7 luglio 2022 14:39

Il Bitcoin preserva l'anonimato?

di Redazione

Bitcoin (BTC) è davvero una criptovaluta anonima come molti credono? No! Vediamolo in dettaglio in questo contenuto.

"Bitcoin (BTC) è una valuta anonima che consente il pagamento sul dark web". Questa è una delle frasi preferite dalle persone che criticano BTC per essere anonimi. Sì, anche Bitcoin (BTC), il re delle criptovalute, non è privo di critiche. È accusato di favorire l'attività di terroristi e persone che si dedicano al riciclaggio di denaro. Per una buona ragione, sarebbe anonimo. Ma è questo il caso? Non proprio, ed è quello che ti mostreremo.

Perché si dice che Bitcoin (BTC) sia anonimo?

Se molte persone credono che BTC sia una valuta digitale anonima, è in primo luogo perché può essere estratta da chiunque in qualsiasi momento. Senza fornire il proprio indirizzo di casa (o sede della società), indirizzo IP o altre informazioni personali, chiunque può estrarre BTC. Insomma, è come se tutti i minatori lavorassero dietro una stanza buia ricoperta da un velo nero e molto opaco.

Inoltre, un portafoglio BTC può essere scaricato senza fornire (ancora una volta) alcuna informazione personale sull'utente. È anche possibile trasferire i token ad altri portafogli in modo sicuro, senza rivelare la tua identità. Risultato: i bitcoin (BTC) estratti sono veramente anonimi.

Quindi, in teoria, Bitcoin (BTC) è una criptovaluta anonima. Ma questo è solo in teoria! Ben diversa, infatti, la realtà, per la presenza dei controllori dei mercati finanziari, o in termini più classici “regolatori finanziari”. Stabiliscono standard relativi alle risorse digitali e Bitcoin (BTC) non fa eccezione.

No, Bitcoin (BTC) non è anonimo

In verità, Bitcoin (BTC) è tutt'altro che anonimo. Se così fosse, infatti, non sarebbe possibile risalire alle operazioni. Spiegazioni.

Con la blockchain di BTC, tutte le transazioni sono elencate. Ovviamente, nei dati che vengono salvati, non compare né il nome né il cognome. Quello che appare nella blockchain è piuttosto una sequenza di numeri che corrispondono all'indirizzo pubblico del suo portafoglio. Quindi, se il miner utilizza ogni volta lo stesso indirizzo per queste transazioni, queste transazioni verranno elencate e sarà possibile risalire al proprietario dell'indirizzo.

Ma come può una stringa di numeri portare al proprietario? È semplice. Basta già sapere che i token non compaiono per magia in un portafoglio. Lo inseriscono necessariamente perché un altro miner li ha inviati, tramite uno scambio (uno scambio di criptovaluta). Tuttavia, tutti gli scambi sono tenuti a identificare i propri clienti in

conformità con i principi Know Your Consumer (KYC).
Se hai un portafoglio, le tue informazioni sono conservate dalla tua borsa. Se richiesto da un'autorità, lo scambio potrebbe fornire loro le tue informazioni o inviare loro il tuo indirizzo IP che si avvicina alla tua posizione. Quindi, no, Bitcoin (BTC) non è così anonimo come pensiamo e gli esempi che lo dimostrano sono innumerevoli.

Slik Road, l'esempio più notevole

Siamo nel 2008, l'età d'oro del Bitcoin (BTC). È appena apparso e poche persone ne sentono parlare. Per i pochi che ne sono a conoscenza, la descrizione che ne viene data è sempre la stessa: *"È una moneta che non necessita di terzi di fiducia e non è regolata né dagli Stati né da altre autorità. È efficiente e consente scambi transfrontalieri".* Poiché non è controllato, la crittografia sta iniziando a sedurre.

Alcuni anni dopo, è stato lanciato un sito di e-commerce. Tuttavia, questo non è un sito come gli altri. Innanzitutto, è disponibile sul dark web. Poi offre in vendita solo prodotti poco etici. Il suo nome è Silk Road, un'invenzione di Dread Pirate Roberts (DPR). DPR decide che le transazioni verranno effettuate solo con Bitcoin (BTC).

Sfortunatamente per DPR, qualche anno dopo nel 2013 verrà catturato dall'FBI che riuscì a rintracciarlo dalle transazioni BTC. Gli agenti dell'FBI si infiltrano tra gli acquirenti di prodotti sulla piattaforma. Allo stesso tempo, scoprono un indirizzo IP non mascherato che li porta direttamente ai server con sede in Islanda. Grazie a questo indirizzo tracciano le transazioni sulla blockchain di BTC e risalgono a DPR.

La fine della storia è questa: l'FBI arresta DPR e mette le mani su una scorta di oltre 26.000 BTC che verrà poi messa all'asta. Ora ecco la morale: non credere mai che le transazioni Bitcoin (BTC) non possano essere rintracciate. Detto questo, è ancora possibile rimanere anonimi con il re delle criptovalute.

Come mantenere l'anonimato con Bitcoin (BTC)?

Esistono molte tecniche per rendere anonimo BTC. Una delle più efficaci è utilizzare i servizi del frullatore. L'obiettivo è mescolare i BTC di più utenti. In questo modo è difficile, se non impossibile, identificare l'esatta provenienza dei token.
Sebbene la miscelazione sia un metodo collaudato, ha un difetto. Per l'utente, è essenziale affidarsi a una terza parte che gli affidi i fondi. Un altro problema: le tue transazioni possono essere confuse con quelle di persone che svolgono attività meno legali. Alla fine, potresti ritrovarti coinvolto in storie di cui non conosci né la testa né la coda.

In breve, Bitcoin (BTC) è anonimo? No e no! Il primo no è dire che in verità è solo il suo design che gli permette di indossare un manto di anonimato. Il secondo no è più ovvio, perché significa che le transazioni in realtà non vengono eseguite in segreto. Possono essere tracciati utilizzando la blockchain di Bitcoin (BTC).

(Gaétan Lajeune su Futura-Tech del 02-07/2022)