di Lorenzo Savastano*


# *Crypto-scam*: la truffa finanziaria al tempo dei *digital asset*

## 1. Nuovo linguaggio, vecchio mondo

Il termine inglese "*scam*" ha un'origine incerta. Potrebbe derivare dal britannico "*scamp*" (parola ottocentesca per indicare un "*vagabondo*") o dall'irlandese antico "*cam*" (che vuol dire "*sballato*") o, ancora, dal danese "*skam*" (una ruvida crasi tra i termini "*vergogna*" e "*farsa*", ovvero "*shame*" e "*sham*")[1].
Ad ogni modo, la parola ha assunto l'attuale significato di "*truffa*" solo nel 1963, quando fu utilizzata, con questa accezione, sulla rivista americana "*Time*". Sarà, poi, la pubblicazione degli esiti di una clamorosa inchiesta condotta dal *Federal Bureau of Investigation* (FBI), nel 1980, a consacrare il termine nel linguaggio comune, quando 19 funzionari governativi furono condannati per corruzione e associazione a delinquere.
Il nome dell'operazione? *AB-Scam*, ovviamente[2].
Oggi, nell'epoca della profusione degli anglismi, il termine "*scam*" **è associato in tutto il mondo a un suffisso con il quale, ormai, sembra formare una endiadi inossidabile: "***crytpo*".

Le *crypto-scam*, ovvero le truffe finanziarie collegate alla circolazione di *asset* digitali, sono infatti un fenomeno crescente e di crescente preoccupazione, con un valore che, nei soli Stati Uniti, ha sfiorato i 4 miliardi di dollari nel 2023, con un balzo in avanti del 53% rispetto al 2022[3].
Il presente contributo tenta di fornire una sorta di "*studio anatomico*" di questo nuovo genere di truffe, ad uso degli operatori di polizia che – sempre più, nel prossimo futuro – saranno tenuti a familiarizzare con i nomi moderni e sgargianti di un mondo che, tuttavia, resta oscuro quanto antico: quello del *crimine finanziario*.

## 2. Le fasi tipiche del *crypto-scam*

Operativamente, possiamo suddividere la dinamica della truffa in due momenti costitutivi essenziali, ancorché tipologicamente variabili: la fase di raccolta dei capitali dagli investitori e la fase di "*fuga*" dei collocatori/*scammers*, il c.d. *rug-pull*[4].


## 2.a. La fase di raccolta

La fase di raccolta dei capitali virtuali è lo stadio iniziale della truffa. Si tratta di una fase che, solitamene, si svolge totalmente nel mondo digitale: agli investitori viene proposta la vendita di un *token*, il cui valore economico è collegato alla realizzazione di un progetto di investimento scritturato all'interno del protocollo informatico della *blockchain* di riferimento.
Nella maggior parte dei casi, i *token* sono proposti agli investitori nell'ambito di:
- una *Initial Token Offering* (ITO), anche denominata *Initial Coin Offering* (ICO)[5], dove gli *asset* digitali sono venduti in cambio di valute aventi corso legale o di una valuta virtuale tendenzialmente stabile come *ether* o *bitcoin* (c.d. *paired currency*);

- meccanismi di *Launchpad* (noti anche come "*incubatori di criptovaluta*" o *Initial Exchange Offering* – IEO), in base ai quali *token* di nuova emissione sono riservati, a un prezzo vantaggioso, a coloro che – prima del lancio ufficiale – abbiano vincolato altri *token* già esistenti sulla *blockchain* del progetto.

In questa prima fase, l'obiettivo è dare *credibilità* al progetto, in modo da drenare liquidità dal mercato degli investitori che, attratti da forti (ma talvolta inconsistenti) prospettive di guadagno, cedono le proprie valute legali o virtuali in cambio dei *token* promossi dai collocatori.
A questo punto la dinamica dello *scam* è comprensibile mediante gli ordinari strumenti dell'economia di mercato: l'elevato numero di transazioni – sospinte da poderose campagne di *social marketing* in apposite *boiler room* presenti su piattaforme *social* come Reddit, Telegram o Twitter – contribuisce a innescare un *sentiment* di "*euforia*" sui *crypto*-mercati, aumentando la domanda dei *token* collegati al progetto, a fronte di un'offerta limitata.
Il valore economico "percepito" (e quindi il prezzo di acquisto) dell'*asset* digitale, pertanto, si eleva esponenzialmente e così anche l'accumulazione del capitale investito nell'iniziativa, seppure in assenza di un effettivo "decollo" del progetto sottostante.

## 2.b. La fase di *rug pull*

La massiccia raccolta di capitali dal pubblico degli entusiasti investitori crea le premesse per la fase finale dello *scam*: il *rug pull*, ovvero la repentina scomparsa del progetto e la (contestuale) "*fuga*" dei truffatori.
Tipicamente, il "*tappeto può essere tirato via*" (traduzione letterale di "*rug pull*") in tre modalità prevalenti:
- *liquidity stealing*: tramite l'attivazione di specifici *smart contract,* gli *scammers* sottraggono l'intero ammontare di valuta virtuale confluita nella *liquidity pool* associata al *token* in promozione, indirizzando il flusso di denaro digitale verso uno o più *wallet* riconducibili agli autori della truffa, disperdendone *de facto* le tracce.
Attesa la modalità di *exit* utilizzata dai truffatori, si tratta di una manovra fraudolenta solitamente impiegata in ambienti di finanza decentralizzata (*Decentralized Finance* – DeFi), dove gli *asset* digitali possono essere trattenuti in *wallet ad hoc* o – più comunemente – convertite in altre *crypto* (anche presenti su altre *blockchain*, c.d. *chain hopping*) e movimentate in modo volutamente complesso da un *wallet* all'altro;

- *sell orders limiting/malicious code*: in questa modalità di frode gli *smart contract* alla base del funzionamento del *token* sono programmati in modo da inibire agli utenti l'effettuazione di alcune azioni essenziali per finalizzare l'operazione di investimento, come ad esempio la possibilità di cedere le *res* digitali ad altri compratori *retail* su un mercato secondario;

- *pump-and-dump*: dopo l'iniziale decollo del valore del *token* (*pump*), si assiste al suo vertiginoso tracollo (*dump*). Il motivo della svalutazione, tuttavia, non è legata all'improvvisa scomparsa del progetto (c.d. *hard rug-pull*), quanto a scelte di

investimento da parte degli sviluppatori non coerenti con la logica iniziale della *tokenomics* presentata agli investitori (c.d. *soft rug-pull*).
Proprio per questo motivo, talvolta, gli schemi di *pump-and-dump* sono presentati più come un dilemma etico connesso alla manipolazione del mercato, piuttosto che come un vero e proprio atto truffaldino.

## 3. Vecchio mondo, nuove regole

Il fenomeno dei *crypto-scam* continuerà a essere una sfida insidiosa per le agenzie di *law enforcement* globali nei prossimi anni. Tuttavia, l'affermarsi di un'embrionale regolamentazione del settore – soprattutto in ambito unionale – sembra aver posto un primo, significativo, argine allo straripamento di questo genere di truffe.
Il riferimento è, in particolare, al Regolamento n. 1114/2023/UE (c.d. MiCAR – *Market in Crypto Asset Regulation*), che entrerà definitivamente in vigore entro il 31 dicembre 2024.
In particolare, il nuovo Regolamento, nel parificare la disciplina delle offerte al pubblico delle cripto-attività con quella vigente nel campo degli strumenti finanziari, ha introdotto un preciso obbligo di pubblicazione di un *white paper* associato a iniziative "promozionali" volte alla raccolta di *asset* virtuali sul mercato dei risparmiatori.
Nello specifico, il legislatore unionale ha evidenziato che, benché non vi sia un obbligo di descrizione dei rischi da ritendersi "*imprevedibili*", le informazioni inerenti ai *token* oggetto di emissione contenute nel *white paper* o nelle pertinenti comunicazioni di *marketing*, anche se effettuate attraverso *social media*, dovrebbero essere "*corrette, chiare e non fuorvianti*" [6].
Si tratta di un presidio preventivo importante: un "*documento di impianto*" del progetto carente di informazioni chiare, lineari e coerenti o finanche presentate agli investitori in modo approssimativo e poco professionale (come avvenuto nella vicenda denominata *Squid Token Scam* del novembre 2021), potrebbe difatti celare un intento truffaldino da parte dell'emittente.
Soprattutto, si tratta di un tentativo per contrapporre all'oscurità dei nuovi mercati digitali l'antidoto principale contro i sordidi tentativi di truffa finanziaria: la *chiarezza* delle informazioni.

***Ufficiale della Guardia di finanza***

**Note**
**1** - Fonte: *en.wiktionary.org, voce "Scam"*.
**2** - Per l'operazione l'FBI ha utilizzato un truffatore di nome *Melvin Weinberg*, che ha poi ispirato il personaggio di Irving Rosenfeld nel film *American Hustle* del 2013. Un interessante approfondimento sull'indagine AB-*scam* è reperibile sul sito ufficiale dell'agenzia statunitense (www.fbi.gov), nella sezione "*history*".
**3** - *Cfr*. FBI, *Internet Crime Report 2023*, pag. 12 e ss.. Per comprendere la dimensione del fenomeno, basta comparare il valore delle truffe connesse a valute digitali registrate negli USA nel 2023 (3,96 miliardi di dollari), con il valore complessivo di tutte le truffe *online* riportate nel medesimo anno (12,5 miliardi di dollari): oltre un terzo sono "*figlie degenere*" della tecnologia *blockchain*.
**4** - Tra i vari contributi presenti in rete, si segnalano, per chiarezza e schematicità: GJORGJEV J., *What are crypto exit scams, and how to protect against them?*, pubblicato su *cointelegraph.com* in data 8 aprile 2024; PUGGIONI V., *Crypto rug pulls: What is a rug pull in crypto and 6 ways to spot it*, pubblicato su *cointelegraph.com* in data 6 febbraio 2022.
**5** - Una panoramica esaustiva delle modalità con le quali possono essere emessi *token* all'interno di una *blockchain*, si rinvia a: AVELLA F., *I termini essenziali per navigare tra le cripto-attività*, in AA.VV. (a cura di AVELLA F.), *Bitcoin e Digital Asset*, Il Sole 24 Ore, 2023, pagg. 11 e ss..
**6** - Operativamente, tali oneri comunicativi sono poi sottoposti a una preventiva autorizzazione da parte dell'autorità di vigilanza, quando si tratta di c.d. asset-referenced token o di electronic-money token.
**7** - Al riguardo, l'avvento dell'intelligenza artificiale generativa potrebbe rappresentare una vera e propria minaccia per la sua capacitò di produrre testi verosimili e sorprendentemente accurati. Un rischio, del resto, sottolineato nel rapporto di Europol denominato "*ChatGPT: The impact of Large Language Models on Law Enforcement*", pubblicato il 27 marzo 2023.