Apéndice A

Resultado del proceso de extracción de datos: Parsifal

En el siguiente apéndice se encuentran las tablas generadas tras el proceso de extracción de datos. Dado el número de artículos revisados ha sido necesario dividir cada una de las tablas en dos partes, de forma que la información se mostrase adecuadamente en el formato de este documento.

En el primer par de tablas encontramos encontramos el objetivo de investigación de los diferentes artículos revisados, desde la perspectiva de la detección de fraude (tablas A.1 y A.2).

En el segundo, las definiciones del concepto de fraude dadas en cada uno de los artículos revisados (tablas A.3 y A.4).

En el tercer par de tablas se observan las técnicas de Machine Learning estudiadas por cada uno de los artículos, así como la técnica finalmente seleccionada por su rendimiento (tablas A.5 y A.6).

Para finalizar, en el último par de tablas encontramos las características más relevantes asociadas con la técnica seleccionada y su rendimiento (tablas A.7 y A.8).

Ref.	Study objective regarding fraud detection
[46]	Study the models, the datasets, and the underlying technology, thus identifying the existing gaps and proposing improvement ideas that can detect scams early.
[78]	Recognition of transactions used for cover communication
[48]	Detect illicit transactions for anti-money laundering
[74]	Summarization of the existing public blockchain and consortium blockchain abnormal behavior awareness methods
[10]	To address the sampling risk and financial audit inefficiency in ledger business operations
[6]	Address the problems of fraud and anomalies in the Bitcoin network, which are common problems in e-banking and online transactions.
[9]	Detect Bitcoin Generator Scams pages and prevent people from being victimised
[63]	To use the Blockchain technology to present a new method for detecting anomalies in Bitcoin with more appropriate efficiency
[72]	To detect phishing scams on Ethereum by mining its transaction records
[5]	Investigate the applicability of deep learning and machine learning techniques for anti-money laundering in cryptocurrency
[38]	An in-depth evaluation of ensemble learning methodologies for anomaly detection in the blockchain network ecosystem
[58]	Proposition of a blockchain and smart contract-based approach to achieve robust Machine Learning algorithm for e-commerce fraud detection by facilitating inter-organizational collaboration
[42]	Make a comprehensive review that studies the applicability of IDS (Intrusion Detection System) in detecting Ethereum-based attacks
[49]	Propose a blockchain-based click fraud detection and prevention scheme for online advertising is proposed to deal with advertisement click fraud
[36]	Propose a method to detect Ponzi scheme contracts on Ethereum-CTRF (Code and TransactionRandom Forest)
[19]	Propose a Ponzi scheme contract detection method called MTCformer (Multi-channel Text Convolutional Neural Networks and Transofrmer)
[64]	Propose a detection model for detecting Ponzi schemes in smart contracts using bytecode

Tabla A.1: Tabla con los resultados del objetivo investigador de las referencias bibliográficas estudiadas, con un enfoque basado en la detección de fraude (parte 1 de 2)

Ref.	Study objective regarding fraud detection
[11]	Propose an image-based scam detection method using an attention capsule network (SE-CapsNet) focused on Ethereum
[52]	Investigate the untrusted users of cryptocurrency transaction services, and propose a methodology to identify suspicious users based on their reputation score
[29]	To detect illicit accounts based on their transaction history using the XGBoost classifier
[61]	Survey the application of artificial intelligence techniques to address these challenges for cryptocurrencies with their vast amount of daily transactions, trades and news that are beyond human capabilities to analyze and learn from
[18]	Collects real-world samples and proposes an approach to detect Ponzi schemes implemented as smart contracts on the blockchain
[59]	Conduct an intensive study that explores key security concerns, detailing existing threats and weaknesses of the Bitcoin system and its main technologies including the blockchain protocol
[77]	Introduce a detection method for Ponzi schemes, base on the SMOTEENN algorithm for solving data imbalance.
[70]	Propose a new methodology (ContractWard) to detect vulnerabilities in smart contracts with machine learning techniques
[4]	Propose a data-driven robust method for detecting abnormal contract accounts over the Ethereum Blockchain
[57]	Propose a machine learning-based method, which introduces automated signing of blockchain transactions, while including also a personalized identification of anomalous transactions
[73]	Introduce a novel machine learning-based analysis model by introducing the shared child nodes for smart contract vulnerabilities
[45]	classify the DDoS detection techniques according to blockchain technology
[43]	Proposes a detection mechanism called Ethereum Phishing Scam Detection (Eth-PSD) that attempts to detect phishing scam-related transactions using a novel machine learning-based approach
[47]	Analyze Ethereum token transactions, characterize key economic agents' behavior from their transaction patterns, and explore their identifiability through interpretable machine learning models
[2]	Provide a methodology to predict classification of accounts as malicious or benign
[3]	Propose a new framework called BChainGuard for cyberthreat detection in blockchain
[33]	Proposed a machine-learning–blockchain-based smart-contract system that improves security, reduces consumption, and can be trusted for real-time medical applications

Tabla A.2: Tabla con los resultados del objetivo investigador de las referencias bibliográficas estudiadas, con un enfoque basado en la detección de fraude (parte 2 de 2)

Ref.	Study definition of fraud for the presented use case
[46]	Ponzi schemes, money laundering, Pump and Dump, cryptojacking, phishing, fake wallets/accounts, exchange scams, HYIP, ransomware, DDoS attack
[78]	N/A
[48]	Money-laundring actions.
[74]	Suspicious account behaviour, node pattern behaviour, identity interference, ponzi schemes, money laundering
[10]	VAT-compliance violations, incorrect bookkeeping rules patterns, fraudulent financial statements, generic deviations from the norms and other errors.
[6]	Fraudulent transactions, based on unusual patterns that do not conform to expected behavior.
[9]	Scam people base on a HYIP (High Yield Investment Program) called "Bitcoin Generator"
[63]	Abnormal and fraudulent behaviors
[72]	A hotbed of various cybercrimes, specially phishing scams
[5]	Money laundering activities
[38]	suspicious activity, cybercrime, phishing and Ponzi Schemes (HYIP)
[58]	N/A
[42]	Exploiting of different Ethereum vulnerabilities, ciberattacks or suspicious transactions
[49]	suspicious or illicit clicks on advertisements
[36]	Ponzi schemes
[19]	Ponzi schemes
[64]	Ponzi schemes

Tabla A.3: Tabla con los resultados de la definición de fraude utilizada en las referencias bibliográficas estudiadas (parte 1 de 2)

Ref.	Study definition of fraud for the presented use case
[11]	Ponzi schemes
[52]	Untrusted users generating transactions, or hacked accounts acting on behalf of their owners
[29]	Money laundering, bribery, phishing
[61]	money laundering, Ponzi schemes, fake ICOs, pump-and-pump schemes
[18]	Ponzi schemes
[59]	Exploited threats and weaknesses of the Bitcoin system2
[77]	Ponzi schemes
[70]	Vulnerability exploitations in smart contracts
[4]	Abnormal schemes to hide behind smart contracts
[57]	Abnormal or anomalous transactions
[73]	Exploiting of smart contracts vulnerabilities
[45]	Exploiting DDoS attacks and IoT devices-hijacking
[43]	phishing scam-related transactions
[47]	suspicious/abnormal/outlier agent-behaviour
[2]	malicious accounts operations
[3]	Exploiting blockchain and smart contract vulnerabilities
[33]	Unauthenticated operations on medical applications

Tabla A.4: Tabla con los resultados de la definición de fraude utilizada en las referencias bibliográficas estudiadas (parte 2 de 2)

	Machine Learning technique studied																			
Ref.	ANN	AB	AE	BAG	CNN	DNN	DT	GNN	IF	J48	LR	NB	NN	PAC	RF	SGD	SNN	SVM	XGB	KM	KNN
[46]		X		X			X	X	X	X	X	X			**X**	X		X	X		X
[78]					**X**																
[48]								**X**													
[74]						**X**		X					X						X	X	
[10]	X		X				X		X		X	X			**X**			X			X
[6]															**X**				X		
[9]	**X**											X			X			X			X
[63]																				**X**	
[72]									X		X	X						**X**			
[5]						X									**X**						X
[38]	X	X		X					X		X	X			X			X	**X**		X
[58]	X											X		**X**		X					
[42]	X	X	X				X	X		X					X	X		X	X		X
[49]	X			**X**														X	X		X
[36]					X		X								**X**			X	X		X
[19]	X				**X**										X			X			
[64]									**X**						X			X	X		

Tabla A.5: Tabla con los resultados de los diferentes usos de técnicas de Machine Learning en las referencias bibliográficas estudiadas. Método con mejor rendimiento con fondo sombreado (parte 1 de 2)

	Machine Learning technique studied																				
Ref.	ANN	AB	AE	BAG	CNN	DNN	DT	GNN	IF	J48	LR	NB	NN	PAC	RF	SGD	SNN	SVM	XGB	KM	KNN
[11]	X	X			X										X				X		
[52]							X					X	X					X			
[29]																			X		
[61]	X	X		X	X	X				X	X	X	X		X			X	X	X	X
[18]							X		X						X			X	X		
[59]																				X	
[77]					X										X						
[70]		X													X			X	X		X
[4]		X		X			X								X				X		
[57]	X								X						X						
[73]																X					X
[45]	X	X													X			X	X		X
[43]							X			X		X									X
[47]	X										X				X			X			
[2]															X			X	X	X	
[3]	X										X				X			X			X
[33]																		X			

Tabla A.6: Tabla con los resultados de los diferentes usos de técnicas de Machine Learning en las referencias bibliográficas estudiadas. Método con mejor rendimiento con fondo sombreado (parte 2 de 2)

Ref.	Year	Preemptive/Counteracting	Selected ML technique	F-Score	Supervised/Unsupervised
[46]	2023	Preemptive solution	RF - Random Forest	99.51	Supervised
[78]	2023	Counteracting solution	CNN - Convolutional Neural Network	99.282	Supervised
[48]	2022	Counteracting solution	GNN - Graph Neural Network	91.6	Unsupervised
[74]	2022	Counteracting solution	DNN - Deep Neural Network	99.6	Supervised
[10]	2022	Counteracting solution	RF - Random Forest	99.25	Supervised
[6]	2022	Counteracting solution	RF - Random Forest	92.0	Supervised
[9]	2022	Preemptive solution	ANN - Artificial Neural Network	99.0	Supervised
[63]	2022	Counteracting solution	k-means - k-means clustering	N/A	Supervised
[72]	2020	Preemptive solution	SVM - Support Vector Machine	90.8	Supervised
[5]	2022	Counteracting solution	RF - Random Forest	99.0	Supervised
[38]	2022	N/A	XGBoost - Gradient Boosting	N/A	Supervised
[58]	2022	Preemptive solution	PAC - Passive-Aggresive Classifier	98.22	Unsupervised
[42]	2022	Counteracting solution	N/A	N/A	N/A
[49]	2022	Preemptive solution	Bagging - Bootstrap Aggregating	96.29	Unsupervised
[36]	2022	Preemptive solution	RF - Random Forest	90.9	Supervised
[19]	2021	Preemptive solution	CNN - Convolutional Neural Network	89.0	Supervised
[64]	2021	Preemptive solution	IF - Isolation Forest	88.0	Supervised

Tabla A.7: Tabla con los resultados de las características más relevantes de las referencias bibliográficas estudiadas (parte 1 de 2)

Ref.	Year	Preemptive/Counteracting	Selected ML technique	F-Score	Supervised/Unsupervised
[11]	2021	Preemptive solution	CNN - Convolutional Neural Network	94.44	Supervised
[52]	2021	Counteracting solution	NB - Naive Bayes	97.0	Supervised
[29]	2020	Counteracting solution	XGBoost - Gradient Boosting	99.4	Supervised
[61]	2020	Counteracting solution	N/A	N/A	N/A
[18]	2019	Preemptive solution	RF - Random Forest	79.0	Supervised
[59]	2018	N/A	N/A	N/A	N/A
[77]	2022	Preemptive solution	CNN - Convolutional Neural Network	98.0	Supervised
[70]	2020	Preemptive solution	XGBoost - Gradient Boosting	96.18	Supervised
[4]	2022	Preemptive solution	N/A	89.67	Supervised
[57]	2019	Preemptive solution	IF - Isolation Forest	N/A	Unsupervised
[73]	2021	Preemptive solution	kNN - k-Nearest Neighbours	92.87	Supervised
[45]	2022	Preemptive solution	N/A	N/A	N/A
[43]	2022	Preemptive solution	kNN - k-Nearest Neighbours	98.11	Supervised
[47]	2021	Preemptive solution	RF - Random Forest	86.5	Supervised
[2]	2021	Preemptive solution	RF - Random Forest	87.95	Supervised
[3]	2022	Preemptive solution	RF - Random Forest	98.8	Supervised
[33]	2022	Preemptive solution	N/A	N/A	N/A

Tabla A.8: Tabla con los resultados de las características más relevantes de las referencias bibliográficas estudiadas (parte 2 de 2)

Bibliografía

[1] J Abreu. «Hipótesis, método & diseño de investigación (hypothesis, method & research design)». En: *Daena: International Journal of Good Conscience* 7.2 (2012), págs. 187-197.

[2] Rachit Agarwal, Shikhar Barve y Sandeep Kumar Shukla. «Detecting malicious accounts in permissionless blockchains using temporal graph properties». En: *Applied Network Science* 6.1 (2021), págs. 1-30.

[3] Suliman Aladhadh et al. «BChainGuard: A New Framework for Cyberthreats Detection in Blockchain Using Machine Learning». En: *Applied Sciences* 12.23 (2022), pág. 12026.

[4] Ali Aljofey et al. «A Feature-Based Robust Method for Abnormal Contracts Detection in Ethereum Blockchain». En: *Electronics* 11.18 (2022), pág. 2937.

[5] Johrha Alotibi et al. «Money Laundering Detection using Machine Learning and Deep Learning». En: *International Journal of Advanced Computer Science and Applications* 13.10 (2022).

[6] Tehreem Ashfaq et al. «A Machine Learning and Blockchain Based Efficient Fraud Detection Mechanism». En: *Sensors* 22.19 (2022), pág. 7162.

[7] *Ataque de día cero*. 2023. URL: `https://es.wikipedia.org/wiki/Ataque_de_d%C3%ADa_cero` (visitado 27-05-2023).

[8] *Auth0: An Introduction to Ethereum and Smart Contracts*. 2023. URL: `https://auth0.com/blog/an-introduction-to-ethereum-and-smart-contracts-part-2/` (visitado 22-03-2023).

[9] Emad Badawi, Guy-Vincent Jourdan y Iosif-Viorel Onut. «The "Bitcoin Generator" Scam». En: *Blockchain: Research and Applications* 3.3 (2022), pág. 100084.

[10] Alexander Bakumenko y Ahmed Elragal. «Detecting anomalies in financial data using machine learning algorithms». En: *Systems* 10.5 (2022), pág. 130.

[11] Lingyu Bian et al. «Image-based scam detection method using an attention capsule network». En: *IEEE Access* 9 (2021), págs. 33654-33665.

[12] *BibText.org: Your BibTeX resource.* 2023. URL: http://www.bibtex.org (visitado 30-04-2023).

[13] *Bitnode: Bitcoin propagation time.* 2023. URL: https://bitnodes.io/dashboard/#blocks-propagation-time (visitado 25-04-2023).

[14] *Blockchain Developer: Introduction.* 2023. URL: https://developer.bitcoin.org/devguide/block_chain.html (visitado 22-03-2023).

[15] *Boletin Oficial del Estado: miércoles 5 de abril de 2023, Núm. 81.* 2023. URL: https://www.boe.es/boe/dias/2023/04/05/ (visitado 29-04-2023).

[16] Amiangshu Bosu et al. «Understanding the motivations, challenges and needs of blockchain software developers: A survey». En: *Empirical Software Engineering* 24.4 (2019), págs. 2636-2673.

[17] *Business Blockchain HQ: Blockchain Fundamentals.* 2023. URL: https://businessblockchainhq.com/blockchain-fundamentals/ (visitado 19-03-2023).

[18] Weili Chen et al. «Exploiting blockchain data to detect smart ponzi schemes on ethereum». En: *IEEE Access* 7 (2019), págs. 37575-37586.

[19] Yizhou Chen et al. «Improving Ponzi scheme contract detection using multichannel TextCNN and transformer». En: *Sensors* 21.19 (2021), pág. 6417.

[20] People's Bank of China. *Progress of Research & Development of E-CNY in China.* 2021.

[21] *CoinMarketCap: Global Cryptocurrency Charts.* 2023. URL: https://coinmarketcap.com/charts/ (visitado 29-04-2023).

[22] *Comisión Federal de Comercio - USA: Lo que hay que saber sobre las criptomonedas y las estafas.* 2023. URL: https://consumidor.ftc.gov/articulos/lo-que-hay-que-saber-sobre-las-criptomonedas-y-las-estafas (visitado 19-03-2023).

[23] *El Pais: China prohibe toda la actividad vinculada a las criptomonedas.* 2023. URL: https://elpais.com/economia/2021-09-24/china-prohibe-toda-la-actividad-vinculada-a-las-criptomonedas.html (visitado 25-03-2023).

[24] Abeer ElBahrawy et al. «Evolutionary dynamics of the cryptocurrency market». En: *Royal Society open science* 4.11 (2017), pág. 170623.

[25] Meryam Essaid, Sejin Park y Hong-Taek Ju. «Bitcoin's dynamic peer-to-peer topology». En: *International Journal of Network Management* 30.5 (2020), e2106.

[26] *European Parliament: Legislative Observatory 2021/0241(COD).* 2023. URL: https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2021/0241(COD)&l=en (visitado 29-04-2023).

[27] *Expansión: PIB España.* 2023. URL: https://datosmacro.expansion.com/pib/espana (visitado 24-03-2023).

[28] *Expansión: PIB Estados Unidos.* 2023. URL: https://datosmacro.expansion.com/pib/usa (visitado 24-03-2023).

[29] Steven Farrugia, Joshua Ellul y George Azzopardi. «Detection of illicit accounts over the Ethereum blockchain». En: *Expert Systems with Applications* 150 (2020), pág. 113318.

[30] *Finantials Times: What is tokenisation really?* 2023. URL: https://www.ft.com/content/ba6a1e4c-db2e-340e-9ed1-9bdc4fe654b6 (visitado 19-03-2023).

[31] *Funcas: Bitcoin en El Salvador, un año después.* 2023. URL: https://www.funcas.es/odf/bitcoin-en-el-salvador-un-ano-despues/#:~:text=En%5C%20septiembre%5C%20de%5C%202021%5C%2C%5C%20El,balance%5C%20no%5C%20parece%5C%20ser%5C%20favorable. (visitado 25-03-2023).

[32] Rosa M Garcia-Teruel y Héctor Simón-Moreno. «The digital tokenization of property rights. A comparative perspective». En: *Computer Law & Security Review* 41 (2021), pág. 105543.

[33] Rajkumar Gaur et al. «A Machine-Learning–Blockchain-Based Authentication Using Smart Contracts for an IoHT System». En: *Sensors* 22.23 (2022), pág. 9074.

[34] *Geekflare: Una guía detallada sobre los tipos de nodos de cadena de bloques.* 2022. URL: https://geekflare.com/es/blockchain-nodes-guide/ (visitado 19-03-2023).

[35] Maricelly Gómez Vargas, Catalina Galeano Higuita y Dumar Andrey Jaramillo Muñoz. «El estado del arte: una metodologıa de investigación». En: (2015).

[36] Xuezhi He, Tan Yang y Liping Chen. «CTRF: Ethereum-Based Ponzi Contract Identification». En: *Security and Communication Networks* 2022 (2022).

[37] *High-Yield Investment Program (HYIP): Definition and Fraudulence.* 2023. URL: https://www.investopedia.com/terms/h/high-yield-investment-program.asp (visitado 26-05-2023).

[38] Sabri Hisham, Mokhairi Makhtar y Azwa Abdul Aziz. «Combining Multiple Classifiers using Ensemble Method for Anomaly Detection in Blockchain Networks: A Comprehensive Review». En: *International Journal of Advanced Computer Science and Applications* 13.8 (2022).

[39] Yang Hu, Harold Glenn A Valera y Les Oxley. «Market efficiency of the top market-cap cryptocurrencies: Further evidence from a panel framework». En: *Finance Research Letters* 31 (2019), págs. 138-145.

[40] *IBM: Machine Learning.* 2023. URL: `https://www.ibm.com/mx-es/analytics/machine-learning` (visitado 18-03-2023).

[41] *IBM: Tecnología Blockchain.* 2023. URL: `https://www.ibm.com/es-es/topics/blockchain` (visitado 18-03-2023).

[42] Arkan Hammoodi Hasan Kabla et al. «Applicability of intrusion detection system on Ethereum attacks: a comprehensive review». En: *IEEE Access* (2022).

[43] Arkan Hammoodi Hasan Kabla et al. «Eth-PSD: A Machine Learning-Based Phishing Scam Detection Approach in Ethereum». En: *IEEE Access* 10 (2022), págs. 118043-118057.

[44] S Keerthana y Suvanam Sasidhar Babu. «Ensuring Cloud Storage Security in Multi-Keyword Search for Multiple Data Owners and Users». En: (2018).

[45] Zulfiqar Ali Khan y Akbar Siami Namin. «A Survey of DDOS Attack Detection Techniques for IoT Systems Using BlockChain Technology». En: *Electronics* 11.23 (2022), pág. 3892.

[46] Lakshmi Priya Krishnan et al. «Scams and Solutions in Cryptocurrencies—A Survey Analyzing Existing Machine Learning Models». En: *Information* 14.3 (2023), pág. 171.

[47] Xiao Fan Liu et al. «Characterizing key agents in the cryptocurrency economy through blockchain transaction analysis». En: *EPJ Data Science* 10.1 (2021), pág. 21.

[48] Wai Weng Lo et al. «Inspection-L: self-supervised GNN node embeddings for money laundering detection in bitcoin». En: *Applied Intelligence* (2023), págs. 1-12.

[49] Qiuyun Lyu et al. «BCFDPS: A Blockchain-Based Click Fraud Detection and Prevention Scheme for Online Advertising». En: *Security and Communication Networks* 2022 (2022).

[50] Georgi Marinov. «Panel Non-Stationarity Methods in Macro-and Microeconomic Studies». En: *Bridging Microeconomics and Macroeconomics and the Effects on Economic Development and Growth.* IGI Global, 2021, págs. 79-102.

[51] Monia Milutinović et al. «Cryptocurrency». En: - 1 (2018), págs. 105-122.

[52] Ruchi Mittal y Mahinder Pal Singh Bhatia. «Detection of Suspicious or Un-Trusted Users in Crypto-Currency Financial Trading Applications». En: *International Journal of Digital Crime and Forensics (IJDCF)* 13.1 (2021), págs. 79-93.

[53] Satoshi Nakamoto. «Bitcoin: A peer-to-peer electronic cash system». En: *Decentralized business review* (2008), pág. 21260.

[54] *Oracle: ¿Qué es big data?* 2023. URL: `https://www.oracle.com/es/big-data/what-is-big-data/` (visitado 18-03-2023).

[55] *Parsifal: About Parsifal.* 2023. URL: `https://parsif.al/about/` (visitado 29-04-2023).

[56] Cristina Pérez-Solà et al. «Another coin bites the dust: an analysis of dust in UTXO-based cryptocurrencies». En: *Royal Society open science* 6.1 (2019), pág. 180817.

[57] Blaž Podgorelec, Muhamed Turkanović y Sašo Karakatič. «A machine learning-based method for automated blockchain transaction signing including personalized anomaly detection». En: *Sensors* 20.1 (2019), pág. 147.

[58] Tahmid Hasan Pranto et al. «Blockchain and Machine Learning for Fraud Detection: A Privacy-Preserving and Adaptive Incentive Based Approach». En: *IEEE Access* 10 (2022), págs. 87115-87134.

[59] Mohamed Rahouti, Kaiqi Xiong y Nasir Ghani. «Bitcoin concepts, threats, and machine-learning security solutions». En: *Ieee Access* 6 (2018), págs. 67189-67205.

[60] *Ripio: ¿Qué es un token y cómo funciona?* 2023. URL: `https://launchpad.ripio.com/blog/que-es-un-token-y-como-funciona` (visitado 18-03-2023).

[61] Farida Sabry et al. «Cryptocurrencies and artificial intelligence: Challenges and opportunities». En: *IEEE Access* 8 (2020), págs. 175840-175858.

[62] Simanta Shekhar Sarmah. «Understanding blockchain technology». En: *Computer Science and Engineering* 8.2 (2018), págs. 23-29.

[63] Mohammad Javad Shayegan et al. «A collective anomaly detection technique to detect crypto wallet frauds on bitcoin network». En: *Symmetry* 14.2 (2022), pág. 328.

[64] Xiajiong Shen, Shuaimin Jiang y Lei Zhang. «Mining bytecode features of smart contracts to detect Ponzi scheme on blockchain». En: *Computer Modeling in Engineering & Sciences* 127.3 (2021), págs. 1069-1085.

[65] Harsh Sheth y Janvi Dattani. «Overview of blockchain technology». En: *Asian Journal For Convergence In Technology (AJCT) ISSN-2350-1146* (2019).

[66] Duarte Paulo Gonçalves Cabral Teles. «Data protection with Ethereum blockchain». Tesis doct. Instituto Politecnico do Porto (Portugal), 2018.

[67] Philip Treleaven, Richard Gendal Brown y Danny Yang. «Blockchain technology in finance». En: *Computer* 50.9 (2017), págs. 14-17.

[68] Rhyme Upadhyaya y Aruna Jain. «Cyber ethics and cyber crime: A deep dwelved study into legality, ransomware, underground web and bitcoin wallet». En: *2016 International Conference on Computing, Communication and Automation (ICCCA).* IEEE. 2016, págs. 143-148.

[69] Qin Wang et al. «Exploring web3 from the view of blockchain». En: *arXiv preprint arXiv:2206.08821* (2022).

[70] Wei Wang et al. «Contractward: Automated vulnerability detection models for ethereum smart contracts». En: *IEEE Transactions on Network Science and Engineering* 8.2 (2020), págs. 1133-1144.

[71] Mark Weber et al. «Anti-money laundering in bitcoin: Experimenting with graph convolutional networks for financial forensics». En: *arXiv preprint arXiv:1908.02591* (2019).

[72] Jiajing Wu et al. «Who are the phishers? phishing scam detection on ethereum via network embedding». En: *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 52.2 (2020), págs. 1156-1166.

[73] Yingjie Xu et al. «A novel machine learning-based analysis model for smart contract vulnerability». En: *Security and Communication Networks* 2021 (2021), págs. 1-12.

[74] Chuyi Yan et al. «Blockchain abnormal behavior awareness methods: a survey». En: *Cybersecurity* 5.1 (2022), pág. 5.

[75] Rui Zhang, Rui Xue y Ling Liu. «Security and privacy on blockchain». En: *ACM Computing Surveys (CSUR)* 52.3 (2019), págs. 1-34.

[76] Shijie Zhang y Jong-Hyouk Lee. «Analysis of the main consensus protocols of blockchain». En: *ICT express* 6.2 (2020), págs. 93-97.

[77] Shuhui Zhang et al. «Ethereum Ponzi Scheme Detection Based on PD-SECR». En: *Security and Communication Networks* 2022 (2022).

[78] Zijian Zhang et al. «A Multi-Dimensional Covert Transaction Recognition Scheme for Blockchain». En: *Mathematics* 11.4 (2023), pág. 1015.