

# Inhaltsverzeichnis

---

<b>Vorwort</b> .....	<b>9</b>
<b>1 Einleitung</b> .....	<b>11</b>
<b>2 Internet: Das Netz der Netze</b> .....	<b>17</b>
2.1 Historischer Überblick.....	17
2.2 Packet switching theory und offene Netzwerkarchitektur – zwei wesentliche Erfolgskomponenten .....	18
2.3 Das ARPANET .....	19
2.4 Der Wandel vom ARPANET zum Internet .....	20
2.5 Der Wandel vom ehemals wissenschaftlichen Informationsnetz zur kommerziellen „Spielwiese“ .....	29
2.6 Wer regiert das Internet? .....	32
2.7 Notwendigkeit der Entwicklung elektronischer Zahlungsverfahren ...	35
2.7.1 Nachteile herkömmlicher Zahlungssysteme .....	36
2.7.2 Zwölf Grundanforderungen an Digital Cash-Systeme .....	39
2.8 Allgemeine Begriffsabgrenzungen.....	41
2.8.1 Digital Cash .....	41
2.8.2 Smart Cards .....	42
<b>3 Die Treiber der Entwicklung virtuellen Geldes</b> .....	<b>45</b>
3.1 Kreditkartengesellschaften als primäre Triebkräfte.....	47
3.2 Banken als primäre Triebkräfte .....	48
3.2.1 Banken im Aufbruch – Eine neue Ära beginnt .....	50
<b>4 Status quo der Zahlungsverfahren im Internet</b> .....	<b>53</b>
4.1 Zahlungsverfahren unter Verwendung herkömmlicher Kreditkarten .....	53
4.2 Nachteile bei der Verwendung von Kreditkarten im Internet .....	56
4.2.1 Das Hauptproblem: Keine Kleinst- und Mikrobetrags- transaktionen bei Verwendung von Kreditkarten.....	57
<b>5 Die großen Barrieren eines „freien“ Zahlungsverkehrs via Internet</b> .....	<b>59</b>
5.1 Softwareaspekte .....	59
5.2 Hardwareaspekte .....	59
5.3 Sicherheit .....	61
5.3.1 Grundsätze der Kryptographie .....	63
5.3.2 Die fünf Grundsätze der Verschlüsselung .....	64

- 5.3.3 Verschlüsselungsverfahren ..... 65
  - 5.3.3.1 Secret-Key-Kryptographie (symmetrisch) ..... 65
    - 5.3.3.1.1 DES (Data Encryption Standard) ..... 66
    - 5.3.3.1.2 IDEA (International Data Encryption Algorithm) ..... 67
  - 5.3.3.2 Public-Key-Kryptographie (asymmetrisch) ..... 67
    - 5.3.3.2.1 RSA (Rivest, Shamir, Adleman) ..... 68
  - 5.3.3.3 Das Zusammenspiel von DES und RSA ..... 69
  - 5.3.3.4 Einweg-Hash-Funktionen ..... 69
  - 5.3.3.5 Steganographie – eine ausgesprochen effektive Methode der Geheimhaltung ..... 70
  - 5.3.3.6 Erfolgreiches Key-Management ..... 72
- 5.3.4 Die Bedeutung adäquater Schlüssel ..... 72
- 5.3.5 Ansatzpunkte für die Kryptoanalyse ..... 73
- 5.3.6 Gibt es hundertprozentige Sicherheit? ..... 75
- 5.4 Kryptographie als Basiselement digitaler Signaturen ..... 78
  - 5.4.1 Anforderungen an digitale Signaturen ..... 78
  - 5.4.2 Digitale Signaturen in der Praxis ..... 78
  - 5.4.3 Nachteile digitaler Signaturen ..... 79
- 5.5 Das Double-spending-Problem ..... 80
- 5.6 Anonymität ..... 80
  - 5.6.1 Das Konzept der blind signatures ..... 81
  - 5.6.2 „Nachweisbare“ Anonymität ..... 82

**6 Die Kryptokontroverse ..... 85**

- 6.1 Mögliche Ausformungen einer Kryptoregulierung ..... 86
- 6.2 Pro und kontra staatliche Kontrolle von Kryptographieverfahren ..... 87
  - 6.2.1 Der Stellenwert von Trust-Centern ..... 90
- 6.3 Jede Kryptographiebeschränkung kann umgangen werden ..... 91
- 6.4 Kryptographie im internationalen Vergleich ..... 92
  - 6.4.1 Wassenaar Arrangement ..... 92
  - 6.4.2 Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) ..... 93
  - 6.4.3 Europäische Union ..... 94
  - 6.4.4 Deutschland ..... 95
    - 6.4.4.1 Das Informations- und Kommunikationsdienstegesetz (IuKDG) ..... 95
  - 6.4.5 Österreich ..... 96
  - 6.4.6 Vereinigte Staaten von Amerika ..... 97
  - 6.4.7 Frankreich ..... 98

<b>10 Entwicklungstendenzen des Zahlungsverkehrs im Internet</b> .....	<b>157</b>
10.1 Praxisbeispiele eines DC-Wirtschaftsverkehrs .....	161
10.2 Resümee der DC-Systeme .....	163
10.3 Weiterreichende Problemstellungen .....	164
<b>11 Schlußbemerkungen</b> .....	<b>167</b>
<b>12 Quellenregister</b> .....	<b>169</b>
12.1 Verzeichnis der zitierten Quellen .....	169
12.2 Web-Seiten mit Links und Informationen zu den verschiedensten Themenbereichen .....	171
12.3 Allgemeine Literatur .....	172
12.4 Historische Entwicklung des Internets und des World Wide Web .....	173
12.5 Internet-Organisationen .....	174
12.6 Demographische und statistische Informationen .....	175
12.7 Kryptographie und Steganographie .....	176
12.8 Internationale Kryptoregelungen .....	177
12.9 Geldpolitik .....	178
12.10 Protokolle .....	179
12.11 Banken und das Internet .....	180
12.12 DC-Systeme .....	181
<b>13 Glossar</b> .....	<b>185</b>
<b>14 Index</b> .....	<b>191</b>

<b>7 Der Stellenwert staatlicher und zentralbankmäßiger Regulierung und Kontrolle .....</b>	<b>100</b>
7.1 Wer soll die Emissionsberechtigung für digitales Geld besitzen? Wer soll die Aufsicht führen? .....	102
7.1.1 Substitution von Bargeld.....	104
7.2 Die Problematik der Verwendung eines international verflochtenen Netzwerkes .....	106
7.3 Staatliche Kontrolle versus anonymes DC-Geld .....	107
7.4 Zinsen .....	107
7.5 Die Einhebung von Steuern via Internet .....	108
 <b>8 Die Welt der Internet-Protokolle .....</b>	<b>113</b>
8.1 Protokolle für sichere WWW-Verbindungen .....	113
8.1.1 Secure Sockets Layer (SSL)-Protocol .....	114
8.1.2 Secure Hypertext Transfer Protocol (S-HTTP).....	115
8.2 Secure Electronic Transaction (SET) .....	116
8.3 Home Banking Computer Interface (HBCI) .....	119
8.4 Joint Electronic Initiative (JEPI) .....	121
 <b>9 Die ersten Gehversuche – DC-Systeme der ersten Generation</b>	<b>125</b>
9.1 Allgemeine Charakteristika elektronischer Zahlungssysteme der ersten Generation .....	125
9.2 Allgemein verwendbare DC-Systeme auf Softwarebasis.....	128
9.2.1 Ecash .....	128
9.2.2 NetCash .....	133
9.2.3 Millicent .....	135
9.3 DC-Systeme auf Scheckbasis .....	136
9.3.1 NetBill .....	136
9.3.2 NetCheque .....	138
9.3.3 Checkfree .....	139
9.4 DC-Systeme auf Basis von Kreditkarten .....	139
9.4.1 CyberCash .....	140
9.4.2 First Virtual .....	141
9.5 DC-Systeme auf Smart Card-Basis.....	142
9.5.1 Mondex .....	143
9.5.2 CAFE (Conditional Access for Europe).....	145
9.5.3 Quick .....	147
9.5.4 Smart Card-Systeme mit Schattenkonten .....	149
9.5.5 Smart Cards ohne Internet-Anbindung.....	150
9.6 Zusammenfassung .....	151