Cassandra Crossing/ Tracciare i Bitcoin

(508)—La notizia che i Bitcoin sarebbero anonimi è stata largamente esagerata; vediamo perché.

Cassandra Crossing/ Tracciare i Bitcoin

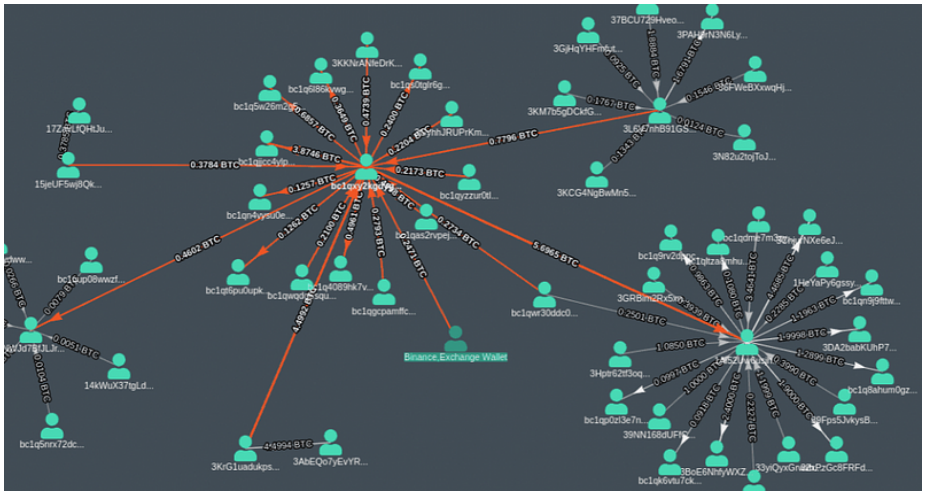

Figure 1: Bitquery's Coinpath sample output

(508)—La notizia che i Bitcoin sarebbero anonimi è stata largamente esagerata; vediamo perché.

20 luglio 2022—Tutti conoscono i Bitcoin.

Molti sono convinti di conoscerli abbastanza da poterli usare. Molti sono anche convinti che i Bitcoin siano una moneta "anonima".

Parlare di anonimato (digitale) in questo contesto sarebbe complesso, anche perché semmai i Bitcoin sono una moneta "pseudonima".

Ma certamente nel mondo reale (informatico e non informatico), che chiameremo "digitale ed analogico", le transazioni in Bitcoin possono essere tracciate e ricondotte a persone reali. Avviene tutti i giorni.

E' possibile spiegare come e perché senza parlare di crittografia e protocolli? Ci proviamo, ma è necessaria qualche premessa.

Il motivo principale per cui è possibile tracciare i Bitcoin è che **i Bitcoin non esistono**.

Si, nessuno possiede un singolo Bitcoin. Esistono solo le transazioni in Bitcoin, registrate sulla blockchain.

La blockchain pubblica di Bitcoin altro non è che un elenco completo ed ordinato di tutte le transazioni effettuate con i Bitcoin, a partire da 12 gennaio 2009 (data di nascita della blockchain di Bitcoin) fino al momento attuale.
Non si tratta nemmeno di una quantità di dati enorme; oggi sono meno di 417 GB. Starebbe su un piccolo disco USB; ci sono contabilità aziendali di PMI molto più grandi.

In questa "contabilità" ci sono due tipi di transazioni, quelle "normali", in cui un certo ammontare di Bitcoin cambia di proprietà, e le "transazioni di conio" di nuovi Bitcoin, generate automaticamente dai server che gestiscono la blockchain e contemporaneamente coniano nuovi Bitcoin.
Queste transazioni di conio si verificano al realizzarsi di certe condizioni, che però non sono qui di interesse.

Una "persona" (o meglio un indirizzo Bitcoin) "possiede" un certo numero di Bitcoin, numero che può essere calcolato solo dall'esame dell'intera "contabilità" Bitcoin, importo che può essere calcolato da chiunque sommando crediti e debiti delle transazioni con quell'indirizzo sull'intera blockchain.

Ovviamente le transazioni non contengono nomi di persone, ma solo gli indirizzi Bitcoin di chi paga e chi riceve la transazione. Possiamo assimilare questi indirizzi a degli IBAN di conti correnti.

Come si tracciano gli scambi dei Bitcoin? Nelle transazioni non ci sono dati personali, IP od altre informazioni che possano far risalire all'autore od al beneficiario di una transazione. E gli indirizzi Bitcoin non sono ovviamente riconducibili direttamente a nessuno.

Come le normali attività investigative, il tracciamento di una transazione Bitcoin è una procedura empirica, basata non solo sulla conoscenza dell'intera blockchain Bitcoin (che tutti possono vedere) ma anche su informazioni "empiriche" provenienti dal mondo analogico.

Infatti chi vuole spendere Bitcoin deve prima procurarseli. Come può fare?

In tre modi.

Il primo, improponibile oggi per persone normali, è coniarne di nuovi.

Il secondo è comprarli da qualcuno, in cambio di contanti od altro.
Questo era il modo normale di comprare Bitcoin fino a pochi anni fa.
Di solito si faceva rispondendo ad annunci Ebay che offrivano Bitcoin in cambio di una certa somma di valuta.
Il compratore pagava la somma con la carta di credito ed indicava il suo indirizzo Bitcoin, dove, se la controparte era onesta, riceveva i Bitcoin. Con buona pace di qualunque forma di anonimato, visto che gli utenti Ebay ed i possessori di carte di credito sono registrati.

Il terzo, di gran lunga il più comune al giorno d'oggi, è comprarli su un "exchange" come Coinbase o Binance.

Si tratta di enti di diritto privato del tutto equivalenti ad una banca, ed altrettanto regolati, normati e sorvegliati da enti statali.
Chi vuole ottenere i Bitcoin in questo modo apre un account (wallet) su un exchange.
Il risultato è un "conto corrente" in valuta privo di IBAN tradizionale, dove i contanti possono essere versati e prelevati solo con mezzi di pagamento a loro volta registrati (ad esempio una carta di credito od un conto corrente "vero"), più una serie di "conti correnti paralleli" (cioè di indirizzi) nelle criptovalute più popolari, incluso ovviamente Bitcoin.
Sul conto in valuta, di solito in dollari od in euro, l'utente trasferisce una certa somma di denaro. Poi per cambiarlo trasferisce il denaro su uno dei suoi "conti" in criptovaluta.
Per ogni "conto in criptovaluta" vengono forniti i relativi indirizzi, per poter effettuare transazioni nella blockchain di Bitcoin o della criptovaluta utilizzata.

Ora, poiché chi ha aperto l'account ha dovuto fornire tutti i documenti che sarebbero necessari per aprire un conto corrente bancario, è evidente che i relativi indirizzi Bitcoin, ed anche delle altre criptovalute dell'account, sono legati a filo doppio con una persona fisica.
Ecco che tutti gli exchange esistenti sono "punti di partenza" per rilevare l'identità di un utente dell'exchange che effettui transazioni Bitcoin, e seguendo le sue tracce, in avanti ed all'indietro nella contabilità dei Bitcoin, identificare tutte le transazioni che ha effettuato.

Analoghi appigli per il tracciamento sono dati da tutti gli indirizzi Bitcoin che corrispondono a persone o siti identificati per i più svariati motivi.
Ad esempio l'IRS, l'Agenzia delle Entrate americana, piomba immediatamente sulle spalle di qualunque cittadino americano che effettui un cash-out su un conto corrente normale, per incassare (beato lui) i suoi guadagni (si spera leciti, ancorché speculativi) in Bitcoin.

Ma anche gli acquisti su siti "questionabili" o decisamente "dark" una volta che questi siti siano stati scoperti (avete presente l'"affaire" Silkroad?), diventano miniere di informazioni per tracciare parti rilevanti della blockchain di Bitcoin (oops, volevo dire della "contabilità dei Bitcoin").

Esistono agenzie, ma anche aziende private, che "vendono" questi servizi di tracciamento ed identificazione, e che ovviamente hanno attinto a piene mani a tutte le possibili fonti di informazione.

Ora, i più esperti sui Bitcoin a questo punto potrebbero giustamente obiettare che il loro wallet è di tipo "freddo", cioè non si trova un exchange ma è un wallet di tipo classico, come tutti quelli che esistevano nei primi anni dell'era dei Bitcoin, e che quindi non usa nessun exchange e non ha questi problemi.

Potrebbero anche obiettare che un wallet ha in realtà non uno ma un numero infinito di indirizzi, e che una persona avveduta, ne usa uno diverso per ogni transazione, che per inciso è il modo "corretto" di usare i Bitcoin per preservare l'anonimato.

La risposta però non cambia di molto.
Certo, il lavoro di intelligence sulla blockchain diventa molto più difficile, ma non cambia come tipologia.

La risposta è di nuovo nell'integrazione tra "contabilità sulla blockchain" ed informazioni provenienti dal mondo analogico.
Anche se un utente usa gli indirizzi una volta sola, se uno dei corrispondenti conosce la sua identità od un suo riferimento, la deanonimizzazione è, investigativamente parlando, ad un passo.

Riassumendo; un utente Bitcoin può fare grossi danni al proprio "anonimato", e la maggior parte degli utenti Bitcoin, specialmente dell'ultima ora, se li fanno regolarmente.

Ma anche un utente accorto ha "contro" di sé aziende che hanno a disposizione quantità di informazioni enormi, nonché agganci con agenzie varie a tre o quattro lettere. Quindi, non essere tracciati se si utilizzano correntemente i Bitcoin e li si vuole anche convertire in valuta ordinaria è impresa che non solo richiede disciplina e pignoleria, ma che resta comunque difficile per non dire disperata.

Un'ultima obiezione; una parte delle operazioni di tracciamento appena descritte non sono prove certe ma induttive. In questo caso potrebbero essere "smontate" in un'aula di tribunale. Certo, questo è senz'altro vero, ma in altre situazioni, tipo il pagamento delle tasse o la fase investigativa di un'indagine, la controparte si "accontenta" anche di tracciamenti parzialmente induttivi.

Per concludere l'elenco delle possibili obiezioni; chi vuole mantenere un anonimato "forte", utilizzerà solo criptovalute più sofisticate dei Bitcoin, che tecnicamente rendono difficilissimo o quasi impossibile risalire da un indirizzo ad un altro, come ad esempio XMR-Monero.

Dobbiamo convenire anche con questa obiezione, ma ripetere che l'anonimato offerto dalle criptovalute come Monero è "solo" digitale; giova ricordare che il tracciamento ibrido digitale-analogico può offrire sicuramente opportunità di deanonimizzazione di transazioni anche in queste situazioni.

Ma ovviamente questa… questa è un'altra storia.

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica "Quattro chiacchiere con Cassandra"
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero

By Marco A. L. Calamari on July 25, 2022.

Canonical link

Exported from Medium on January 2, 2024.