

Uso criminale delle criptovalute: come le forze dell'ordine indagano sul riciclaggio digitale

Maria Cattini | 17/04/2025 | Sicurezza digitale

Uso criminale delle criptovalute: Le criptovalute hanno rivoluzionato il settore finanziario, offrendo transazioni rapide, decentralizzate e spesso anonime. Tuttavia, la stessa tecnologia che abilita l'innovazione economica è anche sfruttata dai criminali per riciclaggio di denaro, frodi e finanziamento del terrorismo.

Come possono gli investigatori contrastare questo fenomeno? Quali strumenti esistono per tracciare le transazioni illecite? Un recente manuale, *Financial Investigations and Analysis for Emerging Money Laundering Risks: Criminal Use of Cryptocurrency*, a cura di Federico Paesano per il programma COPOLAD III, fornisce una guida dettagliata per le forze dell'ordine e gli analisti finanziari.

[Scarica la nostra Guida](#)

Criptovalute e crimini finanziari

Perché i criminali usano le criptovalute?

Le criptovalute attraggono attività illecite per diverse ragioni:

- Pseudonimato: nonostante le transazioni siano registrate su blockchain, l'identità dei proprietari dei wallet non è immediatamente visibile.
- Globalità: eliminano i confini geografici e i controlli bancari tradizionali.
- Irreversibilità: una volta confermata, una transazione non può essere annullata.
- Strumenti di anonimizzazione: come i mixer di criptovalute e il chain hopping (scambio tra più blockchain).

Le principali criptovalute usate per il crimine

- Bitcoin (BTC): la criptovaluta più diffusa, spesso usata per transazioni illecite nonostante la sua tracciabilità.
- Monero (XMR): progettata per garantire il massimo anonimato, è la preferita nei mercati del darknet.
- Ethereum (ETH) e stablecoin: usate per transazioni rapide, spesso in frodi e schemi Ponzi.

Metodi criminali con le criptovalute

1. Riciclaggio di denaro digitale

Il riciclaggio di denaro tramite criptovalute avviene in diverse fasi:

- Stratificazione (Layering): i fondi illeciti vengono trasferiti attraverso molteplici wallet e scambiati

con altre criptovalute.

- **Integrazione:** il denaro riciclato rientra nel sistema economico, spesso con acquisti immobiliari o beni di lusso.

2. Ransomware e cybercrimine

Gli attacchi ransomware sono tra le attività più comuni finanziate con criptovalute. I criminali infettano i computer con malware, chiedendo riscatti in Bitcoin o Monero.

3. Finanziamento del terrorismo

Gruppi terroristici utilizzano criptovalute per trasferire fondi senza passare dai sistemi bancari tradizionali. Le stablecoin e le reti come Lightning Network rendono ancora più difficile il tracciamento.

4. Truffe e frodi

Le truffe in ambito crypto comprendono:

- **Schemi Ponzi:** promesse di rendimenti irrealistici per attirare investitori.
- **Fake ICO (Initial Coin Offerings):** lancio di criptovalute inesistenti per raccogliere fondi e poi scomparire.
- **Romance scam e phishing:** inganni via social media per rubare criptovalute.

Tecniche investigative per le forze dell'ordine

1. Tracciamento delle transazioni sulla blockchain

Nonostante l'apparente anonimato, le transazioni su blockchain sono pubbliche e permanenti. Le forze dell'ordine possono usare strumenti di **blockchain analytics** come:

- **Chainalysis:** traccia i flussi di criptovalute e identifica wallet sospetti.
- **Elliptic e CipherTrace:** strumenti per il monitoraggio delle transazioni.
- **GraphSense:** un software open-source che analizza blockchain.

2. Identificazione dei wallet privati

I **wallet non custodial** (o unhosted wallets) sono difficili da tracciare, ma possono essere identificati attraverso:

- **Analisi degli indirizzi IP** associati ai wallet.
- **Incrocio dei dati** con exchange e fornitori di servizi (VASPs).
- **Sequestri hardware:** dispositivi come Ledger o Trezor contengono tracce digitali che possono essere estratte dagli investigatori.

3. Monitoraggio delle transazioni sospette

Gli **exchange di criptovalute** devono rispettare normative antiriciclaggio (AML) e segnalare transazioni sospette. Alcuni indici di rischio (*red flag indicators*) includono:

- Alte somme trasferite in breve tempo.
- Uso eccessivo di mixer o privacy coins.
- Conversione rapida da criptovalute a contante.

4. Cooperazione internazionale

Le indagini sulle criptovalute richiedono collaborazione tra diverse giurisdizioni. Alcuni strumenti chiave includono:

- INTERPOL e Europol: facilitano il coordinamento tra forze di polizia internazionali.
- Mutual Legal Assistance Treaties (MLATs): trattati bilaterali per condividere informazioni su crimini finanziari.
- Joint Investigative Teams (JITs): squadre investigative comuni tra paesi alleati.

Regolamentazione e conformità

Le normative globali sulle criptovalute

Organismi come il **Financial Action Task Force (FATF/GAFI)** hanno introdotto regolamenti per contrastare il riciclaggio di denaro con le criptovalute:

- Travel Rule: obbliga gli exchange a raccogliere dati sugli utenti che effettuano transazioni superiori a una soglia prestabilita.
- AML/CFT Regulations: obblighi di antiriciclaggio per i fornitori di servizi crypto.
- Obblighi di registrazione per gli exchange e wallet provider.

Sfide nella regolamentazione

- Differenze tra le giurisdizioni: ogni paese ha regolamenti diversi, rendendo difficile l'armonizzazione.
- Tecnologie emergenti: le nuove soluzioni blockchain, come le DeFi (Finanza Decentralizzata), rendono ancora più difficile il monitoraggio.
- Privacy vs. Sicurezza: il bilanciamento tra la tutela della privacy e il contrasto ai crimini finanziari è una sfida per legislatori e autorità.

Rafforzare le capacità investigative

Il documento del programma COPOLAD III offre diverse raccomandazioni per migliorare le indagini sulle criptovalute:

- Formazione avanzata per le forze dell'ordine: gli investigatori devono essere addestrati nelle tecniche di analisi blockchain.
- Collaborazione tra pubblico e privato: partnership con exchange e aziende di analisi blockchain per migliorare la tracciabilità delle transazioni.
- Adozione di tecnologie AI per il tracciamento: gli strumenti basati su intelligenza artificiale possono aiutare a identificare pattern di riciclaggio di denaro.

<https://www.coondivido.it/attacchi-informatici-alle-criptovalute/>

L'uso criminale delle criptovalute è una sfida sempre più complessa, ma grazie ai progressi nelle tecniche investigative e nelle normative globali, è possibile contrastare il riciclaggio di denaro e il finanziamento del terrorismo. La chiave sta nella collaborazione internazionale, nell'adozione di tecnologie avanzate e nella formazione continua degli investigatori.

Le criptovalute non sono di per sé criminali, ma la loro regolamentazione e il monitoraggio delle transazioni sono essenziali per prevenire gli abusi e garantire la sicurezza finanziaria globale.

Vuoi approfondire queste tematiche? Scarica il Manuale

[Manuale_criptovalute_PDFDownload](#)

Uso criminale delle criptovalute: Le criptovalute hanno rivoluzionato il settore finanziario, offrendo transazioni rapide, decentralizzate e spesso anonime. Tuttavia, la stessa tecnologia che abilita l'innovazione economica è anche sfruttata dai criminali per riciclaggio di denaro, frodi e finanziamento del terrorismo.

Come possono gli investigatori contrastare questo fenomeno? Quali strumenti esistono per tracciare le transazioni illecite? Un recente manuale, *Financial Investigations and Analysis for Emerging Money Laundering Risks: Criminal Use of Cryptocurrency*, a cura di Federico Paesano per il programma COPOLAD III, fornisce una guida dettagliata per le forze dell'ordine e gli analisti finanziari.

[Scarica la nostra Guida](#)

Criptovalute e crimini finanziari

Perché i criminali usano le criptovalute?

Le criptovalute attraggono attività illecite per diverse ragioni:

- Pseudonimato: nonostante le transazioni siano registrate su blockchain, l'identità dei proprietari dei wallet non è immediatamente visibile.
- Globalità: eliminano i confini geografici e i controlli bancari tradizionali.
- Irreversibilità: una volta confermata, una transazione non può essere annullata.
- Strumenti di anonimizzazione: come i mixer di criptovalute e il chain hopping (scambio tra più blockchain).

Le principali criptovalute usate per il crimine

- Bitcoin (BTC): la criptovaluta più diffusa, spesso usata per transazioni illecite nonostante la sua tracciabilità.
- Monero (XMR): progettata per garantire il massimo anonimato, è la preferita nei mercati del darknet.
- Ethereum (ETH) e stablecoin: usate per transazioni rapide, spesso in frodi e schemi Ponzi.

Metodi criminali con le criptovalute

1. Riciclaggio di denaro digitale

Il riciclaggio di denaro tramite criptovalute avviene in diverse fasi:

- Stratificazione (Layering): i fondi illeciti vengono trasferiti attraverso molteplici wallet e scambiati con altre criptovalute.
- Integrazione: il denaro riciclato rientra nel sistema economico, spesso con acquisti immobiliari o beni di lusso.

2. Ransomware e cybercrimine

Gli attacchi ransomware sono tra le attività più comuni finanziate con criptovalute. I criminali infettano i computer con malware, chiedendo riscatti in Bitcoin o Monero.

3. Finanziamento del terrorismo

Gruppi terroristici utilizzano criptovalute per trasferire fondi senza passare dai sistemi bancari tradizionali. Le stablecoin e le reti come Lightning Network rendono ancora più difficile il tracciamento.

4. Truffe e frodi

Le truffe in ambito cripto comprendono:

- Schemi Ponzi: promesse di rendimenti irrealistici per attirare investitori.
- Fake ICO (Initial Coin Offerings): lancio di criptovalute inesistenti per raccogliere fondi e poi scomparire.
- Romance scam e phishing: inganni via social media per rubare criptovalute.

Tecniche investigative per le forze dell'ordine

1. Tracciamento delle transazioni sulla blockchain

Nonostante l'apparente anonimato, le transazioni su blockchain sono pubbliche e permanenti. Le forze dell'ordine possono usare strumenti di **blockchain analytics** come:

- Chainalysis: traccia i flussi di criptovalute e identifica wallet sospetti.
- Elliptic e CipherTrace: strumenti per il monitoraggio delle transazioni.
- GraphSense: un software open-source che analizza blockchain.

2. Identificazione dei wallet privati

I **wallet non custodial** (o unhosted wallets) sono difficili da tracciare, ma possono essere identificati attraverso:

- Analisi degli indirizzi IP associati ai wallet.
- Incrocio dei dati con exchange e fornitori di servizi (VASPs).
- Sequestri hardware: dispositivi come Ledger o Trezor contengono tracce digitali che possono essere estratte dagli investigatori.

3. Monitoraggio delle transazioni sospette

Gli **exchange di criptovalute** devono rispettare normative antiriciclaggio (AML) e segnalare transazioni sospette. Alcuni indici di rischio (*red flag indicators*) includono:

- Alte somme trasferite in breve tempo.
- Uso eccessivo di mixer o privacy coins.
- Conversione rapida da criptovalute a contante.

4. Cooperazione internazionale

Le indagini sulle criptovalute richiedono collaborazione tra diverse giurisdizioni. Alcuni strumenti chiave includono:

- INTERPOL e Europol: facilitano il coordinamento tra forze di polizia internazionali.
- Mutual Legal Assistance Treaties (MLATs): trattati bilaterali per condividere informazioni su crimini finanziari.
- Joint Investigative Teams (JITs): squadre investigative comuni tra paesi alleati.

Regolamentazione e conformità

Le normative globali sulle criptovalute

Organismi come il **Financial Action Task Force (FATF/GAFI)** hanno introdotto regolamenti per

contrastare il riciclaggio di denaro con le criptovalute:

- Travel Rule: obbliga gli exchange a raccogliere dati sugli utenti che effettuano transazioni superiori a una soglia prestabilita.
- AML/CFT Regulations: obblighi di antiriciclaggio per i fornitori di servizi crypto.
- Obblighi di registrazione per gli exchange e wallet provider.

Sfide nella regolamentazione

- Differenze tra le giurisdizioni: ogni paese ha regolamenti diversi, rendendo difficile l'armonizzazione.
- Tecnologie emergenti: le nuove soluzioni blockchain, come le DeFi (Finanza Decentralizzata), rendono ancora più difficile il monitoraggio.
- Privacy vs. Sicurezza: il bilanciamento tra la tutela della privacy e il contrasto ai crimini finanziari è una sfida per legislatori e autorità.

Rafforzare le capacità investigative

Il documento del programma COPOLAD III offre diverse raccomandazioni per migliorare le indagini sulle criptovalute:

- Formazione avanzata per le forze dell'ordine: gli investigatori devono essere addestrati nelle tecniche di analisi blockchain.
- Collaborazione tra pubblico e privato: partnership con exchange e aziende di analisi blockchain per migliorare la tracciabilità delle transazioni.
- Adozione di tecnologie AI per il tracciamento: gli strumenti basati su intelligenza artificiale possono aiutare a identificare pattern di riciclaggio di denaro.

<https://www.coondivido.it/attacchi-informatici-alle-criptovalute/>

L'uso criminale delle criptovalute è una sfida sempre più complessa, ma grazie ai progressi nelle tecniche investigative e nelle normative globali, è possibile contrastare il riciclaggio di denaro e il finanziamento del terrorismo. La chiave sta nella collaborazione internazionale, nell'adozione di tecnologie avanzate e nella formazione continua degli investigatori.

Le criptovalute non sono di per sé criminali, ma la loro regolamentazione e il monitoraggio delle transazioni sono essenziali per prevenire gli abusi e garantire la sicurezza finanziaria globale.

Vuoi approfondire queste tematiche? Scarica il Manuale

[Manuale_criptovalute_PDFDownload](#)