June 2026

TU TRADERS UNION · RESEARCH

CRYPTO MARKETS · FRAUD AWARENESS STUDY

Crypto Scams and Investor Protection

A proprietary study of 1,500 cryptocurrency investors measuring real exposure to scams, due diligence behavior and the gap between perceived and actual fraud detection ability.

58%
ENCOUNTERED SCAM ATTEMPTS

23%
CONSISTENTLY VERIFY PROJECTS & EXCHANGES

37%
"CONFIDENT" YET STILL LOST MONEY

TU Research Team
A. Chabaniuk · C. Soni · D. Blystone

Methodology
CAWI · 95% confidence · ±2.5%

Sample
1,500 crypto investors

Table of Contents

01 Executive Findings

TU

TU proprietary research suggests crypto investors are highly aware of fraud risks, yet many still fail to perform basic due diligence. In a survey of 1,500 cryptocurrency investors, 58% encountered scam attempts, while only 23% consistently verify project teams, smart contract audits and exchange security measures. The findings reveal a significant gap between scam awareness and actual protective behavior.

✓ **Scam exposure is widespread.** **58%** of crypto investors reported encountering at least one scam attempt during the past 12 months.

- ✓ **Phishing remains the most common threat.** **46%** of respondents encountered phishing emails, fake websites or wallet-draining links.
- ✓ **Verification practices remain inconsistent.** Only **23%** always verify project teams, audits and tokenomics before investing.
- ✓ **Experience improves fraud detection.** Investors with 5+ years are roughly **2.4×** less likely to suffer scam losses than those under 2 years (**41%** vs **17%**).
- ✓ **A perception gap exists.** Although **74%** believe they can identify scams, **37%** of them admitted losing money to fraudulent projects or platforms.
- ✓ **AI-generated scams are emerging rapidly.** Deepfake videos and impersonation campaigns are increasingly difficult for investors to identify.

Risk warning: Cryptocurrencies are highly volatile and exposed to fraud risks. This research is informational only and is not investment advice.

02 Introduction & Research Questions

TU

Cryptocurrency markets have created unprecedented opportunities for retail investors. However, they have also become a fertile environment for fraud, phishing campaigns, rug pulls, fake token launches, impersonation attacks and AI-generated scams.

As crypto adoption expands, scammers continue to develop increasingly sophisticated methods of exploiting investor behavior. Deepfake videos, fake exchange websites, fraudulent airdrops and social media impersonation schemes have become common features of the digital asset ecosystem.

The study focuses on five key questions

- How often do crypto investors encounter scams?
- Which scam types are most common?
- How do investors verify projects and exchanges?
- Which investor groups are most vulnerable?
- Do investors overestimate their ability to detect fraud?

03 Glossary

Phishing
A fraud technique where attackers create fake websites, emails or messages to steal credentials, private keys or wallet access.

Rug pull
A scam where developers launch a crypto project, attract investment and then abruptly withdraw liquidity or abandon the project.

Fake token launch
A fraudulent token release impersonating a legitimate project or using fabricated metrics to lure investors.

Wallet-draining link
A malicious smart contract or signature request that, once approved, transfers tokens or NFTs from the victim's wallet.

Deepfake promotion
AI-generated video or audio content that impersonates a real person to promote fraudulent investments.

Pig butchering
A long-form social engineering scam where attackers build trust over weeks before convincing victims to invest in fake platforms.

Smart contract audit
Independent review of a smart contract's code to identify security vulnerabilities or fraudulent design.

CAWI
Computer-Assisted Web Interviewing — an online survey methodology for standardized data collection.

04 Institutional Validation

Cryptocurrency fraud has become one of the most closely monitored risks in digital asset markets. Regulators, blockchain analytics firms, law enforcement agencies and financial institutions have all reported a sharp increase in scam activity as crypto adoption expands globally.

Chainalysis research highlights that cryptocurrency-related fraud remains one of the largest categories of illicit crypto activity. According to its Crypto Scam Revenue report, crypto fraud generated an estimated **$12.4 billion** in illicit revenue during 2024, while "pig butchering" scams grew by nearly **40% year-over-year**. Scammers are increasingly leveraging AI, deepfakes, impersonation tactics and large-scale social engineering campaigns.

The **FBI's Internet Crime Complaint Center (IC3)** consistently identifies cryptocurrency investment fraud as one of the fastest-growing categories of financial crime. According to the FBI Internet Crime Report, internet crime losses reached a record **$16.6 billion** in 2024, with cryptocurrency investment scams accounting for a substantial share of reported financial damage.

Europol research suggests that artificial intelligence is significantly increasing the sophistication of financial fraud. The agency's IOCTA warns that AI-generated content, deepfake videos, synthetic identities and automated social engineering techniques are making fraud schemes increasingly difficult for retail investors to identify.

The **CFA Institute** emphasizes the importance of due diligence, information verification and behavioral discipline. In *Behavioral Finance: The Second Generation*, the Institute highlights that investors are frequently influenced by overconfidence, confirmation bias and narrative-driven decision-making — tendencies that weaken risk assessment and increase vulnerability to misleading information.

OECD research suggests that financial literacy alone does not fully protect investors from fraud. Many individuals understand basic financial concepts but struggle to apply risk assessment and verification practices consistently when faced with urgency or persuasive marketing. **FINRA Investor Education Foundation** research similarly finds that investor confidence often exceeds actual financial capability — fraud victims frequently display high self-confidence and optimism.

Key institutional takeaways

$12.4B
crypto fraud revenue 2024 (Chainalysis)

$16.6B
internet crime losses 2024 (FBI IC3)

+40%
pig butchering scam growth YoY (Chainalysis)

Investors seeking independent analysis of cryptocurrency projects can follow research and market insights from TU experts on Telegram: **Anton Kharitonov** (cryptocurrency market analysis) and **Viktoras Karapetjanc** (technical and macroeconomic research).

05 Theoretical Framework

TU

From a behavioral finance perspective, cryptocurrency scams succeed primarily by exploiting human psychology rather than technical vulnerabilities. Fraudulent schemes are most effective when they trigger emotional decision-making and bypass rational risk assessment.

Cognitive biases that increase vulnerability

BIAS	MECHANISM
FOMO	Encourages investors to act quickly to avoid perceived missed opportunities
Authority bias	Excessive trust in perceived experts, influencers, celebrities or public figures
Social proof	Following the actions of others, particularly during market enthusiasm
Urgency pressure	Artificial time constraints that reduce the likelihood of independent verification
Overconfidence	Overestimating one's ability to identify risks and detect fraudulent behavior

How fraudsters exploit these biases

Social engineering tactics

- Celebrity endorsements and influencer marketing
- Fabricated partnerships with well-known companies
- Manipulated social media engagement metrics
- Fabricated user testimonials and success stories

Technical & AI-enabled tactics

- Fake audit reports and security certifications
- AI-generated videos and voice recordings
- Deepfake impersonations of real people
- False scarcity claims and limited-time offers

Behavioral research suggests investors often believe they are less vulnerable to fraud than other market participants. Studies from CFA Institute, OECD/INFE and FINRA Foundation indicate confidence in one's ability to identify scams frequently exceeds actual fraud-detection capability. Effective scam prevention therefore depends not only on financial knowledge but on disciplined verification processes, critical thinking and awareness of behavioral biases.

06 Methodology & Research Team

TU

To evaluate how investors approach crypto security and scam prevention, TU conducted a proprietary CAWI study focused on fraud awareness, verification behavior and investor experience.

1,500 CRYPTO INVESTORS	**18–65** AGE RANGE
5 regions N. AMERICA · EUROPE · ASIA · LATAM · EM	**95%** CONFIDENCE
±2.5% SAMPLING DEVIATION	**CAWI** SURVEY METHOD

Eligibility: respondents who purchased cryptocurrency during the previous 24 months.

Research team

Anastasiia Chabaniuk · Author
Research design and interpretation

Chinmay Soni · Fact-checker
Data validation & statistical verification

Dan Blystone · Editor-in-Chief
Editorial & methodological supervision

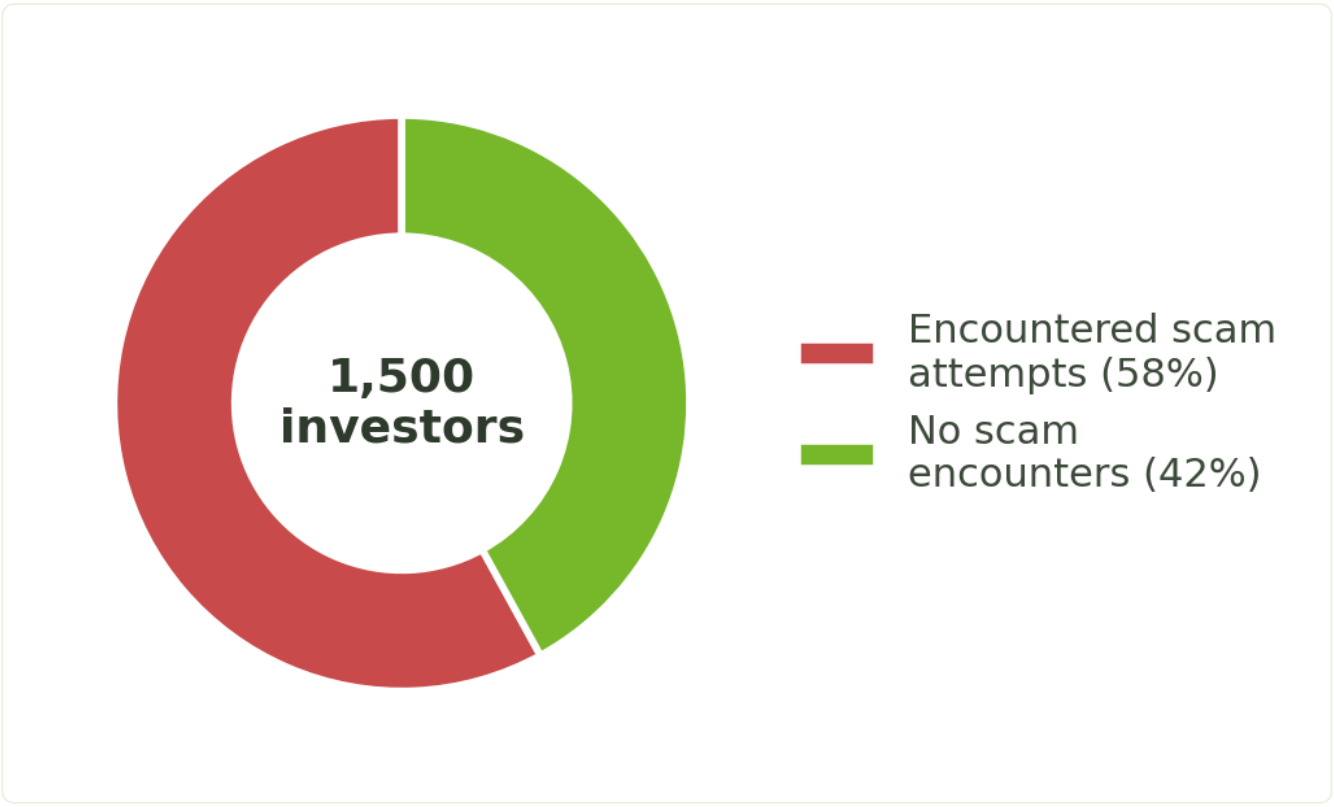
A. Mastykin · O. Tkachenko · TU Research
Data collection and analysis

07 Survey Results

TU

Scam exposure

Respondents were asked whether they had encountered any crypto scam attempt during the previous 12 months.



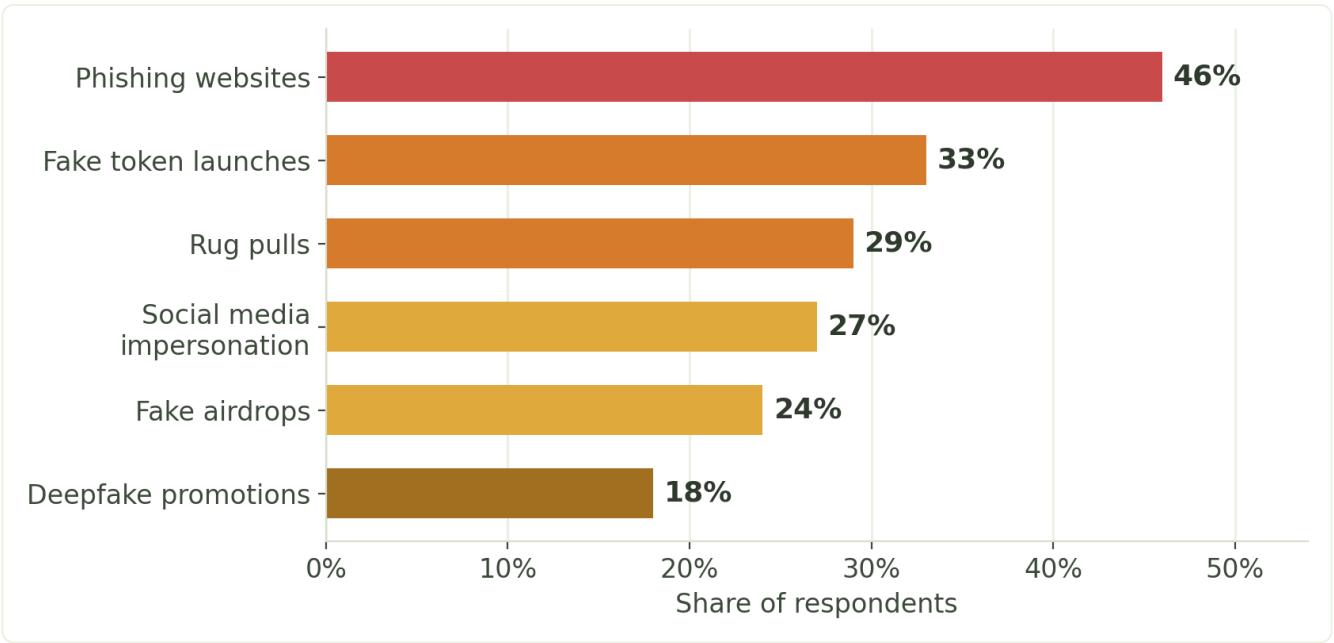
Scam attempt exposure among crypto investors (past 12 months)

INSIGHT

Scam exposure has become a normal part of crypto investing — the majority of investors now encounter at least one fraud attempt per year.

Most common scam types

Scam exposure remains widespread, but not all threats occur with the same frequency. Traditional fraud techniques continue to dominate, while newer AI-driven scams are emerging rapidly.



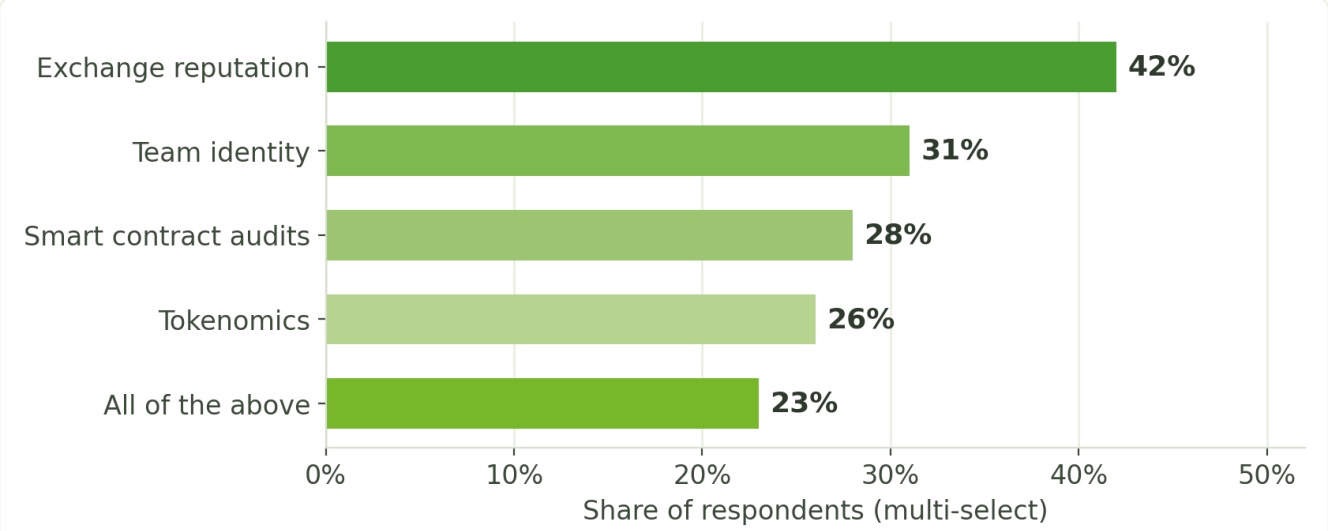
SCAM TYPE	SHARE ENCOUNTERING
Phishing websites	46%
Fake token launches	33%
Rug pulls	29%
Social media impersonation	27%
Fake airdrops	24%
Deepfake promotions	18%

INSIGHT

Traditional phishing remains more common than advanced AI scams. However, deepfake promotions at 18% are notable — this category barely existed two years ago and may rise sharply as AI tools improve.

Verification behavior

Respondents were asked what checks they perform before investing.



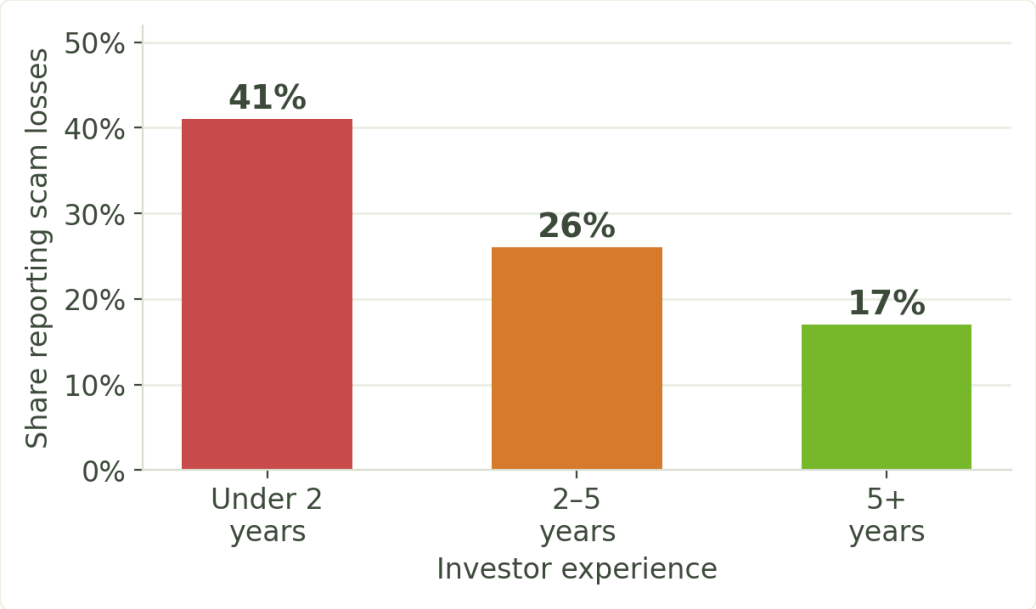
Investor verification practices (multi-select)

INSIGHT

Comprehensive due diligence remains relatively uncommon. Exchange reputation (42%) is checked most often, but smart contract audits (28%) and tokenomics (26%) — the technical checks that catch most rug pulls — remain minority practices.

Scam losses by experience

Experience appears to be one of the strongest factors influencing fraud resilience. Investors who have spent more time in the cryptocurrency market tend to develop stronger due diligence habits, better risk awareness and greater skepticism toward unusually attractive opportunities.



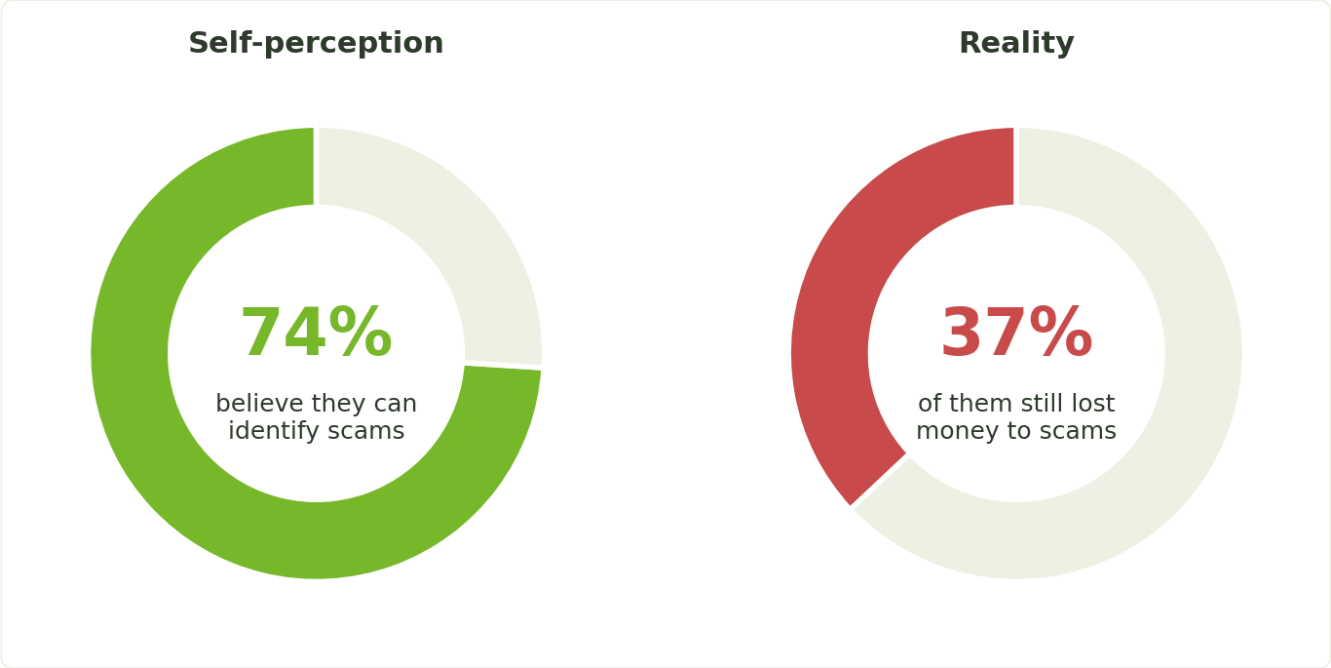
Share of investors reporting scam losses, by years of experience

INSIGHT

Experience significantly reduces vulnerability — 5+ year investors lose money at less than half the rate of newcomers. Time in the market appears to be a stronger fraud defense than financial education alone.

Self-perception vs reality

Respondents were asked whether they believe they can reliably identify crypto scams, allowing direct comparison between confidence and actual outcomes.



Self-perceived fraud detection vs actual scam losses

74%
believe they can identify crypto scams

→

37%
of them still lost money to fraudulent schemes

INSIGHT

Confidence consistently exceeds actual protection. The perception gap explains why fraud-detection campaigns often underperform — investors who most need verification are often the ones who feel they need it least.

08 Practical Implications

TU

The research suggests awareness alone is not enough to protect investors from fraud. Closing the gap between knowledge and behavior requires structured verification and behavioral discipline:

- **Always verify project teams** and official communication channels.
- **Treat urgency and guaranteed-return promises as warning signs** — legitimate opportunities rarely require immediate action.
- **Confirm smart contract audits through independent sources**, not only project websites.
- **Avoid connecting wallets to unknown applications** or signing transactions you don't fully understand.

- **Verify exchange licenses, security history and proof-of-reserves reports** before transferring significant assets.
- **Be cautious of celebrity endorsements and AI-generated content** — deepfake quality has surpassed the average investor's ability to detect it.
- **Use hardware wallets** for long-term storage to limit exposure to wallet-draining attacks.
- **Follow a structured due diligence process** before every investment — not only for unfamiliar projects.

Beyond individual verification, fraud resilience depends on the quality of the platforms used. Regulated exchanges with established security records, transparent operational practices and proven fraud-prevention infrastructure reduce exposure to a meaningful share of common scam vectors. Platform choice is itself a form of due diligence.

09 Conclusion

TU

The research confirms that crypto fraud is no longer an edge-case risk — it is a structural feature of the current market. 58% of investors now encounter scam attempts annually, phishing remains the dominant attack vector, and AI-enabled techniques are emerging fast enough that 18% of investors already encountered deepfake promotions. At the same time, only 23% perform comprehensive due diligence, and the perception gap (74% confident vs 37% actually losing money) shows that fraud awareness does not translate into protective behavior on its own.

The practical implication is direct: in crypto markets, the marginal value of additional fraud education is small; the marginal value of structured verification is large. Treating every investment as a checklist exercise — team, audit, exchange, tokenomics, security — addresses each weakness this research identifies. Experience eventually delivers the same discipline, but at the cost of losses incurred along the way. The structured route is the cheaper one.

10 Data Sources & References

TU

- Europol. *EU Serious and Organised Crime Threat Assessment (EU-SOCTA).*
- CFA Institute. *Behavioral Finance: The Second Generation.*
- OECD/INFE (2023). *International Survey of Adult Financial Literacy.*
- FINRA Investor Education Foundation. *The National Financial Capability Study.*
- FBI. *Internet Crime Report 2024 (IC3).*
- Chainalysis. *Crypto Scam Revenue 2024 — pig butchering YoY growth.*
- World Economic Forum. *Global Risks Report 2025.*
- Traders Union. *Cryptocurrency Scams List 2026.*
- Traders Union. *How To Spot Crypto Scams And Protect Your Investments.*
- IdSurvey. *CAWI Methodology Overview.*