

Índice

Capítulo I

La revolución de las criptodivisas como los nuevos medios de pago..... 11

1. Introducción.....	11
2. Historia de las criptodivisas	12
Proyectos basados en Bitcoin.....	14
Otras implementaciones.....	15
3. Nivel de implantación de las criptodivisas	16
¿Qué opinan los países al respecto?	18
Pero entonces, ¿en dónde podría efectuar pagos con bitcoins?	18
4. Cómo hemos planteado el libro.....	20

Capítulo II

Conceptos teóricos sobre Bitcoin.....23

1. Contexto tecnológico	23
2. Un gran problema atajado poco a poco.....	24
Los generales bizantinos y la solución propuesta por Bitcoin	25
3. Conceptos criptográficos generales.....	27
Por qué la criptografía simétrica no es suficiente.....	27
El soporte de la criptografía asimétrica a las criptodivisas.....	28
4. La generación de direcciones y claves privadas	31
La codificación: Base58Check.....	31
La aplicación real	35
Generación de direcciones y claves privadas.....	36
El formato WIF	38
5. Las transacciones.....	40
6. El concepto de prueba de trabajo	46
La prueba de trabajo para prevenir el envío de spam.....	49



7. Bloques, minería y proof of work en Bitcoin	51
El sentido de la prueba de trabajo de Bitcoin.....	52
La implementación del proof of work en Bitcoin	53
¿Por qué ceder tiempo de procesamiento?	53
La carrera por crear la cadena de bloques más larga.....	56
Los pools de minería: la explotación eficiente de una materia prima escasa.....	57
Cadenas de bloques experimentales.....	59
8. Conceptos a retener.....	60

Capítulo III

Empezando a manejar nuestros bitcoins63

1. Consideraciones a la hora de elegir tu primera cartera	63
Carteras en local.....	63
Carteras en la nube	79
Almacenamiento en frío.....	80
Carteras mentales, unas carteras particulares.....	84
2. Sé cómo almacenarlos pero... ¿Cómo los consigo?	88
Minería	88
Faucets y programas de Pay To Click	89
Compraventa	91
3. Otros usos avanzados	96
Las direcciones multifirma.....	97
Ofreciendo servicios a cambio de bitcoins.....	100
4. ¿Dónde está mi backup?	110
5. Conceptos a retener.....	112

Capítulo IV

El proceso de investigación ante la presencia de criptodivisas 113

1. Usos con fines delictivos de las criptodivisas.....	113
2. Por dónde empezar cuando tenemos acceso al equipo.....	115
3. Identificando el uso de monederos	121
4. Investigando sin monederos	123
Cómo consultar blockchain.info	123
Desplegando nuestro propio explorador de la cadena de bloques	128
5. Conceptos a retener.....	132



Capítulo V

Explotando Elasticsearch para las criptodivisas	135
1. La pila ELK	135
2. Recuperación de información: Logstash.....	136
Funcionamiento básico de Logstash	136
Trabajo con logs y el poder de <code>grok{}</code>	139
Otros plugins de Logstash.....	143
3. Indexando información con Elasticsearch.....	144
Preparación de Elasticsearch	145
Ejemplo básico de inserción en Elasticsearch.....	145
4. Trabajando la información con Kibana	146
Explorando la información.....	147
Visualización de información usando gráficos.....	149
Dashboarding	150
5. Monitorizando el precio de las criptodivisas	151
Eliminando información de prueba.....	151
API de <code>coinmarketcap.com</code>	152
Recopilación de información	153
Monitorizando el precio de las criptodivisas	156
Otras ideas de proyectos.....	157
6. Conceptos a retener.....	158

Capítulo VI

Más allá de Bitcoin.....	159
1. La creación de criptodivisas alternativas	159
La vía rápida.....	160
Multichain y las cadenas de bloques privadas	163
2. Otros usos de la filosofía de Bitcoin	173
Namecoin	173
Colored coins y la cadena de bloques de Bitcoin.....	177
Ethereum y los smart contracts	184
Bitmessage	189
3. Conceptos a retener.....	194

Capítulo VII

Los próximos pasos	197
---------------------------------	------------



1. Hacia una economía libertaria	197
2. El concepto de cadena de bloques	199
3. El riesgo de centralización de la cadena de bloques.....	199
La minería y la capacidad de cómputo.....	200
El almacenamiento de información como metadatos.....	201
4. Lo que nos espera... ..	203
 Anexos	 205
Anexo A: Preparación del entorno de laboratorio.....	205
Sistema operativo	205
Software adicional.....	205
Descarga de los scripts del repositorio.....	206
Anexo B: Relación de proyectos mencionados de software libre vinculados a las criptodivisas	206
 Referencias.....	 209
 Índice alfabético	 221
 Índice de imágenes y tablas	 225