

## Kasus Penipuan Online Bermodus Pelatihan Trading Kripto Di Indonesia Tahun 2025

Salsabila Putri I. Simbolon<sup>1)</sup>, Nia Malika Aulia<sup>2)</sup>, Rendi Cahaya Sinaga<sup>3)</sup>, Miftahul Choir Saragih<sup>4)</sup>, Kristine Manasye Simanjuntak<sup>5)</sup>, Dian G. Purba<sup>6)</sup> ✉

<sup>1)2)3)4)5)6)</sup> Program Studi Ekonomi Pembangunan, Fakultas Ekonomi, Universitas Simalungun Pematangsiantar

### Abstrak

Penelitian ini bertujuan untuk Menganalisis secara sistematis bentuk, karakteristik, dan mekanisme operasional modus penipuan online bermodus pelatihan trading kripto yang marak terjadi di Indonesia pada tahun 2025. Penelitian ini menggunakan metode kualitatif yang berdasarkan riset atau data sekunder yang ada di buku, media, ataupun internet. Hal ini dilakukan karena penulis tidak melakukan observasi secara langsung ke lapangan atau ke informan sehingga hanya membutuhkan data sekunder. Selain itu, hasil dan pembahasan penelitian ini memberikan hasil bahwa diketahui Bentuk dan Mekanisme Penipuan Online Bermodus Pelatihan Trading Kripto, Faktor Penyebab Penipuan ini bisa terjadi dan Implikasi Terhadap Regulasi, Pengawasan Digital, dan Edukasi Masyarakat.

**Kata Kunci:** *Penipuan Online;Trading Kripto*

---

Copyright (c) 2019 Nama Penulis

✉ Corresponding author :

Email Address : [bilas8372@gmail.com](mailto:bilas8372@gmail.com)

### PENDAHULUAN

Maraknya perkembangan teknologi digital di Indonesia pada tahun 2025 tidak hanya membawa peluang ekonomi, tetapi juga meningkatkan kerentanan masyarakat terhadap kejahatan siber, khususnya penipuan bermodus investasi dan pelatihan trading kripto. Dari data Otoritas Jasa Keuangan (OJK) melalui Satgas Pemberantasan Aktivitas Keuangan Ilegal (Satgas PASTI) menunjukkan bahwa hingga pertengahan Oktober 2025 telah tercatat 297.217 kasus penipuan online dengan total kerugian mencapai Rp7 triliun, menandakan skala ancaman yang semakin serius.

Salah satu modus yang paling menonjol adalah tawaran pelatihan trading kripto palsu, di mana pelaku yang mengaku sebagai "profesor investasi" asal Amerika Serikat yang memanfaatkan media sosial seperti Instagram dan Facebook untuk mengarahkan korban masuk ke grup WhatsApp sebagai ruang operasi utama. Berdasarkan temuan Direktorat Reserse Siber Polda Metro Jaya, pelaku menggunakan grafis pasar palsu, testimoni fiktif, dan prediksi pasar yang direkayasa untuk menciptakan ilusi kredibilitas sebelum akhirnya meminta korban mentransfer dana dengan iming-iming keuntungan tinggi. Investigasi lebih lanjut mengungkap bahwa jaringan ini bersifat terorganisir dan beroperasi lintas negara, dibuktikan dengan ditemukannya ratusan grup WhatsApp serupa berisi ribuan korban potensial. Rendahnya tingkat pemulihan kerugian hanya sekitar 2% dana yang berhasil diblokir sebelum dipindahkan pelaku sehingga menggambarkan tingginya efektivitas

manipulasi psikologis (social engineering) yang digunakan serta lemahnya kewaspadaan digital masyarakat. Situasi ini menegaskan perlunya penguatan literasi digital, peningkatan mekanisme pengawasan, serta koordinasi aparat penegak hukum dalam mencegah penipuan investasi yang semakin kompleks dan adaptif.

Berdasarkan latar belakang tersebut ada beberapa rumusan masalah yang diajukan untuk penelitian ini seperti, Bagaimana bentuk dan mekanisme yang digunakan pelaku dalam menjalankan penipuan online bermodus pelatihan trading kripto yang digunakan oleh sindikat pada tahun 2025 di Indonesia, Faktor apa saja yang menyebabkan masyarakat rentan menjadi korban, khususnya terkait literasi digital, manipulasi psikologis, dan penggunaan media sosial oleh pelaku, dan Bagaimana upaya dan efektivitas penanganan yang dilakukan oleh Otoritas Jasa Keuangan (OJK), Satgas PASTI, serta aparat penegak hukum dalam mengidentifikasi, menindak, dan memulihkan kerugian korban serta Implikasi kasus ini terhadap kebutuhan peningkatan regulasi, pengawasan digital, dan edukasi masyarakat untuk mencegah penipuan online dengan modus serupa di masa mendatang.

Adapun tujuan penulisan penelitian ini yaitu, Menganalisis secara sistematis bentuk, karakteristik, dan mekanisme operasional modus penipuan online bermodus pelatihan trading kripto yang marak terjadi di Indonesia pada tahun 2025, Mengidentifikasi dan menjelaskan faktor-faktor yang meningkatkan kerentanan masyarakat terhadap penipuan tersebut, termasuk aspek literasi digital, teknik manipulasi psikologis, serta pemanfaatan media sosial oleh pelaku, dan Mengevaluasi efektivitas penanganan yang dilakukan oleh OJK, Satgas PASTI, dan aparat penegak hukum dalam proses identifikasi, penindakan, serta pemulihan kerugian korban serta Merumuskan implikasi dan rekomendasi strategis terkait peningkatan regulasi, pengawasan aktivitas digital, dan edukasi publik guna mencegah terulangnya kasus serupa di masa mendatang.

## METODOLOGI

Dalam penelitian ini menggunakan pendekatan Penelitian kualitatif yang bertujuan memperoleh gambaran seutuhnya mengenai suatu hal menurut pandangan manusia yang diteliti. Penelitian kualitatif berhubungan dengan ide, persepsi, pendapat, atau kepercayaan orang yang diteliti; kesemuanya tidak dapat diukur dengan angka (Elidawaty, 2021).

Data yang digunakan pada penelitian ini adalah data sekunder yang berasal dari berbagai sumber di Internet atau Media lainnya. Dimana data sekunder juga Data ini berfungsi melengkapi dan mendukung informasi yang ada pada penelitian ini(Hafni Sahir, 2021) , laporan tahunan, literature dan dokumen lain yang berhubungan dengan masalah penelitian. . Penelitian ini menggunakan data yang bersumber dari Otoritas Jasa Keuangan, dan beberapa media lainnya seperti jurnal penelitian dan artikel berita.

Alasan kami melakukan penelitian ini dengan menggunakan metode kualitatif dengan berdasarkan data sekunder dikarenakan metode ini sangat relevan dengan beberapa kejadian kasus nyata di Indonesia tanpa harus melakukan wawancara atau observasi ke lapangan secara langsung kepada pihak yang terkait.

## HASIL DAN PEMBAHASAN

Adapun beberapa hasil dan pembahasan yang kami dapatkan setelah melakukan riset secara online dari berbagai sumber yang ada di Internet ataupun Artikel berita menggunakan metode kualitatif didapat hasil dan pembahasan yaitu sebagai berikut :

### **Bentuk dan Mekanisme Penipuan Online Berkedok Pelatihan Trading Kripto pada Tahun 2025 di Indonesia**

Penipuan online bermodus pelatihan trading kripto pada tahun 2025 menunjukkan pola kerja yang sangat terstruktur dan didesain menyerupai aktivitas edukasi investasi yang sah. Mekanisme operasionalnya dimulai dari tahap rekrutmen korban melalui penyebaran iklan berbayar di berbagai platform media sosial seperti Instagram dan Facebook. Iklan tersebut biasanya menampilkan sosok yang mengaku sebagai "profesor investasi" asal Amerika Serikat, lengkap dengan identitas akademik palsu dan narasi otoritatif yang memberikan kesan profesional. Strategi ini merupakan tahap awal dari teknik social engineering, di mana pelaku membangun kepercayaan melalui citra legitimasi dan keahlian yang dikonstruksi secara sengaja.

Tahap berikutnya adalah pengalihan komunikasi ke dalam grup WhatsApp yang diposisikan sebagai ruang pelatihan eksklusif. Pada titik ini, mekanisme penipuan semakin intensif melalui penyampaian materi pelatihan palsu, tampilan grafik pasar buatan, dan testimoni fiktif yang menampilkan keberhasilan peserta lain. Pelaku juga menampilkan prediksi pasar yang tampak akurat, yang sebenarnya dihasilkan melalui manipulasi informasi atau memanfaatkan pergerakan saham yang dapat diprediksi secara sederhana. Ketika prediksi tersebut terbukti "tepat", korban semakin yakin terhadap kredibilitas instruktur palsu dan merasa berada dalam komunitas yang aman.

Setelah kepercayaan terbentuk, pelaku masuk ke tahap eksekusi finansial dengan meminta korban melakukan transfer dana ke rekening yang dikendalikan oleh sindikat. Dana tersebut dijanjikan akan dikelola dalam bentuk aset kripto berisiko tinggi dengan imbal hasil besar dalam waktu singkat. Pada tahap ini, pelaku sangat memanfaatkan psikologis korban, terutama fear of missing out (FOMO) dan keinginan untuk memperoleh keuntungan cepat. Setelah dana ditransfer, pelaku menghilang dan seluruh komunikasi dihentikan, dan mengakhiri rangkaian penipuan.

Keseluruhan pola operasional ini menunjukkan bahwa sindikat pelaku bekerja secara lintas negara, memanfaatkan kelemahan regulasi digital, celah pengawasan transaksi, serta kerentanan psikologis masyarakat. Struktur yang rapi yang dimulai dari rekrutmen, pembentukan kepercayaan, operasi dalam grup tertutup, hingga pengosongan rekening korban menjadi bukti bahwa modus ini bukan tindakan acak atau asal-asalan, tetapi merupakan bentuk kejahatan digital terorganisir yang memanfaatkan kemajuan teknologi komunikasi secara optimal.

### **Faktor Penyebab Kerentanan Masyarakat sebagai Korban dalam Penipuan Online**

Setelah dilakukan beberapa riset mengenai Korban dalam Penipuan Online, maka ada beberapa faktor yang menyebabkan kerentanan Masyarakat sebagai Korban Dalam Penipuan Online yaitu :

### **a. Rendahnya Literasi Digital**

Banyak masyarakat belum cukup memahami cara kerja internet, risiko kejahatan siber, atau bagaimana melindungi data pribadinya. Kondisi ini membuat mereka lebih mudah menjadi korban penipuan karena tidak bisa membedakan mana konten atau tawaran yang aman dan mana yang mencurigakan. Studi menunjukkan bahwa literasi digital di Indonesia masih dalam level sedang, dan kurangnya pemahaman ini memperbesar peluang seseorang menjadi korban penipuan daring. Sehingga program edukasi seperti sosialisasi literasi digital dan pelatihan keamanan daring sangat penting untuk mengurangi risiko ini.

### **b. Manipulasi Psikologis oleh Pelaku**

Pelaku penipuan online sering menggunakan teknik social engineering yaitu teknik manipulasi psikologis untuk membangun kepercayaan. (Misalnya, berpura-pura menjadi pihak berwenang atau "ahli investasi" agar korban merasa aman). Dalam konteks investasi ilegal, korban dapat digoda dengan janji keuntungan besar atau dibuat merasa "berteman" melalui chat agar akhirnya tertarik memasukkan uang. Karena manipulasi seperti ini sangat halus dan meyakinkan, banyak orang yang tidak menyadari bahwa mereka sedang dimanfaatkan sampai terlambat.

### **c. Pemanfaatan Media Sosial dan Platform Komunikasi Digital sebagai Alat Operasional Utama**

Media sosial seperti Facebook, Instagram, WhatsApp, dan Telegram menjadi "ladang subur" bagi penipu karena mudah menjangkau banyak orang dan membentuk grup atau komunitas palsu. Pelaku menggunakan platform ini untuk menyebarkan konten promosi yang tampak meyakinkan, menyampaikan testimoni fiktif, atau membangun "kelas" digital agar korban merasa berada di lingkungan yang kredibel. Kurangnya literasi media sosial membuat sebagian orang kesulitan mengenali identitas palsu atau perilaku mencurigakan di platform digital.

### **d. Adanya Keterbatasan Mekanisme Pengawasan dan Pelaporan**

Mekanisme pengawasan dan pelaporan kejahatan siber di masyarakat masih belum optimal. Banyak orang belum tahu ke mana harus melapor atau merasa tidak yakin bahwa laporannya akan ditindaklanjuti secara serius.

Dari sisi institusi, meski telah ada upaya sosialisasi dan kampanye literasi digital, laporan kejahatan seperti social engineering masih sulit diusut secara menyeluruh karena keterbatasan kapasitas penegakan hukum dan kebijakan pengawasan. Situasi ini menciptakan celah besar bagi pelaku yang terus beroperasi tanpa terlalu khawatir akan konsekuensi, karena risiko tertangkap atau kehilangan dana oleh korban cenderung rendah.

## **Upaya Penanganan dan Efektivitas OJK, Satgas PASTI, dan Aparat Penegak Hukum**

Dalam menilai efektivitas penanganan kasus penipuan online bermodus pelatihan trading kripto pada tahun 2025, ada tiga aspek yang perlu ditelaah secara kritis: kecepatan respons, kapasitas investigatif, dan pemulihan kerugian korban. Ketiganya tidak selalu sejalan, sehingga penting untuk tidak hanya menilai upaya pemerintah dari tindakan represif semata.

### **d. Kecepatan Respons Terhadap Laporan Publik**

Saluran pelaporan OJK dan Satgas PASTI seperti call center, website, dan Whistleblowing System, pada dasarnya cukup mudah diakses. Namun, efektivitasnya sering terganggu karena beberapa kendala teknis dan struktural:

- a) Pelaku memanfaatkan akun media sosial sekali pakai, sehingga sulit dilacak bila sudah dihapus.
- b) "Lembaga pelatihan trading" palsu tidak berizin, sehingga tidak tercatat dalam sistem pengawasan OJK.
- c) Dana yang sudah berpindah melalui crypto-mixing atau exchange luar negeri mempersempit ruang intervensi cepat.

Secara kritis, ini menunjukkan bahwa arsitektur pengawasan OJK masih kurang adaptif terhadap dinamika kejahatan aset digital yang sangat cepat berubah.

**e. Kapasitas Investigatif Aparat Penegak Hukum**

Di sisi lain, kepolisian siber telah meningkatkan kemampuan digital forensic, namun sindikat internasional memiliki struktur operasi yang lebih kompleks. Pelaku memanfaatkan: server luar negeri, VPN berlapis, identitas digital palsu, dan skema multi-level baiting (korban direkrut oleh korban lain).

Akibatnya proses pelacakan meskipun dilakukan, sering berakhir pada identifikasi level "pengumpul korban" saja, bukan aktor utama. Ini menandakan bahwa efektivitas aparat hukum terbatas oleh kapasitas lintas-negara dan keterbatasan regulasi terkait crypto tracing di Indonesia.

Meski demikian, beberapa kasus berhasil diungkap karena kerja sama dengan perusahaan forensik blockchain dan Interpol. Artinya, kapasitas investigasi mulai berkembang, tetapi belum merata di seluruh wilayah.

**f. Pemulihan Kerugian Korban**

Efektivitas pada tahap pemulihan kerugian ini paling lemah, korban jarang bisa mendapatkan pengembalian dana karena: aset kripto dialihkan ke wallet yang tidak dapat dilacak, proses hukum terhadap pelaku sering terhenti pada tingkat perantara lokal, tidak ada mekanisme kompensasi institusional bagi korban platform ilegal.

Salah satu asumsi umum "penegakan hukum pasti bisa mengembalikan dana korban" ternyata keliru. Dalam praktiknya, pemulihan hampir mustahil kecuali dana belum sempat dipindahkan ke jaringan blockchain internasional.

**g. Evaluasi Keseluruhan**

Secara Objektif, efektivitas penanganan pemerintah dapat dikatakan moderate, namun belum memadai. Ada kemajuan dalam koordinasi dan penindakan, tetapi belum mampu mengimbangi dinamika kejahatan digital yang bersifat transnasional, sangat cepat, dan berbasis teknologi kripto.

### **Implikasi Terhadap Regulasi, Pengawasan Digital, dan Edukasi Masyarakat**

Kasus penipuan online berkedok pelatihan trading kripto memperlihatkan bahwa sistem perlindungan saat ini belum cukup kuat, sehingga terdapat beberapa implikasi penting yang harus segera ditindaklanjuti oleh regulator dan pemangku kepentingan.

**a. Kebutuhan Regulasi yang Lebih Kuat dan Spesifik**

Kasus semacam ini menegaskan bahwa diperlukan regulasi yang lebih detail dan tegas untuk menutup celah modus operasi penipuan kripto. OJK sudah menunjukkan inisiatif melalui pedoman keamanan siber untuk penyelenggara aset keuangan digital guna memperkuat keamanan dan integritas.

Selain itu, Satgas PASTI menetapkan bahwa hanya entitas yang berizin dari OJK yang diperbolehkan menawarkan aktivitas kripto, dan entitas ilegal terus diblokir. Regulasi yang lebih spesifik misalnya kewajiban registrasi edukator kripto, audit konten promosi, dan transparansi pengelolaan dana peserta dapat membantu mencegah penipuan yang berkedok edukasi investasi.

#### **b. Penguatan Pengawasan Aktivitas Digital**

Kasus ini juga mempertegas perlunya sistem pengawasan digital yang lebih agresif dan real-time. Pengalaman Satgas PASTI dalam memblokir 507 entitas keuangan ilegal pada pertengahan 2025 menunjukkan bahwa pemblokiran masih menjadi strategi reaktif.

Idealnya, mekanisme takedown otomatis dan kolaborasi antar instansi (OJK, Kominfo, Satgas PASTI) perlu diperkokoh agar platform ilegal bisa dinonaktifkan lebih cepat sebelum merugikan korban lebih banyak. Selain itu, peningkatan keamanan siber penyelenggara aset digital harus menjadi prioritas agar risiko penipuan dengan modus digital semakin diminimalkan.

#### **c. Pentingnya Edukasi Masyarakat secara Sistematis**

Salah satu solusi jangka panjang yang sangat penting adalah edukasi keuangan digital secara masif dan berkelanjutan. OJK sudah menginisiasi "Bulan Literasi Kripto (BLK) 2025" untuk mendorong pemahaman masyarakat mengenai risiko aset kripto dan cara investasi yang bijaksana. Selain itu, OJK menyelenggarakan kuliah umum untuk generasi muda agar mereka memahami risiko kripto, bukan hanya mengejar tren. Edukasi semacam ini harus lebih dari sekadar teori: harus ada studi kasus penipuan nyata, simulasi, dan akses ke platform literasi interaktif agar masyarakat bisa mengenali taktik penipu.

#### **d. Sinergi Antar-Pemangku Kepentingan**

Kasus ini juga menggarisbawahi perlunya kolaborasi lintas lembaga yang lebih erat. OJK dan Satgas PASTI sudah memiliki struktur seperti Indonesia Anti-Scam Centre (IASC) sebagai pusat koordinasi pelaporan penipuan. Namun, agar efektivitasnya maksimal, lembaga-lembaga seperti Kementerian Komunikasi, Kominfo, dan aparat penegak hukum harus semakin terintegrasi dalam sistem pengawasan dan penindakan. Dengan kerja sama yang kuat, laporan penipuan bisa ditindak lebih cepat, dan edukasi masyarakat bisa lebih terarah melalui kampanye terpadu.

## **SIMPULAN**

Kesimpulan yang dapat diambil berdasarkan pembahasan penelitian yang telah dilakukan mengenai Kasus Penipuan Online Bermodus Pelatihan Kripto Di Indonesia Tahun 2025, maka dapat disimpulkan sebagai berikut:

Kasus penipuan online bermodus pelatihan trading kripto di Indonesia tahun 2025 menunjukkan bahwa perkembangan teknologi digital tidak selalu diikuti oleh kesiapan masyarakat dan sistem pengawasan negara. Modus yang digunakan pelaku mulai dari identitas palsu, pelatihan daring fiktif, manipulasi psikologis, hingga penggunaan platform media sosial membuktikan bahwa bentuk penipuan semakin canggih dan terstruktur. Kerentanan masyarakat semakin diperparah oleh rendahnya literasi digital, lemahnya mekanisme pelaporan, serta keterbatasan regulasi yang belum mengakomodasi pola kejahatan berbasis aset digital.

Upaya penanganan oleh OJK, Satgas PASTI, dan aparat penegak hukum pada dasarnya sudah berjalan melalui pemblokiran entitas ilegal, peningkatan patroli siber, dan sosialisasi edukasi konsumen. Namun, efektivitasnya masih terkendala pada lambatnya respons awal, kurangnya kapasitas investigatif digital forensik, serta kesulitan pemulihan kerugian karena dana korban cepat dialihkan ke platform luar negeri. Situasi ini menegaskan kebutuhan mendesak untuk memperkuat regulasi, memperluas pengawasan aktivitas digital, dan meningkatkan literasi masyarakat sebagai bentuk pencegahan jangka panjang.

## Referensi :

- Afrizal, & Marliyah. (2021). Analisis Terhadap Cryptocurrency (Perspektif Mata Uang, Hukum, Ekonomi Dan Syariah). Jurnal Ekonomi Da Bisnis.
- Elidawaty, P. (2021). Metodologi Penelitian Manajemen. Yayasan Kita Menulis.
- Finsensia Riti, Y. (2024). PENIPUAN MELALUI MEDIA SOSIAL BAGI MASYARAKAT. In Jurnal CSDS (Vol. 3, Issue 1).
- Hafni Sahir, S. (2021). Metodologi Penelitian. KBM Indonesia. [www.penerbitbukumurah.com](http://www.penerbitbukumurah.com)
- Kurnia. (2022). Penipuan Digital di Indonesia: Modus, Medium, Rekomendasi. Jurnal Manajemen Dan Bisnis.
- Naqvi. (2023). Mitigation strategies against the phishing attacks: A systematic.
- Rahmawan, B. A., Robbani, N. A., & Mafruhat, A. Y. (2022). DAMPAK CRYPTOCURRENCY TERHADAP SISTEM MONETER: SEBUAH TINJAUAN PUSTAKA SISTEMATIS.