

Índice

Prólogo por Leif Ferreira, CEO de Bit2Me	13
Capítulo I	
Introducción a la web3	17
1. Desde la web0 a web3.....	17
2. La web 1.0	18
3. La web 2.0	19
4. La web 3.0	19
Descentralización y Blockchain.....	21
Ciberseguridad en la web3	23
Perfiles en el mundo web3	24
SmartContract	27
Wallet	30
DApp.....	31
Gas.....	34
Token.....	35
NFT	36
5. Tokenomics y una breve historia.....	45
6. Resumiendo: La visión Web3 y conceptos	49
Capítulo II	
La evolución de la Blockchain: Ethereum	55
1. Evolución de la blockchain: Desde payments a data	55
2. ¿Qué es Ethereum?	57
Ethereum Virtual Machine (EVM).....	58
¿Smart Contracts?	60
Solidity no es un lenguaje de alto nivel	62
Se compila a bytecode.....	62

Application Binary Interface (ABI)	63
Programar Smart Contracts es programar API REST	64
3. Multichain	65
¿Por qué?	65
Ecosistema y Comunidad (y capital).....	67
Ventajas y desafíos	68
 Capítulo III	
Desarrollo de Smart Contracts	71
1. Introducción al desarrollo de Smart Contracts.....	71
2. Remix IDE.....	74
Interfaz gráfica de Remix	74
3. Desarrollo de Smart Contracts en Solidity	82
Estructura de los proyectos en Solidity	82
Estructura básica de un contrato	83
Tipos de datos y variables	84
Tipos de memoria.....	85
Funciones y eventos	87
Manejo de fondos y datos	90
Control de flujo de la lógica	93
Transacciones entre contratos	96
Modificadores custom	99
Gas.....	102
Herencia y composición.....	104
4. Reto: Desarrollo de un Smart Contract ENS	106
¿Cómo funciona?	107
 Capítulo IV	
Profundizando en la infraestructura Web3.....	115
1. Dapp.....	115
Almacenamiento descentralizado y “off-chain”	117
IPS (Inter Planetary File System).....	118
Infraestructura web3.....	121
Nodos	123
RPCs.....	125
Proveedores de Servicio.....	126
Gasless.....	127

2. Desarrollo de Smart Contracts avanzado	128
Tokens Fungibles (como el ERC-20).....	128
Tokens No Fungibles (como ERC-721).....	129
3. Conceptos avanzados del desarrollo web3	131
Method calling	131
Función fallback.....	134
Multichain	134
Optimizaciones de gas: Gasless	137
Proxies.....	140
Idea General	141
Cómo funciona.....	142
Implementación en Solidity	143
Vulnerabilidad y funcionamiento del proxy.....	144
Problemas y descentralización	146
Tipos de implementación de Proxies	147
Diamond Pattern	148
Transparent proxy pattern.....	149
UUPS proxy pattern.....	150
Minimal Proxy Contract	151

Capítulo V

Vulnerabilidades.....156

1. Vulnerabilidades	156
Re-Entrancy.....	156
Ejemplo: Re-Entrancy en código	158
Mitigación	159
Integer Overflow	160
Ejemplo: Integer Overflow en código	160
Mitigación	161
TX.Origin	161
Ejemplo: tx.origin en código.....	163
Mitigación	164
Fallos en el control de acceso.....	164
Ejemplo: fallo en el control de acceso en código.....	165
Mitigación	166
Funciones ‘Legacy’	166
Ejemplo: malos tips.....	167
DoS a la lógica	168
Mitigación	170

Unprotected suicide o selfdestruct	170
Ejemplo: delegatecall en código	171
Mitigación	172
Signature Replay Attack.....	172
Ejemplo: Signature Replay Attack en código	174
Mitigación	175

Capítulo VI

Security Guidelines en SmartContracts.....	176
1. Malas prácticas.....	176
2. Buenas prácticas.....	179

Capítulo VII

Making lab: Pentesting en Web3	188
1. ‘making’ lab	188
2. Metodología.....	189
Pruebas en la blockchain.....	190
Pruebas en DApp.....	190
EIP-1470 o SWC.....	191
SCSVS.....	192
3. Herramientas y ‘distros’	194
4. Visualización de información y datos	197
Etherscan	197
Surya	200
5. Análisis estático.....	204
Slither	204
Remix SSA.....	209
6. Decompiladores	210
Etherevm	211
7. Ejecución simbólica.....	213
Mythril.....	213
8. Fuzzing	217
Echidna.....	218
Property testing.....	218
9. Plataforma CTF: level_up!.....	223
Cómo funciona el juego: Reto Interact	225

Reto Ownership.....	228
Jugando a la Re-Lottery	230
Hack to Snippet Delegated.....	234
Consiguiendo NFT para demostrar el nivel	238
Reto NavajaNegra 2022	240
Fichero: contract-address.json.....	242

