

Contents

Preface	xi
Book Notes	xii
1 Introduction	1
What Can Emerge	3
Technical Challenges	5
Political Challenges	9
How to Use This Book	12
2 Cryptography	15
Introduction	15
Private-Key Encryption	19
Public-Key Encryption	24
Signature-Only Systems	29
Discrete Log Signature Schemes	32
Blinded Digital Signatures	33
Hash Algorithms	34
Secret Sharing	40
Bit Commitment	40
Zero-Knowledge Proofs	41
Kerberos	46
Political Concerns	47
3 Cash Protocols	49
Digital Checks	49
Digital Cashier's Checks	53
Simple Anonymous Cash	55

	Traceable Anonymous Cash	57
	Cash without Choices	62
4	Flexible Cash	67
	Universal Electronic Cash	68
		75
5	A Product Overview	75
	On- or Off-Line	79
	Encryption and Security	82
	Certificates and Repudiation	84
	Anonymity	87
6	First Virtual	88
	A Model Transaction	92
	Trying Before Buying	93
	Possible Attacks	95
	How to Set Up a First Virtual Storefront	103
	Final Assessment	105
7	HTTP and Cash	107
	S-HTTP	111
	SSL	114
	Using a Secure Link	118
	JEPI and UPP	121
	Final Assessment	123
8	IBM's iKP	124
	1KP	125
	2KP	126
	3KP	128
	Final Assessment	131
9	NetCash and NetCheque	131
	NetCash	136
	NetCheque	138
	How to Set Up a NetCash and NetCheque Storefront	138
	Pay Per View (PPV)	138
	Final Assessment	139

10	CyberCash	141
	Credit Cards	142
	Cash Transactions	144
	Bit-Level Details of CyberCash	144
	The Internet Payment Framework	151
	How to Set Up a CyberCash Storefront	153
	Final Assessment	153
11	CyberCoin	155
	Transaction Details	156
	Final Assessment	157
12	SET	159
	Overview of the Transactions	160
	Certificates and SET	160
	The Transaction Data Flow	164
	Final Assessment	171
13	CheckFree	175
	CheckFree's Wallet	176
	How to Set Up a CheckFree Storefront	177
	Final Assessment	177
14	Open Market	179
	First Virtual vs. Open Market	181
	How to Set Up an Open Market Storefront	182
	Final Assessment	184
15	CAFE	185
	Cryptographic Foundations	186
	Final Assessment	187
16	DigiCash	189
	A Sample Transaction	191
	How to Set Up a DigiCash Storefront	193
	Final Assessment	196
17	Citibank's Transaction Cards	199
	Transactions	200
	Multiple Currencies and Credit	202

	Decentralized, Off-Line Transactions	204
	Anonymity and Citibank's System	206
	Final Assessment	206
		209
18	Smart Cards	210
	Mondex	214
	Visa Cash	215
	Final Assessment	217
		218
19	Millicent	218
	Millicent Scrip	222
	Anonymity and Refreshing	224
	Integrating Millicent with HTTP	226
	Legal Details	227
	Final Assessment	229
		230
20	MicroMint	230
	Minting Coins	231
	Details of Minting	234
	A Practical Example	235
	Anonymity	236
	Final Assessment	237
		238
21	PayWord	238
	Minting Details	239
	Final Assessment	241
		242
22	Magic Money	242
	Setting Up a Magic Money Server	245
	The Magic Money Client	246
	A Sample Transaction	247
	Final Assessment	249
		249
23	NetBill	249
	A Simple Exchange	251
	Encryption Details	251
	Setting Up a NetBill Storefront	252
	Final Assessment	253
		254
24	EDI	253
	X12 Standard	254

25	Security	261
	Hardware Problems	262
	Software Weaknesses	267
	Algorithmic Failures	270
	Summary	272
		273
26	Money Past	273
	Wampum and Beaver Pelts	275
	Tobacco Reigns	276
	A Penny Printed Is a Penny Earned	277
	A Brave New Bimetallism	278
	Biddle's Bank	280
	The Greenback Era	282
	Cross of Gold	283
	Gold in the 20th Century	284
	Conclusions	285
		289
27	Future Cash	289
	Token- versus Account-Based Money	290
	Anonymity in the Future	291
	What Is Money?	294
		299
28	Card Trader 2010	299
		305
29	Other Voices	305
	Regulation	305
	Privacy	311
	Q & A with Dave Banisar	312
	Q & A with Stewart Baker	315
		321
	Appendix A: Digital Cash Patents	321
		341
	Appendix B: Internet Sources	341
	Commercial Providers WWW Pages	341
	Other Important Sources	342
	Places to Buy	342
		345
	Bibliography	345
		355
	Index	355