FUORI CONTROLLO

di STEFANO PIAZZA

Chi si nasconde dietro le criptovalute

Non solo le truffe alla Bankman-Fried. L'arresto del fondatore della piattaforma Binance ha svelato anche i canali di finanziamento di Hamas, al Qaeda e Isis

NEI GUAI Sam Bankman-Fried, 31 anni, fondatore nel 2019 della piattaforma di interscambio di criptovalute Ftx, fallita nel 2022. Rischia una condanna a 110 anni

Lo scorso 21 novembre, Binance, noto exchange globale di criptovalute, e il suo fondatore, **Changpeng Zhao**, hanno riconosciuto la propria responsabilità in atti di riciclaggio di denaro e violazione delle sanzioni statunitensi. Il ceo di Binance «ha ammesso il suo coinvolgimento nelle accuse, sottolineando la mancanza di un sistema efficace per contrastare tale fenomeno». Dopo le ammissioni **Zhao** si è dimesso dalla carica e ha raggiunto un accordo con il Dipartimento di Giustizia degli Stati Uniti che prevede il pagamento di una sanzione pari a 4,3 miliardi di dollari per chiudere la vicenda. Al suo posto come nuovo ceo di Binance è stato nominato **Richard Teng**, già responsabile globale dei mercati regionali dell'exchange. Quindi tutto risolto? No: il Dipartimento di Giustizia, la Commodity Futures Trading Commission e il Dipartimento del Tesoro Usa hanno avviato un'azione legale congiunta contro Binance e il suo fondatore.

Nell'atto d'accusa si legge di come **Zhao** si sia adoperato per la crescita e l'aumento dei guadagni, tuttavia lo avrebbe fatto agendo in totale spregio delle regole approfittando anche dei buchi normativi. È stato inoltre provato come **Zhao** incoraggiava i suoi collaboratori ad agire in linea con quanto sostiene lo scrittore **Arthur Blonch** nella Legge di Murpy: «È più facile ottenere un perdono che un permesso».

Binance è accusata di aver consentito più di 100.000 transazioni in sostegno ad attività come il terrorismo e il traffico di droga. Ma c'è di più perché la piattaforma exchange avrebbe consentito più di 1,5 milioni di transazioni in valuta virtuale che violavano le sanzioni statunitensi e tra coloro che ne hanno beneficiato ci sono le Brigate al-Qassam di Hamas, la Jihad islamica palestinese (nell'ultimo anno hanno raccolto più di 200 milioni di dollari in criptovalute), al-Qaeda e lo Stato islamico. Il governo israeliano ha dichiarato di aver congelato i conti crittografici associati a gruppi come Hamas, la Jihad islamica palestinese e altri. La mossa ha cercato di interrompere - seppur tardivamente - un percorso che ha permesso loro di raccogliere milioni di dollari in criptovalute nel corso degli anni. I portafogli collegati ad Hamas e alla Jihad islamica palestinese hanno accumulato quasi 135 milioni di dollari tra agosto 2021 e giugno di quest'anno, secondo il *Wall Street Journal* che cita una ricerca delle società di analisi blockchain Elliptic e BitOK con sede a Tel Aviv. Altra pesantissima incriminazione riguarda un ulteriore meccanismo sviluppato sempre da Binance «per avvertire gli utenti di alto profilo nel caso fossero stati oggetto di indagini da parte delle forze dell'ordine». In base all'accordo di conciliazione **Changpeng Zhao** ha riconosciuto la propria responsabilità in merito alla violazione del Bank Secrecy Act, legge americana che disciplina il contrasto riciclaggio di denaro, oltre «ad aver indotto un'istituzione finanziaria a compiere analoghe violazioni». Per queste accuse il Dipartimento di Giustizia ha consigliato al tribunale di comminare una multa di 50 milioni di dollari all'ormai ex ceo di Binance che a seguito del pagamento di una cauzione pari a 175 milioni di dollari è stato rilasciato in attesa del processo fissato per il 23 febbraio 2024. Nella bufera Binance è finito persino **Cristiano Ronaldo**. Il calciatore è stato colpito da una class action presentata da alcuni querelanti che sostengono di aver subito perdite a causa della sua promozione di Binance. In un documento depositato il 27 novembre presso un tribunale in Florida si afferma che «**Ronaldo** ha promosso, assistito e/o partecipato attivamente all'offerta e alla vendita di titoli non registrati in coordinamento con Binance». A metà del 2022 Binance aveva avviato una partnership pluriennale con il calciatore portoghese per promuovere una serie di token non fungibili (Nft) di sua proprietà, con almeno tre collezioni dedicate alla stella del calcio e collegate a Binance.

Nella sua prima dichiarazione pubblica come ceo di Binance, **Richard Teng** ha affermato: «La mia competenza normativa influenzerà l'approccio di Binance in modo diverso rispetto al passato». Quello che è certo è che ora le autorità di vigilanza degli Stati Uniti vigileranno come mai prima. La vicenda di **Changpeng Zhao** ricorda molto da vicino quella del 31enne **Sam Bankman-Fried**, fondatore della piattaforma di interscambio di criptovalute Ftx (oggi fallita), che lo scorso 3 novembre è stato condannato da una giuria federale di New York per tutti i sette capi d'accusa per i quali era stato processato. Ora quello che era stato definito il «re delle crypto» rischia una condanna a 110 anni di carcere. Il processo è durato solo un mese e ha visto la pubblica accusa contare sul pentimento e la cooperazione di numerosi ex stretti collaboratori di **Bankman-Fried**. L'imputato in aula ha provato a difendersi affermando «di non aver mai voluto truffare nessuno e di aver voluto costruire una nuova industria regolamentata».

I giudici però non gli hanno creduto perché l'accusa ha portato in aula testimoni che hanno raccontato di come **Bankman-Fried** chiedeva ai suoi collaboratori «di truccare bilanci e di commettere reati, tra i quali facilitare segretamente i passaggi di fondi da Ftx al fondo hedge collegato Alameda Research». Ftx, nata nel 2019, in due anni aveva milioni di clienti e più di un miliardo di dollari di giro d'affari. Il fallimento avvenne nel 2022, quando si scoprirono buchi finanziari e una serie di truffe che portarono a bruschi ribassi delle criptovalute e alla fuga di clienti con i loro capitali. La procura ha definito «il re delle crypto» «uno spregiudicato miliardario impegnato in una colossale truffa che ha usato fondi di clienti, ingannandoli, per propri investimenti rischiosi, acquisti di immobili di lusso, donazioni politiche e spese personali per una vita da jet set tra i potenti». Gli avvocati di **Bankman-Fried** hanno dichiarato che il loro assistito «continuerà a sostenere la propria innocenza e a battersi contro le accuse», ma il procuratore federale di Manhattan, **Damian Williams**, la pensa diversamente: «Se l'industria delle cryptocurrency è nuova, e protagonisti quali **Sam Bankman-Fried** possono essere nuovi, questo genere di corruzione è antica. Questo caso è sempre stato incentrato sulle menzogne, l'inganno e il furto». Ora **Bankman-Fried** potrebbe dover affrontare altri processi in quanto è accusato di truffa bancaria e tangenti.

© RIPRODUZIONE RISERVATA

«COLLETTA» Raccolta fondi dell'Isis tramite criptovalute

POTENZIALE ALLARGAMENTO DEL CONFLITTO, MENTRE ISRAELE BOMBARDA IL SUD DI GAZA

Nave da guerra Usa attaccata nel Mar Rosso

Colpite anche imbarcazioni mercantili. Sospetti sulle milizie yemenite pro Iran

Israele ha allargato ieri la manovra terrestre al settore sud di Gaza. Lo ha confermato la radio militare: «Stanno operando a nord di Khan Yunis. In quell'area ci sono mezzi blindati che hanno iniziato ad attaccare obiettivi di Hamas» Secondo l'emittente, l'esercito intende così estendere le proprie attività di terra, dopo che nei giorni scorsi sono stati utilizzati ripetutamente i bombardamenti dell'artiglieria, della aviazione e della marina.

Grande preoccupazione invece per ciò che accade nel Mar Rosso; il cacciatorpediniere americano Uss Carney ieri ha risposto a droni e missili lanciati dal territorio dello Yemen controllato dai ribelli sciiti Houthi. Lo ha riferito un funzionario del Pentagono che ha precisato che il cacciatorpediniere era intervenuto in soccorso di due mercantili che navigavano nel Mar Rosso, al largo del porto yemenita di Hodeidah, che sono rimasti entrambi danneggiati da attacchi di droni. Una delle due navi colpite, sottolinea il sito del giornale israeliano *Haaretz*, è di una compagnia britannica di proprietà di **Danny Ungar**, figlio del magnate delle spedizioni israeliano **Rami Ungar**.

Il Pentagono ha confermato i fatti riguardo l'attacco alla Uss Carney e ad altre imbarcazioni commerciali e ha affermato «che offrirà informazioni non appena saranno disponibili». I cacciatorpedinieri statunitensi che operano nella regione hanno abbattuto numerosi droni nelle ultime settimane in un contesto di aumento degli incidenti che ha coinciso con gli attacchi israeliani contro Hamas. La settimana scorsa l'Uss Carney ha abbattuto un veicolo aereo senza pilota Kas-04 di fabbricazione iraniana mentre stava scortando una petroliera americana e una nave commerciale battente bandiera statunitense. Il drone proveniva da una zona dello Yemen controllata dagli Houthi.

John Kirby portavoce del Consiglio di sicurezza nazionale degli Stati Uniti, ha detto che «non ci sono negoziati ufficiali al momento per una nuova pausa umanitaria o per il rilascio degli ostaggi», anche se ha affermato che gli Stati Uniti «sperano che i colloqui riprendano sulla buona strada». **Kirby**, ai microfoni del programma *Meet the Press* della Nbc, ha aggiunto «È inaccettabile che alla Croce Rossa non sia stato concesso l'accesso agli ostaggi tenuti prigionieri a Gaza. Hamas ha accettato di consentire alla Croce Rossa l'accesso a questi ostaggi mentre era in vigore la pausa e, naturalmente, ciò non è accaduto e non sta ancora accadendo».

S. Pia.

© RIPRODUZIONE RISERVATA

SPIAZZATO Joe Biden, 81 anni

L'INTERVISTA **MARCO RAMILLI**

«Il pericolo frodi in Italia è alto Ecco le più diffuse»

L'esperto: «I controlli stanno aumentando, ma non bastano Serve anche educazione finanziaria e da noi è insufficiente»

Marco Ramilli è un esperto internazionale di sicurezza informatica, ceo e co-fondatore di Yoroi.

Che giudizio possiamo dare della vicenda Binance?

«Esprimere un giudizio su questo settore, sostanzialmente nuovo e caratterizzato da normative a "macchie di leopardo", è complesso. Mentre in alcuni Stati le regole sono diventate chiare, in altri rimangono oscure e in evoluzione. L'implementazione di controlli mirati e l'istituzione di regolamenti rigorosi, simili a quelli applicati agli istituti di credito o alle società di gestione del risparmio, insieme alla necessità di fornire prove dettagliate sulle transazioni e autenticare gli utilizzatori, rappresentano nuovi strumenti introdotti dai regolatori che certamente hanno contribuito a individuare frodi o attività poco trasparenti. Tuttavia, al di là di questi controlli, è cruciale promuovere la formazione degli utenti, ossia dei clienti, di questi nuovi servizi finanziari. In Paesi come l'Italia, l'educazione finanziaria non è ancora sufficientemente diffusa, contribuendo così al proliferare delle frodi».

Si parla molto di truffe legate alle criptovalute: quali sono le più comuni e come evitarle?

«Iniziamo con le truffe verso le Ico (Initial coin offering): offerte iniziali di criptovalute che raccolgono fondi per progetti finti o inesistenti. Gli investitori che desiderano affrontare tali tipologie di investimento dovrebbero condurre approfondite ricerche sul team, sul progetto e sulla effettiva realizzazione prima di partecipare a qualsiasi Ico. Poi citerei la "Pump and dump fraud", che coinvolge le manipolazioni del mercato. I truffatori acquistano massicciamente una criptovaluta per innalzarne il prezzo (pump) e poi vendono improvvisamente tutto in unica transazione (dump), causando una forte volatilità del mercato ed un effetto trascinamento. In assenza di regolamentazioni internazionali specifiche su una quota massima di negoziazione su criptovalute, gli investitori dovrebbero valutare la possibilità di evitare l'emotività e di agire considerando la reale possibilità di essere nel mezzo di un "pump and dump". Il fenomeno potrebbe durare per alcuni giorni. Poi ci sono le truffe di phishing: queste truffe, ormai tradizionali, coinvolgono tentativi di ottenere informazioni personali o chiavi private di wallet o exchange, attraverso falsi siti web o e-mail che sembrano autentiche. Lo "Scam mining", invece, simula servizi di mining in cloud (generazione di criptovaluta) promettendo rendimenti elevati giustificati da macchine di mining molto performanti. I servizi fasulli possono mostrare rendimenti (nell'area riservata) fittizi e nel momento in cui gli operatori iniziano a richiedere gli incassi (trasferimento fondi verso il proprio istituto di credito) essi spariscono. Ci sono poi i wallet fraudolenti: app o portali degli falsi che cercano di rubare le chiavi private degli utenti al fine di impossessarsi delle proprie valute elettroniche. E, infine, le truffe di investimento: programmi che promettono rendimenti elevati senza rischio, spesso promossi attraverso social media o e-mail».

Secondo gli esperti sulle sanzioni del Consiglio di sicurezza dell'Onu contro Pyongyang, hacker legati alla Corea del Nord sono stati responsabili di furti di criptovalute per un valore di quasi 1,7 miliardi di dollari nel 2022. Chi sono?

«Tipicamente quanto ci si riferisce ad attori della Corea del Nord ci si riferisce al gruppo Lazzarus. Il termine è, infatti, spesso utilizzato per descrivere gruppi di cyber criminali sospettati di avere legami con il regime di Pyongyang. Il gruppo Lazarus è stato associato a diversi attacchi informatici di ampia portata, tra cui il noto attacco al sistema bancario bangladese nel 2016, nonché al ransomware WannaCry nel 2017. Questi hacker sono spesso accusati di condurre attività cyber criminali per finanziare il governo nordcoreano o per scopi di spionaggio. È importante notare che l'attribuzione degli attacchi informatici a gruppi specifici può essere complessa, poiché gli hacker spesso cercano di mascherare la loro vera identità. Gli esperti di sicurezza informatica e le agenzie di intelligence internazionali fanno del loro meglio per analizzare le prove digitali e determinare l'origine degli attacchi ma la certezza è sempre difficile da garantire. La prevenzione dipende molto dal tipo di organizzazione (o privato) da difendere. Come pratica generale, per comprendere la difesa da adottare, consiglio di considerare la propria infrastruttura compromessa e di rispondere alla doma: cosa fare nel momento in cui sono certo che l'attaccante è all'interno della mia "rete" ?».

Spesso le cronache parlano degli hacker russi, cinesi e iraniani. Se dovessimo stilare una classifica chi sono i più pericolosi e perché?

«Non ritengo sia appropriato stilare una classifica basata sulla "pericolosità" degli attori criminali, poiché ognuno di essi ha scopi e obiettivi diversi. In particolare, abbiamo osservato che gli attori all'interno dell'ecosistema iraniano si distinguono per la loro pericolosità ed efficienza nel settore "energetico". Da parte russa, ci sono attori molto attivi nel settore dello spionaggio, mentre ex-militari russofoni si concentrano su attacchi contro istituti di credito. Altri attori sono attivi nel settore del ransomware, specializzandosi in attacchi contro organizzazioni private».

S. Pia.

© RIPRODUZIONE RISERVATA

CEO Marco Ramilli è co-fondatore di Yoroi, che si occupa di cyber risk

Con i Bitcoin si rischia la crisi idrica

Dopo una sola transazione servono i litri di un'intera piscina per raffreddare i centri dati surriscaldati. Con questo trend il consumo di acqua crescerà del 40%

Un recente studio pubblicato da Cell Reports Sustainability stima che una singola transazione di Bitcoin consuma in media 16.000 litri di acqua, una quantità equivalente a riempire una piscina da giardino. Questo consumo è particolarmente preoccupante in aree con scarsità d'acqua, come l'Asia centrale e gli Stati Uniti.

Nel 2021, Greenidge Generation, una società che produce Bitcoin ed energia, ha attirato l'attenzione per aver presumibilmente scaricato grandi volumi di acqua calda nel lago Seneca di New York. Nel 2019 la società aveva riconvertito una centrale elettrica abbandonata, aumentando e emissioni di carbonio e i l consumo di acqua. I residenti hanno espresso preoccupazione sul fatto che gli scarichi di acqua calda stiano riscaldando il lago Seneca oltre gli standard statali di qualità dell'acqua. Nel 2023, i gruppi ambientalisti hanno citato in giudizio la Greenidge Generation per aver violato il Clean Water Act e altre normative ambientali, ma la causa è stata archiviata. Nonostante questo caso di alto profilo e la minaccia incombente di una crisi idrica globale, l'utilizzo dell'acqua da parte della rete Bitcoin è rimasto relativamente sottostimato.

Tra i due e i tre miliardi di persone in tutto il mondo già soffrono di carenza idrica, una situazione destinata a peggiorare nei prossimi decenni. A causa delle crescenti preoccupazioni internazionali sulla disponibilità di acqua potabile è fondamentale comprendere l'impronta idrica dell'estrazione di Bitcoin e il suo impatto. Si stima che l'attività di mining di Bitcoin sia responsabile del consumo di 1.572,3 gigalitri (gl) di acqua nel 2021. (Il mining è ciò che permette alla rete Bitcoin di funzionare, creando nuovi blocchi sulla blockchain e verificando le transazioni Bitcoin. Le transazioni vengono verificate dai miner che utilizzano un hardware speciale per risolvere dei puzzle matematici).

Una migliore comprensione dell'impronta idrica di Bitcoin aiuterà a facilitare lo sviluppo di un approccio responsabile per gestire la limitata fornitura di acqua dolce. **Alex de Vries**, il ricercatore che sta esaminando l'impronta della criptovaluta, prevede un aumento di oltre il 40% del consumo di acqua se la tendenza continuerà in questo modo. L'aumento è dovuto al meccanismo di «Proof of Work» (PoW) ad alta intensità energetica che è alla base del mining di Bitcoin. È un processo che richiede una notevole potenza di calcolo, con conseguente necessità di sistemi di raffreddamento estesi per i centri dati e le centrali elettriche. L'affidamento a fonti di energia rinnovabili per **de Vries** non è sufficiente a compensare l'impatto ambientale a causa della loro limitata disponibilità. Il ricercatore indica invece il modello PoS («Proof of Stake»), a cui Ethereum è passato nel 2022, come un'alternativa più sostenibile. Il PoS riduce la necessità di hardware ad alta intensità energetica consentendo alle criptovalute di aumentare la probabilità di convalida delle transazioni.

Mentre la comunità delle criptovalute guarda al futuro, **de Vries** avverte «che vanno abbandonate le pratiche non sostenibili». Se non adattano la loro tecnologia, rischiano di trovarsi in una partita persa contro la sostenibilità ambientale, uno scenario che potrebbe avere gravi implicazioni per la redditività a lungo termine del settore. Gli sviluppatori di criptovalute devono quindi trovare nuovi modi per ridurre il consumo di acqua e l'impatto energetico del mining. Il passaggio a modelli di consenso più sostenibili, come il PoS, è una possibilità, ma è necessario un ulteriore lavoro e volontà per garantire che queste soluzioni siano efficaci.

S. Pia.

© RIPRODUZIONE RISERVATA