TL;DR – Bitget Anti-Scam Month Research Report (2025)

Crypto scams have entered a new era—driven by AI deepfakes, social engineering, and deceptive project fronts. This report, co-authored by Bitget, SlowMist, and Elliptic, analyzes the most prevalent scam tactics from 2024 to early 2025 and outlines how users and platforms can respond.

The three most dangerous scam types today are:

1. Deepfake impersonation – using synthetic videos to promote fake investments;

2. Social engineering scams – including job offer Trojans, phishing bots, and fake staking offers;

3. Modern Ponzi schemes – wrapped in DeFi, NFT, or GameFi branding.

Scams now exploit trust and psychology as much as technology. From wallet takeovers to multimillion-dollar frauds, the attacks are becoming more personalized, more believable, and harder to detect.

In response, Bitget has launched an Anti-Scam Hub, strengthened platform protections, and collaborated with SlowMist and Elliptic to trace illicit funds, dismantle phishing networks, and flag scam behavior across blockchains.

The report offers real-world case studies, a scam red flags checklist, and best practices for users and institutions. Bottom line? In an age where AI can mimic anyone, security must start with skepticism—and end with collective defense.

Navigating the New Frontier: Unmasking Scams in the Evolving Crypto Landscape

1. Executive Summary

In January 2025, Hong Kong police arrested 31 members of a deepfake scam ring that stole $34 million by impersonating crypto executives—just one of 87 similar operations dismantled across Asia in Q1 alone (SlowMist, 2025 Crypto Crime Report). This isn't speculative. From AI-generated videos of Singapore's Prime Minister to fake endorsements from Elon Musk, deepfake-driven trust attacks are now a daily threat.

This report, co-authored by Bitget, SlowMist, and Elliptic, unpacks how crypto scams have evolved—from clumsy phishing attempts to AI-enhanced psychological manipulation. In 2024, nearly 40% of high-value frauds involved deepfake technology. And behind most scams—whether Trojan job offers or Ponzi-like "staking platforms"—is some form of social engineering designed to exploit trust, fear, or greed.

Crypto scams aren't just draining wallets—they're eroding trust in the industry itself.

At Bitget, our security systems intercept daily attempts to exploit user trust—spanning login anomalies, phishing attempts, and fake app downloads. In response, we've launched a dedicated Anti-Scam Hub, developed proactive user protection tools, and partnered with global leaders like SlowMist and Elliptic to dismantle scam networks and trace illicit fund flows.

This report maps the shifting threat landscape, surfaces the most dangerous tactics in play today, and outlines practical strategies for both users and institutions to build meaningful defenses. In an era where AI can mimic anyone's face, security must be skeptical by design.

2. Introduction: The Evolving Threat Landscape

Cryptocurrency's borderless design is its greatest strength—and its biggest risk. As decentralized protocols now lock over $98 billion in total value and institutional participation grows, the same technologies powering innovation are also enabling a new generation of crypto scams.

These are not the rudimentary phishing attempts of the past. The 2023–2025 cycle has seen a dramatic escalation in both scale and sophistication. In 2024 alone, global crypto users lost over **$4.6 billion** to scams—marking a **24% increase year-on-year** (Chainalysis, 2025 Crypto Crime

Report). From deepfake-led impersonations to full-blown Ponzi ecosystems disguised as “staking rewards,” scammers are now leveraging AI, psychological manipulation, and social platforms to deceive even the most seasoned users.

Three tactics dominate the threat landscape:

- **Deepfake impersonation**, often involving videos of public figures endorsing fake platforms;
- **Social engineering schemes**, from Trojan job tests to phishing tweets;
- And **Ponzi-like frauds**, repackaged under DeFi, GameFi, or NFT branding.

Most alarming is the psychological evolution of these threats: victims are not just tricked—they’re gradually persuaded. Scammers aren’t merely after passwords—they’re after behavioral blind spots.

But with new threats come new defenses. Collaborative innovation across the ecosystem has accelerated. Bitget’s behavioral analytics now flag suspicious patterns in real-time; Elliptic’s cross-chain forensics trace assets across multiple blockchains; and SlowMist’s threat intelligence has helped expose phishing rings across Asia.

This report synthesizes insights from real-world case studies, field research, and operational data across Bitget, SlowMist, and Elliptic. It outlines the tactics most responsible for asset losses today—and offers practical strategies for users, regulators, and platforms to push back.

Scams may evolve, but so can our defenses. This report shows how.

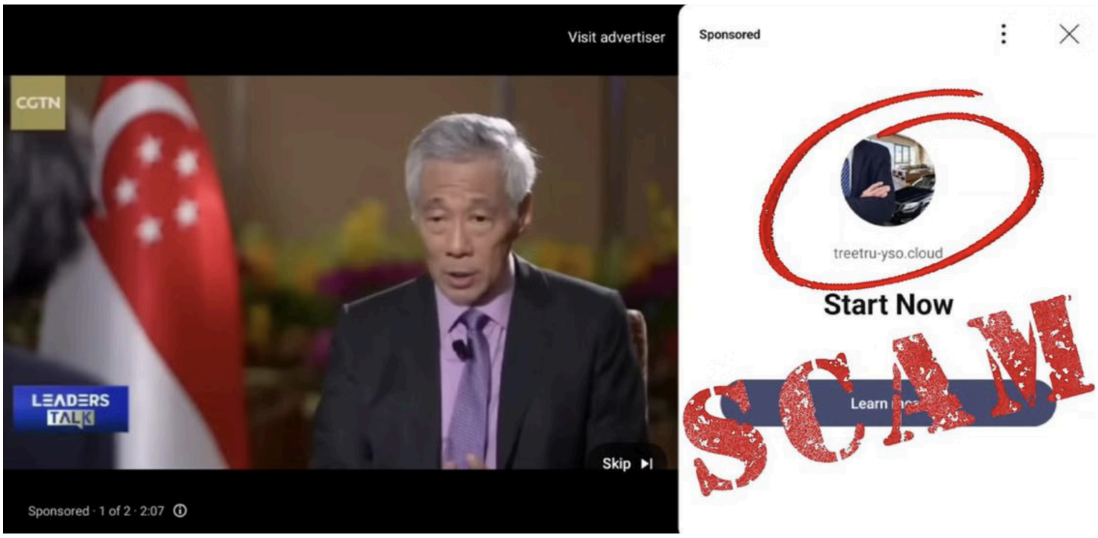
3. The Anatomy of Modern Crypto Scams: Top 10 Scams in 2024 - 2025

As blockchain technology becomes increasingly widespread and the value of crypto assets continues to rise, scams have also grown more complex, covert, and technologically advanced. A new trend has emerged, characterized by “high-tech disguises + psychological manipulation + on-chain inducement.” Over the past two years, scammers have continued to evolve their tactics by leveraging artificial intelligence, social engineering, and traditional fraud models, creating a more deceptive and damaging scam ecosystem. Among the most rampant tactics are deepfake technology, social engineering strategies, and modified Ponzi and pyramid schemes.

I. Deepfakes: The Collapse of Trust

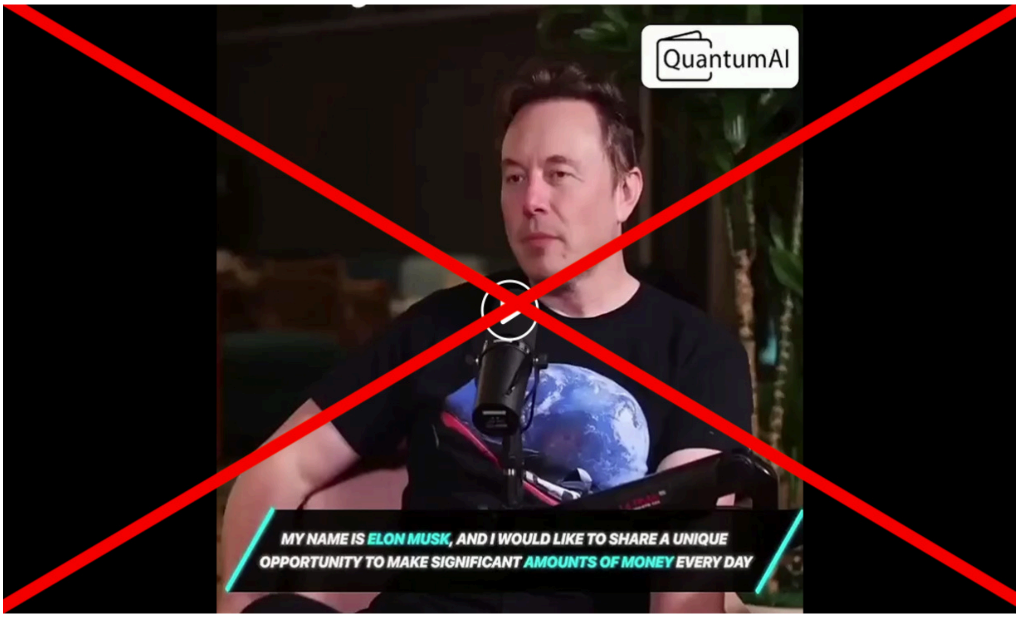
Between 2024 and 2025, the rapid advancement of generative AI has led to the swift rise of a new type of scam: trust-based fraud using deepfake technology. The essence of this tactic lies in attackers using AI synthesis tools to fabricate audio and video likenesses of well-known project founders, exchange executives, or community KOLs in order to mislead users. These fabricated materials are often highly realistic—attackers can mimic facial expressions and voice tones of their targets, and even generate videos with "official branding" in the background, making it extremely difficult for ordinary users to distinguish real from fake. Here are several typical scenarios:

(1) Deepfake Celebrity Videos Promoting Investment
Deepfake technology enables scammers to easily "invite celebrities to endorse" fraudulent schemes. For example: Videos of Singapore Prime Minister Lee Hsien Loong and Deputy Prime Minister Lawrence Wong were deepfaked and used to promote so-called "government-endorsed crypto investment platforms."



(https://www.zaobao.com.sg/realtime/singapore/story20231229-1458809)

Tesla CEO Elon Musk has also “frequently appeared” in fake investment giveaway schemes:


QuantumAI
MY NAME IS ELON MUSK, AND I WOULD LIKE TO SHARE A UNIQUE OPPORTUNITY TO MAKE SIGNIFICANT AMOUNTS OF MONEY EVERY DAY

(https://www.rmit.edu.au/news/factlab-meta/elon-musk-used-in-fake-ai-videos-to-promote-financial-scam)

These types of videos are often disseminated via social platforms such as X, Facebook, and Telegram. To create a façade of "official authority," scammers typically disable comment functions, enhancing the illusion of legitimacy and luring users into clicking on malicious links or investing in specific tokens. This form of attack exploits users' inherent trust in "authoritative figures" or "official channels," making it highly deceptive.

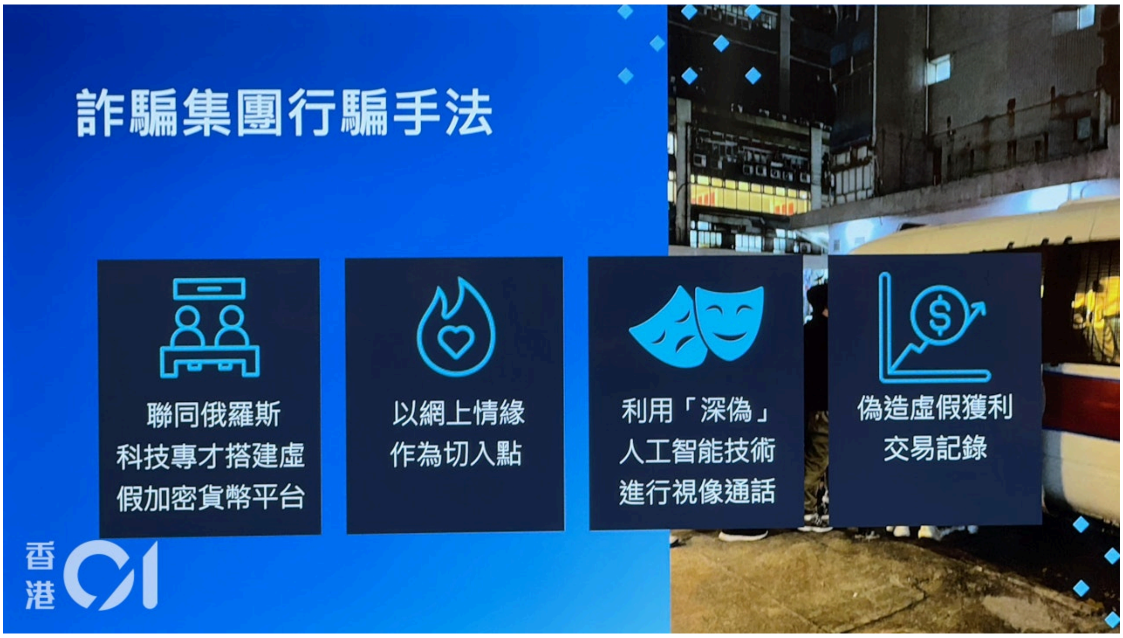
(2) Bypassing KYC Verification

Scammers use AI technology to forge facial videos, combining deepfake techniques with victims' photos to create dynamic images that can even respond to voice commands. They attempt to bypass KYC (Know Your Customer) systems of exchanges or wallet platforms in order to gain control of accounts and steal assets.

(3) Virtual Identity Investment Scams

Between 2024 and 2025, police forces in Hong Kong and Singapore have successively dismantled multiple deepfake-driven scam groups. For example, in early 2025, Hong Kong police arrested 31 suspects in a case involving a total amount of 34 million HKD, with victims spread across Singapore, Japan, Malaysia, and other Asian countries. These organizations typically exhibit the following characteristics:

- Employing graduates with media-related expertise to assist in creating sophisticated virtual identities and content.
- Setting up numerous phishing groups on Telegram, where fake identities portrayed as "highly educated, gentle, and friendly" approach targets.
- Using the scheme of "making friends → guiding investments → withdrawal obstacles" to lure users into investing in fake platforms.
- Simulating chat logs, customer service conversations, and earnings screenshots to build a "realistic and credible" illusion of platform operations.
- Creating hurdles such as "activating computing power" and "withdrawal reviews" to induce continuous top-ups, effectively constructing a Ponzi scheme.



詐騙集團行騙手法

聯同俄羅斯科技專才搭建虛假加密貨幣平台

以網上情緣作為切入點

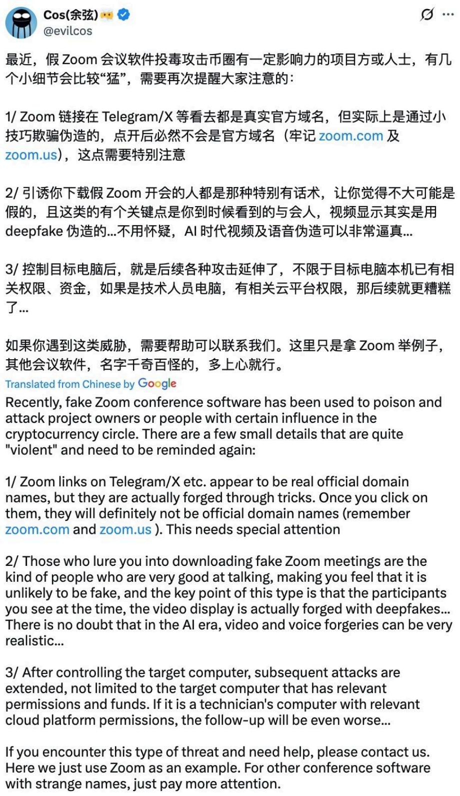
利用「深偽」人工智能技術進行視像通話

偽造虛假獲利交易記錄

(https://user.guancha.cn/main/content?id=1367957)

(4) Deepfake + Zoom Phishing

Scammers impersonate Zoom by sending fake meeting invitations with links that prompt users to download trojan-infected “meeting software.” During the meeting, the so-called “participants” may even use deepfake videos to disguise themselves as executives or technical experts, manipulating victims into further clicking, authorizing actions, or transferring funds. Once compromised, scammers can remotely control the device, steal cloud data, or private keys.



Cos(余弦)
@evilcos

最近，假 Zoom 会议软件投毒攻击币圈有一定影响力的项目方或人士，有几个小细节会比较“猛”，需要再次提醒大家注意的：

1/ Zoom 链接在 Telegram/X 等看去都是真实官方域名，但实际上是通过小技巧欺骗伪造的，点开后必然不会是官方域名（牢记 zoom.com 及 zoom.us），这点需要特别注意

2/ 引诱你下载假 Zoom 开会的人都是那种特别有话术，让你觉得不大可能是假的，且这类的有个关键点是你到时候看到的与会人，视频显示其实是用 deepfake 伪造的...不用怀疑，AI 时代视频及语音伪造可以非常逼真...

3/ 控制目标电脑后，就是后续各种攻击延伸了，不限于目标电脑本机已有相关权限、资金，如果是技术人员电脑，有相关云平台权限，那后续就更糟糕了...

如果你遇到这类威胁，需要帮助可以联系我们。这里只是拿 Zoom 举例子，其他会议软件，名字千奇百怪的，多上心就行。

Translated from Chinese by Google

Recently, fake Zoom conference software has been used to poison and attack project owners or people with certain influence in the cryptocurrency circle. There are a few small details that are quite "violent" and need to be reminded again:

1/ Zoom links on Telegram/X etc. appear to be real official domain names, but they are actually forged through tricks. Once you click on them, they will definitely not be official domain names (remember zoom.com and zoom.us). This needs special attention

2/ Those who lure you into downloading fake Zoom meetings are the kind of people who are very good at talking, making you feel that it is unlikely to be fake, and the key point of this type is that the participants you see at the time, the video display is actually forged with deepfakes... There is no doubt that in the AI era, video and voice forgeries can be very realistic...

3/ After controlling the target computer, subsequent attacks are extended, not limited to the target computer that has relevant permissions and funds. If it is a technician's computer with relevant cloud platform permissions, the follow-up will be even worse...

If you encounter this type of threat and need help, please contact us. Here we just use Zoom as an example. For other conference software with strange names, just pay more attention.

(https://x.com/evilcos/status/1920008072568963213)

From a technical perspective, these deepfake scams typically leverage AI synthesis tools such as Synthesia, ElevenLabs, and HeyGen to generate high-quality video or audio content within minutes. Once the content is created, scammers distribute it widely across platforms like X, Telegram, and YouTube Shorts.

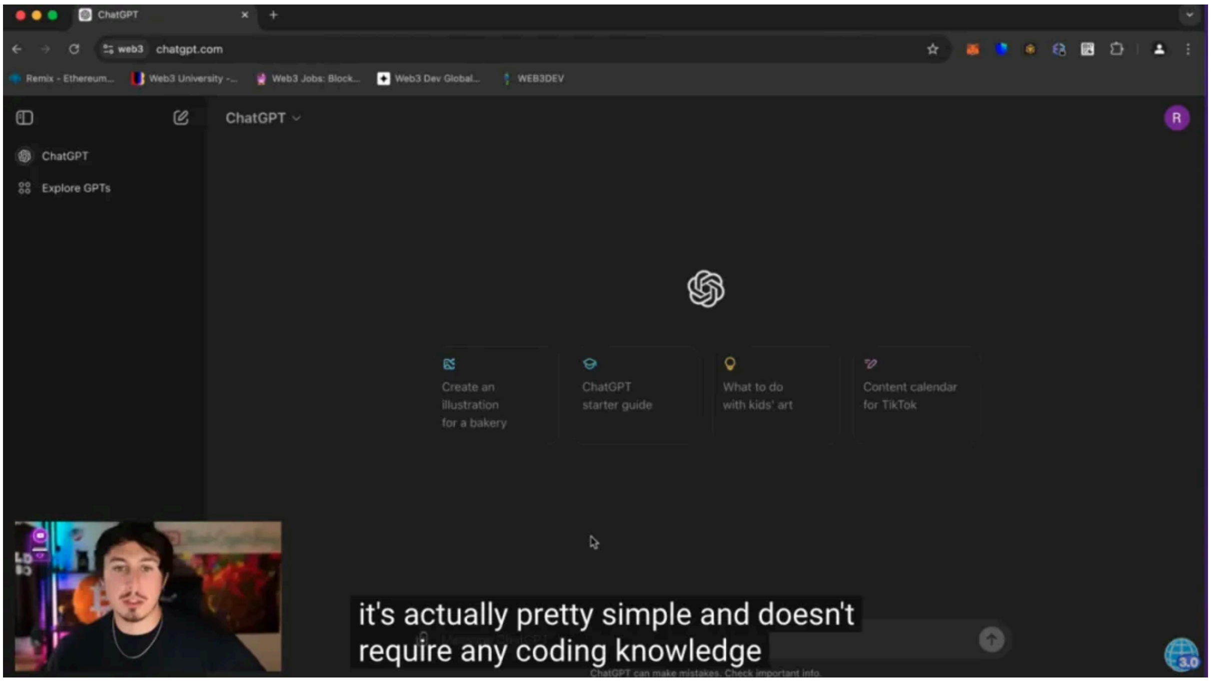
Deepfake technology is becoming a critical component in the AI-driven scam ecosystem. In the AI era, the credibility of visual and auditory content has significantly declined. Users must verify any “authoritative information” related to asset operations through multiple channels and avoid blindly trusting “familiar faces or voices.” At the same time, project teams should acknowledge the brand risks posed by AI forgery and establish a sole trusted channel for information dissemination, or employ on-chain signature broadcasting for identity verification, thereby mechanistically resisting forgery attacks.

II. Social Engineering Strategies: Exploiting Psychology

Complementing high-tech methods are low-tech yet highly effective social engineering attacks. People are the weakest and most overlooked link, causing many users to underestimate the threats posed by social engineering. Scammers often manipulate user behavior through disguise, guidance, intimidation, and other tactics, exploiting psychological vulnerabilities to gradually achieve their fraudulent goals.

(1) AI Arbitrage Bot Scams

AI has become a hallmark technology for boosting productivity, and scammers have quickly jumped on this trend by labeling their schemes with “ChatGPT”—a buzzword that sounds cutting-edge and credible, thereby lowering users’ guard.



it's actually pretty simple and doesn't require any coding knowledge

The scam usually starts with a detailed video tutorial. In the video, the scammer claims that the arbitrage bot’s code is generated using ChatGPT, which can be deployed on blockchains like Ethereum to monitor new token launches and price fluctuations, conducting arbitrage through flash loans or price differences. They emphasize that “the bot automatically completes all the logic for you, and you only need to wait for the profits to arrive.” This narrative strongly aligns with many users’ preconceived notion that “AI = easy money,” further lowering their guard.

With packaging language that reduces the user’s technical threshold, users are guided to visit a highly simulated Remix IDE interface (which is actually a fake page). From the interface alone, it is difficult to distinguish real from fake. Users are asked to paste the so-called “contract code written by ChatGPT.” After deployment, users are told to inject startup funds into the contract address as the initial arbitrage principal, while the scammers imply that “the more you invest, the higher the returns.” Once users complete these steps and click the “Start” button, what awaits them is not a steady stream of arbitrage profits but a complete loss of control over their funds. Because the code users copy and paste already contains backdoor logic—once the contract is activated, the injected ETH is immediately transferred to a wallet address preset by the scammers. In other words, the entire “arbitrage system” is essentially a beautifully packaged money-grabbing tool.

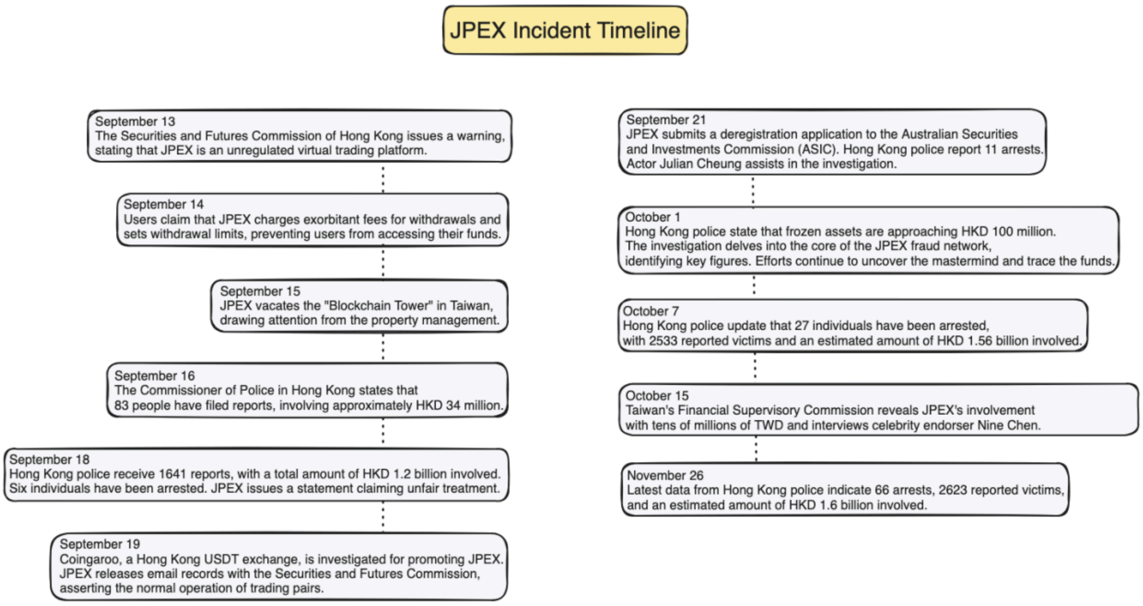
SlowMist’s analysis reveals that these scams often employ a “wide net with small inducements” strategy. Each victim’s loss may only amount to tens or hundreds of dollars. Although the amounts are relatively small, scammers still achieve steady and considerable illegal profits by distributing tutorials on a large scale and luring many users into the trap. Because each victim loses only a modest sum and the process appears to be “self-operated” rather than a direct fraudulent transfer, most victims choose to accept their loss and do not pursue further investigation. What is even more alarming is that these scams are easily rebranded and relaunched: by simply changing the bot’s name or swapping a few page templates, scammers can go back online and continue their fraud.

Other recurring tactics under the social engineering umbrella include Trojan-laced job offers, fake interview coding assignments, phishing links seeded under tweets or in Telegram DMs, address poisoning with similar-looking wallet strings, “Pi Xiu” honeypot tokens that block selling, and rebate scams disguised as staking platforms. These schemes prey on either trust (via personal outreach), greed (via exaggerated returns), or confusion (via fake interfaces and chat logs). While their wrappers change, the outcome is the same—loss of funds through subtle, self-initiated compromise.

III. Ponzi Schemes: Old Tricks with a New Facade

Despite the rapidly evolving crypto ecosystem, traditional Ponzi schemes and pyramid scams have not disappeared; instead, they have undergone a “digital evolution” by leveraging on-chain tools, social viral growth, and AI-powered deepfakes. These scams typically disguise themselves in new concepts like DeFi, NFTs, and GameFi, packaged as project fundraising, liquidity mining, or platform token staking. Fundamentally, they remain classic Ponzi schemes where “new money fills old holes.” Once the cash flow breaks or the operators cash out and exit, the entire system collapses quickly.

A notable example that shook Hong Kong in 2023 was the JPEX incident. This platform, claiming to be a “global cryptocurrency exchange,” heavily promoted itself through local physical advertisements and celebrity endorsements, pushing its platform token JPC, which promised “high and stable returns.” Operating without regulatory approval and with a severe lack of disclosure, it lured a large number of users. In September 2023, the Hong Kong Securities and Futures Commission publicly named it “highly suspicious,” followed by a police crackdown known as the “Iron Gate Operation,” resulting in multiple arrests. By the end of 2023, the case involved over 1.6 billion HKD and more than 2,600 complainants, potentially making it one of the largest financial fraud cases in Hong Kong’s history.



JPEX Incident Timeline

September 13
The Securities and Futures Commission of Hong Kong issues a warning, stating that JPEX is an unregulated virtual trading platform.

September 14
Users claim that JPEX charges exorbitant fees for withdrawals and sets withdrawal limits, preventing users from accessing their funds.

September 15
JPEX vacates the "Blockchain Tower" in Taiwan, drawing attention from the property management.

September 16
The Commissioner of Police in Hong Kong states that 83 people have filed reports, involving approximately HKD 34 million.

September 18
Hong Kong police receive 1641 reports, with a total amount of HKD 1.2 billion involved. Six individuals have been arrested. JPEX issues a statement claiming unfair treatment.

September 19
Coingaroo, a Hong Kong USDT exchange, is investigated for promoting JPEX. JPEX releases email records with the Securities and Futures Commission, asserting the normal operation of trading pairs.

September 21
JPEX submits a deregistration application to the Australian Securities and Investments Commission (ASIC). Hong Kong police report 11 arrests. Actor Julian Cheung assists in the investigation.

October 1
Hong Kong police state that frozen assets are approaching HKD 100 million. The investigation delves into the core of the JPEX fraud network, identifying key figures. Efforts continue to uncover the mastermind and trace the funds.

October 7
Hong Kong police update that 27 individuals have been arrested, with 2533 reported victims and an estimated amount of HKD 1.56 billion involved.

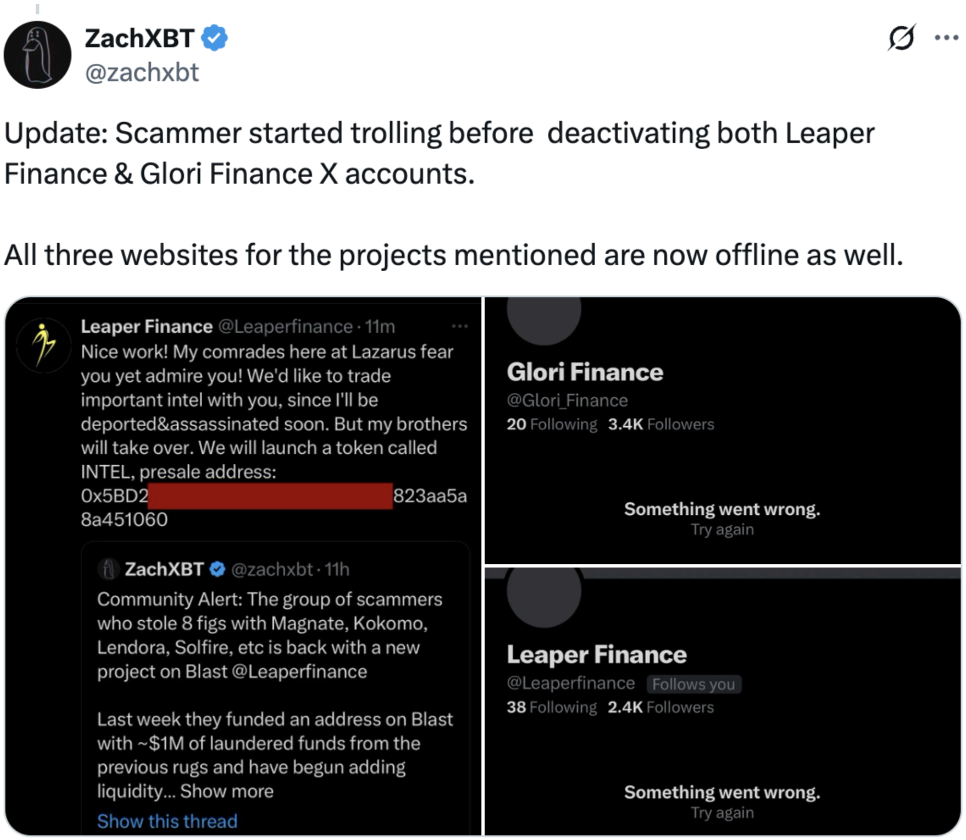
October 15
Taiwan's Financial Supervisory Commission reveals JPEX's involvement with tens of millions of TWD and interviews celebrity endorser Nine Chen.

November 26
Latest data from Hong Kong police indicate 66 arrests, 2623 reported victims, and an estimated amount of HKD 1.6 billion involved.

Moreover, the typical patterns of on-chain Ponzi projects continue to evolve. In 2024, blockchain analyst ZachXBT exposed a notorious scam gang deploying a new project called Leaper Finance on the Blast chain. This group had previously operated multiple projects such as Magnate, Kokomo, Solfire, and Lendora, cumulatively stealing tens of millions of dollars. They used forged KYC documents and fake audit reports, laundered funds in advance, and artificially inflated on-chain metrics to lure users into investing. After the project's TVL (Total Value Locked) surged to several million dollars, they quickly drained the liquidity in a classic "Rug Pull" exit.

What's more alarming is that this group repeatedly targeted multiple mainstream chains including Base, Solana, Scroll, Optimism, Avalanche, and Ethereum, employing a rapid "skin change and rebrand" scam rotation.

For example, their Zebra Lending project deployed on the Base chain once reached a TVL of over $310,000; on Arbitrum, their Glori Finance project hit a peak TVL of $1.4 million. Both projects were forks of Compound V2. These projects used capital extracted from other scams like Crolend, HashDAO, and HellHoundFi as seed funds, creating a closed loop of fraud.



ZachXBT @zachxbt

Update: Scammer started trolling before deactivating both Leaper Finance & Glori Finance X accounts.

All three websites for the projects mentioned are now offline as well.

Leaper Finance @Leaperfinance · 11m
Nice work! My comrades here at Lazarus fear you yet admire you! We'd like to trade important intel with you, since I'll be deported&assassinated soon. But my brothers will take over. We will launch a token called INTEL, presale address:
0x5BD2[redacted]823aa5a 8a451060

ZachXBT @zachxbt · 11h
Community Alert: The group of scammers who stole 8 figs with Magnate, Kokomo, Lendora, Solfire, etc is back with a new project on Blast @Leaperfinance

Last week they funded an address on Blast with ~$1M of laundered funds from the previous rugs and have begun adding liquidity... Show more

Show this thread

Glori Finance
@Glori_Finance
20 Following 3.4K Followers

Something went wrong.
Try again

Leaper Finance
@Leaperfinance Follows you
38 Following 2.4K Followers

Something went wrong.
Try again

Compared with traditional Ponzi schemes, digital scams have the following new characteristics:

- Stronger technical disguise: They create an illusion of “technical innovation” by leveraging open-source smart contracts, NFT packaging, and accumulation of on-chain data, misleading users into believing these are legitimate, compliant DeFi products.
- Complex rebate structures: Using terms like “yield farming,” “staking rewards,” and “node dividends” to cloak the flow of funds, the actual operation involves multiple layers of siphoning and internal-external market manipulation.
- Social fission propagation: They heavily rely on WeChat groups, Telegram channels, and KOL livestreams to drive users to invite new members, forming a classic pyramid-style viral spread model.
- Gamified interfaces and identity forgery: More projects adopt game-like UIs and use NFTs as project mascots to create a “youthful” and “legitimate” image. Some even combine AI face swapping and Deepfake technology to forge images or videos of project founders or endorsers, increasing credibility.

For example, in February 2025, hackers hijacked the Twitter (X) account of Tanzanian billionaire Mohammed Dewji and used Deepfake technology to forge videos promoting a fake token, $Tanzania, raising $1.48 million within hours. Similar forgeries have been widely used to fake founder videos, fabricate meeting screenshots, and create fake team photos, making it increasingly difficult for victims to discern authenticity.

For a quick overview, refer to the Scam Red Flags Table below, which summarizes key warning signs and simple defenses.

Scam Type	Common Signs	How to Protect Yourself
Deepfake Impersonation	“Official-looking” videos of CEOs, officials, or KOLs promoting investments	Always verify via official site or announcement channels
AI Arbitrage Bot Scam	YouTube tutorials claiming “auto-profit” bots with ChatGPT-generated code	Never deploy code from unknown sources or fund contracts blindly
Trojan Job Offers	LinkedIn offers followed by urgent test links or cloned coding tasks	Run code in sandbox; confirm with company directly
Phishing Comments (X/Twitter)	Top tweet replies linking to fake airdrops or staking pages	Never click links from social media comments; verify the source
Address Poisoning	Small incoming transfers from lookalike wallet addresses	Use your wallet’s address book and double-check every transaction
Pi Xiu Honeypot Tokens	A new token pumps quickly—but you can’t sell it	Check contract functions before buying; avoid “guaranteed” profits
Fake Staking/Miner Rebates	Telegram offers with “double returns,” fake dashboards, or staged user chats	Avoid projects that offer rebates for deposits with no on-chain logic
Airdrop Traps	Free tokens appear in wallet that lead to phishing links or malicious contracts	Don’t interact with unsolicited tokens or sites asking for approvals

How to stay protected: Be skeptical of unsolicited contact—whether via LinkedIn, Telegram, or email. Never run unfamiliar code or install files from strangers, especially under the guise of job tests or app demos. Bookmark official sites, use browser plugins like Scam Sniffer, and never connect wallets to unknown links. Trust isn’t just earned in crypto—it must be verified.

4. Fortifying the Digital Frontier: Bitget's Multi-Layered Security Architecture

In an era where sophisticated cyber threats increasingly target digital assets, Bitget has architected a comprehensive security framework designed to protect users at every touchpoint. This section delineates the strategic measures implemented across account protection, investment scrutiny, and asset safeguarding.

1) Account Protection: Proactive Measures Against Unauthorized Access

Bitget employs a suite of real-time monitoring tools to detect and alert users of any anomalous activities. Upon logging in from a new device, users receive detailed email notifications encompassing anti-phishing codes, verification codes, login locations, IP addresses, and device specifics. This immediate feedback loop enables users to identify and address unauthorized access attempts promptly.

To mitigate impulsive actions potentially induced by scams, Bitget has instituted a dynamic cooling-off period. Triggered by indicators such as unusual login locations or suspicious transactions, this mechanism imposes a temporary suspension on withdrawals—ranging from one to twenty-four hours—allowing users to reassess and confirm the legitimacy of waccount activities.

Furthermore, Bitget offers an official verification channel, allowing users to authenticate communications and effectively prevent phishing attacks.

2) Investment Scrutiny: Rigorous Evaluation of Digital Assets

Recognizing the proliferation of high-risk tokens in the crypto market, Bitget has developed an exhaustive due diligence process for asset listing. This includes comprehensive background checks on project teams, in-depth analyses of tokenomics, assessments of valuation and distribution models, and evaluations of community engagement levels.

To further fortify this process, Bitget implements a dual-layer security audit system. Internal blockchain security engineers conduct meticulous code reviews to identify vulnerabilities. At the same time, external audits by esteemed third-party firms provide an additional layer of scrutiny. Post-listing, Bitget's proprietary on-chain monitoring system continuously surveils transactions and contract interactions in real time. This system is designed to adapt and evolve, continually updating its threat models to respond promptly to emerging risks.

3) Asset Safeguarding: Comprehensive Protection of User Holdings

Bitget employs a dual-wallet strategy, utilizing both hot and cold wallets to enhance security. The majority of digital assets are stored in offline, multi-signature cold wallets, significantly reducing exposure to cyberattacks.
Complementing this, Bitget maintains a substantial Protection Fund, valued at over $300 million, to compensate users in the event of platform-related security incidents.

For Bitget Wallet users, additional security features include phishing website alerts, built-in contract risk detection tools, and the innovative GetShield security engine. GetShield continuously scans decentralized applications, smart contracts, and websites, detecting potential threats before user interaction.

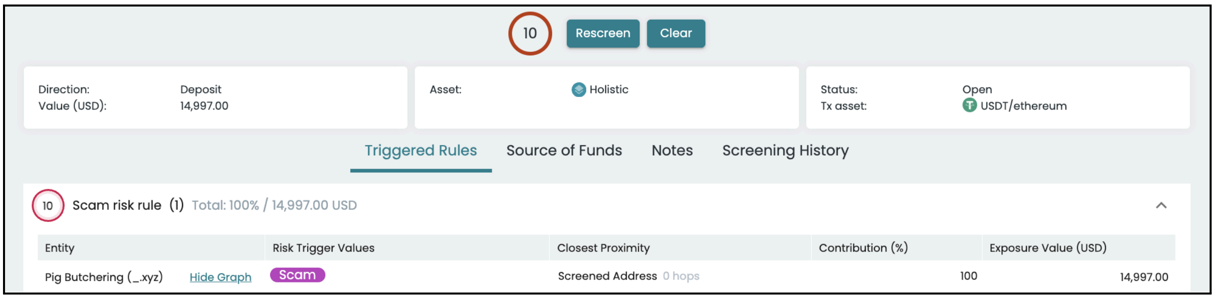
Through this multi-faceted security approach, Bitget not only safeguards user assets but also reinforces trust in its platform, setting a benchmark for security standards in the cryptocurrency exchange industry.

5. Tracking and flagging scam-related funds on the blockchain

Earlier sections of this report described how scammers obtain cryptocurrency through a variety of methods, including by using deepfake technology. Scammers will typically attempt to move the cryptocurrency they've acquired elsewhere and ultimately convert it to fiat currency. These movements can be tracked, especially with the help of blockchain analytics tools. Blockchain analytics tools fall into three main categories: 'transaction monitoring', 'address screening', and investigative tools. This section considers how transaction monitoring tools help detect and flag scam-related funds, making it more difficult for scammers to use their stolen cryptocurrency.

Transaction monitoring tools are widely used by cryptocurrency exchanges, including Bitget. The tools scan incoming and outgoing transactions with the aim of identifying and flagging potential risk. A common use case would be checking every user deposit received to identify potential risks. Most user deposits (i.e., those by normal users) will not be identified as high-risk, the deposit will be processed automatically and the user's account will be credited almost instantaneously. A deposit of funds originating from a known scam will be flagged as high-risk.

It is possible to look at real examples of transaction monitoring in action. The image below shows a user deposit to a cryptocurrency exchange being analysed by a transaction monitoring tool. In this case, the tool identifies that the funds are being sent by an address associated with a 'pig butchering' investment scam. The tool assigns the transaction a maximum risk score of 10/10. As a result, the user's account will not be automatically credited, and the activity will be escalated for manual review by the business's compliance team.



Direction: Deposit
Value (USD): 14,997.00

Asset: Holistic

Status: Open
Tx asset: USDT/ethereum

10 Scam risk rule (1) Total: 100% / 14,997.00 USD

Entity	Risk Trigger Values	Closest Proximity	Contribution (%)	Exposure Value (USD)
Pig Butchering (_.xyz) Hide Graph	Scam	Screened Address 0 hops	100	14,997.00

Sophisticated illicit entities are aware of transaction monitoring tools. These illicit entities sometimes undertake particular on-chain transactions to attempt to obfuscate (i.e., hide) their funds. One common example is 'layering' of funds: sending funds through numerous intermediary addresses in an attempt to separate them from their origin. Sophisticated transaction monitoring tools therefore trace through unlimited intermediary addresses, allowing the criminal origin of the funds to be identified. Illicit entities have also been seen to increasingly utilise cross-chain bridging; this is focussed on in the next subsection.

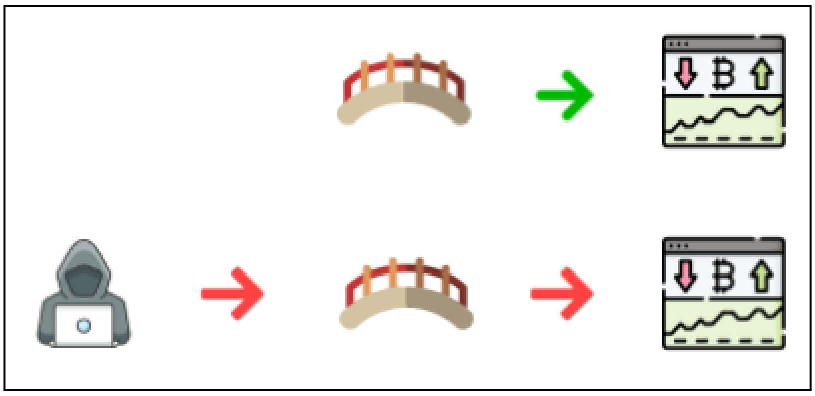
5.1. Cross-chain bridging

A wide range of blockchains have been introduced in the last several years. Users may be drawn to a particular blockchain as it hosts specific cryptocurrencies, decentralised applications or other services. Cross-chain bridges enable users to transfer value from one blockchain to another, in many cases, almost instantaneously. While bridges are primarily used by everyday blockchain users, they are increasingly being exploited by illicit entities, including scammers, to move funds between different blockchains. There are several reasons a scammer may use cross-chain bridges, including:

- **Accessing obfuscation opportunities:** Certain obfuscation services may only be available on certain blockchains. For example, many cryptocurrency mixer websites only handle Bitcoin. Illicit entities are known to bridge onto one blockchain to utilise a particular obfuscation service, and then bridge away to another blockchain afterwards.

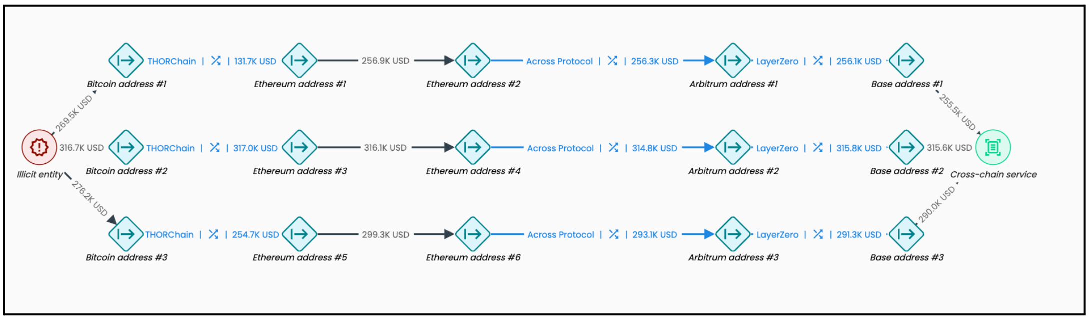
- **Reduced tracking:** Moving funds between blockchains can increase the difficulty of following the funds. Even if an investigator can manually follow a single cross-chain movement, repeated cross-chain transfers can slow down the investigator considerably, and make it less viable for the investigator to manually follow all trails if the funds have been split up (a case study below shows how, with certain tools, tracing these cross-chain funds introduces no additional work for the investigator).

Additionally, illicit entities know that some automated transaction monitoring tools may stop tracing a bridge. The top part of the image below represents a transaction monitoring tool that stops at bridges when traversing the blockchain to identify potential illicit activity. Using these types of tools, a cryptocurrency exchange checking a deposit can only see the funds coming from the bridge and cannot see further. The bottom of the image shows Elliptic's transaction monitoring tool, which is used by Bitget. It automatically traces through the example bridge, ensuring visibility of the illicit entity involved in this particular activity.



The case study below describes how one illicit entity utilises a range of bridges and blockchains in a large-scale and systematic attempt to launder cryptocurrency, and how the activity can be seen in certain tools.

Case study: The screenshot of Elliptic's Investigator tool below shows how an illicit entity uses cross-chain bridges to move funds across multiple blockchains before ultimately depositing them at a cryptocurrency service.



Focusing on the top row, activity starts on the left with the entity holding funds on the Bitcoin blockchain, the entity then bridges the funds to Ethereum, transfers the funds to another address on Ethereum, and subsequently bridges to Arbitrum, then to Base, before depositing the funds into a service. The image highlights two additional instances where the same exact pattern is repeated. Although not shown here, this same pattern occurs more than ten additional times, reflecting a highly systematic effort to launder the funds.

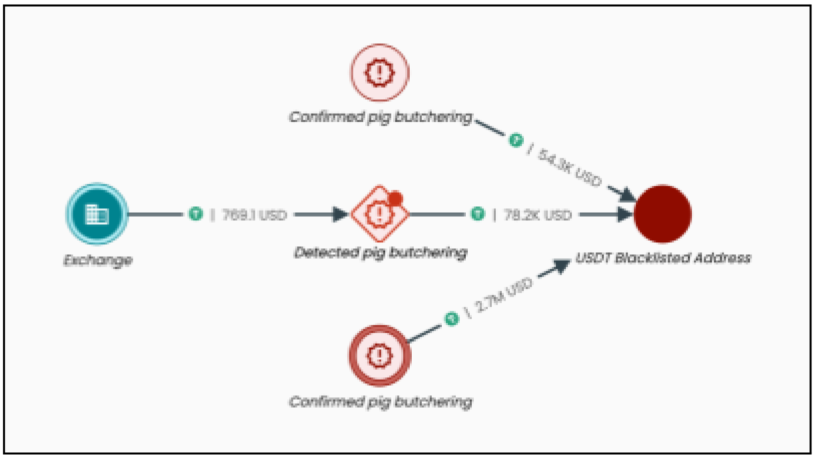
The objective behind this behaviour appears to be twofold: first, to delay or disrupt investigators tracing the flow of funds; and second, to prevent the receiving cryptocurrency service from easily identifying the funds' illicit origin. However, with the help of a blockchain investigation tool like the above that supports automated cross-chain bridge tracing, investigators can follow these movements seamlessly. Similarly, transaction monitoring tools with bridge-tracing capabilities, such as Elliptic's, which is utilised by Bitget, can automatically detect the full path of the funds back to the illicit entity.

5.2 How behaviours and patterns can be used to detect scam funds

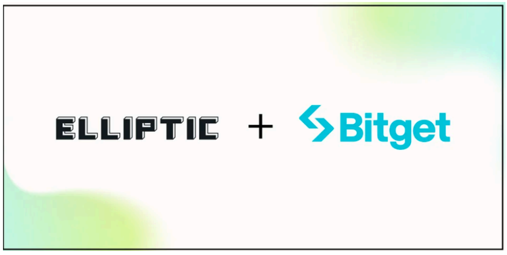
The earlier examples involved cryptocurrency addresses known to be used by illicit entities, for example, addresses used in pig butchering scams. Address attributions like this often come from working with victims and law enforcement, as well as from numerous other data collection approaches. The huge scale at which scams are now perpetrated (as well as other factors including underreporting) means that not all addresses can always be identified through these approaches.

Because of this, some transaction monitoring tools incorporate behaviour-based detection as an additional line of defence. Behaviours and patterns are automatically analysed to deduce whether a particular address is performing on-chain actions that align with scam activity, and interactions with such addresses can be flagged appropriately. This behavioural analysis is typically conducted through purpose-built behavioural detection models, some of which leverage machine learning approaches. At the time of writing, Elliptic's behavioural detection methods can identify over 15 types of scams, including 'pig butchering', 'address poisoning', and 'ice phishing'; detection capabilities are always expanding.

The example below illustrates how behavioural detection can help prevent potential victims from sending cryptocurrency to scam-related addresses. The example includes three addresses associated with a pig butchering scam. The top and bottom addresses were identified through victim reports. The middle address had not been previously reported, but was flagged by behavioural detection as potentially involved in pig butchering activity.



A payment from a cryptocurrency exchange was made to this detected address. Had the exchange used behavioural detection alerts, the risk could have been identified prior to the exchange sending the transaction, potentially preventing users from losing funds. All three 'pig butchering' addresses eventually then sent funds to another address, which was subsequently blacklisted by Tether. This froze the USDT that the address held - further confirming the illicit nature of the funds involved.



Click here to read about how Bitget improved its risk prevention by 99% through utilising Elliptic's blockchain analytics tools; these industry leading tools support over 50 blockchains and feature automated cross-chain bridge tracing and behavioural detection.

6. Recommendations and Best Practices

Faced with an ever-evolving array of scam tactics, users must cultivate clear self-protection awareness and technical identification skills. To this end, SlowMist proposes the following core anti-fraud recommendations:

(1) Enhance the ability to discern authenticity of social media content
Never click on any links in comment sections or group chats—even if they appear "official." For critical actions such as wallet connections, airdrop claims, or staking operations, always verify through the project's official website or trusted community channels. It is recommended to install security plugins like Scam Sniffer to detect and block phishing links in real time, reducing the risk of accidental clicks.

(2) Be cautious of risks introduced by AI tools
With the rapid advancement of large language models, various new AI tools have emerged. The MCP (Model Context Protocol) standard implementation has become a key bridge connecting LLMs with external tools and data sources. However, the widespread adoption of MCP also brings new security challenges. SlowMist has published a series of MCP security articles, advising relevant project teams to conduct self-assessments and reinforce defenses in advance.

(3) Leverage on-chain tools to identify risky addresses and Ponzi scheme traits
For tokens suspected to be "rug pulls" or fraudulent projects, it is recommended to use anti-money laundering and tracking tools such as MistTrack to check project-related address risks or quickly assess through GoPlus's Token Security Detection tool. Combine this with platforms like Etherscan or BscScan to see if victims have issued warnings in comment sections. Exercise heightened caution with high-yield projects, as abnormally high returns often imply extremely high risk.

(4) Do not trust "scale" or "success stories" blindly
Scammers often fabricate an atmosphere of profitability through large Telegram groups, fake KOL endorsements, and fake profit screenshots. Generally, projects can be transparently verified through GitHub repositories, on-chain contract audits, and official website announcements. Users should learn to independently verify information sources.

(5) Beware of Social-Trust-Based “File-Induction” Attacks

An increasing number of attackers use platforms like Telegram, Discord, and LinkedIn to send malicious scripts disguised as job offers or technical test invitations, luring users into executing high-risk files.

For users:

- Be vigilant about suspicious job or freelance offers that require downloading or running code from platforms such as GitHub. Always verify the sender’s identity through the company’s official website or email, and avoid falling for enticing phrases like “limited-time high-paying tasks.”
- When handling external code, strictly review the project source and author background; refuse to run unverified high-risk projects. It is recommended to execute suspicious code within virtual machines or sandbox environments to isolate potential risks.
- Stay cautious with files received on Telegram, Discord, and similar platforms: disable auto-downloads, manually scan files, and be wary of requests to run scripts under the guise of “technical tests.”
- Enable multi-factor authentication and regularly update strong passwords, avoiding password reuse across platforms.
- Do not click on any meeting invitations or software download links from unknown sources. Develop a habit of verifying domain legitimacy and confirming official platform origins.
- Use hardware wallets or cold wallets to manage large assets, minimizing exposure of sensitive information on internet-connected devices.
- Regularly update your system and antivirus software to maintain protection against the latest malware and viruses.

If you suspect your device is infected, immediately disconnect from the internet, transfer funds to safe wallets, remove malicious programs, and if necessary, reinstall the operating system to minimize losses.

For enterprises:

- Regularly organize phishing simulation exercises to train employees in identifying spoofed domains and suspicious requests.
- Deploy email security gateways to block malicious attachments and continuously monitor code repositories to detect any leakage of sensitive information.
- Establish a phishing incident response mechanism that integrates technical defenses with employee awareness. This multi-layered strategy helps minimize the risks of data breaches and asset losses.

(6) Remember the “Fundamental Principles” for Investment Judgment

- High returns promised = high risk: Any platform claiming “stable high returns” or “guaranteed profits” should be treated as highly risky.

- Referral-based viral growth is a typical red flag: Projects that reward users for recruiting others or set up “team bonus” mechanisms can generally be preliminarily identified as pyramid schemes.
- Use on-chain analysis tools to identify abnormal fund flows: Platforms like MistTrack can help track large irregular fund movements and analyze cash-out paths of teams.
- Verify audit firms and team transparency: Some projects rely on “fake audit reports” or audits by small firms as a formality. Users should check if the smart contracts are audited by credible third-party firms and if audit reports are publicly available.

In summary, crypto scams in the AI era have evolved from mere “tricks” to a combination of “technical and psychological” manipulations. Users must both improve technical recognition capabilities and strengthen psychological defenses:

- Verify more, act less impulsively: Never blindly trust something just because it comes from “someone familiar, an authoritative video, or an official background.”
- Ask more questions, transfer less funds: For any asset-related operation, clarify the underlying principles, verify sources, and confirm security.
- Be less greedy, be more skeptical: The more a project promises “guaranteed profits,” the more caution is needed.

Meanwhile, users are encouraged to study the Blockchain Dark Forest Selfguard Handbook authored by SlowMist founder Cos, to master fundamental on-chain anti-scam knowledge and build an additional layer of self-protection. In case of theft, users can seek assistance from the SlowMist team.

Only by fully understanding scam mechanisms, enhancing information discrimination ability, increasing awareness of security tools, and strengthening operational safety practices can users safeguard their assets in this digital era filled with temptations and risks. Security is not a one-time action but a continuous state of awareness. Building a complete cognitive system and fundamental defense habits is the only way to navigate steadily through the digital age and avoid scam pitfalls.

7. Conclusion: Charting the Path Forward

Five years ago, avoiding scams meant “don’t click suspicious links.” Today, it’s “don’t trust your own eyes.”

As AI-generated videos, fake recruitment pipelines, and tokenized Ponzi schemes redefine how trust is weaponized, the next stage of crypto security depends not just on smarter tech—but on collective defense. Bitget, SlowMist, and Elliptic are already collaborating to share intelligence, automate fund tracing, and flag behavioral red flags across ecosystems.

The takeaway is clear: security can't rely on isolated measures. It must be networked, continuous, and user-centric.

That's why Bitget is doubling down on:

- **AI red-teaming** to test vulnerabilities against emerging scam tactics
- **Collaborative data sharing** with compliance partners and regulators
- **Education initiatives**, like the Anti-Scam Hub, to equip users with real-time threat awareness

Scammers will keep evolving. So must we. Because in this industry, the most valuable currency isn't Bitcoin—it's trust.