

Actu'
Web

3^e édition

Darknet

Mythes et réalités

Jean-Philippe Rennard



Table des matières

Préface à la troisième édition	7
Préface à la seconde édition	9
Introduction	13
I Fondations	17
1 Des darknets au Darknet	19
1 Web et deep web	21
2 Internet et réseaux pair-à-pair	25
3 Des darknets au Darknet	30
2 Cryptographie	33
1 Une histoire ancienne	33
2 La cryptographie moderne	38
2.1 Cryptographie à clé secrète	40
2.2 Cryptographie à clé publique	42
3 Pretty Good Privacy	45
4 Les États et la cryptographie	47
4.1 Cypherpunk	51
4.2 Les Crypto Wars sont plus intenses que jamais	54
II Outils	63
3 Les outils du Darknet	65
1 Open source et GNU/Linux	65
2 Premiers pas	70
2.1 Les Proxies web	70
2.2 Les VPN	71
3 Au cœur du Darknet	72

Table des matières

3.1	Les Mixnets	72
3.2	Tor	77
	Comment accéder au réseau Tor ?	78
	Comment fonctionne le réseau Tor ?	81
	Tor est-il sûr ?	85
3.3	Freenet/Hyphanet	89
	Comment accéder à Hyphanet ?	90
	Comment fonctionne Hyphanet ?	91
3.4	I2P	94
	Comment accéder à I2P ?	95
	Comment fonctionne I2P ?	96
4	Au-delà des classiques	97
4.1	GNUnet	97
4.2	Retroshare	97
5	Messagerie électronique	98
5.1	Les boîtes mails anonymes	99
5.2	Les services d'e-mails sécurisés	100
5.3	OpenPGP	102
	OpenPGP : confidentialité et anonymat	102
5.4	La messagerie instantanée	103
5.5	Les appareils mobiles	105
6	Demain ?	108
4	Les cryptomonnaies	111
1	D'où viennent les cryptomonnaies ?	112
1.1	Origines	112
1.2	Les cypherpunks et la cryptomonnaie	112
	Hashcash	114
	b-money	114
	Bit gold	115
2	Les Bitcoins	116
2.1	Comment se procurer des Bitcoins ?	117
	Les portefeuilles web	117
	Les portefeuilles locaux	119
	Les autres formes de portefeuilles	121
	Comment acheter des Bitcoins ?	122
2.2	Comment payer avec des Bitcoins ?	124
	Le suivi des transactions	125
	Frais de transaction	125
3	Comment fonctionnent les Bitcoins ?	126
3.1	Hachage	127

3.2	Portefeuilles et adresses	128
3.3	Transactions	129
	Sortie	129
	Entrée	129
3.4	La blockchain	131
	Réseau et consensus	132
	Blocs	133
	Preuves de travail	133
4	Un système qui doit encore gagner en maturité	138
4.1	Minage et consommation d'énergie	138
4.2	Le problème du passage à l'échelle	140
5	Bitcoins et anonymat	141
6	Les cryptomonnaies « anonymes »	144
6.1	PrivateSend	145
6.2	Autres extensions permises par l'existence de masternodes	146
7	Au-delà du réseau bitcoins	147
7.1	Vers une blockchain soutenable ?	147
7.2	Le réseau Lightning	149
8	Blockchains, confidentialité, anonymat et censure	151
8.1	Messageries	153
8.2	Gestion des données personnelles (Decentralized Identity)	154
8.3	VPN et réseaux pairs à pairs	154
8.4	Systèmes de stockage décentralisés	155
III	Usages	157
5	Noirceurs	159
1	Marchés noirs	159
1.1	La fin d'une impunité fantasmée ?	166
2	Politique et complotisme	170
3	Noirceurs	173
4	Un contenu diversifié	176
6	Darknet et libertés	181
1	Surveillance de masse	182
1.1	L'affaire Snowden	182
1.2	Surveillance de masse et démocratie	186
2	Droit d'alerte	195
2.1	WikiLeaks	195
2.2	Les émules	199
3	Censure et dissidences	201

Table des matières

3.1	Dissidences	201
3.2	Censure	206
3.3	Liberté d'information	210
IV	Annexes	215
A	Se protéger sur Internet	217
1	Les bases	220
1.1	Système d'exploitation	220
1.2	Mots de passe	221
1.3	Suppression des données	222
1.4	Cryptographie	223
1.5	MAC Spoofing	223
2	La navigation	224
2.1	Cookies	224
2.2	Moteurs de recherche	225
3	Les échanges	227
3.1	E-mails	227
3.2	Métadonnées	227
4	Connexions	227
4.1	Hotspots Wi-Fi	227
4.2	DNS	228
4.3	VPN	228
5	Cloud	229
B	Glossaire	231
	Bibliographie	239
	Table des encadrés	252
	Table des figures	253
	Table des matières	257
	Crédits	261
	Index	262