Lesen und Schreiben in der Schule gelernt haben, bleibt das Arbeiten eines Computers für die meisten im Verborgenen. Zudem ist die Grammatik einer Computersprache nach dem strengen Gesichtspunkt der Nützlichkeit und mathematischen Prinzipien aufgebaut[9)].

Datenpakete für den Informationsaustausch zwischen Computern

Damit Computer im „Cyberspace“ kommunizieren können, müssen die Informationen in strukturierter Form ausgetauscht werden:

- Die Daten werden in Pakete „geschnürt“ und mit Ziel und Absender versehen. Zum Schutz gegen Verfälschungen werden sie durch eine *Checksumme* angereichert, über die sich fehlerhafte Bits sogar korrigieren lassen. Allgemein werden diese als *Pakete* oder *Frames* (*Rahmen*) bezeichnet, was ein sehr treffender Ausdruck ist.

Remote Procedure Calls

- Die Rechner können auch Instruktionen untereinander austauschen, wobei sich diese allerdings nicht auf die Maschineninstruktionen beziehen, sondern auf einer abstrakteren Ebene angesiedelt sind: *Remote Procedure Calls*. Ist die Laufzeitumgebung auf dem entfernen Computer bekannt, lassen sich Anweisungen auch direkt übermitteln: *JavaScript* ist hierfür ein bekanntes Beispiel und vollzieht sich im Webbrowser millionenfach.

9 siehe *Noam Chomskys* Generative Grammatiken

- In Kapitel 6 zeigen wir, dass sich auch das die Computer verbindende Netzwerk programmieren lässt. Dies ist der Beginn einer neuen Ära des Internets: *Software Defined Networking*. SDN

Daten (und Instruktionen) im Cyberspace (der digitalen Welt) sind zustandslos, d. h. es sind Bitfolgen und Zahlenobjekte, die ohne ihre besondere Interpretation (durch einen Computer) bedeutungslos sind, auch wenn sie ggf. eine innere Struktur aufweisen[10].

Kommt nun aber ein Computer ins Spiel, ändern sich die Verhältnisse: Durch das Hinzufügen von Energie und dem im Steuerungswerk des Computers „verdrahteten“ Ablaufprogramms beginnen die Daten „zu leben“ und werden schrittweise (im Takt der CPU) verarbeitet. Hierbei können die Daten in drei verschiedenen Zuständen auftreten [Bild 1.1-7]:

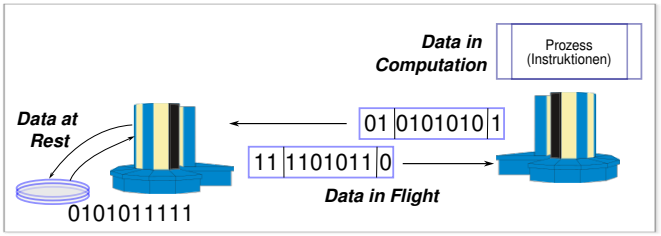


Bild 1.1-7 Zustände von Daten in der digitalen Welt: links eine sog. Storage Node, rechts eine Computational Node; Netzwerkkomponenten nicht gezeigt

1. Daten werden vom Computer verarbeitet und liegen damit in seinem Hauptspeicher. Data in Computation
2. Daten werden zwischen Computern ausgetauscht und über ein Netzwerk übertragen. Data in Flight
3. Daten liegen auf einem Datenträger vor und können von dort wieder gelesen werden. Data at Rest

Die Lauffähigkeit des Computers determiniert die Verfügbarkeit und Nutzung von Daten im Cyberspace.

Beim *Internet of Things* (IoT) bzw. bei sog. *Smart Devices* findet eine Vorverarbeitung der Daten auf einem (leistungsmäßig begrenzten) lokalen Computer (Device) statt, der mit dem Internet (drahtlos) verbunden ist, wo die Daten für weitere Auswertungen – ggf. mit unserer Einwilligung, aber immer ohne unser Zutun – genutzt werden können (siehe Kapitel 10). Smart Devices und IoT

10 Verschlüsselte Daten sind immer so aufgebaut, dass sie sich praktisch nicht von einer Zufallsfolge unterscheiden.

1.1.6 Interaktion des digitalen Raums mit der Wirklichkeit

Die Abbildung eines Objektes aus der realen Welt in den digitalen Raum bedeutet praktisch in jedem Fall die Bereitstellung eines mathematischen Modells, das lediglich die wesentlichen Eigenschaften des „realen“ Objektes beinhaltet. Was bedeutet dies?

Objekt-ID

- Inventarisierung und eindeutige Beschreibung eines Objektes im digitalen Raum:

Digitaler Avatar

  - Jedes Objekt in der realen Welt muss zunächst durch eine *Objekt-ID* eindeutig gekennzeichnet sein und somit identifiziert werden können. Häufig bedient man sich hierbei einer sog. UUID (*Unique User Identifier*).
  - Jedes (individuelle) Objekt wird somit eindeutig abgebildet. Das „lebende“ Objekt – durch seine Objekt-ID zu identifizieren – besitzt im Zustand „Data in Computation“ einen aktiven, aber begrenzten Raum im Hauptspeicher des Rechners.

Reduziertes Objekt

- Das digitale Objekt ist in den meisten Fällen eine Reduktion des realen Objektes:
  - Die komplexen Eigenschaften eines realen Objektes müssen reduziert, programmtechnisch erfasst und somit digitalisiert werden.
  - Das Objekt besitzt eine Anzahl von *Eigenschaften*, deren Messwert und Typ bekannt sein muss (z. B. der obere und untere Blutdruckwert einer Person).
  - Diese Attribute werden typischerweise in Tabellenstrukturen mit *Typ* und *Wert* festgehalten.

Automaten und Computer

- Die Modellierung der Dynamik digitaler Objekte kann nach unterschiedlichen Prinzipien (Klassen) stattfinden. Die beiden wichtigsten sind hier:
  - Das Objekte wird als *Deterministischer Endlicher Automat* (DEA) dargestellt, der eine genau bestimmte Anzahl von Eingangs- und Ausgangszuständen hat.
  - Das Objekt ist *Turing-vollständig*, kann also jeden beliebigen Zustand annehmen und nutzt dabei die Eigenschaften des Computersystems, auf dem es läuft.

Lebensdauer digitaler Avatare

- Das Objekt und seine Eigenschaften unterliegen Transformationen:
  - Objekt und Eigenschaften werden zum Zeitpunkt X (mit Wert Y) registriert und zum Zeitpunkt Z gelöscht (wobei die Löschung nicht permanent zu sein braucht).
  - Während dieses *Life Cycles* werden die Attribute des Objekts erfasst und protokolliert.
  - Das Objekt selbst wird kommissioniert und dekommissioniert (also ins Leben gerufen oder „retired“).
- Wir benötigen eine Schnittstelle, um von der realen Welt auf das digitale Objekt zuzugreifen (und es zu steuern):
  - Das digitale Objekt kann über *Sensoren* Daten als *Nachrichten* aus der realen Welt erhalten, die sein dynamisches Verhalten prägt.
  - Die hierdurch vorgenommene Zustandsänderung (Daten des folgenden Zustands) kann mittels *Generatoren* in die reale Welt gespiegelt werden.

- Das digitale Objekt kann zusätzlich über *Aktuatoren* verfügen, mit denen es mit der realen Welt interagieren kann, und diese Interaktion wiederum über Sensoren verarbeiten.

In Bild 1.1-8 sind die zentralen Elemente zusammengefasst. Die Objekte im digitalen Raum sind dabei rein fiktiv oder virtuell – sofern sie nicht über Sensoren mit der realen Welt kommunizieren und diese Information in den virtuellen Raum mit aufnehmen: Die Programme sind *Instruktionen*, die *Daten* sind künstlich und werden über die Schnittstellen vermittelt.

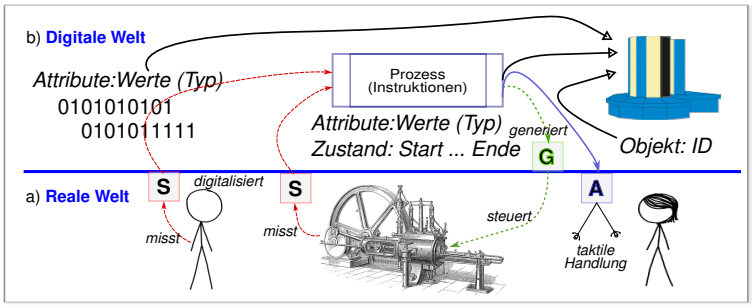


Bild 1.1-8 Abbildung der a) realen auf b) die digitale Welt

S: Sensor, G: Generator, A: Aktuator

Rolle der IT-Systeme

Zur Abbildung dieser Daten werden IT-Systeme benötigt, die während der Erfassung des Objekts lauffähig sind und über die gegebenen Daten und Instruktionen verfügen. Dies muss nicht notwendigerweise ein einzelnes System sein, sondern kann sich über ein Netzwerk erstrecken (*Cloud*), in dem die Informationen ausgetauscht werden.

Die Verfügbarkeit der Daten und ihre Verarbeitung benötigt elektrische Energie. Steht diese nicht zur Verfügung, besteht die digitale Welt nicht weiter: Weder können Daten eingespeist noch abgerufen werden. Hieraus folgt, dass die Daten zumindest im „virtuellen Speicher“ eines IT-Systems vorrätig sein müssen. Daten und Instruktionen können aber auf einem Datenspeicher – der keine weitere Energie benötigt – persistent abgelegt und bei Bedarf wieder eingelesen werden. Da sich die „reale Welt“ weiter bewegt, hat sich die „reale“ nun von der „digitalen“ Welt (dem *Avatar*, wie später beschrieben wird) entfremdet.

1.1.7 Unternehmens- und Geschäftsprozesse im digitalen Raum

Computer werden zu „Commodity“

Waren am Anfang der Computerzeit diese Systeme vor allem für naturwissenschaftliche (Fließkommazahl-) Berechnungen vorgesehen (speziell, was die Simulation von Nuklearexplosionen betraf), so war doch schnell klar, dass mit der aufkommenden Computertechnologie mühsame, manuelle Prozesse nun von Maschinen durchgeführt werden können.

Hierzu zählt auch das Hochrechnen von potenziellen Gewinnern bei Wahlen. 1952 wurde bei der Präsidentschaftswahl in den USA der schnellste damals verfügbare Computer, die UNIVAC (*Universal Automatic Calculator*), eingesetzt, um den Wahlausgang zwischen *„Ike" Dwight Eisenhower* und *Richard Nixon* zu bestimmen.

In Deutschland wurde erst 1965 die damalige Wahl zum Bundestag durch Computer-Hochrechnungen ergänzt[11)].

Computer im Unternehmens-einsatz

Damit war das Tor aufgestoßen, Computer auch für Alltagsaufgaben in Unternehmen einzusetzen, wie z. B. für

- Buchhaltung und Kontoführung sowie
- Lagerverwaltung und Inventarisierung,

auch wenn die Eingabe der Daten noch mühevoll und die Darstellung der Ergebnisse noch eingeschränkt waren. Üblicherweise fand das auf sog. „Midrange"-Computern statt, die in den 60er und 70er Jahren des letzten Jahrhunderts von vielen Firmen hergestellt wurden (*IBM*, *Nixdorf*, *Wang*, *Honeywell*, *Triumph-Adler*, *Olivetti* – um nur einige zu nennen).

Bei großen Datenmengen ist der Computer schnell im Vorteil, auf Grundlage der verfügbaren Eingangsdaten Analysen vorzunehmen. Die Crux ist hierbei die Erfassung und somit Bemessung der Bestände, die per Hand (der Mensch als Sensor) vorgenommen werden muss. Dies wird auch als *permanente Inventur* verstanden.

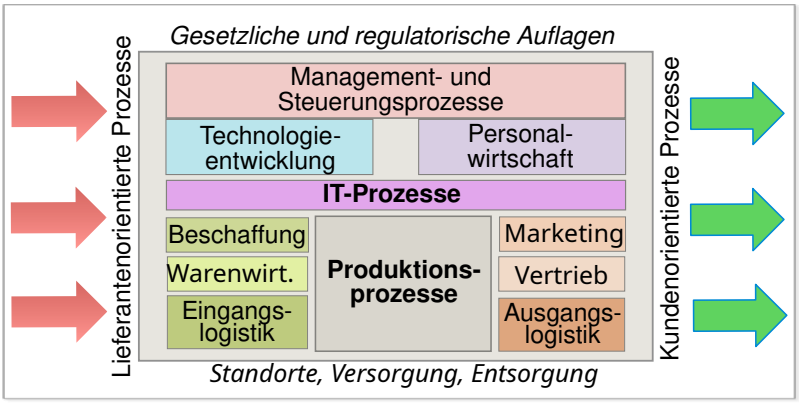


Bild 1.1-9 Die vielfältigen Unternehmensprozesse unter Berücksichtigung von Lieferanten- und Kundenprozessen mit IT als Querschnittsfunktion

Supply Chain Digitalisierung

Bild 1.1-9 lehnt sich an das „added value" (*Wertschöpfung*) Unternehmensmodell von *Porter* (für ein Industrieunternehmen) an. Wir sehen, dass IT-Systeme die innerbetrieblichen Unternehmensprozesse als Querschnittsfunktion unterstützen. Ab ca. 1985

11 Der am Ende des Kapitels verlinkte Film aus der späteren „WDR Computernacht" ist ein historischer Hochgenuss, wobei unklar ist, ob die zusammengeschnittenen Sequenzen repräsentativ sind.

wurden diese dann auch eingesetzt, um die *Supply Chain* mit den Lieferanten zu digitalisieren. Für die Warenwirtschaft wichtig war die Einführung der *European Article Number* (EAN), die maschinenlesbar als Strichcode konzipiert wurde.

Enterprise Resource Planning

Objekte der realen Welt werden somit computergerecht erfasst und aufbereitet, und Änderungen können kurzfristig ermittelt und hieraus Aktionen wie z. B. Warenbestellungen vorgenommen und auch automatisiert werden: *Enterprise Resource Planning* (ERP) war entstanden. Die Datenbestände werden hierbei von Prozessen automatisch erfasst und verarbeitet, was die betriebliche Ablauforganisation deutlich beschleunigt. Da dies auf digitalem Weg erfolgt, werden die Datenbestände zu Informationen, die durch ein betriebliches Informationssystem zu verarbeiten sind. Dies ist Gegenstand des ARIS-Konzepts (*Architektur integrierter Informationssysteme*), das an der Universität des Saarlandes von *August-Wilhelm Scheer* entwickelt wurde.

Betrachten wir die linke Seite von Bild 1.1-9, so können wir feststellen, dass schon sehr früh die Kommunikation mit den Zulieferern digitalisiert wurde. In Bezug auf die Lieferketten fand um 2005 das webbasierte Protokoll SOA (*Service Oriented Architecture*) Einzug in das Beschaffungswesen (*Procurement*), speziell wenn es sich nicht um physische Produkte, sondern um Dienstleistungen handelt.

Digitale Geschäftsprozesse mit Endkunden

Mit der Verbreitung des Internet und der verfügbaren Verschlüsselung der Anwenderdaten mittels der *Secure Socket Layer* (SSL) in Webbrowsern ergab sich auch die Möglichkeit, die Digitalisierung der Geschäftsprozesse auch für die Endkunden voranzutreiben.

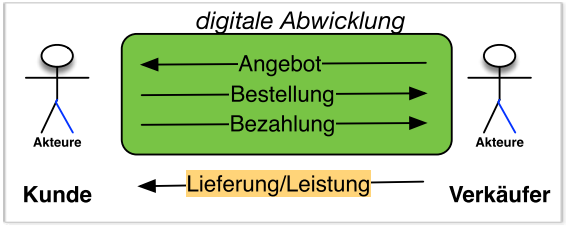


Bild 1.1-10 Geschäftsprozess mit seinen vier relevanten Unterprozessen. Die oberen Unterprozesse können komplett digital abgewickelt werden.

Bild 1.1-10 illustriert den Geschäftsprozess, der in die Einzelprozesse

- Angebotserstellung, — Offer
- Bestellung, — Order
- Bezahlung sowie — Payment
- Lieferung — Delivery

unterteilt werden kann. Augenscheinlich ist es möglich, sowohl das Angebot als auch die Bestellung (und bei digitalen Produkten wie z. B. einem Hörbuch auch die Lieferung) komplett zu digitalisieren. Dies war die Geburtsstunde von *Amazon* und anderen Online-Händlern, die sowohl die früher üblichen Versandhändler (wie *Neckermann* mit dem berühmten „Neckermann-Katalog“) vom Markt verdrängten als auch sich für den

Einzelhandel aufgrund des nahezu unerschöpflichen Angebots zu einer ernsthaften Konkurrenz entwickelten.

Zahlungsdienstleister wie *American Express*, *Visa* oder auch *Mastercard* stellten zeitgleich ihre Abrechnungssysteme von Papier auf das Internet um, indem beim Einzelhändler geeignete Terminals für den Transfer genutzt werden können und sich somit der Bezahlprozess digital abwickeln lässt.

Internet-Ökonomie

Auf mobilen Endgeräten wie dem Smartphone kann der Kunde nun praktisch medienbruchfrei auf Geschäftsprozesse digital zugreifen, wobei die Anbieter wie *Apple* und *Google* auch ihre eigenen *Payment-Systeme* integriert haben: Die digitale Internet-Ökonomie ist komplettiert.

1.2 Die Virtualisierung der Welt

Von Virtualisierung reden wir, wenn Objekte der digitalen Welt so aufbereitet werden, dass diese die Sinne des Menschen ansprechen.

Im Grunde ist dies das Gegenteil der Digitalisierung:

Digitalisierung

- Objekte der realen Welt werden hier entnommen und in der digitalen Welt abgebildet. Die Digitalisierung ist auf realen Daten aufgebaut (*Sensorik*): Sie ist ein (eingeschränktes) Abbild der realen Welt.

Virtualisierung

- Objekte der digitalen Welt werden in die reale Welt projiziert. Bei der Virtualisierung stehen berechnete – und somit im Grunde genommen fiktive – Daten bereit, die in die reale Welt mittels Schnittstellen (*Generatoren*) übertragen werden.

Virtuelle Welten

Bei Computerspielen sind Sensoren das Keyboard oder der Controller, mit denen wir Daten in die „digitale“ Welt einspeisen und das Handlungsgeschehen steuerbar machen, als wären wir mit dieser Welt verschmolzen, die uns nun als „virtuelle“ Welt[12)] erscheint.

Hin- und Rückkanal

Mit anderen Worten: Zwischen der realen Welt und der virtuellen Welt gibt es sowohl einen Hin- als auch einen Rückkanal. Der Datenkanal (also der Generator aus Bild 1.1-8) ist aber auf die menschlichen Sinnesorgane angepasst. Welche Konsequenzen und Möglichkeiten das mit sich bringt, wollen wir uns in den nächsten Abschnitten anschauen und ansatzweise modellieren.

1.2.1 Virtuelle Welten im digitalen Raum

Was ist aber nun eine „virtuelle Welt“ und was kennzeichnet diese als Objekte im „digitalen Raum“?

12 Virtual Reality

Zunächst halten wir einmal fest, welchen Datenbestand die virtuelle Welt aufweist. Hierbei können wir unterscheiden:

Typ 1: Virtuelle Welt als Abbild der realen Welt

Die virtuelle Welt speist sich vollumfänglich von der realen Welt und ist ein Abbild. Dies können wir aus Bild 1.2-1 gut nachvollziehen: Unterschiedliches Kartenmaterial liegt den virtuellen Welten

- *https://www.google.com/maps*,
- *https://www.openstreetmap.org* sowie
- *https://openinframap.org*

zugrunde und bilden einen (domain-)spezifischen Teil der Realität ab.

Typ 2: Virtuelle Welt zur „Anreicherung" der realen Welt

Die virtuelle Welt besteht sowohl aus Daten der Realwelt, die aber zusätzlich mit Daten aus dem digitalen Raum angereichert wird. Dies werden wir uns unter dem Stichwort „Augmented Reality" noch genauer anschauen.

Typ 3: Rein fiktive virtuelle Welten

Die virtuelle Welt ist rein fiktiv und eine Spielewelt. Ihre Herkunft hat sie aus sog. *Textadventures*, die auch als *Multi User Dungeon* (MUD) bezeichnet werden. Die ersten computerbasierten Spielewelten kamen bereits 1970 heraus und waren daher vollständig textbasiert, ggf. ergänzt mit sog. ASCII-Grafiken.

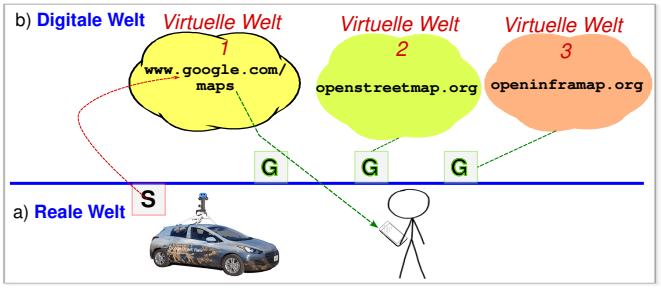


Bild 1.2-1 Kartenmaterial als virtuelle „Typ 1"-Welt a) reale Welt mit Sensoren und dem Smartphone als Display-Einheit b) die digitale Welt mit unterschiedlichen Inkarnationen der virtuellen Welten

S: Sensor, G: Generator

Diese „virtuellen Welten" sind aber im Gegensatz zu dem bislang in diesem Kapitel Gesagten nicht abstrakt, sondern sie benötigen eine computerbasierte Instanz, die die Kontrolle der „Werte" ermöglichen muss:

Was ist eine virtuelle Welt?

Die virtuelle digitale Welt wird durch ein Regelwerk aufgezogen, dessen Instantiierung durch physisch existierende Computer-Netzwerke (*Cloud*, *Blockchain*) „realisiert" werden. Das Regelwerk ist in Form von *Protokollen* beschrieben. Zusammen mit den *Computersystemen* stellt dies die Inkarnation einer Technologie dar, die als *Plattform* bezeichnet wird. Die Abbildung der virtuellen Welt in die reale Welt erfolgt über ein (Display-)Device, das mehrere Sinneseindrücke erzeugen kann.

Das Problem für den Nutzer in Bezug auf die virtuellen Welten vom **Typ 1** und **Typ 2** ist die Korrektheit der Information: Falls fehlerhafte und/oder unvollständige Sensordaten vorliegen oder die Daten im digitalen Raum falsch zugeordnet worden bzw. veraltet sind, kann dies zu erheblichen Auswirkungen führen. Das Navi führt uns gerne dort entlang, wo es keine Straßen gibt.

Bei **Typ 3** virtuellen Welten kann der Effekt auftreten, dass die virtuelle Welt einen größeren Realismus aufweist als die reale Welt. Der Nutzer gleitet somit (intellektuell) in die virtuelle Welt hinüber und verliert die „Bodenhaftung" in der realen Welt.

Avatare

In der virtuellen Welt können auch Personen abgebildet werden, der *Avatar*, der ähnliche Eigenschaften aufweist wie die reale Person. Wir bezeichnen den Avatar daher auch als *digitalen Zwilling* und stellen die sich hieraus wachsenden Implikationen in Kapitel 10 vor.

1.2.2 Interaktion mit der virtuellen Welt

Wenn wir über Objekte in der virtuellen Realität reden, sind dies digitale Objekte, die über eine Maschine/Mensch-Schnittstelle in unser Bewusstsein geraten. Sie sind durch unsere Sinne gefilterte Objekte. Was bedeutet das?

Der Mensch hat bekanntlich „fünf" Sinne, mit denen er die Umwelt wahrnimmt:

Tabelle 1.2-1 Einordnung der menschlichen Rezeptoren (eigene Abschätzung)

Sensor	Rezeptor	Datenrate	Nettorate	Erläuterung
Auge	Zäpfchen (ca. 6 Mio.)	5 Gbit/s	unklar	Gesichtssinn
Ohr	Trommelfell → Schnecke	1 Mbit/s	unklar	Hörsinn
Ohr	Schnecke	unklar	unklar	Lagesinn
Nase	Riechschleimhaut	4 kbit/s	10 bit/s	Geruchssinn
Zunge	Geschmacksknospen	unklar	unklar	Geschmackssinn
Zunge	Fadenpapillen	unklar	unklar	Tastsinn der Zunge
Haut	Hitze-Nozizeptoren	unklar	unklar	Temperatursinn
Haut	C-taktile Fasern (ca. 1 Mio.)	unklar	unklar	Tastsinn
Körper	Nozizeptor	unklar	unklar	Schmerzsinn

Diese tabellarische Darstellung ist selbstverständlich nicht vollständig noch kann deren Korrektheit validiert werden. Es erscheint aber einleuchtend, dass diejenigen Rezeptoren mit dem größten (reduzierten) Informationsgehalt für das Gehirn von zentraler Bedeutung sind.

Emulation virtueller Ereignisse in die Realwelt

Wir berücksichtigen dabei, dass die wichtigsten Informationsquellen Wellen (elektromagnetisch, Schall) sind, die wir im Prinzip sehr gut technisch nachbilden können. Werden zudem Kräfte simuliert (wie z. B. ein sich bewegendes Jahrmarkts-U-Boot), dann sind die Eindrücke so komplex und korreliert, dass sich ein *sensorisches* Ergebnis hieraus ableiten lässt, das von der Realität kaum mehr zu unterscheiden ist.

Dieser Zusammenhang ist bei den Computerspielen gut zu beobachten: Die Animation muss in Bild und Ton stimmig sein, damit ein „Ego Shooter“ funktioniert. Bei einem Konsolenspiel darf auch gern der *Controller* zum gegebenen Ereignis vibrieren.

Es erscheint einsichtig, dass sich gerade ein junger Mensch mit einerseits sehr offenen Sinnen und andererseits mit noch wenig Erfahrungen zu diesen Illusionen herangezogen fühlt.

Realismus und Realität

Wir halten fest, dass es möglich ist, über die Computer/Mensch-Schnittstelle eine virtuelle Umgebung für den Menschen zu schaffen, die der Programmierung im *Cyberspace* folgt:

- Die Menge der Daten, die über den Gesichtssinn übertragen werden können, bestimmt den „*Realismus*“ der virtuellen Welt.
- Die Interaktion des Menschen zur Steuerung von Objekten in der virtuellen Welt ist Maß für die „*Realität*“, d. h. das *Einbezogensein*.

Hohe Datenrate → hoher Energieverbrauch

Dem steht gegenüber, dass eine realistische Abbildung der virtuellen Welt sich nur mit einer großen Menge von Daten über den Generator (vgl. Bild 1.1-8) erzielen lässt. Die Objekte im Cyberspace sind immer strukturierte Information. Um deren Inhalt zu ermitteln, müssen sie (fehlerfrei) erzeugt, dekodiert und übertragen werden. Bei optischen Informationen mit ihrem hohen Informationsgehalt [Tab. 1.2-1] bedeutet das einen erheblichen Rechenaufwand und eine große Bitrate, sprich Bandbreite der Datenverarbeitung. Dies können nur spezielle und leistungsfähige *Grafikprozessoren* (GPUs) bereitstellen, die über dedizierte Hardware-Beschleunigung verfügen. Hierbei ist in allen Fällen Effizienz gefragt: Jede Operation auf der Bit-Ebene benötigt elektrische Energie, um den Schaltvorgang vorzunehmen.

1.2.3 Anreicherung der realen Welt durch Informationen aus dem digitalen Raum: Augmented Reality

Ein Spezialfall liegt vor, wenn die Informationen aus dem digitalen Raum die Wahrnehmung der realen Welt ergänzen sollen: *Augmented Reality* (AR).

Hierbei ist Folgendes zu beachten:

- Die virtuelle Realität muss die reale Welt (modellhaft) geeignet abbilden können.
- Für einzelne Objekte der virtuellen Welt (der *Avatar*) müssen steuerbare Attribute vorliegen, die es ermöglichen, das korrespondierende Objekt in der realen Welt zu „bereichern“.
- Diese Informationen müssen dem Nutzer in der realen Welt „erfassbar“ zugänglich gemacht werden.

In diesem Fall können wir von einem Verbundsystem Sensor/Generator sprechen, das die reale mit der virtuellen Welt verbindet. Notwendig ist ferner eine quasi Echtzeitbearbeitung der Sensordaten durch den Computer und die gleichzeitige Bereitstellung der hieraus generierten Informationen für den handelnden Menschen.

In Anbetracht der Tab. 1.2-1 kann der Computer viel mehr Informationen aus der Realwelt „abzapfen“ und zudem mehrere Quellen verknüpfen, wozu ein Mensch nicht in der Lage wäre. Dies kann z. B. im Bereich Wartung von komplexen Maschinen durchaus vorteilhaft eingesetzt werden.

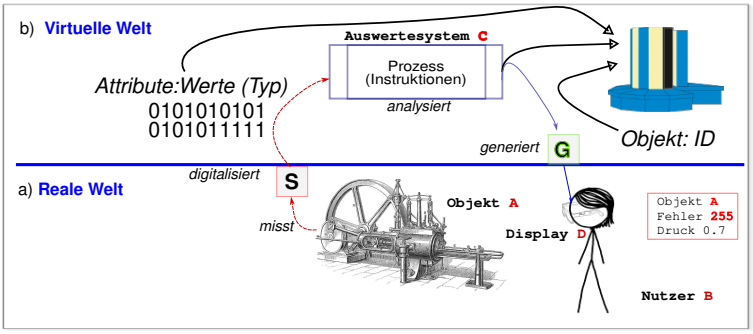


Bild 1.2-2 Modellhafter Einsatz von Augmented Reality zwischen Objekten und Beobachtern in der realen Welt (a) und die Abbildung der Objekte in der virtuellen Welt (b) mit Ausgabe von Fehlermitteilungen über die AR-Brille (Display D)

G: Generator, S: Sensor

Smart Glasses

Augmented Reality kennen wir vor allem von AR-Brillen verschiedener Hersteller, die um das Jahr 2015 angeboten wurden. Die Brille spielte hierbei aber nur eine Rolle für die Informationsausgabe. Will man AR effizient in der Praxis nutzen, sind einige Randbedingungen zu beachten:

- Das auszuwertende Objekt **A** der Realwelt muss über geeignete Sensoren verfügen und qualifiziert modelliert worden sein. Hierzu müssen wohldefinierte Schnittstellen vorliegen, die eine bidirektionale Kommunikation zwischen **A** und dem Auswertesystem **C** erlauben. **C** kann hierbei durch einen Service in der Cloud realisiert werden.

- Es muss eine Echtzeitverbindung zwischen realer und virtueller Welt vorhanden sein. Die Übertragung der Informationen zum AR-Display **D** sollte drahtlos erfolgen.
- Ein Rückkanal von AR-Brille **D** zum Auswertesystem **C** ist vorhanden, damit das spezifische Objekt **A** automatisch von **C** identifiziert und seine Attribute ausgewertet und mitgeteilt werden können.
- Ein weiterer Rückkanal kann über die Mitteilung der Positionen der Hände und Finger (über die Brille oder andere Sensoren) aufgebaut werden, was aber herausfordernd ist.
- Die Informationsdarstellung auf **D** ist zu standardisieren, d. h. der Nutzer **B** muss nicht für jedes System **A** speziell geschult werden.

AR im Einsatz

Beim Einsatz von AR ist Folgendes zu bedenken:

- Der Engpass in diesem System ist der Mensch. Die Informationsvermittlung aus der virtuellen Welt und ihre Darstellung in der realen Welt hat so zu erfolgen, dass der beteiligte Mensch nicht überfordert und abgelenkt wird.
- Hieraus ergibt sich unmittelbar die Frage nach der Mensch/Maschinen-Schnittstelle, also dem *User Interface*. Diese stellt sich seit Anbeginn des Computereinsatzes und ist immer noch nicht zufriedenstellend gelöst.
- Die Objekte in der realen Welt müssen digital erfasst und ihre Attribute bestimmt worden sein. Gibt es kein „Match“ zwischen digitaler und realer Welt, bekommt der Beobachter falsche Daten angezeigt. Somit gilt es auch hier, die Frage der Authentizität und der Korrektheit digitaler Informationen zu beantworten.
- Wird AR z. B. für Wartungsarbeiten von Maschinen eingesetzt, kann der Rückkanal d. h. von der realen in die digitale Welt, zur Übermittlung von Objekt-IDs genutzt werden, falls beispielsweise auf der Maschine QR- oder Barcodes angebracht sind, die diese mitteilen.

Diese anwendungstechnischen Fragen sind bis dato nicht gelöst. AR-Lösungen sind daher immer herstellerspezifisch und somit im Einsatz eingeschränkt.

Verzichtet man auf eine *Objekt-ID*, müsste der Computer **C** die reale Welt a priori kartographiert und Zugang zu den gesamten visuellen Informationen der AR-Brille haben; sprich: Die Brille **D** fungiert als *Kamera* (Spion) und überträgt diese Informationen permanent und mit hoher Datenrate an das Auswertesystem **C**.

Wir werden in den nächsten Abschnitten sehen, dass dies ein entscheidendes Anwendungskriterium sog. *Large Language Models* (LLM), sprich *Artificial Intelligence* (AI) ist.

1.2.4 Besitztum an digitalen Objekten: Cybercurrency und Non-Fungible Token (NFT)

Die Objekte in der digitalen Welt sind ausschließlich binäre Daten: Instruktionen oder Daten, die als Zahlen dargestellt werden können.

Grundgerüst: Zufallszahlen

Im Prinzip sind Zahlen zustandslos, d. h. sie können einfach gewählt werden. Hierbei tritt das Phänomen auf, dass Zahlen entweder in einer algebraischen Struktur geordnet (z. B. in aufsteigender Reihenfolge) oder rein zufällig gewählt werden können.

In diesem Fall kann mein Nachbar nicht abschätzen oder ermitteln, welche „Zufallszahlen“ ich mir ausgedacht habe. Dieser *Nachbar* kann aber auch ein Automat sein. Im Speziellen ist es der Lotto-Automat, der zweimal pro Woche die Lottozahlen zieht: *Zufallszahlen* sind die Grundlage der Kryptographie:

> Alle Schlüssel[13)], die wir nutzen, werden nach dem Prinzip der *Zufälligkeit* erzeugt und benötigen genügend *Entropie* zu ihrer qualifizierten Erzeugung.

Die im digitalen Raum erzeugten Objekte sind Zahlenfolgen. Diesen Zahlenfolgen kann jedoch eine Struktur mitgegeben werden. Bild 1.1-6d hat dies für die Belegung im Hauptspeicher gezeigt, und Bild 1.1-7 illustriert dies für Data-in-Flight. Dieses System können wir auch auf persistente Daten (also auf einer Festplatte beispielsweise) übertragen. Betrachten wir diese Zahlenfolge als digitales Objekt, muss ich wissen, wie ich an dieses herankomme.

Wir können uns dieses digitale Objekt vorstellen wie ein Gemälde, das von *Picasso* oder anderen großartigen Malern erstellt wurde. Im Grunde sind dies auch nur „Farbkleckse“, die aber gemeinsam ein Bild ergeben. In der realen Welt können wir Bilder fälschen, sodass sie sich beim Anschauen nicht vom Original unterscheiden lassen. Lediglich eine Untersuchung des materiellen Status gibt hierüber Auskunft.

Besitz → Wissen

In der digitalen Welt gibt es keine „Substanz“; alle Informationen und Daten können komplett verlustfrei kopiert werden und unterscheiden sich daher nicht von den Ursprungswerten. Daher gibt es auch keinen „Besitz“ an Daten (sieht man einmal von einem physischen Datenträger ab, der die einzige Kopie dieser Daten beinhaltet). In der digitalen Welt müssen wir die digitalen Objekte, die wir besitzen, an einem Ort im digitalen Raum unterbringen, zu dem nur wir den Zugang kennen (*Wissen*): Damit können wir eine Bindung zwischen Besitzer und digitalem Objekt vornehmen: *Non-Fungible Token*.

Instantiierung der virtuellen Welt: Plattformen

Das Regelwerk sieht hierbei folgende hierarchisch gegliederte Mechanismen vor [17] [Bild 1.2-3]:

① Die *Persistenzschicht*, die beschreibt, wo und wie die Daten physisch abgelegt werden.

② Die *Authentisierungsschicht*, die es einem potenziellen Nutzer ermöglicht festzustellen, wer der Ersteller oder der „Besitzer“ der Daten ist.

13 Mit Ausnahme der Passwörter, die wir selber vergeben.

③ Die *Verifikationsschicht*, mit der die Korrektheit der abgelegten Daten belegt und ermittelt werden kann.

④ Die *Blockchain-Schicht*, die die einzelnen Datenbestände unlösbar und nachvollziehbar miteinander verknüpft.

⑤ Die *Anwendungsschicht*, mit der der Zugriff auf die Daten (samt Protokollierung) geregelt wird.

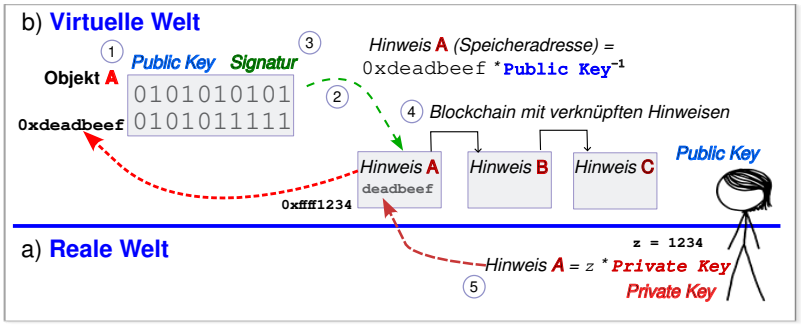


Bild 1.2-3 Non-Fungible Token im virtuellen Raum: a) Platzierung des Objekts an einer Speicheradresse im virtuellen Raum, b) Berechnung der Speicheradresse durch eine verknüpfte Identität in der realen Welt mittels eines public und private Keys; der private Key darf in der virtuellen Welt nicht öffentlich verfügbar sein. Erklärung von ① bis ⑤ siehe oben.

Solche Systeme können entweder als zentrale Dienste von z. B. Regierungen bereitgestellt werden oder aber *föderiert* sein – also von einer Gruppe von assoziierten Betreibern betrieben werden, was beispielsweise auf den bekannten Bitcoin ₿ zutrifft. Zentrale Aufgabe dieses Systems ist es, den Zugang zu den Daten (d. h. deren „Benutzung“) zu regeln und zu protokollieren. Dies basiert auf einer Abmachung (Vertrag) zwischen „Besitzer“ der Daten und dem System sowie dem System und den „Nutzern“ der Daten.

Internet Scam

Es erscheint einleuchtend, dass derjenige, der Kenntnisse über das System besitzt, sich die digitalen Objekte hierin beschaffen bzw. erschleichen kann: Das System ist ein *Scam*. Es wurde nur geschaffen, um gutgläubigen Benutzern „Geld aus der Tasche zu ziehen“, ohne einen wirklichen Mehrwert zu bieten (der sowieso komplett „immateriell“ ist und sich einer Bewertung entzieht).

Wie auch beim Geld besteht der „Wert“ darin, dass dieser zu einem gegebenen Zeitpunkt zu einer „Leistung“ umgemünzt werden kann. Dies ist nichts anderes als ein Versprechen. Wie wir anfangs des Kapitels gesehen haben, verbürgt sich beim Geld hierfür der Staat. Bei den digitalen Welten gibt es aktuell hierfür noch keine anerkannten Ansätze. Daher sind die gängigen Plattformen für „digitale Objekte“ für Internetbetrug prädestiniert.

Public-Key-Verfahren als Fundament der digitalen Welt

Ein digitales Objekt können wir uns wie die Kombination eines Bankschließfachs mit einer öffentlichen Galerie vorstellen:

In der öffentlichen Galerie liegt mein Picasso, den jeder ansehen kann. Zudem kann jeder überprüfen, dass er sich in meinem Besitz befindet. Den „Picasso“ kann ich aber auch „verkaufen“, sodass dieser den Besitzer wechseln kann.

Wie kann das funktionieren? Hierbei hilft uns die spezielle Mathematik auf den ganzen Zahlen, die wir als Algebra über einem endlichen Zahlenkörper kennengelernt haben [Bild 1.2-3].

Rezept zur Generierung von NFTs

1. Wir generieren für eine Identität in dieser virtuellen Welt sowohl einen öffentlichen Schlüssel K_{pub} als auch den zugehörigen privaten Schlüssel K_{priv}. Beide sind im Grunde genommen nur Zahlen, die aber eine besondere Eigenschaft aufweisen:
   - Die Mathematik (das Protokoll) in diesem System (der Plattform) verlangt nun, dass das Produkt von $K_{priv} \otimes K_{pub} \equiv 1$ ist; Modulo einer großen Primzahl p. Dies stellt die *Umkehroperation* auf der Plattform dar. p nennen wir die Ordnung der (mathematischen) Gruppe.
   - K_{pub} und K_{priv} sind einmalig im System, der Plattform. Die Identität ist einfach K_{pub}, die jeder kennt und kennen darf. K_{priv} ist unbedingt geheim zu halten.
2. Zur Identifikation eines zugehörigen digitalen Objekts **A** wird eine Zufallszahl z benötigt. Diese wird mit K_{priv} multipliziert, wobei der resultierende Wert die *Speicheradresse* als $\texttt{Hinweis}_{\texttt{A}}$ (*Token*) ergibt, der an einer öffentlich bekannten Stelle im System hinterlegt wird.
   - $\texttt{Hinweis}_{\texttt{A}}$ beinhaltet nun die Adresse, an der das digitale Objekt auf der Plattform platziert ist.
   - Das digitale Objekt **A** kann zusätzlich mit dem public Key K_{pub} sowie einer digitalen Signatur ergänzt werden, die die Nutzung von K_{priv} erfordert. Dieses Objekt ist sodann *immutable*, also vor Veränderungen geschützt.
3. Unter Mitteilung der Adresse $\texttt{Hinweis}_{\texttt{A}}$ oder falls jemand zufällig darauf stößt, kann nun über den Hinweis und den öffentlichen Schlüssel K_{pub} festgestellt werden, wer der Besitzer dieses Objekts im virtuellen Raum ist bzw. wer das Objekt dort hinterlegt hat.
4. Die Plattform (das Regelwerk) stellt sicher, dass sich keine unautorisierte Kopie meines digitalen Objektes im System erstellen lässt, wofür dann noch digitale Signaturen benötigt werden (und ergänzend zu $\texttt{Hinweis}_{\texttt{A}}$ hinterlegt werden kann).
5. Die Plattform sorgt ferner dafür, dass es keine Überschneidungen der Hinweise für dieses beschreibende digitale Objekte geben darf. Ist der digitale Raum groß genug (dies ergibt sich durch den Wert der Primzahl p), kann dies weitgehend garantiert werden (sofern korrekt umgesetzt).