

DOI: <https://doi.org/10.38035/rrj.v7i4><https://creativecommons.org/licenses/by/4.0/>

Modus Penipuan Investasi *Non-Fungible Token* (NFT) dalam *Blockchain* Solana

Monica Margaret¹, Mizu Athaya Yusuf²

¹Universitas Budi Luhur, Jakarta Selatan, Indonesia, monica.margaret@budiluhur.ac.id

²Universitas Budi Luhur, Jakarta Selatan, Indonesia

Corresponding Author: monica.margaret@budiluhur.ac.id¹

Abstract: *The focus of this research is to identify the factors that make investors victims of fraud in the context of NFT investments. The theoretical foundation used in this study is the Lifestyle Exposure Theory, which helps in understanding how investors' lifestyles influence their risk of being scammed. This research employs a qualitative approach with a case study method through interviews to gain an in-depth understanding of fraudulent patterns in NFT projects. Data analysis is conducted using a descriptive approach to thoroughly illustrate and explain the phenomenon, providing insights into the factors that make investors vulnerable to fraud in the context of NFT investments. Lack of self-control and minimal verification of information make investors more susceptible to fraudulent schemes. The habitual factors identified above demonstrate their role as victims in fraud schemes, a concept known as Participating Victims.*

Keyword: *Fraud, Victim, Lifestyle Exposure Theory, Non-Fungible Token, Solana Blockchain.*

Abstrak: Fokus penelitian ini adalah untuk mengidentifikasi faktor-faktor yang menjadikan investor sebagai korban penipuan dalam konteks investasi NFT. Landasan teori yang digunakan dalam penelitian ini adalah Teori Paparan Gaya Hidup (*Lifestyle Exposure Theory*), yang membantu dalam memahami bagaimana gaya hidup *investor* dapat mempengaruhi risiko penipuan yang mereka hadapi. Penelitian ini menggunakan pendekatan kualitatif dengan metode studi kasus melalui wawancara untuk mendapatkan pemahaman yang mendalam tentang pola penipuan yang terjadi dalam proyek NFT. Analisis data dilakukan dengan menggunakan pendekatan deskriptif sehingga dapat menggambarkan dan menjelaskan fenomena yang terjadi secara rinci dan mendalam, serta memberikan wawasan tentang faktor-faktor yang membuat investor rentan untuk menjadi korban penipuan dalam konteks investasi NFT. Kurangnya kontrol diri dan minimnya verifikasi informasi membuat investor lebih mudah terjebak dalam modus penipuan. Faktor-faktor kebiasaan yang telah dilakukan diatas menunjukkan peranan dirinya sebagai korban dalam modus penipuan atau yang dikenal dengan istilah *Participating Victims*

Kata Kunci: Penipuan, Viktim, Lifestyle Exposure Theory, *Non-fungible token*, Blockchain Solana

PENDAHULUAN

Pesatnya kemajuan jaringan internet telah memberikan manfaat yang relatif sangat besar dalam perkembangan teknologi, informasi serta komunikasi yang pada saat ini masih dan akan terus berkembang, serta berdampak pada kemajuan peradaban manusia modern. Kita menjadi sangat tergantung pada kelebihan dan kemudahan teknologi yang ditawarkan Teknologi online tidak hanya mempermudah aktivitas sehari-hari, tetapi juga dapat menjadi sumber penghasilan jika dimanfaatkan dengan bijak (Ngafifi, 2014). Salah satu perkembangan teknologi yang signifikan adalah mata uang kripto dan NFT (*Non-Fungible Token*), yang menjadi aset digital yang sedang berkembang pesat di dunia maya. Dalam beberapa waktu terakhir, semakin banyak masyarakat yang mulai mengenal dan menjadikan NFT sebagai sumber pendapatan, baik melalui perdagangan aset digital maupun pembuatan dan penjualan NFT. Kehadiran NFT telah mendorong banyak pengusaha untuk mengembangkan proyek NFT mereka sendiri dengan tujuan tertentu (Budi Lestari, Putra, & Torbeni, 2022). Dalam mempertimbangkan investasi pada proyek NFT, para *investor* sering memperhatikan beberapa aspek fundamental, salah satunya adalah roadmap atau visi dan misi proyek tersebut.

Namun, seiring dengan perkembangan ini, kejahatan juga ikut berkembang dengan cara-cara yang berbeda. Salah satu bentuk kejahatan yang terkait dengan mata uang kripto dan NFT adalah penipuan. Penipuan virtual yang sering terjadi saat ini seringkali terkait dengan NFT, yang berdampak signifikan pada integritas mata uang kripto di mata masyarakat, serta merugikan secara finansial para investor yang menjadi korban akibat kurangnya kewaspadaan dalam menjalani kehidupan mereka. Menurut Pasal 378 KUHP di Indonesia, penipuan didefinisikan sebagai tindakan seseorang yang menggunakan nama palsu, martabat palsu, tipu muslihat, atau rangkaian kebohongan untuk menggerakkan orang lain agar menyerahkan barang atau memberikan utang atau menghapuskan piutang, dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum. Penipuan merupakan proses atau perbuatan menipu, baik dalam bentuk perbuatan atau cara menipu, atau dalam bentuk peristiwa atau keadaan yang menyesatkan. Pelaku penipuan dapat dihukum dengan pidana penjara maksimal empat tahun (Moeljatno, 2007).

Pola modus penipuan proyek NFT melalui Blockchain Solana sering terjadi dalam lingkungan virtual. Para penipu seringkali membawa dan menjanjikan para *investor* dengan roadmap yang menarik, seni yang indah, dan komunitas palsu yang mereka ciptakan untuk membuat para investor merasa aman dan nyaman dalam melakukan investasi (Kshetri, 2022). Dalam menghadapi fenomena ini, sangat penting untuk meningkatkan kesadaran dan pengetahuan masyarakat tentang risiko modus penipuan proyek NFT. Pendidikan dan sosialisasi yang lebih luas tentang praktik yang aman dan langkah-langkah pencegahan penipuan perlu ditingkatkan. Selain itu, tindakan hukum yang tegas terhadap pelaku penipuan kripto juga perlu dilakukan untuk memberikan efek jera dan melindungi para investor.

Untuk memahami fenomena ini dengan lebih baik, peneliti menggunakan pendekatan *Lifestyle-Exposure Theories Of Victimization* (Hindelang, Gottfredson, & Garofalo, 1978). Pendekatan ini mengasumsikan bahwa melakukan investasi adalah bagian dari gaya hidup para investor yang bertujuan untuk bertahan hidup. Namun, gaya hidup ini juga membawa risiko tinggi terhadap menjadi korban penipuan, meskipun upaya telah dilakukan untuk meminimalkan probabilitas menjadi korban penipuan investasi yang sering mereka lakukan. Maraknya kasus penipuan proyek NFT yang menimpa para investor menunjukkan pentingnya menggali lebih dalam dampak yang terjadi dalam kehidupan masyarakat. Peneliti menyadari bahwa fenomena ini merupakan sebuah isu yang merugikan bagi banyak orang. Hal ini menjadi keresahan dalam kehidupan sehari-hari masyarakat yang menggunakan internet sebagai sarana transaksi dan investasi. Oleh karena itu, peneliti tertarik untuk menjadikan fenomena ini sebagai topik penelitian, dengan fokus pada kurangnya sosialisasi dan minimnya informasi mengenai fenomena dan dampak merugikan yang dialami oleh masyarakat.

METODE

Dalam konteks ini, peneliti akan mengumpulkan data dan informasi terinci mengenai kerugian finansial, kerugian reputasi, serta dampak emosional dan psikologis yang dialami oleh para korban penipuan. Selain itu, peneliti juga akan menganalisis faktor-faktor yang mempengaruhi dampak dari penipuan kasus NFT ini, seperti karakteristik transaksi kripto, mekanisme penipuan yang digunakan, serta tingkat pemahaman dan pengetahuan investor tentang mata uang kripto.

Observasi dilakukan dengan mengamati tindakan pelaku penipuan melalui proyek NFT dalam Blockchain Solana ini mengembangkan aksinya agar kejahatan yang dilakukan dapat memikat para korban dan menghilangkan jejak kejahatannya, seperti mulai dari cara pelaku melakukan tindakan awal pada saat menarik minat korban dalam berinvestasi melalui NFT hingga ketika pelaku akhirnya dapat menjalankan aksinya dan melakukan penipuan, setelah mendapatkan keinginannya, pelaku langsung melarikan diri. Selain itu observasi lainnya dengan mengamati calon korban yang menjadi korban pelaku penipuan NFT khususnya pada platform Blockchain Solana tersebut. Observasi lainnya itu dengan mengamati dampak yang diperoleh investor lainnya yang juga menjadi korban pelaku penipuan NFT tersebut. Pada observasi yang dilakukan peneliti juga menggali bagaimana dampak dan respon korban ketika mengetahui bahwa dirinya telah menjadi korban penipuan NFT.

Wawancara sebagai metode pengumpulan data primer yang penting. Wawancara ini akan memungkinkan peneliti untuk mendapatkan pemahaman yang mendalam tentang perspektif, pengalaman, dan pandangan subjek terkait dengan fenomena yang sedang diteliti. Wawancara juga memberikan kesempatan bagi peneliti untuk mengajukan pertanyaan yang relevan, menggali lebih dalam, dan memperoleh informasi kualitatif yang bernilai tentang dampak fenomena tersebut. Dengan demikian, wawancara menjadi alat yang efektif dalam menggali persepsi dan pengalaman subjek penelitian. Selain pengumpulan data primer melalui observasi dan wawancara, peneliti juga akan menggunakan studi literatur sebagai metode pengumpulan data sekunder.

Studi literatur melibatkan pencarian, pengumpulan, dan analisis terhadap sumber-sumber informasi yang relevan yang telah dipublikasikan sebelumnya, seperti; artikel jurnal; buku; laporan penelitian; website online; regulasi terkait dengan topik penelitian. Dalam penggabungan ketiga metode tersebut, peneliti akan menggunakan pendekatan triangulasi untuk memperoleh keakuratan dan kevalidan data. Pendekatan triangulasi melibatkan penggunaan berbagai sumber data, metode pengumpulan data, dan perspektif untuk mengonfirmasi dan memperkuat temuan penelitian (Sugiyono, 2015).

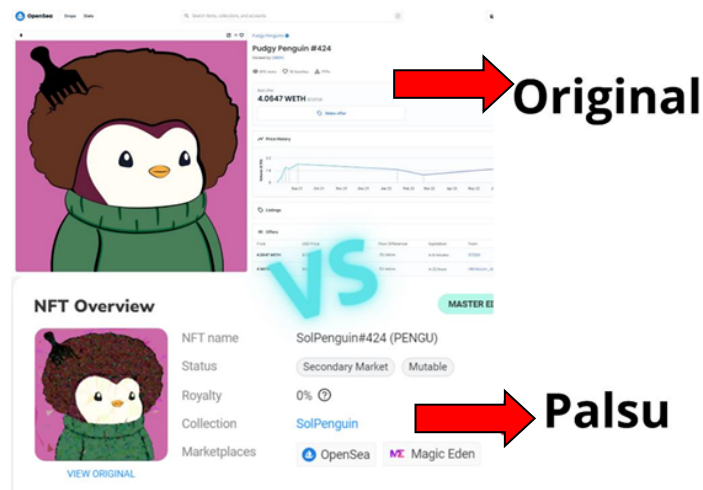
Pada subjek kali ini peneliti memilih narasumber yang telah melakukan transaksi NFT dan *Cryptocurrency* lebih dari sepuluh (10) kali, yang dimana ketiga narasumber tersebut pula sudah mendapatkan keuntungan atau profit yang besar dan banyak melalui transaksi yang sudah pernah mereka lakukan, dan juga peneliti memilih ketiga narasumber tersebut juga karena dimana ketika subjek mendapatkan keuntungan yang besar melalui transaksi tersebut maka semakin tinggi dan banyak pula risiko yang didapat, dimana ketiga subjek tersebut menjadi korban dari modus penipuan NFT.

HASIL DAN PEMBAHASAN

Indikasi Modus Penipuan Non-Fungible Token (NFT)

Dalam skema penipuan ini, para pelaku dengan sengaja menciptakan dan menjual NFT palsu dengan mengklaim bahwa NFT tersebut adalah aset unik yang memiliki nilai tinggi atau bias disebut sebagai plagiarisme. Mereka menggunakan berbagai metode manipulatif untuk menciptakan ilusi keaslian dan keunikan pada NFT palsu mereka. Salah satu metode yang sering digunakan oleh penipu dalam penipuan NFT palsu adalah dengan melakukan pencurian karya seni digital yang populer atau menciptakan karya palsu yang meniru gaya atau konten yang sedang diminati. Mereka dengan mudah dapat mengunduh karya seni digital yang

terpampang di platform daring, dan kemudian memanipulasi karya tersebut untuk menciptakan Salinan palsu yang terlihat identik dengan aslinya. Dengan demikian, mereka dapat menciptakan kesan bahwa NFT palsu tersebut adalah aset yang langka dan unik. Tidak hanya itu, penipu juga sering menggunakan klaim palsu yang menghubungkan NFT palsu mereka dengan selebritas atau tokoh terkenal. Mereka mungkin menggunakan foto atau citra selebritas yang terkenal dan mengklaim bahwa NFT tersebut adalah karya seni eksklusif yang dikurasi atau disetujui oleh selebritas tersebut.



Sumber: Hasil Tangkap Layar Pribadi
Gambar 1. Perbandingan NFT Palsu dan Asli

Dengan melakukan hal ini, penipu berharap dapat mempengaruhi calon pembeli yang tidak mengetahui keaslian asset tersebut, dan menciptakan kesan bahwa NFT palsu tersebut memiliki nilai yang tinggi karena keterkaitannya dengan tokoh terkenal. Dalam upaya menjual NFT palsu ini, pelaku akan menggunakan berbagai strategi dan trik yang dirancang untuk menarik minat calon pembeli yang tidak curiga. Mereka mungkin memanfaatkan platform pasar NFT yang masih belum teratur atau menjalankan kampanye pemasaran agresif untuk menarik perhatian pembeli yang tidak curiga. Beberapa penipu bahkan mungkin menggunakan *bot* atau akun palsu untuk menciptakan ilusi bahwa ada minat yang tinggi terhadap NFT palsu mereka. Dengan adanya penawaran yang tinggi, penipu berharap dapat menciptakan kesan bahwa NFT palsu tersebut juga memiliki nilai yang berupa sangat tinggi sehingga dapat diminati oleh banyak masyarakat umum.

Scam Proyek NFT

Penipuan dalam proyek *Non-Fungible Token* (NFT) merupakan salah satu bentuk kejahatan yang sering terjadi dalam industri aset digital, termasuk dalam ekosistem *Blockchain* Solana. Modus ini melibatkan penciptaan proyek NFT palsu yang tampak sah dan menawarkan peluang investasi dengan keuntungan tinggi. Pelaku penipuan menyusun *roadmap*, *whitepaper* palsu, serta menciptakan tim pengembang fiktif untuk meningkatkan kredibilitas proyek mereka. Strategi ini dirancang untuk menarik calon investor yang tergiur oleh prospek keuntungan yang dijanjikan.

Menurut wawancara dengan salah satu narasumber, karakteristik utama proyek NFT yang berpotensi melakukan penipuan adalah ketidakjelasan identitas pemilik serta tidak adanya tim pengembang yang valid. Hal ini memberikan indikasi bahwa proyek tersebut dikelola secara tersentralisasi oleh individu atau kelompok tertentu tanpa adanya transparansi yang memadai.

Skema penipuan ini umumnya dimulai dengan kampanye pemasaran agresif melalui berbagai *platform* daring, termasuk media sosial, forum komunitas, dan iklan *digital*. Pelaku menggunakan teknik pemasaran yang meyakinkan, sering kali dengan klaim bahwa proyek

mereka merupakan inovasi terobosan di industri NFT. Untuk memperkuat validitasnya, mereka juga menciptakan deskripsi proyek yang menarik dan dokumen pendukung yang terlihat autentik. Setelah berhasil menarik minat investor, mereka mengarahkan calon korban untuk membeli token proyek dengan berbagai metode pembayaran berbasis cryptocurrency. Namun, setelah dana terkumpul dalam jumlah signifikan, pelaku akan menghilangkan jejak dan meninggalkan investor dengan token yang tidak bernilai.

Phishing dan Pencurian Data (*Wallet Dusting*)

Dalam ekosistem *digital* yang terus berkembang, pelaku kejahatan siber menggunakan berbagai metode untuk memperoleh akses ke informasi keuangan korban. Dalam konteks *Blockchain* Solana, metode yang umum digunakan adalah *phishing* dan pencurian data melalui skema *wallet dusting*. Modus operandi ini melibatkan pengiriman NFT palsu ke dompet digital korban dengan tampilan yang menyerupai aset NFT populer. Korban yang tidak curiga sering kali menganggap NFT tersebut sebagai aset yang sah dan mencoba untuk menjualnya. Namun, saat transaksi dilakukan, pelaku memperoleh akses penuh ke dompet digital korban dan dapat mencuri seluruh aset yang tersimpan di dalamnya.

Salah satu narasumber mengungkapkan pengalamannya terkait serangan *wallet dusting*, di mana ia menerima NFT yang tampak menyerupai aset NFT yang sedang tren di pasaran. Ketika mencoba menjualnya, dompet digitalnya diambil alih oleh pelaku, yang mengakibatkan kehilangan seluruh aset digital yang dimilikinya. Modus ini menunjukkan bahwa pelaku penipuan memanfaatkan manipulasi psikologis dengan menciptakan ilusi kepemilikan aset yang berharga, sehingga korban terdorong untuk bertransaksi tanpa menyadari bahwa tindakan tersebut membuka celah keamanan bagi pelaku untuk mengakses dompet digital mereka.

Rug Pull

Salah satu bentuk penipuan paling merugikan dalam ekosistem NFT adalah *rug pull*, yaitu tindakan di mana pengembang proyek NFT secara tiba-tiba menarik seluruh dana *investor* dan menghentikan pengembangan proyek. Pelaku penipuan menciptakan pasar NFT palsu dengan tampilan yang meyakinkan, termasuk tim pengembang fiktif, *roadmap* proyek yang tampak inovatif, serta ulasan positif yang direkayasa oleh *influencer* atau figur publik di komunitas NFT.

Pelaku menggunakan berbagai *platform* media sosial seperti Twitter dan Discord untuk mempromosikan proyek mereka, menarik perhatian *investor* dengan janji keuntungan tinggi dalam waktu singkat. Investor yang termotivasi oleh fenomena *fear of missing out* (FoMO) cenderung melakukan investasi tanpa melakukan verifikasi menyeluruh terhadap kredibilitas proyek. Namun, setelah dana yang terkumpul mencapai jumlah tertentu, pelaku akan menarik seluruh aset likuiditas dari *platform* dan menghilang, meninggalkan *investor* dengan token yang tidak memiliki nilai pasar.

Salah satu faktor utama yang memungkinkan keberhasilan *rug pull* adalah ketidaktransparanan dalam ekosistem proyek NFT. *Blockchain* Solana, yang dikenal dengan sifatnya yang *decentralized*, sering kali dimanfaatkan oleh pelaku untuk menyembunyikan identitas mereka dan menghindari deteksi. Selain itu, kurangnya regulasi yang jelas di sektor NFT semakin mempermudah pelaku untuk menjalankan aksi penipuan tanpa konsekuensi hukum yang signifikan. Hal ini menunjukkan pentingnya upaya pengawasan dan pengembangan kebijakan yang lebih ketat untuk melindungi investor dari risiko penipuan di pasar NFT.

Risiko Paparan Gaya Hidup dalam Modus Penipuan NFT

Dalam konteks penipuan NFT, teori *Lifestyle Exposure* menjelaskan bagaimana pola gaya hidup seseorang, termasuk aktivitas daring, dapat meningkatkan risiko menjadi korban

kejahatan. Partisipasi aktif dalam transaksi NFT, ketergantungan pada platform tertentu, serta kecenderungan mengikuti tren (*Fear of Missing Out* atau FoMO) merupakan faktor utama yang meningkatkan kerentanan terhadap modus penipuan NFT di ekosistem Blockchain Solana.

1. Terlalu Sering Terlibat dalam Transaksi NFT

Paparan berulang terhadap aktivitas transaksi NFT meningkatkan risiko menjadi korban skema penipuan. Penipu menciptakan proyek investasi palsu dengan janji keuntungan tinggi, menciptakan *roadmap* dan *whitepaper* yang tampak meyakinkan untuk menarik investor. Namun, setelah dana terkumpul, mereka menghilang, meninggalkan investor dengan aset digital yang tidak bernilai. Berdasarkan wawancara, beberapa korban mengaku mengalami kerugian akibat proyek NFT yang ditinggalkan tanpa pengembangan lebih lanjut.

2. Ketergantungan pada Platform NFT Tertentu

Kebergantungan terhadap satu platform NFT meningkatkan risiko terjebak dalam penipuan. Beberapa platform tidak memiliki sistem keamanan yang ketat, sehingga memungkinkan pelaku untuk menciptakan proyek NFT palsu atau mencuri aset *digital* pengguna. Dalam beberapa kasus, serangan wallet dusting terjadi ketika pengguna menerima NFT palsu yang tampak asli, dan saat mencoba menjualnya, dompet digital mereka diretas dan asetnya dicuri.

3. *Fear of Missing Out* (FoMO) dalam Investasi NFT

FoMO mendorong individu untuk melakukan investasi tanpa analisis mendalam. Pelaku penipuan memanfaatkan taktik ini dengan menciptakan urgensi melalui promosi terbatas, janji keuntungan besar, serta menggunakan dukungan selebriti atau *influencer* untuk membangun kepercayaan palsu. *Investor* yang terburu-buru sering kali terjebak dalam proyek NFT yang ternyata hanya skema penipuan, menyebabkan kerugian finansial yang signifikan.

Analisis terhadap keterlibatan korban dalam investasi NFT menunjukkan bahwa gaya hidup *digital* mereka memainkan peran signifikan dalam meningkatkan risiko menjadi korban penipuan. Faktor-faktor seperti intensitas transaksi, ketergantungan pada *platform* tertentu, dan kecenderungan mengikuti tren tanpa riset yang matang menjadi penyebab utama rentannya individu terhadap modus penipuan NFT dalam ekosistem *Blockchain* Solana.

KESIMPULAN

Berdasarkan analisis yang dilakukan, terdapat tiga faktor utama yang meningkatkan risiko investor menjadi korban penipuan NFT dalam konteks *Lifestyle Exposure Theory*. Pertama, keterlibatan yang terlalu sering dalam transaksi NFT menjadikan individu lebih rentan sebagai target penipuan. Kedua, ketergantungan pada platform tertentu menyebabkan investor terlalu percaya tanpa melakukan riset yang memadai. Ketiga, efek *Fear of Missing Out* (FoMO) mendorong keputusan investasi impulsif akibat tekanan promosi dan keterlibatan selebriti atau *influencer*. Kurangnya kontrol diri dan minimnya verifikasi informasi membuat investor lebih mudah terjebak dalam modus penipuan. Faktor-faktor kebiasaan yang telah dilakukan diatas menunjukan peranan dirinya sebagai korban dalam modus penipuan atau yang dikenal dengan istilah *Participating Victims*, yaitu mereka yang dengan perilakunya memudahkan dirinya berperan sebagai korban.

REFERENSI

Amelia, G. (2021). Penegakan Hukum terhadap Pelaku Tindak Pidana Penipuan Investasi Ilegal Uang Kripto di Perusahaan E-Dinar Coin Cash (EDCCash) Ditinjau dari Undang-Undang No.19 Tahun 2016 Perubahan atas Undang-Undang No.11 Tahun 2008. *Jurnal Riset Ilmu Hukum*, 1(2), 117-123.

- Andres, S. (2021). *Solana in a Nutshell: The Definitive Guide to Enter the World of Decentralized Finance, Lending, Yield Farming, Dapps and Master it Completely*. WB Publishing.
- Brown, S. D. (2016). Cryptocurrency and Criminality: The Bitcoin Opportunity. *The Police Journal: Theory, Practice and Principles*, 1-13.
- Budi Lestari, N. E., Putra, A. M., & Torbeni, W. (2022). Mengenal NFT Arts sebagai Peluang Ekonomi Kreatif di Era Digital. *SENADA (Seminar Nasional Manajemen, Desain dan Aplikasi Bisnis Teknologi)*, 5, 342-357. Retrieved from <https://eprosiding.idbbali.ac.id/index.php/senada/article/view/656>
- Budiastanti, D. E. (2017). Perlindungan Hukum Terhadap Korban Tindak Pidana Penipuan Melalui Internet. *Jurnal Cakrawala Hukum*, 8(1), 22-32.
- Coufano, G. (2022). *The Solana Blockchain In A Nutshell*. Retrieved from FourWeekMBA: <https://fourweekmba.com/solana-blockchain/>
- Djanggih, H., & Qamar, N. (2018). Penerapan Teori-Teori Kriminologi dalam Penanggulangan Kejahatan Siber (Cyber Crime). *Pandecta*, 10-23.
- Gumilang, G. S. (2016). Metode penelitian kualitatif dalam bidang bimbingan dan konseling. *Jurnal Fokus Konseling*, 2(2).
- Hindelang, M. J., Gottfredson, M. R., & Garofalo, J. (1978). *Victims of Personal Crime: An Empirical Foundation for a Theory of Personal Victimization*. Ballinger Publishing Company.
- Huda, N., & Hambali, R. (2020, Maret). Risiko dan Tingkat Keuntungan Investasi Cryptocurrency. *Jurnal Manajemen dan Bisnis*, 17(1).
- Huda, S., & Santoso, H. A. (2018). Identifikasi Pola Fraud dalam Transaksi Online. *Jurnal Atmaluhur*, 8-9. Retrieved from <http://jurnal.atmaluhur.ac.id/index.php/knsi2018/article/view/362>
- Indrabayu, A., & Destiwati, R. (2022, Agustus 29). Pengaruh Komunikasi Intrapersonal dan Fear of Missing Out terhadap Hedonisme pada Generasi Z di Denpasar. *Management Studies and Entrepreneurship Journal (MSEJ)*, 3(4), 2169-2175. <https://doi.org/10.37385/msej.v3i4.783>
- Kalsum, T. U., Fredricka, J., Yulianti, L., Kanedi, I., & Sukmo, A. (2022). The Importance of Digital Security in the 4.0 Industrial Revolution. *Jurnal Dehasen Untuk Negeri*, 1(1), 37-40.
- KBBI. (n.d.). *Kamus Besar Bahasa Indonesia*. Retrieved 2023, from <https://kbbi.web.id>
- Kshetri, N. (2022). Scams, Frauds, and Crimes in the Nonfungible Token Market. *Computer*, 55(4), 60-64. <https://doi.org/10.1109/MC.2022.3144763>
- Kugler, L. (2021). Non-fungible tokens and the future of art. *Communications of the ACM*, 64(9), 19-20.
- McGinnis, P. (2020). *Fear of Missing Out: Practical Decision-Making in a World of Overwhelming Choice*. Sourcebooks.
- Moeljatno. (2007). *KUHP (Kitab Undang-Undang Hukum Pidana)*. Jakarta: Bumi Aksara.
- Moleong, L. J. (2018). *Metodologi Penelitian Kualitatif* (Edisi revisi, Cetakan ke-38). PT Remaja Rosdakarya.
- Ngafifi, M. (2014). Kemajuan Teknologi dan Pola Hidup Manusia dalam Perspektif Sosial Budaya. *Jurnal Pembangunan Pendidikan: Fondasi dan Aplikasi*, 2(1). <https://doi.org/10.21831/jppfa.v2i1.2616>
- Pemerintah Indonesia. (1999). *Undang-Undang Nomor 8 Tahun 1999 Pasal 1 Ayat (1) Tentang Perlindungan Konsumen*. Jakarta: LL Setneg No.3821. Retrieved from <https://peraturan.bpk.go.id/Home/Download/33784/UU%20Nomor%208%20Tahun%201999.pdf>
- Pemerintah Indonesia. (2016). *Undang-Undang Nomor 19 Tahun 2016 Pasal 1 Ayat (2) Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi*

- dan Transaksi Elektronik*. Jakarta: LL Setneg No.5952. Retrieved from <https://peraturan.bpk.go.id/Home/Download/26676/UU%20Nomor%2019%20Tahun%202016.pdf>
- Picardo, E. (n.d.). What is Solana (SOL) and How Does SOL Crypto Work? Retrieved from Investopedia: <https://www.investopedia.com/solana-5210472>
- Pratt, T. C., & Turanovic, J. J. (2015). Lifestyle and Routine Activity Theories Revisited: The Importance of "Risk" to the Study of Victimization. *Victims and Offenders*.
- Rahamanto, T. Y., Kav, J. H., & Kuningan, J. S. (2019). Penegakan Hukum Terhadap Tindak Pidana Penipuan Berbasis Transaksi Elektronik. *Jurnal Penelitian Hukum De Jure*, 19(1), 31.
- Rejeb, A., Rejeb, K., & Keogh, J. G. (2021). Cryptocurrencies in Modern Finance: A Literature Review. *Etikonomi*, 20(1), 93-118. <https://doi.org/10.15408/etk.v20i1.16911>
- Rusmana, A. (2015). Penipuan dalam Interaksi Melalui Media Sosial. *Jurnal Kajian Informasi & Perpustakaan*, 3(2), 187-194.
- Saputra, N. (2018). Dampak Cryptocurrency Terhadap Perekonomian Indonesia. *Seminar Nasional Royal SENAR*, 491-496.
- Setiawan, E., & P. (2020). Analisis Potensi dan Risiko Investasi Cryptocurrency di Indonesia. *Jurnal Manajemen Teknologi*, 19(2), 130-144.
- Singh, S. (2022). *Solana: Speed & Scale*. Independently Published.
- Solana Foundation. (n.d.). There are no bad questions about... blockchain basics. Retrieved from Solana: <https://solana.com/learn/blockchain-basics>
- Solana Foundation. (n.d.). There are no bad questions about... NFTs. Retrieved from Solana: <https://solana.com/learn/nfts>
- Trompeter, G. M., Carpenter, T. D., Desai, N., Jones, K. L., & Jr, R. A. (2013). A Synthesis of Fraud-Related Research. *Auditing: A Journal of Practice & Theory*, 32(1), 287-321.
- Umar, Z., Polat, O., Choi, S. Y., & Teplova, T. (2022). Dynamic Connectedness between NFTs, DeFi, and Conventional Financial Assets. *Pacific-Basin Finance Journal*.
- Zunaida, D. (2018). Identification of Perceptions of Investment Tendency. *Pekomnas*, 3(1), 53-62. <https://doi.org/10.30818/jpkm.2018.2030106>