DAFTAR PUSTAKA

Auer, D. (2019). *ICO whitepapers: A critical analysis. Journal of Blockchain Research.*

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. (2015). SoK: Research perspectives and challenges for Bitcoin and cryptocurrencies. In 2015 IEEE Symposium on Security and Privacy (pp. 104–121). IEEE. https://doi.org/10.1109/SP.2015.14

Buchanan, B., Smith, R., & Clark, D. (2025). ECDSA cracking methods. International Journal of Cybersecurity Research.

Chainalysis. (2024). The 2024 crypto crime report. Chainalysis. https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction/

Corbellini, A. (2020). Elliptic curve digital signature algorithm (ECDSA). https://andrea.corbellini.name/2020/11/18/ecdsa/

Federal Bureau of Investigation. (2024). FBI releases annual internet crime report. https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report

Gao, Y., Zhang, X., & Liu, H. (2024). Attacking ECDSA with nonce leakage by lattice sieving. Cryptology ePrint Archive.

Hankerson, D., Menezes, A., & Vanstone, S. (2004). Guide to elliptic curve cryptography. Springer.

Howell, S. T., Niessner, M., & Yermack, D. (2020). Initial coin offerings: Financing growth with cryptocurrency token sales. The Review of Financial Studies, 33(9), 3925–3974. https://doi.org/10.1093/rfs/hhz131

Huynh, P. D., Dau, S. H., Huppert, N., & Nguyen, G. T. (2024). Serial scammers and attack of the clones: How scammers coordinate multiple rug pulls on decentralized exchanges. arXiv. https://arxiv.org/abs/2412.10993

Johnson, D., Menezes, A., & Vanstone, S. (2001). The elliptic curve digital signature algorithm (ECDSA). International Journal of Information Security, 1(1), 36–63. https://doi.org/10.1007/s102070100002

Josh Kamps, & Bennett Kleinberg. (2018). To the moon: Defining and detecting cryptocurrency pump-and-dumps. Crime Science, 7(1), 18.

https://doi.org/10.1186/s40163-018-0093-5. Diakses dari Springer Journal Article

Kiltz, E., Masny, D., & Pan, J. (2023). *On the security of ECDSA with biased nonces. Journal of Cryptology.*

Lubis, Y., Rusydi, I., & Elyas, A. H. (2024). *Implementasi Algoritma Kriptografi Tanda Tangan Digital Qrcode Pada Dokumen Dengan Menggunakan Metode Riverst Shamir Adleman (RSA).* Jurnal Warta Dharmawangsa, 18(4), 1429–1439. https://doi.org/10.46576/wdw.v18i4.5247

Mikalef, P., dkk. (2024). Crypto-Cognitive Exploitation: Integrating Cognitive, Social, and Technological Perspectives on Cryptocurrency Fraud. Telematics and Informatics. https://doi.org/10.1016/j.tele.2024.102208

Momtaz, P. P. (2020). Initial coin offerings. PLOS ONE, 15(5), e0233018. https://doi.org/10.1371/journal.pone.0233018

Moriai, S. (2021). Digital signature and its applications in modern information systems. IEEE Communications Surveys & Tutorials.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf

Osaki, Y. (2024). Extended attacks on ECDSA with noisy multiple bit nonce leakages. Journal of Cryptographic Engineering.

Puthiyidam, J. J., Kumar, S., & Nair, R. (2024). Temporal ECDSA: A timestamp and signature mask enabled ECDSA algorithm for IoT client node authentication. IEEE Access.

Wong, K., Wang, Y., & Li, J. (2023). Real threshold ECDSA. IEEE Transactions on Information Forensics and Security.