Web3 反欺詐手冊

Web3 反欺詐手冊

2024.10

目录

前言

嗨，所有讀到這本 Web3 反欺詐手冊的朋友們，你好。

當下 Web3 行業的規模體量已經得到了極大的擴張。根據 @CMC 的數據統計，截至本手冊開始寫作的 2024 年 8 月末，加密市場總規模已經達到 2 萬億美元，相當於英偉達總市值的三分之二，或者港股總市值的一半。

加密資產總市值

而這些快速增長的產業大多發生在不受監管的場景下，在一定程度上不可避免地招致了違法犯罪活動的污染。因此，不論你是剛剛才開始了解加密貨幣的新手，還是已經有非常豐富鏈上互動經驗的 OG，相信你都或多或少會對來自內部或外部對加密行業的負面批評——諸如「加密貨幣是洗錢工具」、「加密貨幣錢包並不安全」、「詐騙空氣幣橫行」等言論有所耳聞。

儘管這類指責通常過分誇大甚至扭曲事實，但對任何一個普通 Web3 用戶而言，這個市場都不像傳統金融市場那樣安全，稍有不慎，一筆交易甚至一個簽名都有可能讓你損失掉賬戶地址裡所有的錢。

為此我們撰寫了這本反詐防騙手冊，嘗試通過對不同階段用戶可能遭遇的欺詐手段進行詳細拆解，以幫助讀者朋友們識別並規避這些威脅，相信對新手小白與幣圈老手都有所幫助。

接下來，讓我們開始吧。

糟糕的信息來源：你可能從一開始就被騙了

許多投資者第一次接觸 Web3 相關概念，都是在社交網站、自媒體平台、網絡社群等場景，這類場景往往魚龍混雜。成熟的投資者尚且需要在大量噪音與謠言中尋找真正有效的信息，經驗不足的投資者很難不被欺詐信息所干擾。

正因如此，許多不法分子利用客觀存在的信息壁壘，對缺乏相關知識的圈外用戶進行欺詐，手段包括扭曲或虛構事實、偷竊賬戶密鑰、騙取賬戶權限等，這也是行業被污名化的重要原因。

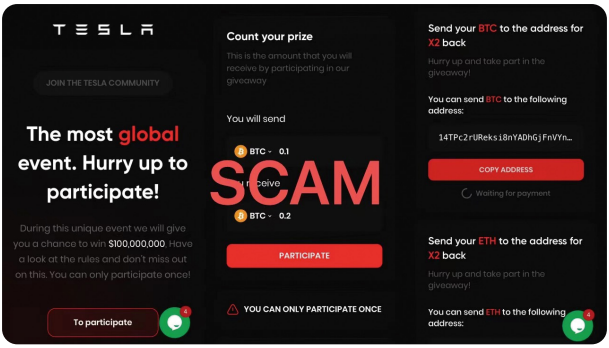
短視頻二維碼欺詐

诱誘導受害者掃描二維碼跳轉至第三方欺詐網站是經典的欺詐手段。在傳統場景下，受害者往往會被要求提交隱私信息、安裝有害軟件，或者進入欺詐網絡社群。近年來，隨著加密經濟規模的快速擴張，這個手法在行業內也得到了應用。

以下是典型的冒充埃隆·馬斯克的欺詐案例——

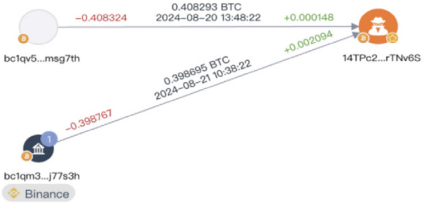
這位影響力巨大的名人因近期頻繁提及區塊鏈相關概念，而對加密貨幣二級市場造成了較大的衝擊。有不法分子利用人工智能工具偽造了一段影像，其中「馬斯克」聲稱觀眾掃描視頻中出現的二維碼，將能夠參與由特斯拉公司發起的比特幣返利活動。欺詐者通過向 Youtube 投稿或發起直播的形式，向網友們投放這個欺詐視頻。

訪問欺詐網站 teslainc2x[.]org 後，網站會要求受害者向某個特定的地址轉賬，並聲稱在活動期間僅有一次機會獲取雙倍的回報。



欺詐信息

這是非常典型的投資返利詐騙，通過 BitracePro 區塊鏈數據分析畫布可以看到，已經有兩名受害者向欺詐地址轉入了比特幣，然而並沒有收到「雙倍返還」。



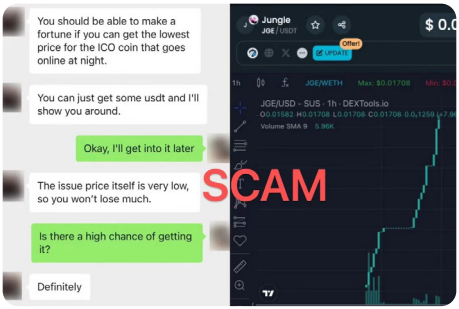
視頻二維碼欺詐案例資金分析

社交媒體詐騙

除了通過投放欺詐信息等待獵物上鉤外，還存在大量投資理財類詐騙活動是通過社會工程學方法精細運作的。詐騙者往往會以「帶你賺錢」為由，一步步教導受害者創建錢包、購買加密貨幣、參與投資賺錢，最後伺機竊走或騙走受害者賬戶裡的資金。

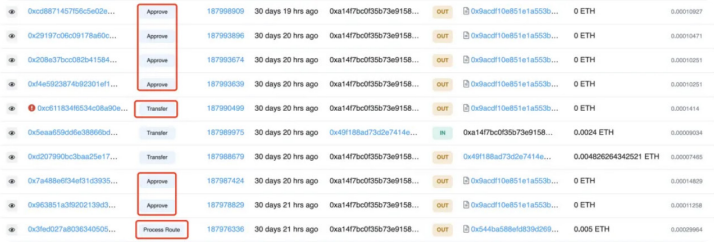
在下面這個案例中，我將為你介紹一個典型手法——

受害者在 TikTok 刷到一條關於比特幣的介紹視頻（實際上是騙子製作並發布的）並留言評論。不久後，便收到視頻發布者的私信，對方聲稱能夠教他投資比特幣。受害者欣然同意，但由於是完全的新手，過程中的每一步都截圖由詐騙者進行指導，導致助記詞在其不了解的情況下洩露。



詐騙者與受害者的聊天記錄

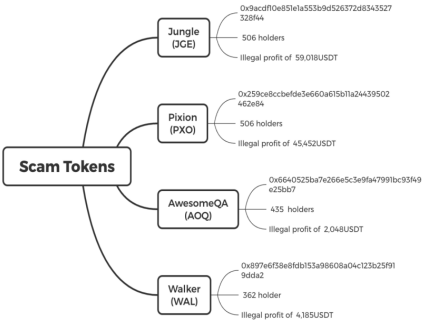
詐騙者推薦的第一個項目是一個名為 Jungle（JGE）的所謂 ICO 代幣（官網 itsjungle[.]me 現已無法訪問，官方推特也已註銷），受害者成功從這筆交易中賺取了 50% 的利潤。



多個受害者的鏈上操作記錄

但事實上鏈上真實發生的故事是，這是一個「貔貅幣」，其他不慎購入的受害者正在鏈上焦急地四處給不同的 DEX 授權以嘗試將代幣賣出，而該受害者的「盈利」只是因為詐騙者給他的地址設置了權限白名單，只有他能夠賣出而已。這是特意為他設計的代幣池，只是為了讓他嘗到甜頭後加大投入。

果然，次日詐騙者再次邀請受害者參與另一代幣的交易，在受害者存入 2.39 ETH 後，詐騙者利用早前獲取的助記詞，將受害者地址中的資產盡數盜取。



詐騙團伙發行的多個欺詐代幣

事後，Bitrace 對 JGE 代幣的發布地址進行了調查，發現該團伙已經至少發行了四個欺詐代幣，獲利超過 130K。如果加上通過非法手段盜取的加密資產，損失數值會更大。

情感詐騙

情感詐騙是一種結合了投資理財類詐騙與交友婚戀類詐騙的欺詐手段，受害者通常為不具備 Web3 知識的圈外高淨值群體。詐騙者會通過詳細的背景調查後虛構人設投其所好，以網絡戀愛的方式要求受害者參與某個並不存在的投資項目。

在「投資」活動的開始，受害者的「投資收益」會快速上漲，然而當受害者想要提取收益，非法平台便會以「交稅」、「滯納金」、「手續費」、「鎖定期」等諸多理由拒絕，並要求受害者加大投入。在這個過程中，受害者會被榨乾錢財，甚至被要求去借貸，直到再無資金可榨取。

不法分子並不同情這些受害者，他們稱後者為「豬」，偽造的人設材料與話術是「豬飼料」，培養感情階段是在「餵豬」，最後的收割自然也就是「殺豬」了。因此，這類騙局往往也被稱為殺豬盤（pig butchering scams），受害者會受到財物與情感的雙重損失。

以「高瑞商學院」殺豬盤案為例——

受害者是一名稍有資產的年輕女性，於 2023 年 2 月在社交軟件中結識了一名年輕多金的男網友，對方自稱正在各地考察投資，會把自己去全國各地考察、投資的照片發給受害者，照片中不經意夾雜著幾張自拍照，照片裡的他開著豪車、戴著名表，加以日常噓寒問暖，令受害者為之傾心。

網戀過程中，詐騙者反覆提及所謂的「高瑞商學院」，並聲稱這是一個區塊鏈投資項目，參與者需要自行購買泰達幣（USDT）用於認購份額，到期後便可連本帶利獲取高額收益。

詐騙者自稱已經參與過多期投資，並賺取了較大收益。為了讓受害者也參與，詐騙者甚至採用了 PUA 手段。

詐騙者與受害者的聊天記錄

受害者花光了自己的資產，並向親友大量借貸後，累計向該項目投入超過 20 萬 USDT，最終網戀對象消失，自己血本無歸。

错误的資管方法：位於加密之旅起點的大坑

不同於傳統 Web2 平台中心化的賬戶登錄與驗證體系，加密貨幣錢包等 Web3 基礎設施並不保留用戶的身份信息、賬戶權限，也不存在傳統互聯網軟件平台常見的銷戶、換綁、身份信息找回等設置。這意味著 Web3 用戶需要自行保管地址密鑰，一旦丟失將導致永久失去對鏈上身份的控制，或者因洩露而導致鏈上資產被竊取。

在 Web3 錢包管理方面，我們應當首先簡單理解什麼是地址私鑰和錢包助記詞。

地址私鑰是一串由數字與字母組成的字符串，用於解密數據或簽署交易。通過導入私鑰，用戶可以在任何錢包程序中「登錄」自己的加密地址並獲得完整的賬戶權限。私鑰通過特定的密碼學方法可以單向推導出另一串特定規則的字符串，後者被稱為地址公鑰，也即我們日常互相轉賬時填寫的資金收付對手方。不難看出，公鑰就像對外公佈的家庭住址，私鑰則像由主人管理的房門鑰匙。

助記詞是私鑰的另一種形式，由來源於特定詞庫的 12、24 或者其他個數的單詞組成，因此具備更高的可讀性與記憶便利性。通過助記詞，錢包可以通過特定的標準派生並管理一組或多組公私鑰對。例如，頗受用戶歡迎的 imToken、TokenPocket 錢包，允許用戶在同一組助記詞下創建多個區塊鏈地址，包括同一區塊鏈下的多個地址，以及不同區塊鏈下的多個地址。通過將助記詞導入支持這類標準的錢包，用戶將能夠找回自己的鏈上資產。

而在地址私鑰之外，部分錢包軟件也支持導出二維碼格式的密鑰，這是一種錢包便利度設置，但其重要性不亞於私鑰或助記詞明文。

部分盜幣者利用投資者對區塊鏈錢包的不了解，會通過各種方式騙取助記詞、私鑰，或錢包操作權限，進而盜取資產。

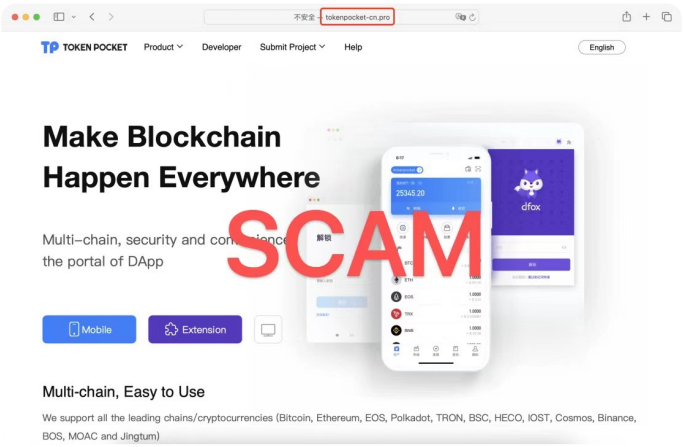
假錢包 APP 盜幣

盜版 APP 是一種常見的惡意軟件應用，通過盜用正版軟件的 LOGO、名稱、頁面素材等方式，誘導受害者下載並使用，以達到危害網絡安全、竊取用戶信息、擅自使用付費業務等目的。

在加密貨幣行業，錢包 APP 是高仿重災區。盜幣者通常的做法是，在真實錢包 APP 的代碼文件中植入惡意代碼，一旦有人安裝了這一惡意軟件並導入自己的助記詞、私鑰，APP 背後的盜幣者就能第一時間獲知受害者的助記詞、私鑰，進而非法轉移受害者的資產。

當下最流行的假錢包 APP 的推廣方式是通過搜索引擎、假錢包官網、假社交媒體賬戶等形式實現的——

在搜索引擎渠道，欺詐者會製作 Crypto 主題的文章或短視頻，嵌入惡意軟件下載鏈接後，通過 SEO 或 SEM 的方式進行推廣。當潛在受害者通過搜索引擎搜索相關關鍵詞——尤其是特定錢包品牌名稱時，這類欺詐鏈接有可能展現在搜索結果首頁甚至首頁第一條。未能分辨真偽的受害者會因此失去自己的資產。



假網站

假錢包官網與假錢包 APP 是配套存在的，通過製作高仿錢包網站並部署在高仿域名中，相比於普通的 SEO 手段更具迷惑性。例如，針對 Tokenpocket 錢包的虛假官網 tokenpocket-cn[.]com，該域名就是真實官方域名 tokenpocket.pro 的高仿，意在誘導投資者下載假錢包 APP。

假 X(Twitter) 賬戶

假社交媒體賬戶也頗為流行，尤其是在 X 等 Web3 用戶常用的社交平台上，活躍著大量以「imToken 中文客服 / 官方」、「imToken SupportTeam」等為名稱的賬戶，意圖對平台資訊進行污染以推廣盜幣 APP。

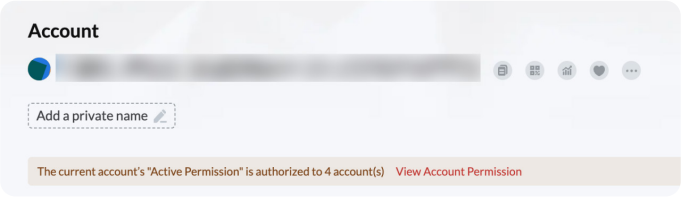
多簽案例

多重簽名錢包是一個重要的資產安全解決方案，區別於普通錢包，多簽錢包需要多個私鑰來進行操作。例如，最常見的 2 對 3 多簽錢包，要求三個私鑰持有者中的至少兩個簽名，才能夠發起一筆交易。其安全性在於，至少需要兩個私鑰同時洩漏，才會對所保管的資產造成威脅。

但這一解決方案反而被盜幣團伙所利用，形成了一個新型變種——多簽盜幣。

在傳統的假錢包騙局中，黑客通過假錢包後台獲取地址私鑰，與用戶共享地址操作權限，雙方都可以將地址內資金轉出。在此類騙局中，盜幣者有兩種選擇，一是當下實施盜竊，清空地址資產，讓用戶發現地址餘額歸零後便不再使用該錢包；二是冒著用戶可能會轉出資金的風險，不立即轉出，而是等待用戶囤積資金，這種操作被不法分子稱為「養魚」。

這種情況下，盜幣者通常不會特別耐心，無論資金大小，會盡快將資金轉走。



多重簽名詐騙中權限被更改的受害者賬戶

而在多簽騙局中，由於用戶失去了自己的賬戶權限，地址會長期處於「只進不出」的狀態。理論上，只要用戶不操作轉出資金，他將永遠不會發現自己已經處於被盜的邊緣。對於盜幣者而言，只需等待不明真相的受害者不斷向錢包轉賬。

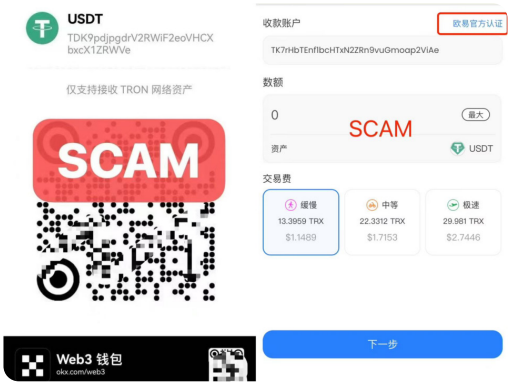
顯然，多簽騙局手法更加隱蔽，成功非法獲取資金的比例更高，威脅也更大。

支付授權騙局

除了多重簽名可能導致投資者失去錢包控制權限之外，針對特定加密資產的授權盜幣現象也更加普遍。其原理在於，區塊鏈允許用戶將自己地址內一定數量的代幣操作權限讓渡給另一個地址，這是通過智能合約來實現的，並且需要用戶執行一筆鏈上交易。

例如，Alice 的地址內擁有 1000 枚 USDT，她通過調用智能合約發起了一筆鏈上交易，交易細節為將自己地址內 100 額度的 USDT 操作權限讓渡給 Bob 的地址。交易成功後，Bob 就可以通過自己的地址發起交易，將 Alice 地址中的不超過 100 USDT 進行轉移，而不再需要 Alice 的再次同意。

盜幣者利用了這一點，將授權鏈接轉換為二維碼，並聲稱這是轉賬支付的二維碼。受害人只需掃碼並發起交易，便會將特定代幣的全部操作權限讓渡給盜幣者。



支付授權騙局

以近期較為流行的高仿轉賬盜幣為例。請注意，上圖右部的界面並非 OKX Web3 錢包的系統轉賬界面，而是盜幣者模仿的網頁。真實的 OKX Web3 錢包轉賬界面並不會這樣展示，更不會標註某個地址為「歐意官方認證」（OKX official certification）。

其真實目的在於，當受害人通過錢包瀏覽器打開釣魚網站後，盜幣者通過高仿的頁面誤導受害人認為自己正在進行轉賬，但實際上提交的交易內容是代幣授權。如果錢包軟體不對交易內容進行校驗和提醒，受害人幾乎無法察覺自己已經受騙。等他們意識到時，詐騙者已經完全掌握了錢包內資產的操作權限。

這種授權詐騙方法構成了重大威脅，因為它利用了智能合約交互的複雜性，以及受害者對技術交易細節的不熟悉，使其成為詐騙者得手的非常有效工具。

假 TG 騙局

Telegram 是 Web3 用戶常用的重要社交軟件之一，因其較高的匿名性而頗受 OTC 商的青睞，也因此盜幣者定向針對這一群體開發了假 Telegram APP。

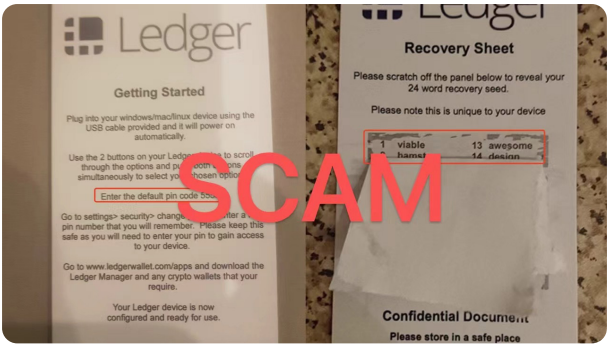
該手法類似前面所提及的假錢包 APP，同樣是在 Telegram APP 程式碼文件中添加惡意程式碼，目的有二——

其一是獲取受害者所有的聊天記錄，部分受害者會通過 Telegram 傳輸或保存自己地址的助記詞、私鑰，通過這種方式盜幣者可以直接竊取資產；

其二是篡改受害者發送的信息，其原理在於自動識別輸入內容，將其中特定形式的信息（例如 0x 開頭的字串）進行替換，發送地址的人在本地客戶端不會察覺任何異常，但另一端的人所收到的則是被替換的地址。這種替換活動一旦發生在常見的轉賬場景下，就會出現一方將加密資產轉入盜幣者地址的情況。

硬件錢包說明書欺詐

硬件錢包是廣受推崇的資產存儲方式，通過隔離網絡與助記詞、私鑰，理論上投資者能夠免受密鑰洩露的風險，但仍然存在特定的方式實現盜竊。接下來我將介紹一種社會工程學盜幣手法——



欺詐團隊製作的假硬件錢包手冊

受害人在第三方電商平台購買某品牌硬件錢包一台，打開包裝後，按照「說明書」上標註的「初始 Pin 碼」打開了硬件錢包，並在備份了「說明書」上印制的「助記詞」後，向錢包地址存入了大量資金，最終失竊。

其原因並非錢包在硬件層面遭到破解，而是被盜幣者提前激活獲取地址助記詞，然後偽造虛假說明書進行二次封裝，再通過非官方的渠道將已激活的硬件錢包銷售給受害人。這表明識別官方電商店鋪，重要性等同於識別官方網站。

通過操縱用戶對硬件錢包的信任，並利用這些設備本質上是安全的假設，詐騙者能夠通過這種精心設計但有效的社會工程策略竊取資產。

當你開始交易加密資產

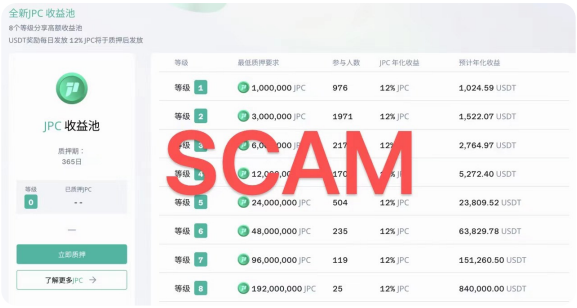
截至目前，你已經可以識別並避開那些虛假信息渠道，並對那些不安全的資產存儲方式有所了解，成功讓自己度過了艱難的「新手期」，接下來就要開始面對真正的挑戰——用自己的真金白銀去市場上參與交易。

你是否認為加密市場上存在可持續的年化收益超過 50% 的理財項目？是否認為用手中閒置的穩定幣去某個「礦池」裡「質押」就能穩定賺到錢？是否認為購買某個代幣去參與「交易所官方」的質押活動就能輕鬆賺錢？如果你的答案都是「是」，那麼你可能危險了。

超高收益的交易所理財騙局

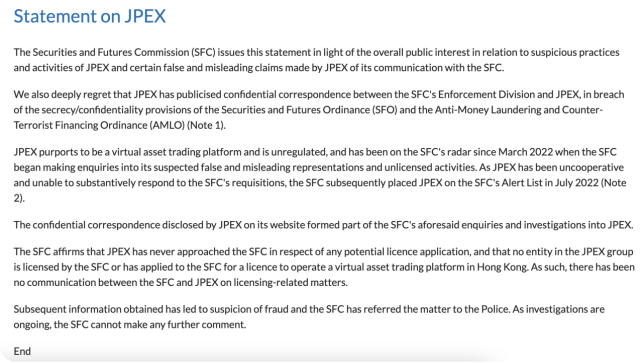
在中心化加密貨幣交易平台購買加密資產是最常見的投資方式之一，部分中心化交易平台的運營方為了吸引更多的用戶資金留存，會推出一些理財產品，例如最常見的質押代幣獲取更多同種或者其他代幣。這類理財產品通常收益率不高且存在額度限制，正常展業的平台也不會將這類理財產品作為主要經營項目。

但某些欺詐平台會虛構理財產品超高收益，吸引大量非專業投資者購買參與，並誘導設置較長的質押週期以限制客戶贖回。等到質押結束，這類理財產品或是無法兌付，或是所兌付代幣已極大貶值，甚至是平台直接跑路（rug），給投資者造成財產損失。



JPEX 高收益騙局

以 2023 年 9 月暴雷的 JPEX 交易所為例。該所的經營方式非常激進，採用餘額返點而非交易手續費返點的邀請模式，鼓勵投資者大量存入加密資產並邀請親朋好友。平台還發行了名為 JPC 的代幣，聲稱該代幣系平台的治理代幣，持有者能夠參與所謂的「節點質押」獲取至少 12% 的穩定年化收益率，通過增加參與資金與鎖定期限，該收益率還會上升。



Statement on JPEX

The Securities and Futures Commission (SFC) issues this statement in light of the overall public interest in relation to suspicious practices and activities of JPEX and certain false and misleading claims made by JPEX of its communication with the SFC.

We also deeply regret that JPEX has publicised confidential correspondence between the SFC's Enforcement Division and JPEX, in breach of the secrecy/confidentiality provisions of the Securities and Futures Ordinance (SFO) and the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (AMLO) (Note 1).

JPEX purports to be a virtual asset trading platform and is unregulated, and has been on the SFC's radar since March 2022 when the SFC began making enquiries into its suspected false and misleading representations and unlicensed activities. As JPEX has been uncooperative and unable to substantively respond to the SFC's requisitions, the SFC subsequently placed JPEX on the SFC's Alert List in July 2022 (Note 2).

The confidential correspondence disclosed by JPEX on its website formed part of the SFC's aforesaid enquiries and investigations into JPEX.

The SFC affirms that JPEX has never approached the SFC in respect of any potential licence application, and that no entity in the JPEX group is licensed by the SFC or has applied to the SFC for a licence to operate a virtual asset trading platform in Hong Kong. As such, there has been no communication between the SFC and JPEX on licensing-related matters.

Subsequent information obtained has led to suspicion of fraud and the SFC has referred the matter to the Police. As investigations are ongoing, the SFC cannot make any further comment.

End

香港證券及期貨事務監察委員會（證監會）關於 JPEX 的聲明

基於這種經營模式，JPEX 吸引了大量非專業投資者的資金，參與者遍佈香港、台灣、內地、新加坡等地，最後惡意 Rugpull。據香港警方披露，案發後有超過 2000 名受害人報案，涉及金額高達 13 億港幣。

此類高收益投資騙局非常危險，因為它們利用看似安全、豐厚的回報和成熟交易平台的信譽的誘惑來瞄準非專業投資者。

貔貅幣欺詐

「只能買不能賣」的騙局除了會發生在中心化平台以外，在去中心化交易所（DEX）裡也會發生，但其原因並不在於 DEX，而在於代幣的發行者。

開發者在區塊鏈上根據特定標準發行一個代幣（Token）時，不僅能夠設置一些基本參數，例如代幣名稱、代碼、數量上限等，還可以限制特定地址對該代幣的訪問權限，例如讓這些地址無法轉賬或賣出所發行代幣等。而當限制範圍幾乎囊括了所有地址僅有少數發行者自身地址能夠訪問時，我們稱這個代幣為「貔貅幣」（honeypot token）。

文如其名，不在白名單列表裡的地址，在買入或者獲取這類代幣後，無法通過常規的手段在 DEX 交易對裡將代幣出售，只能眼看著代幣漲跌無法退出。這類騙局有許多變種——

一種是簡單的限制賣出手法。欺詐者發行貔貅幣並在 DEX 中建立流動性池後，會通過社交平台污染、網絡社群廣播、向知名地址空投等方式推銷這個代幣，同時利用多個地址反覆交易快速拉升幣價。此時如有不明就裡的受害者買入，就會發現自己的賬戶頭寸價值迅速上漲，但卻無法賣出獲利。最後在有足夠多受害者買入代幣後，欺詐者再通過撤回流動性的方式，有效地耗盡所有資金，讓受害者只剩下毫無價值的代幣。

一種是結合了殺豬盤手法的權限可修改貔貅幣。欺詐者在發行貔貅幣後，通過社會工程學手段誘騙新手投資者購買，在早期一到兩個項目中，將目標對象的地址加入白名單允許其賣出獲利，從而騙取受害者的信任。但當受害者加大投入後，欺詐者就不再允許其賣出，完成欺詐。

這種方法具有很強的欺騙性，因為受害者根據最初的成功交易而認為他們正在進行合法的投資。

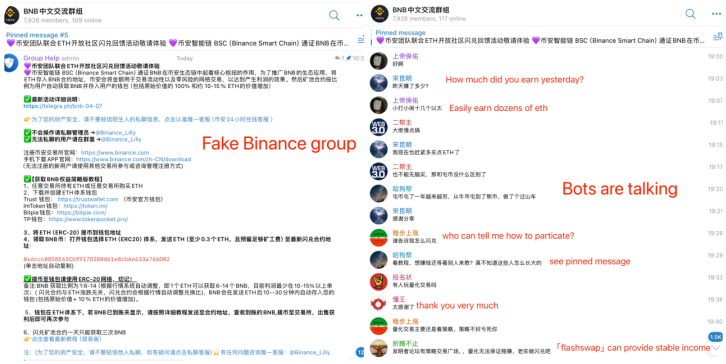
還有一種是針對「聰明錢」地址跟隨者的獵殺。所謂聰明錢，指的是鏈上投資勝率較高的地址，由於區塊鏈公開透明的特性，任何人都能夠觀察到所有地址的交易活動，因此有交易員或情報分析公司會對這類高勝率地址密切關注，當聰明錢地址買入某個代幣時，部分交易員也會選擇跟隨買入。

於是針對這批追隨者地址的貔貅幣騙局出現了，欺詐者在發行代幣並建立流動性池後，會通過調用特定智能合約的方法發起一筆交易將資金池中的代幣發送給聰明錢地址，部分監控機器人可能會將這筆交易錯誤識別為聰明錢地址的買入行為，進而誤導其他跟隨者買入。

這導致一系列來自不知道代幣是貔貅幣的交易員的後續購買。然後，騙子等待足夠數量的受害者買入，然後再撤回流動性，讓追隨者陷入無法出售的代幣的困境。

假幣安礦池騙局

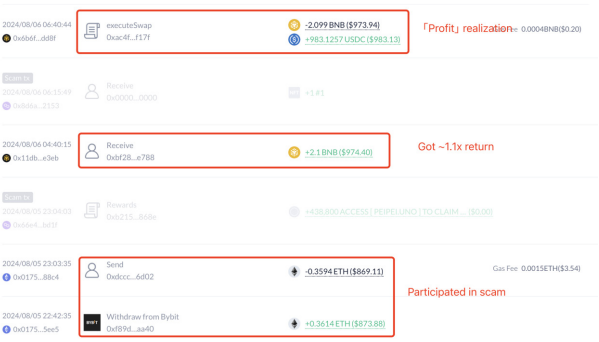
在前面我們提到了冒充特斯拉的「雙倍返還」欺詐手法，這種騙局的主要受眾是不瞭解區塊鏈知識的圈外用戶，接下來我會介紹主要針對圈內用戶、更具迷惑性的「假幣安礦池」欺詐。



假幣安群聊天記錄

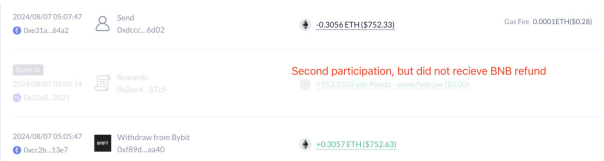
這是一類歷史悠久的欺詐方式，欺詐者通常會以「幣安交易所交流群」、「幣安回饋福利群」等名稱創建 Telegram 社群，隨後填充數千到數萬 Bots 賬戶，以冒充幣安官方社群，通常這個群只有受害者一個人是真人。

欺詐者接著會以「幣安客服」的名義，在假社群中發布信息稱幣安交易所與以太坊基金會合作，正在開展用戶回饋營銷活動，允許用戶使用 ETH 以高於市場匯率的價格換取 BNB 進而賺取差價收益。社群中也會有大量 Bots 模仿真人聊天，宣稱他們通過閃兌（flashswap）賺到了許多錢。



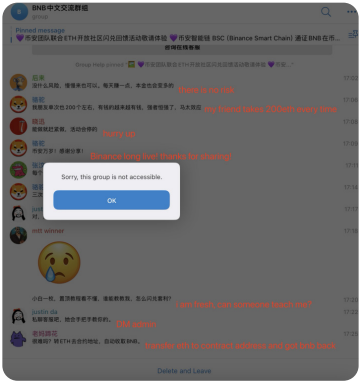
欺詐性誘餌

按照欺詐者的要求，受害人首先需要在以太坊網絡中，向一個智能合約賬戶轉一定數量的 ETH，接著受害人會在 BSC 區塊鏈上收到大約價值 1.1 倍的 BNB 返還，超出市場價格的部分就是受害人的「收益」。



受害者鏈上操作記錄

嘗到甜頭的受害人如果再次參與的話，就不會收到 BNB 返還，接著如果受害人在社群內說自己被騙，就會馬上被管理員封禁並解散群組，至此整個騙局完成。



假幣安群聊天記錄

假 OKX 公鏈持 USDT 領 OKT 騙局

流動性挖礦是加密行業在 DeFi 時代所流行的事物，用戶通過將一定數量的代幣存入某些智能合約地址，便能夠參與 Dapp 治理、獲取投票權、借錢給其他人、為鏈上協議提供安全性等。在這些活動中，存入代幣的用戶可以獲取一定的收益。

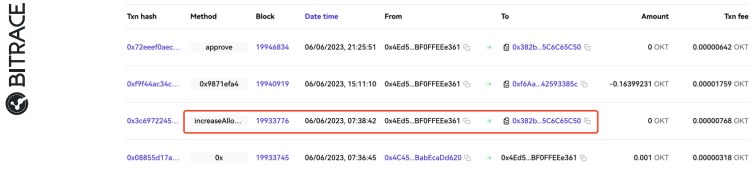
因此有欺詐者假借「流動性挖礦」的名義，設計了大量不同形式的欺詐手法，這裡以針對新手用戶的「假 OKX 公鏈持 USDT 領 OKT」騙局為例進行介紹。

欺詐信息

這一騙局聲稱，用戶只需要在錢包裡存放 USDT，就能持續獲得超高年化收益率的 OKT，並且不存在代幣鎖定期，用戶隨時可以轉移地址裡的資金。

欺詐信息

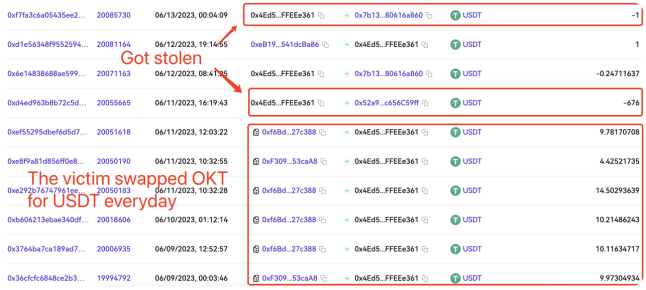
按照欺詐者宣稱的規則計算，即使是最低一檔，參與者的年化收益率也將達到 475%，許多剛剛參與 Crypto 投資，對區塊鏈不甚了解的新手用戶很容易被高收益所欺騙。



Txn hash	Method	Block	Date time	From	To	Amount	Txn fee
0x72eeef0aec...	approve	19946834	06/06/2023, 21:25:51	0x4Ed5...BF0FFEEe361	0x382b...5C6C65C50	0 OKT	0.00000642 OKT
0xf9f44ac34c...	0x9871efa4	19940919	06/06/2023, 15:11:10	0x4Ed5...BF0FFEEe361	0xf6Aa...42593385c	-0.16399231 OKT	0.00001759 OKT
0x3c6972245...	increaseAllo...	19933776	06/06/2023, 07:38:42	0x4Ed5...BF0FFEEe361	0x382b...5C6C65C50	0 OKT	0.0000768 OKT
0x08855d17a...	0x	19933745	06/06/2023, 07:36:45	0x4C45...BabEcaDd620	0x4Ed5...BF0FFEEe361	0.001 OKT	0.00000318 OKT

惡意授權

通常，欺詐者會要求受害人第一時間交互欺詐合約以參與「挖礦」，實際上該合約是給欺詐者地址的無限額度 USDT 的授權。



0xf7fa3c6a05435ee2...	20085730	06/13/2023, 00:04:09	0x4Ed5...FFEEe361	0x7b13...80616a860	USDT	-1
0xd1e56348ff952594...	20081164	06/12/2023, 19:14:55	0xeB19...541dcBa86	0x4Ed5...FFEEe361	USDT	1
0x6e14838688ae599...	20071163	06/12/2023, 08:47:35	0x4Ed5...FFEEe361	0x7b13...80616a860	USDT	-0.24711637
0xd4ecf963b8b72c5d...	20055665	06/11/2023, 16:19:43	0x4Ed5...FFEEe361	0x52a9...c656C59ff	USDT	-676
0xef55295dbef6d5d7...	20051618	06/11/2023, 12:03:22	0xf6Bd...27c388	0x4Ed5...FFEEe361	USDT	9.78170708
0xe8f9a81d856ff0e8...	20050190	06/11/2023, 10:32:55	0xF309...53caA8	0x4Ed5...FFEEe361	USDT	4.42521735
0xe292b76747961ee...	20050183	06/11/2023, 10:32:28	0xf6Bd...27c388	0x4Ed5...FFEEe361	USDT	14.50293639
0xb606213ebae340df...	20018606	06/10/2023, 01:12:14	0xf6Bd...27c388	0x4Ed5...FFEEe361	USDT	10.21486243
0x3764ba7ca189ad7...	20006935	06/09/2023, 12:52:57	0xf6Bd...27c388	0x4Ed5...FFEEe361	USDT	10.11634717
0x36cfcfc6848ce2b3...	19994792	06/09/2023, 00:03:46	0xF309...53caA8	0x4Ed5...FFEEe361	USDT	9.97304934

受害者鏈上操作記錄

在最初的幾天，受害人每天都會收到一定數量的 OKT，一旦他加大投入或者長期未增加投入，欺詐者就會調用 transferfrom 方法，將受害人地址中所有的 USDT 轉走，完成欺詐。

流動性退出騙局

自動做市商（AMM）是最主要的一類去中心化交易平台（DEX），其業務實現原理為通過智能合約為用戶自動報價，而無需點對點撮合。因此需要流動性提供者（LP）向合約中按照特定匯率放入成比例的兩種代幣，用戶的每次兌換行為都會影響合約中的兩種代幣匯率，進而對價格造成影響。例如某個資金池中同時有一定數量的 A、B 兩種代幣，用戶使用自己持有的 A 代幣兌換了一些 B 代幣，使得資金池中 A 代幣數量增加，B 代幣數量減少，將導致以 A 為價格單位的 B 代幣價格上升。

利用這一特點，欺詐者設計了基於 AMM 的流動性退出騙局——

欺詐者首先會在鏈上發行一個代幣（成本不會超過 100 美金），並去主要的 DEX 上為代幣提供流動性，通常會與 WETH 或者 USDT 配對。

接著通過其他手段——例如前文所提到的那些，令其他投資者相信這一代幣是有升值潛力的，進而誘導受害者們買入。

然後，由於受害者們的買入，導致欺詐者發行代幣的價格上升。

最後，欺詐者只需要撤回流動性，就能夠從資金池中提取大量 WETH 或者 USDT（取決於配對的代幣是什麼），相對於這一系列操作極低的手續費成本，欺詐者幾乎是一本萬利。

2024 年 2 月 20 日，河南南陽高新技術產業開發區人民法院判決了一起加密貨幣欺詐案件，被告人因發行虛假加密貨幣並誤導他人充值 5 萬 USDT，後迅速「撤回資金」造成他人損失，而被判詐騙罪。

0x48901ff7b51...	Remove Liqui...	17449205	2022-05-02 8:57:49	PancakeSwap V2: BS...	IN	0xb8a5d9CC...A8Fc76922	508,069.87841896	BEP-20: Blo...rce
0x48901ff7b51...	Remove Liqui...	17449205	2022-05-02 8:57:49	PancakeSwap V2: BS...	IN	0xb8a5d9CC...A8Fc76922	353,488.1150772	Binance-Peg ... (BSC-US...)
0x48901ff7b51...	Remove Liqui...	17449205	2022-05-02 8:57:49	0xb8a5d9CC...A8Fc76922	OUT	PancakeSwap V2: BS...	434,741.30238568	BEP-20: Pan...LPs
0x0dc521e6a9...	Add Liquidity	17449197	2022-05-02 8:57:25	Null: 0x000...000	IN	0xb8a5d9CC...A8Fc76922	434,741.30238568	BEP-20: Pan...LPs
0x0dc521e6a9...	Add Liquidity	17449197	2022-05-02 8:57:25	0xb8a5d9CC...A8Fc76922	OUT	PancakeSwap V2: BS...	630,000	BEP-20: Blo...rce
0x0dc521e6a9...	Add Liquidity	17449197	2022-05-02 8:57:25	0xb8a5d9CC...A8Fc76922	OUT	PancakeSwap V2: BS...	300,000	Binance-Peg ... (BSC-US...)
0x125b6fe7aab...	Transfer	17449003	2022-05-02 8:47:43	0x619E8d64...538ADFfe5	IN	0xb8a5d9CC...A8Fc76922	0.95	BEP-20: Blo...rce
0xdac5af9cf72...	Transfer	17448975	2022-05-02 8:46:19	0xb8a5d9CC...A8Fc76922	OUT	0x619E8d64...538ADFfe5	1	BEP-20: Blo...rce
0xc454d4bdd5...	0x60806040	17448884	2022-05-02 8:41:46	Null: 0x000...000	IN	0xb8a5d9CC...A8Fc76922	2,100,000	BEP-20: Blo...rce
0xace7a2e427...	Multi Send	17448853	2022-05-02 8:40:13	0x1Afe138c...697D2235F	IN	0xb8a5d9CC...A8Fc76922	1,286,698	BEP-20: usd...io
0x248338ab11...	Transfer	17448700	2022-05-02 8:32:34	Binance: Hot Wallet 10	IN	0xb8a5d9CC...A8Fc76922	300,109.1	Binance-Peg ... (BSC-US...)

欺詐者鏈上操作

據區塊鏈瀏覽器顯示， 2022 年 5 月 2 日，欺詐者於 UTC 時間 8:41:46 發行了 BFF 代幣，並於 8:57:25 在 DEX 中創建了 BFF-USDT 交易對，初始投入 30 萬 USDT 與 63 萬 BFF 進資金池，但僅在 24 秒後，欺詐者便撤回了所有流動性。由於在此期間已有受害人大量購入，導致資金池匯率發生變化，欺詐者撤回流動性的行為為他帶來了超過 5 萬 USDT 的非法所得，全程僅花費 25 分鐘。

而同類型的欺詐手法無時無刻不在鏈上發生，且不是每次都能夠幸運追回損失資金，這提醒普通投資者在參與鏈上交易前，務必要了解其中風險。

瘋狂的網絡釣魚：病毒式增長

網絡釣魚（Phishing）是一種通過發送欺騙性郵件、短信、電話或網站，意圖引誘用戶洩露敏感信息或進行惡意操作的攻擊方式。在傳統互聯網時代，這類釣魚活動通常都是為了牟取受害人現金資產或虛擬資產，而近年來隨著加密經濟的發展，越來越多的欺詐者開始盯上 Web3 行業。

以下我們將介紹三種常見的，以不特定對象的加密資產為目標的網絡欺詐手法。

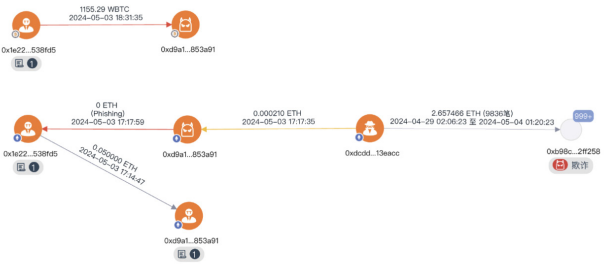
地址投毒

如果你擁有一個正在使用中的區塊鏈地址，那麼你一定會發現自己的地址時不時就會收到一筆極小金額的轉賬，這些轉賬並不會對你的地址使用造成任何影響，它們只是靜靜待在你的轉賬記錄裡。

這其實是當前非常流行的地址投毒釣魚，主要的實現形式是向目標對象轉賬極小金額的ETH、USDT、TRX等代幣，從而污染對方的轉賬記錄，假如目標對象的錢包使用習慣不好，就有可能在轉賬的時候從記錄中複製錯誤的地址，進而將資金錯誤轉賬給欺詐者。

如果更深入考察發起轉賬的投毒地址，會發現它尾部的字符與目標對象的主要交互對手方是一致的，這正是這個騙術的核心障眼法——用來釣魚的地址是針對目標對象定制的同尾號地址。

其實現原理是通過特定程序批量生成區塊鏈公私鑰對，保留那些有特定意義的地址，例如尾號全都是 6、8 等大眾喜愛的數字，這類賬戶通常醒目而有趣，我們稱之為「虛榮地址」或者「靚號」。這種技術同樣可以應用在地址投毒活動中，只不過批量生成的地址是對目標對象地址的模仿。



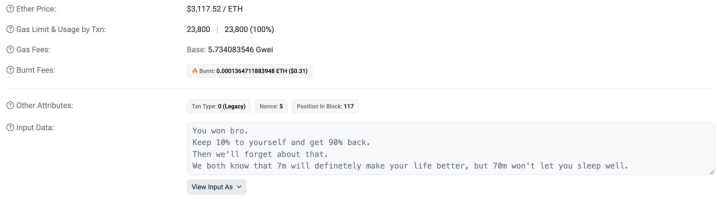
地址投毒相關分析

例如發生在 2024 年 5 月 3 日的史上最大的地址投毒慘案，受害人錯誤向投毒地址轉移了 1155 枚比特幣，當時價值 6800 萬美金。復盤這個案例不難發現，受害人 0x1e22 在當天向自己的新地址 0xd9a1b0b1e1ae382dbdc898ea68012ffcb2853a91 轉入了 0.05 ETH 用於購買 DAI，這一行為迅速被釣魚團夥識別，3 分鐘後便利用 0xd9a1c3788d81257612e2581a6ea0ada244853a91 向受害人發起 0 轉賬。75 分鐘後，受害人複製到錯誤的地址，向釣魚地址轉移了 1155 枚比特幣。

對釣魚地址手續費進行溯源不難發現，上游地址已作案 9836 次，而這只是這類釣魚活動的冰山一角。

廣告代幣

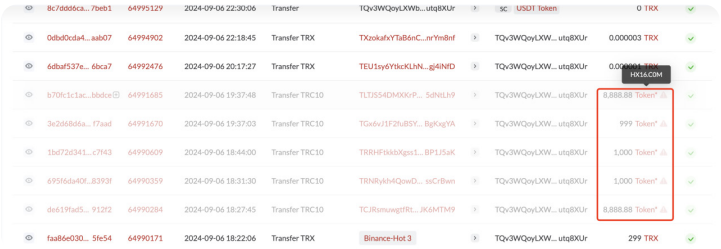
區塊鏈轉賬的時候，通常都可以在交易之外攜帶一些與交易本身無關的信息，例如以太坊官方瀏覽器就支持解析並展示用戶的鏈上留言，這種瀏覽是公開非加密的，因此所有人都可以看見其內容。



釣魚受害者通過鏈上交易給詐騙者留言

在前面提到的 1155BTC 被釣魚事件中，受害人就第一時間通過留言功能向釣魚團伙發聲，聲稱只要退換 90% 就不追究其責任，後續雙方以此建立了聯繫，並最終達成了退還協作，在這過程中雙方都是匿名的。

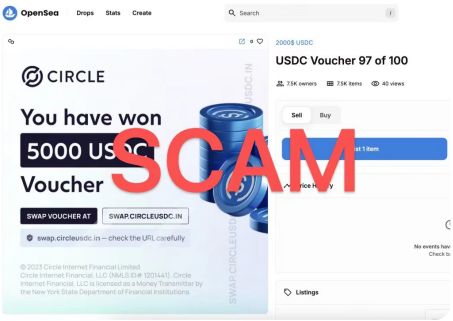
但這種需要工具解析的信息傳遞形式，對於廣告投放者而言仍然不夠醒目直接，為此他們開始通過將代幣符號設置為域名的形式傳遞廣告內容。



廣告代幣

例如主流公鏈之一的 Tron Network，其網絡交易中就存在著大量廣告代幣的轉賬，這些廣告的宣傳對象包括但不限於賭博網站、色情網站、能源租用網站等，也存在大量欺詐鏈接，收到這類代幣的投資者若出於好奇進入網站並交互，就存在資金損失的可能。

而隨著 NFT 經濟的崛起，這類廣告釣魚形式也在非同質化代幣上得到了應用。NFT 玩家想必時常會遇到账戶被空投陌生 NFT 的經歷，這些空投而來的 NFT 大部分都是欺詐網站批量發起的，它們製作精良，會在海報上強調你獲得了數千美元的獎勵，需要進入釣魚網站領取。有的欺詐者還會煞有介事地操縱欺詐 NFT 的價格，使得它們的地板價看上去真的非常昂貴。

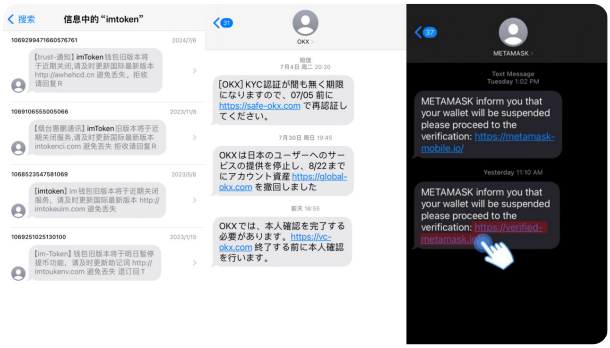


釣魚 NFT

例如上圖中的欺詐 NFT，名為「2000$USDC」，它聲稱你有資格獲取 5000USDC 的獎勵，是一百個幸運兒中的一個。但實際上他給 7500 個地址都空投了，顯然這是一個騙局，訪問海報中出現的網站，只會導致自己的資金損失。

清退簡訊

冒充公檢法或者行業機構，對普通投資者投放釣魚鏈接，是非常流行的應用於 Web3 行業的欺詐手法之一。



欺詐簡訊

在個人信息泄露的情況下，投資者會收到大量欺詐簡訊或郵件，其核心手法為聲稱「舊版本軟件需要更新」，請受害人訪問釣魚網站。對於錢包類型的釣魚簡訊，通常會被要求下載假錢包 APP；對於交易所類型的釣魚簡訊，則通常是殺豬盤。

假錢包釣魚

Bitrace 曾調查過一起案件，2023 年 11 月，知名中心化交易平台 Binance 的聯合創始人趙長鵬被捕入獄，有欺詐者聲稱將資金存放在中心化交易平台並不安全，有受害人出於害怕將資金從 OKX 交易所轉出，過程中私鑰被騙取，導致最終損失 166.7ETH。

這類手法的核心是，利用普通投資者對行業政策的不了解，通過訴諸權威進而恐嚇、誘騙的方式拿到受害人的錢包助記詞或私鑰。

產業分工的盡頭：Crypto Drainer

依據李嘉圖的比較優勢理論，在市場經濟下，各個經濟部門之間總會自發進行分工以提高生產效率，這一理論在 Web3 欺詐領域同樣適用。

其典型特徵在於，位於欺詐產業鏈最前端的技術開發部門不再參與實際的欺詐軟件推廣工作，而是直接面向代理商提供軟件運營服務（SaaS），並從中抽取分成。這種模式使得各類欺詐活動的發起門檻急劇降低，欺詐者僅需專注於軟件推廣。

對於這類 SaaS 提供者，我們稱他們為 Crypto Drainer。

盜幣代理模式

前文中所提到的假錢包 APP 盜幣活動背後，正是在龐大盜幣需求市場中野蠻生長的 Crypto Drainer。他們會對主流加密貨幣錢包軟件進行逆向分析，並修改特定代碼用以獲取目標助記詞，為了幫助代理商管理龐大的助記詞，還會開發專門的管理後台，使得代理商能夠一鍵劃轉受害人的資金或者多簽受害人的地址。

類似傳統互聯網 SaaS 提供商，假錢包類 Crypto Drainer 通常也會有多種代理模式——

例如最常見的直接推廣 Crypto Drainer 的木馬鏈接，這種模式無後台，代理商只需要通過社交軟件、搜索引擎、自媒體平台等渠道引流即可，由 Drainer 執行盜竊並按照比例給代理商分成。

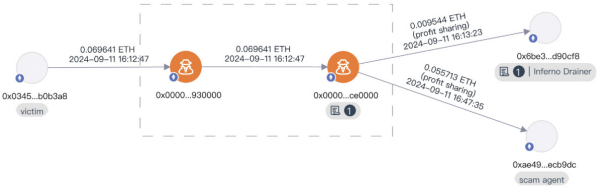
還有針對較大代理商的獨立部署方案，在這個模式下代理商可以自行管理盜幣後台，完成推廣、轉化、盜竊等全部流程，也可以進一步轉包給更下一層級的代理商，以賺取分成費用。

不同模式下的分成比例不同，代理商群體亦有差別，表明盜幣類 SaaS 市場在當下已經相當繁榮。

釣魚代理模式

地址投毒、假冒官方社交賬戶、套利詐騙等以騙取受害人代幣權限的釣魚欺詐手法背後，同樣是專業的 Crypto Drainer 在提供技術甚至運營支持。

以知名的 Inferno Drainer 為例，該團伙通過電報頻道推廣服務，由開發者提供給詐騙分子需要的釣魚網站以支持其詐騙活動，一旦受害者掃描釣魚網站上的二維碼並連接錢包，Inferno Drainer 就會檢查並定位錢包中最有價值且易於轉移的資產，發起一筆惡意交易。



Drainer 模式分析

受害者確認這些交易後，資產便會被非法轉移並處置，其中被盜資產的一定比例歸 Inferno Drainer 的開發者所有，其他部分則歸詐騙分子所有。

再以經典的「帶你賺錢」類型的釣魚欺詐為例，這類騙局的欺詐者通常會在短視頻平台、媒體平台、社交軟件中尋找目標對象，然後主動接近並告知自己有賺取高額收益的渠道，而方法不外乎前文所提及的殺豬盤、虛假礦池等，在受害人產生資金損失後，欺詐者與 SaaS 提供商會分配這筆收益。

這類騙術技術門檻較低，更強調欺詐話術的使用，因此部分 Drainer 在招募代理商的時候，還會提供額外的欺詐 SOP 教學。

場外交易欺詐：最薄弱一環

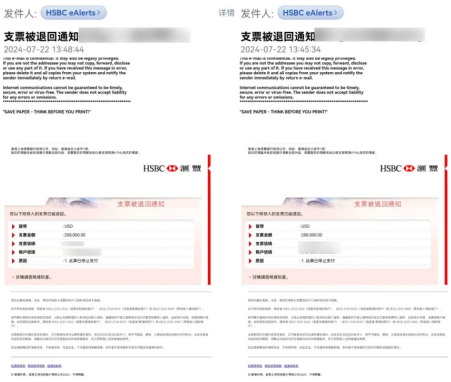
在部分國家或地區，場外交易（OTC）是加密貨幣投資者群體最常用的轉換法幣與 Crypto 的交易方式，這類 OTC 活動可以發生在中心化平台、網絡群組、線下等多種場景，但不論是何種場景，OTC 活動都存在著遭受欺詐的風險。包括但不限於法幣被騙，加密資金被騙，甚至人身安全受到威脅等，以下我們將列舉出一些常見的欺詐手法。

交易所幣商欺詐

對大部分普通投資者而言，在中心化交易平台的 C2C 交易區與幣商進行買賣交易，是最常見的出入金形式。在這個渠道裡，交易所起到了類似擔保平台的作用，除了會對平台內的 C2C 商家進行約束與管理外，還會建立完善的交易程序。

通常的流程是，賣家將預備賣出的代幣交給平台托管，當買賣雙方互相確認款項已支付到賬後，平台再將代幣劃轉給買家。但即便如此，仍然有欺詐的存在空間，以投資者向幣商賣幣的場景為例——

一種常見的騙局是幣商偽造支付記錄。例如通過技術手段修改支付工具的信息顯示，或者甚至只是給手機屏幕截圖進行偽造，聲稱款項已經支付並催促賣家儘快確認交易。投資者一旦輕信，不加以驗證並允許平台劃轉代幣，就會損失這部分資金。



支票欺詐

另一種是利用銀行支票可撤回特性進行欺詐的案例。同樣的交易場景，買家通過銀行支票進行支付，在賣家誤認為資金已完全到賬確認放幣後，再撤回支票騙取代幣。這類欺詐手法的主要對象是不流行使用銀行支票的國家的民眾。

線下交易欺詐

有大量場外交易發生於線下，部分新手投資者認為網絡上容易受騙，更加信任面對面的場景，因此甚至會出現驅車前往數百公里外某個地點進行交易的情況。

目前針對這類對象的欺詐手法有——

欺詐者向受害人收購代幣，要求以現金支付，然後在交易現場收到代幣後，給受害人一袋假幣，甚至是冥幣（祭奠逝者所用的仿鈔）；

欺詐者向受害人收購代幣，使用線上支付工具，但自己並不直面受害人，而是通過匿名軟體僱用第三方人員前往交易地點假裝自己。受害人前期出於謹慎，連續進行小額交易，多次成功後放鬆警惕，一次性向收款地址轉賬大量代幣，但這一筆最大額的交易不會收到現金。受害人意識到受騙後，通常會試圖攔住交易對手並報警，但這無濟於事，因為對方並不知情，且欺詐者完成交易後會刪除所有聊天記錄，無法對證；

欺詐者向受害人出售低價代幣，並要求受害人使用現金交易，但到達現場後會有數名暴徒衝出，將受害人手中的現金搶走。這類手法本質上是利用低價代幣作為誘餌的搶劫，性質極其惡劣，甚至會對受害人的人身安全造成威脅。

線下多簽欺詐

前文提到，假錢包盜幣者會通過假錢包應用程式盜取受害人的助記詞或私鑰，從而非法獲取錢包中的資產，而近年來我們也注意到一類發生於線下場景的多簽盜幣手法。

欺詐者與代幣買家約定在線下某地進行交易，見面後，欺詐者會以「你的地址上有風險資金」、「你的錢包可能被植入了木馬」等理由，要求受害人另外創建區塊鏈錢包用以收款，否則便拒絕交易。受害人通常是驅車從外地前來交易，已經耗費了大量的時間和精力，為了順利完成交易只得照做。

而在受害人創建錢包過程中，欺詐者會在身後偷偷拍下受害人新錢包的助記詞，並發送給同夥。同夥收到後，會立即將受害人的地址設置為多重簽名地址。

接著交易會非常順利地完成，受害人的地址內收到了欺詐者發來的代幣，欺詐者也收到了受害人發來的轉賬或現金。但在交易完成後，受害人才發現自己根本無法操作這個錢包地址，最後只能眼睜睜看著欺詐者將資金轉走。

這種欺詐手法將錢包地址多簽的原因，與假錢包手法中的情況一樣，都是為了不讓受害人將資金轉走。

一些安全建議

不要讓恐懼、貪婪等情緒操控自己

相較於其他領域，Web3 行業具備更高的門檻，這些門檻既包括技術原理方面的理解門檻，也包括基礎設施使用方面的上手成本，以及獲取準確資訊的門檻。盲目自信無視這些壁壘的新人往往會因此掉入陷阱。

例如所謂「黑 U 檢測」類型的欺詐，部分受害人對於不法分子利用加密貨幣進行洗錢的事情有所耳聞，也知道執法部門會對案件中的加密貨幣資金進行追蹤，出於恐懼會點擊欺詐者提供的釣魚連結以檢測自己的地址是否安全，進而被授權盜幣。但實際上檢測地址資金風險的 KYA、KYT 工具根本不需要連接錢包，輸入地址即可查詢，這便是知其然而不知其所以然的壞處，也是讓恐懼情緒操控自己的苦果。

對於新手投資者，最好的選擇永遠是更多地待在自身的認知邊界內，在充分學習了解的基礎上進行小成本的試錯，這是避免欺詐對自己造成重大損害的有效方法。

不要盲目信任，要去驗證

盲目自信之外，盲目他信也是損失的來源。包括相信搜尋引擎的錢包下載連結展示，相信社交平台中博主給出的空投連結，相信主動搭訕的網友會帶你賺錢等。

欺詐方式五花八門，但究其根本都是缺乏驗證。如果你有收藏權威 Web3 數據平台、官方社媒賬號、官方網站，那麼當你想要下載錢包 App 時，就至少有三個渠道能夠交叉驗證網友給你的或者你自己在網上搜尋到的下載連結是否安全；如果你保持了良好的交互習慣，你就會在每次重要交易提交前，在瀏覽器上查看合約的歷史交互紀錄，這樣就能夠第一時間發現異常現象；如果你進了一個群，人人都說自己在賺錢並極力邀請你加入，那麼你至少應該使用 KYA、KYT 工具考察一下相關地址，看是否已被標記為欺詐，而不是盲目衝入。

拒絕輕易相信他人，並持續保持驗證，會讓你的加密之旅變得平坦。

大多數 Crypto Scams 都是老騙術

正如絕大部分 Web3 協議並沒有對傳統互聯網的同類型業務帶來創新一樣，Crypto Scam 也同樣沒有脫離傳統互聯網欺詐的框架。

目前為止，絕大部分涉幣欺詐手法都能在傳統互聯網上找到原型，區別僅僅只是使用區塊鏈技術優化了原有的騙術，或者騙術本身就是以 Crypto 為目標。

例如冒充公檢法的騙局，傳統做法是要求受害人將法幣轉給欺詐者的銀行卡，現在會要求受害人去買幣並轉給特定地址；又例如很多人都知道「雙倍返還」是老騙術，可一旦這個騙術披上區塊鏈技術與 Musk 的外包裝，許多人又不認識了，還以為是技術創新。

深入學習已有的互聯網欺詐手法，將對你識別 Crypto Scam 有所幫助。

沉沒成本不是成本

中國有一句古話叫做「來都來了」，這句話的意思是某人在實現目標的過程中遇到了一些未曾預料的變動，為了不讓之前的付出被浪費，而選擇繼續進行下去。這一心理特點，遭到了欺詐者的廣泛利用。

前文提到的線下多簽欺詐便是如此。受害人從銀行取出大額現金，和朋友一起驅車前往數百公里外的地點，一路小心謹慎，沒想到到達現場後欺詐者會要求他下載新錢包，否則不予交易。受害人此時本可以選擇原路返回，但為了不讓之前的辛苦白費，而堅持參與交易，最後被欺詐者得手。

近期高發的加密貨幣殺豬盤 (Romantic Scam) 也是如此。受害人在開始懷疑對方之前，往往就已經投入了較多的資金，欺詐者利用受害人想要取回本金的心理，以繳稅、湊額度等為由要求加大投入，最終導致受害人越陷越深。

沉沒成本不是成本，面對自己認為是可能的騙局時，及時放棄也是止損的好方法，不應讓過去的付出成為未來決策的依據。

遭遇欺詐後該怎麼辦

遭遇 Crypto Scam 後挽回損失的最重要方式是尋求執法部門的幫助，因此受害人在意識到被騙後的所有挽回行為都應當為成功立案調查服務。

及時止損

在發現資產損失的第一時間，及時發起反制，能夠或多或少減少損失擴大，這些必要的動作包括——

- 如果是助記詞丟失，需快速將其餘資產轉移到安全的場所。這裡的「其餘資產」包括同一條鏈的其他代幣或 NFT，同一組助記詞派生的其他區塊鏈地址的資產，與被盜區塊鏈地址在同一部智能設備中的其他地址的資產等；
- 如果是投資理財類欺詐，則立即停止進一步的投入，並提款退出；
- 如果是授權盜幣，則需要儘快去取消所有地址的可疑授權。

當然，這些反制措施在進行過程中都要遵守前文提到的安全原則，否則存在遭遇其他欺詐的可能。

保護現場並報案

許多人在發現自己被騙、被盜後，第一反應是把被盜錢包、欺詐 App、欺詐者聊天方式刪除，甚至是將設備格式化，地址助記詞也不保留。這種過激行為是無法幫助挽回損失的，一則這並不能從根本解決問題，二則會給後續的調查造成困擾。例如——

- 刪除錢包 APP 將導致安全公司難以驗證是否為假錢包；
- 欺詐 APP 文件中可能會包含一些調查線索；
- 對立案、辦案過程中的取證環節造成影響。

受害人在止損過程中，必須要保護好案發現場。

尋求相關方幫助

這裡的相關方包括與被盜資產存在關聯的平台，以及能夠提供分析服務的安全公司。

假如你的鏈上地址被盜了，你應當時刻保持對資金轉移的關注，一旦發現資金有流入中心化交易平台的情況，便立即聯繫平台客服，要求平台對這個充值地址進行凍結。在你提交的證據足夠清晰的情況下，平台通常會對該賬戶提起 2–7 天的臨時風控，在這期間賬戶資金無法轉移。此時你再去請求執法部門向相關平台發函配合調查即可。

假如你和你身邊的朋友都缺乏對鏈上資金的追蹤能力，那麼你可以尋求專業的區塊鏈安全公司或者數據分析公司（例如 Bitrace）幫你找到被盜、被騙的原因，以及後續資金去向，甚至在案件偵查過程中提供一些幫助。

但不要到處找網友求助，一方面是絕大多數網友的言論都是噪音，對資產找回無益，另一方面目前有許多騙子也會冒充虛擬資產找回專家、某某平台官方客服等身份。

最後

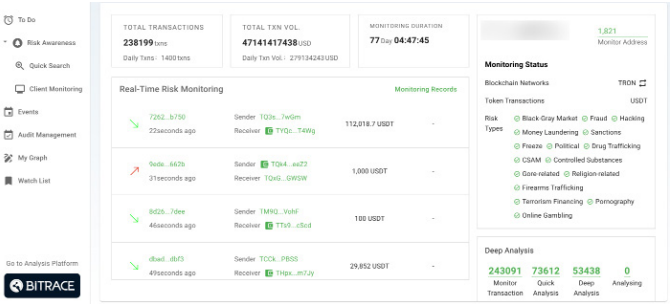
在這本手冊中，我們首先按照普通新手的投資生命週期，分階段介紹了不同時期可能會遇到的欺詐手法，接著對不同類別欺詐背後的原理與防範手段進行了解讀，最後列出了發現被欺詐後挽回損失的方法，旨在揭露常見的以及損害巨大的騙術，防止更多普通投資者遭受損失。

如果你或你身邊的朋友不幸遭遇了 Crypto Scam，也歡迎聯繫 Bitrace，我們將為受害人提供基本的分析幫助。

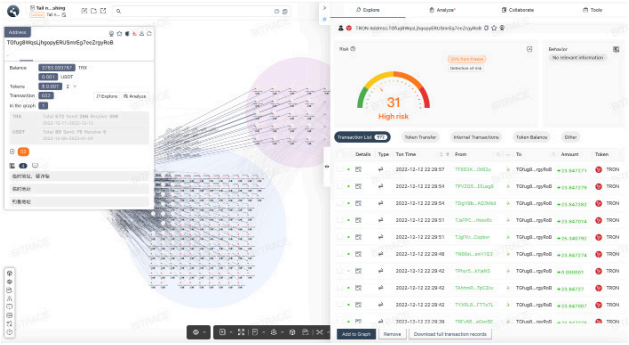
對於有加密資金風險檢測需求的用戶，也歡迎使用我們的產品，以更好地實現風險識別和預防。

對於個人，您可以訪問 https://detrust.bitrace.io/detrust-blacklist/ 並使用由 Bitrace 團隊推出的免費 KYA 小工具，一鍵查詢對手方地址是否具備任何風險，並基於地址風險評分決定是否要與對方進行資金互動。

對於存在較高交易頻率的機構（例如交易所、支付平台、OTC 商等），則可以使用企業版 Detrust 鏈上風險資金監測管理平台，對平台業務地址的全部交易完成監控覆蓋。當風險交易——包括風險資金流入或資金流出至風險地址時，風控人員將通過郵件、社群機器人等渠道收到即時提醒，以便及時處理已發生或即將發生的用戶風險活動。



對於有加密資金追蹤分析需求的團隊或執法機構，Bitrace Pro 可以為您提供可視化分析、實體識別、地址聚類、多方協作、智能監控警報等強大的功能，幫助您快速了解犯罪模式、追蹤資金流動、識別異常並發現新線索，幫助更快、更精準地開展調查。



您可以隨時聯繫我們，獲取產品 Demo。

關於 Bitrace

Bitrace 是一家以加密貨幣風險數據分析為核心的監管科技（Regtech）企業，我們致力於運用 AI 與大數據技術更準確高效地識別、監測鏈上的風險和犯罪活動，為客戶提供領先的監管、合規、調查工具產品與服務支持。

我們聚焦於加密犯罪調查領域，目前已與多國執法機構、Web3 企業進行協作與對接，完成數千起案例服務支持，累計監測數千億風險資金，並成功挽回數十億美元的損失。

網站：bitrace.io
電郵：support@bitrace.io
X（推特）：@Bitrace_team
LinkedIn：@Bitrace Tech

免責聲明

本手冊僅用於公眾教育和提高意識的目的。這是一個非營利性項目，旨在幫助個人更好地了解和防範加密貨幣欺詐。所提供的資訊並不構成法律、財務或專業建議。儘管我們努力確保內容的準確性，作者和出版商對內容的完整性或可靠性不作任何保證。Bitrace 及其關聯方對因使用本手冊而導致的任何損失或損害概不負責。建議讀者根據具體情況尋求專業建議。如有任何問題，歡迎隨時聯繫我們。