01/03/2018

CRIPTOVALUTE: I SISTEMI DI MIXAGGIO PER IL RICICLAGGIO DI DENARO

di Sabrina Familiari

Bisogna rivolgersi a *exchangers*[1] specializzati nella conversione di moneta avente corso legale in criptovalute per poter acquistare e definirsi proprietari di valute virtuali. Non è possibile acquistare bitcoin in maniera del tutto anonima, in quanto, al momento della registrazione, è necessario fornire le proprie generalità allegando i documenti d'identità (o patente di guida o passaporto) nel rispetto degli obblighi del Know Your Customer[2]. Una volta acquistati bitcoin e dopo aver creato il proprio *wallet*[3], il portafoglio virtuale è collegato al proprio conto corrente bancario o alla propria carta di credito. Siccome la rete delle criptovalute utilizza indirizzi[4] bitcoin che non

[1] Gli *exchangers* sono definiti dall'art. 3 del d.lgs. 90/2017 quali "*prestatori di servizi relativi all'utilizzo di valuta virtuale, limitatamente allo svolgimento dell'attività di conversione di valute virtuali da ovvero in valute aventi corso forzoso*". Gli *exchanger* si distinguono in centralizzati e decentralizzati. Tra i primi rientrano Coinbase, Kraken, Bitstamp, TheRockTrading. Lo svantaggio di queste piattaforme è che nel momento in cui vengono versate le criptovalute, ne viene persa la proprietà e la disponibilità. Di contro hanno il vantaggio di lavorare un numero elevato di transizioni. Al contrario gli *exchanger* decentralizzati si basano sulla tecnologia della *blockchain*, che garantisce il controllo dei propri beni, ma elabora un limitato numero di transazioni, con costi di commissioni più elevati.

[2] L'art.17 del d.lgs. 90/2017 prevede che gli intermediari finanziari e gli altri soggetti che svolgono un'attività finanziaria osservano gli obblighi di adeguata verifica della clientela in relazione ai rapporti e alle operazioni inerenti allo svolgimento della loro attività istituzionale o professionale. Gli obblighi di adeguata verifica della clientela consistono nell'identificazione del cliente sulla base di documenti, dati o informazioni ottenuti da una fonte attendibile e indipendente; identificazione dell'identità del titolare effettivo; nella presa conoscenza dello scopo e della natura del rapporto continuativo o della prestazione professionale; nel controllo costante nel corso del rapporto continuativo o della prestazione professionale.

[3] Il *wallet* è un portafoglio elettronico che permette di trasferire bitcoin attraverso la rete a chiunque abbia attivato un indirizzo bitcoin tramite un sistema di crittografia a chiave pubblica-privata.

[4] L'indirizzo è un *hash* della chiave pubblica utilizzata quale identità virtuale dell'utente.

identificano per nome e cognome un utente, nel momento in cui vengono scambiati bitcoin, questi vengono spostati da un indirizzo a un altro e la *blockchain* registra tutte le transazioni eseguite, ovvero i destinatari dei pagamenti, gli indirizzi e il saldo del portafoglio. Un utente può però avere più identità nel sistema e spostare bitcoin tra queste identità.

Esistono tuttavia delle piattaforme che assicurano un acquisto rapido e veloce e totalmente anonimo dove non viene richiesto di rivelare la propria identità. LocalBitcoin[5] è una di queste piattaforme. Su questa piattaforma, una volta inseriti e inviati i propri dati, è possibile acquistare o vendere bitcoin inserendo un semplice annuncio in cui viene indicato il metodo di pagamento e il tasso di cambio. Ancora più rapido è il sistema che consente di scegliere dove acquistare bitcoin in una lista di venditori, inserendo dei parametri inseriti quali la quantità desiderata, il paese di provenienza e il metodo di pagamento [6]. Lo stesso procedimento deve essere seguito nel caso di vendita di bitcoin[7].

Sono stati ideati dei sistemi che assicurano l'anonimato. Quello più diffuso è quello di nascondere le transazioni mescolandole tra quelle di più utenti. Nella forma più semplice, la miscelazione avviene attraverso un server di mixaggio: ogni utente invia un nuovo indirizzo in crittografia, forma il mix e trasferisce la sua moneta al mix, che decodifica e mescola casualmente gli indirizzi nuovi e restituisci bitcoin a ciascuno di essi. Affinchè l'anonimato venga garantito, il *mixer* non deve registrare e rivelare la relazione tra gli indirizzi di *input* e *output*[8].

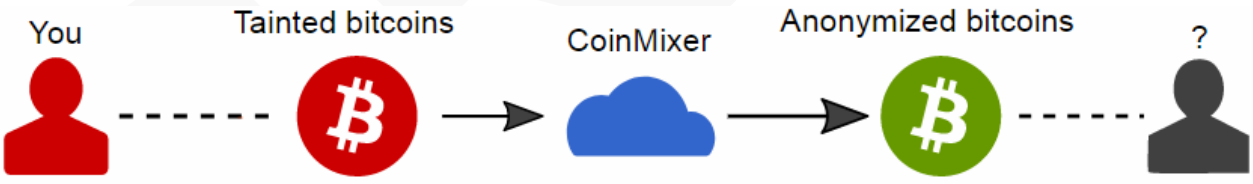

Figura 1. Flusso di lavoro di base di un servizio di Mixing Bitcoin

[5] Il sito internet di riferimento è www.localbitcoin.com

[6] Su questa piattaforma l'acquisto può avvenire anche tramite bonifico bancario o tramite l'acquisto di persona presso ATM bitcoin locali o con carta di debito tramite circle.com.

[7] Le transazioni di vendita vengono effettuate mediante un deposito di garanzia, dove deve comunque essere garantito il metodo di pagamento proposto dal cliente.

[8] Figura 1: Flusso di lavoro di base di un servizio di Mixing Bitcoin. Cfr. https://coinmixer.se/it/bitcoin-mixing-service/come-utilizzare-bitcoin-in-modo-anonimo/#references

Esiste poi un secondo metodo che prende il nome di CoinJoin. Tale sistema è stato introdotto da Gregory Maxwell nel 2013 e funziona sulla base della fiducia tra più utenti che si mettono d'accordo per unire le proprie transazioni e mescolare le proprie monete, senza modificare il protocollo Bitcoin. Tale metodo aumenta la privacy degli utenti in quanto non è più dimostrabile che tutti gli *input* di una transazione provengano dallo stesso *wallet* e quindi dallo stesso utente.

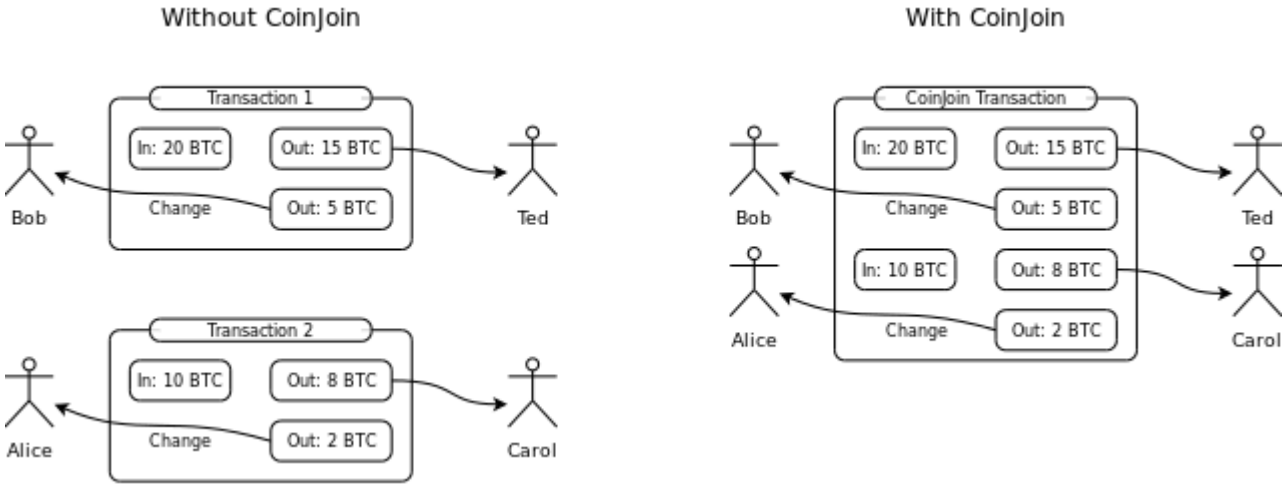

Figura 2. Esempio di idea di base: due transazioni sono unite in una mentre input e output sono invariati.

CoinJoin presenta delle problematiche di garanzia dell'anonimato, in quanto si può avvalere di servizi centralizzati e di registri delle transazioni effettuate che possono non garantire la privacy degli utenti. Per aggirare la problematica della centralizzazione, sono state create diverse implementazioni di transazioni anonime di bitcoin ispirate a CoinJoin, che non richiedono che terze parti siano coinvolte nella registrazione di transazioni miste. Tra queste implementazioni sono da citare CoinShuffle, Dark Wallet, SharedCoins, JoinMarket. Coinshuffle[9] è stato elaborato da alcuni ricercatori dell'Università del Saarland nel 2014 e utilizza il sistema di Coinjoin ricorrendo all'*Elliptic Curve Digital Signature Algorithm* (ECDSA). Essendo la dimensione in bit della chiave pubblica necessaria all'ECDSA circa il doppio della dimensione del livello di sicurezza in bit, viene garantita maggiore sicurezza.

Il software DarkWallet è un portafoglio digitale *open source*, ideato da Cody Wilson, che offusca le transazioni bitcoin effettuate nel mercato *online* rendendo anonimi i dati, ottenendo lo stesso effetto di CoinJoin senza però fare affidamento ad un sistema centralizzato.

[9] Coinshuffle è stato elaborato da alcuni ricercatori dell'Università del Saarland nel 2014.

Accanto ai servizi di mixaggio, sono state create delle monete che incorporano servizi di mixaggio come parte della loro *blockchain*. ZeroCoin utilizza un protocollo ZeroCash, che funziona con un sistema di crittografia che assicura agli utenti di condurre transazioni mascherando l'importo e l'origine del pagamento. Monero, ampiamente utilizzata nel *deep web*, è stata lanciata nel 2014 per garantire privacy e sicurezza. Nel suo portafoglio sono presenti numerosi nodi[10] che si connettono tra di loro con la rete di copertura anonima I2P per limitare il rischio di rivelare informazioni sensibili sulle transazioni[11].

Sono le stesse caratteristiche del protocollo di bitcoin a consentire ai riciclatori di spostare fondi illeciti, visto che è la stessa rete bitcoin a permettere a qualsiasi utente di trasferire soldi a velocità quasi istantanea senza collegarlo ad un indirizzo bitcoin. Se a tali caratteristiche si aggiungono sistemi di mixaggio che aiutano notevolmente ad offuscare la provenienza di fondi illeciti, il rischio di riciclaggio è amplificato e il bersaglio diventa ancora più difficile da individuare.

Il report "*The Internet Organised Crime Threat Assessment*"[12] di Europol del 2015 riporta un'analisi dettagliata delle minacce della criminalità organizzata sulla base dei riscontri delle Forze dell'Ordine dell'Unione Europea. Emerge come siano proprio le criptovalute quelle più utilizzate dalla criminalità organizzata *online*.

Essendo tutte le transazioni chiaramente a disposizione del pubblico, in quanto la *blockchain* lascia traccia di ogni transazione, sono stati creati software di *blockchain analysis* in grado di tracciare e ricostruire ogni spostamento. Come fare però per tracciare flussi che vengono offuscati dai software di mixaggio?

[10] Il software di bitcoin si fonda su una struttura c.d. *peer to peer*, ovvero un'architettura di nodi che svolgono la funzione sia di client sia di server verso gli altri nodi della rete. Con tale sistema gli utenti condividono i medesimi dati molto velocemente, usufruiscono delle stesse risorse

[11] Cfr. www.deepweb.it e www.getmonero.org

[12] Il report è scaricabile dal sito www.europol.europa.eu