Data di pubblicazione: 28 luglio 2017

Servizi di mixing e Monero

di Ottavio Calzone

Abstract

La rete Bitcoin è il primo sistema di pagamenti basato sul concetto di *distributed ledger technology* o *blockchain*. Si tratta di una rete di scambi di valuta virtuale in cui non vi è un'autorità incaricata di validare e registrare le transazioni. La piattaforma Bitcoin non consente però il completo anonimato degli scambi che risultano anche tracciabili. Nel tentativo di garantire anonimato e non tracciabilità sono nati diversi servizi di mixing e, dal 2014, un nuovo sistema di pagamenti basato su tecnologia *blockchain*: Monero. L'autore dell'articolo introduce il lettore, in maniera semplice, al funzionamento dei servizi di mixing per i pagamenti in bitcoin e alle idee alla base della piattaforma Monero. Vengono inoltre introdotti alcuni studi recenti realizzati per testare l'efficacia di questi meccanismi nel garantire la non tracciabilità delle transazioni.

Profilo dell'autore

Ottavio Calzone svolge attività di ricerca in ambito finanziario e bancario. Laureato presso l'Università di Siena dove ha conseguito anche il master in Economia Digitale ed E-Business che lo ha introdotto nello studio delle sinergie fra comportamenti sociali e tecnologie

Keyword bitcoin, blockchain

Sommario

1. Introduzione

La rete Bitcoin è il primo sistema di pagamenti basato sul concetto di *distributed ledger technology* o *blockchain*. Si tratta di una rete di scambi di valuta virtuale via internet in cui non vi è un'autorità incaricata di validare e registrare le transazioni perché tutte le copie del registro si aggiornano in maniera automatica[1].

Le caratteristiche della rete Bitcoin la rendono un sistema potenzialmente utilizzabile anche per transazioni illegali e trasferimenti illeciti di denaro all'estero. Tuttavia gli scambi non sono completamente anonimi e risultano anche tracciabili a partire dal primo avvenuto nel 2009. Ad esempio uno studio condotto dalla società Novetta[2], specializzata nell'analisi dei dati, evidenzia come sia possibile associare informazioni raccolte al di fuori della rete, anche attraverso moduli di registrazione per l'acquisto o vendita di beni, ai codici alfanumerici dei conti contenuti all'interno della rete *Bitcoin*. Inoltre è tecnicamente possibile individuare[3] l'indirizzo IP[4] del computer usato per spedire e ricevere valuta e associare poi ad un conto in *bitcoin*[5], tramite l'indirizzo IP, i dati comportamentali del proprietario del conto, come i siti web che ha visitato.

Per aumentare il grado di anonimato e rendere più difficoltosa la tracciabilità degli scambi è però possibile usare:

- carte prepagate per acquistare i *bitcoin* direttamente da altri utenti, contattabili ad esempio attraverso il sito LocalBitcoins[6], riducendo così al minimo la comunicazione dei propri dati personali;
- programmi, come TOR[7], che consentono di navigare anonimamente sul web;
- servizi di *mixing*.

Il presente lavoro introduce il lettore, in maniera semplificata, al funzionamento dei servizi di mixing per i pagamenti in bitcoin. È inoltre introdotto il funzionamento di un altro sistema di pagamenti, Monero, basato su tecnologia *blockchain* e lanciato nell'aprile 2014 per rendere gli scambi di valuta online anonimi e non tracciabili. Sono infine introdotti alcuni studi, presenti in letteratura, realizzati per testare l'efficacia dei servizi di mixing e di Monero nel garantire la non tracciabilità delle transazioni.

2. Bitcoin: chiavi pubbliche e private

Una chiave privata è una sequenza di caratteri creata in maniera casuale. Da questa chiave, un client Bitcoin usa l'algoritmo crittografico ECDSA (*Elliptic Curve Digital Signature Algorithm*) per calcolare un'altra sequenza di caratteri, la chiave pubblica, univocamente associata a quella privata. Ciò che è criptato con la chiave privata può essere decifrato solo con quella pubblica e viceversa, ma a partire dalla chiave pubblica non è possibile ricostruire la chiave privata che l'ha generata.

La chiave privata permette di autorizzare i pagamenti in uscita e non deve essere resa nota. La chiave pubblica è l'indirizzo da usare per ricevere denaro e può essere comunicata a tutti. Per questo useremo anche i termini di indirizzo o conto Bitcoin per riferirci alla chiave pubblica[8].

Anche se il il bitcoin è chiamato *crytpocurrency*, l'uso della crittografica a chiave pubblica-privata è usato non per nascondere le transazioni, ma per autorizzarle: solo chi è a conoscenza della corretta chiave privata associata ad una chiave pubblica può spendere i soldi disponibili sulla chiave pubblica. È possibile visualizzare in maniera molto semplificata questo funzionamento attraverso un esempio: la chiave pubblica è come un numero di telefono cellulare e la chiave privata come la scheda SIM associata a questo numero. Se riceviamo una telefonata da un determinato numero

allora sappiamo che ad averci chiamato è chi ha la scheda SIM corrispondente. Nel mondo Bitcoin 'ricevere una telefonata' significa ricevere del denaro e chi 'ha effettuato la telefonata' non può rinnegare di averla fatta perché quello che fa fede è il numero che ha chiamato. Questo significa che, una volta fatta una transazione, non è possibile disconoscerla e non è possibile cancellarla. Inoltre l'esempio fa capire perché perdere la propria chiave privata significa perdere il proprio denaro virtuale.

Volendo inviare tutti i bitcoin disponibili su una nostra chiave pubblica creiamo un set di informazioni composto dalla transazione, o dalle transazioni, da cui abbiamo ricevuto il denaro che vogliamo spendere e dalla chiave pubblica del destinatario del pagamento. In questo modo il sistema garantisce che ognuno possa spendere solo soldi che ha ricevuto da una precedente transazione. Il set di informazioni sarà poi firmato con la chiave privata associata a quella pubblica di chi sta inviando denaro e sarà reso noto a tutta la rete Bitcoin. La rete sarà così a conoscenza che quell'ammontare di denaro è ora di proprietà di una nuova chiave pubblica e potrà essere speso solo dalla chiave privata ad essa associata.

Il fatto che si possa spendere solo del denaro ricevuto in una precedente transazione implica che ci debba essere un modo per ottenerlo dalla rete stessa e non da altri utenti che la usano. All'inizio infatti nessun utente avrà a disposizione dei bitcoin da trasferire. Per questo motivo la piattaforma è fatta in modo da remunerare, fino ad un numero massimo di valuta virtuale in circolazione, con nuovi bitcoin (transazioni coinbase) i nodi della rete che si occupano di registrare gli scambi (nodi miner). In realtà questa soluzione non risolve il problema, perché per registrare una transazione c'è comunque bisogno di uno scambio di bitcoin e quindi di qualcuno che li ha in origine. È però un modo per aumentare il numero di valuta in circolazione, permettendo alla rete di crescere. La prima transazione in bitcoin è quindi necessariamente di genesi, in cui non vi è in riferimento a transazioni precedenti.

Le registrazioni fatte dai miner sono note a tutta la rete, anche se i vari nodi sono a conoscenza solo dei codici alfanumerici a cui è associato in ogni istante temporale un certo ammontare di denaro. Oltre ad essere pubbliche, sono ordinate in blocchi fra loro concatenati cronologicamente (blockchain). Le transazioni inserite nello stesso blocco sono considerate avvenute nello stesso momento. Ogni nodo full della rete Bitcoin conserva una copia del registro in cui è memorizzata tutta la catena di blocchi. È possibile così ricostruire i passaggi di proprietà di denaro a partire dalla prima transazione avvenuta nel 2009.

3. Bitcoin: pseudoanonimato e tracciabilità

La rete Bitcoin è un sistema di pagamenti distribuito a cui si può accedere in qualunque posto in cui ci sia una connessione ad internet. Per questo motivo affermare di usare la rete per trasferire del denaro all'estero è in un certo senso fuorviante. Per la rete non esiste il concetto di estero: sono gli scambi commerciali di beni acquistati con il bitcoin che possono avvenire in una nazione o nell'altra, ma la valuta virtuale spedita e ricevuta si troverà sempre e solo sulla rete, registrata simultaneamente su tutti i nodi. Una persona può così ricevere della valuta mentre si trova in Italia, andare negli Stati Uniti, collegarsi alla rete e spendere il proprio denaro elettronico con la stessa

comodità con cui può leggere le proprie email in più nazioni diverse semplicemente accedendo alla casella di posta elettronica. Può inoltre effettuare un cambio fra bitcoin e la valuta del posto usando uno degli oltre 1200 ATM esistenti in 58 paesi[9] che permettono questa operazione.

All'interno della rete Bitcoin sono noti solo codici alfanumerici, ma in molti casi per eseguire uno scambio fra bitcoin ed altri beni è necessario autenticarsi e quindi fornire, oltre alla propria chiave pubblica, anche le proprie credenziali comunicandole al di fuori della rete di pagamenti. In questo modo un osservatore esterno è in grado di associare informazioni personali ad una determinata chiave pubblica. Inoltre è tecnicamente possibile individuare l'indirizzo IP del computer usato per spedire e ricevere valuta ed associare poi ad un conto in bitcoin, tramite l'indirizzo IP, i dati comportamentali del proprietario del conto, come i siti web che ha visitato. Per questo motivo non si parla di anonimato delle transazioni, bensì di pseudo-anonimato.

È possibile usare degli accorgimenti per limitare le informazioni recuperabili al di fuori della rete, come usare carte prepagate per l'acquisto di bitcoin direttamente da altre persone e strumenti che rendono anonimi sul web. Un client Bitcoin permette inoltre di generare diverse coppie di chiavi pubbliche e private: la moneta virtuale ricevuta su un determinato indirizzo può così essere spedita ad un'altra chiave pubblica di cui si dispone e mai resa nota al di fuori della rete.

La possibilità di spedire del denaro elettronico su un indirizzo la cui titolarità non è manifestatamente nota al di fuori della rete e l'accettazione del bitcoin come valuta per i pagamenti in più nazioni sono caratteristiche che rendono questa valuta virtuale utile per evitare la confisca di beni: si è in grado di vendere dei beni in cambio di bitcoin nella nazione che li vuole confiscare ed eseguire la transazione opposta in una giurisdizione differente, magari usando un prestanome.

La rete Bitcoin consente però di tracciare i passaggi di proprietà da conto a conto a partire dalla prima transazione avvenuta nel 2009: un osservatore esterno è così in grado di individuare lo scambio di valuta da un conto noto ad uno non noto. Attraverso dei servizi di mixing[10] si può tuttavia fare in modo che i passaggi di valuta siano tali da non consentire di affermare con certezza che vi sia un legame fra i soldi inviati e quelli ricevuti.

4. Servizi di mixing

All'interno della rete Bitcoin la tracciabilità non può essere eliminata. Per ottenere questo risultato dobbiamo riportare parte dell'informazione al di fuori della rete. Ad esempio ipotizziamo che un utente di nome Bob spedisca dei bitcoin all'indirizzo dell'utente Alice. Un amico di Alice, Andrea, spedisce poi lo stesso ammontare ricevuto da Alice su un altro conto di Bob. Fra Alice ed Andrea non vi è stato scambio di bitcoin e quindi non vi è collegamento diretto all'interno della rete fra il conto di partenza di Bob ed il suo conto finale.

Questo espediente richiede l'esistenza di un'organizzazione al di fuori della rete. In particolare Alice dovrà essere legittimata a ricevere del denaro virtuale senza chiederne la provenienza. Andrea dovrà essere in grado di avere dei bitcoin a disposizione da inviare in ogni momento necessario. Deve esistere una modalità di comunicazione e di scambio di valore sicuro e non tracciabile fra

Alice e Andrea. È necessaria una relazione di fiducia fra Bob e l'organizzazione: Bob sa che dopo aver spedito i fondi, li riceverà, successivamente su un altro conto.

Il limiti principali di questo espediente sono due: la necessità di avere una determinata quantità di bitcoin a disposizione da parte di Andrea e la tracciabilità dello scambio in bitcoin fra Bob ed Alice. Se il denaro spedito da Bob è il frutto di un'operazione illegale, come quello ottenuto da un software che per sbloccare un computer infettato richieda un riscatto[11] in bitcoin, Alice si troverà ad essere associata a questo tipo di transazione. È perciò necessario per Alice essere titolata a ricevere denaro senza chiederne la provenienza.

Per ridurre le tracce dei passaggi di mano del denaro virtuale senza ricorrere ad un'organizzazione complessa come quella appena descritta è possibile affidarsi a dei servizi di mixing. La società di analisi di dati Novetta[12] ha analizzato quattro servizi: Bitmixer[13], Bit Launder[14], Shared Coin[15], Bitcoin Blender[16]. Rivolgendosi a questi servizi si depositano dei bitcoin su dei conti di ingresso e si riprende il denaro virtuale su dei conti di uscita. Il servizio scelto farà in modo che non sia possibile associare direttamente l'ammontare di denaro depositato all'ammontare ritirato alla fine.

Un servizio di mixing applica principalmente due tecniche ottenere questo risultato[17]. La prima tecnica consiste nello spedire i soldi depositati a più conti che a loro volta li inviano ad altri conti. In questo modo la rete dei passaggi di denaro risulterà più grande e più confusa per due motivi: vi sarà una catena più lunga e con più diramazioni fra loro interconnesse. Gli indirizzi che partecipano a questa attività sono chiamati 'conti di rimbalzo' (conti bounce).

Il secondo modo per nascondere le tracce è mischiarle fra loro: raggruppare i fondi di più utenti che si sono rivolti al servizio di mixing in un unico indirizzo, detto conto pool o pot, e poi spedirli nuovamente a più indirizzi.

Un tipico sistema di mixing è quindi composto da uno o più conti:

- di ingresso (gateway o di deposito)
- *bounce*
- *pool*
- di uscita (di *withdrawing*).

Per analizzare il grado di efficacia dei servizi di mixing oggetto di studio, la società Novetta ha utilizzato anche lo strumento di *taint analysis* in passato presente sul sito Blockchain.info[18]. Lo strumento consentiva[19] di verificare il collegamento anche indiretto fra due indirizzi bitcoin. In particolare:

- per *taint analysis* si intende (dato un indirizzo) la percentuale di fondi ricevuti che può essere collegata come proveniente, anche dopo diversi passaggi, da un altro indirizzo
- per *forward taint analysis* si intende (dato un indirizzo) la percentuale di fondi spediti individuabili come ricevuti, anche dopo diversi passaggi, da un altro indirizzo.

Per verificare la bontà dei servizi di mixing si parte dal loro utilizzo: si depositano dei bitcoin in un conto gateway per ritirarli in un indirizzo di uscita e misurare il collegamento fra i due indirizzi

attraverso uno strumento come quello di *taint analysis*. È inoltre possibile un'analisi descrittiva del servizio usato attraverso una rappresentazione grafica in cui i conti sono indicati con dei cerchi e i trasferimenti da indirizzo a indirizzo con delle frecce. L'analisi descrittiva tiene in considerazione anche informazioni come la tempistica in cui avvengono le transazioni, l'ammontare dei fondi scambiati e la quota, fissa o in percentuale, trattenuta come pagamento da parte del servizio di mixing.

I risultati ottenuti da Novetta evidenziano come i servizi di mixing riescano ad eliminare nella maggior parte dei casi il collegamento, in termini di *taint analysis*, fra indirizzi di origine quelli di destinazione. Tuttavia l'analisi descrittiva permette di individuare dei comportamenti tipici di ogni servizio e quindi, nel caso di utilizzo per far perdere le tracce di fondi ottenuti illegalmente, di individuare quello usato per tale scopo.

Nell'articolo *A Complex Web: Bitcoin Mixing Services*[20], l'autore Amit Dori evidenzia come attraverso l'analisi descrittiva, simile a quella condotta dalla società Novetta, sia possibile individuare i probabili conti di uscita. Mentre tutti gli indirizzi che fanno parte di un servizio di mixing sono molto attivi, i conti di uscita sono quelli che ricevono i soldi che saranno ritirati da chi ha usato il servizio: dovrebbero essere così i conti che risultano meno attivi nell'analisi descrittiva.

Sulla base del risultato di queste analisi un servizio di mixing potrebbe migliorare la non tracciabilità delle informazioni cambiando casualmente il proprio comportamento nel corso del tempo, modificando ad esempio i ritardi temporali in cui avvengono i passaggi di valuta o la quota di pagamento richiesta.

5. Monero

Per introdurre un servizio di mixing in maniera nativa all'interno di una tecnologia blockchain, nell'aprile 2014 è stata lanciata una nuova piattaforma di pagamenti in valuta virtuale simile alla rete Bitcoin: Monero[21]. Anche se non si tratta dell'unico caso di tecnologia blockchain nata per essere anonima e non tracciabile, Monero è quella che recentemente ha attirato maggiormente l'interesse dei media[22] principalmente per la possibilità di essere usata per acquisti illegali attraverso il deep web[23].

La rete Monero, che si basa sul protocollo CryptoNote[24], ha una capitalizzazione di quasi seicento milioni di dollari statunitensi[25]. Il valore di un monero, valuta indicata con il simbolo XMR, è di poco più di quaranta dollari. È possibile comprare la valuta in circa venti punti di scambio indicati sul sito ufficiale della piattaforma[26].

Per garantire anonimato e non tracciabilità, lo sviluppo di Monero è focalizzato su due obiettivi:

1. dati due invii di denaro, non rendere possibile affermare che il destinatario sia un'unica persona (non associabilità – *unlinkability*);
2. dati due indirizzi qualsiasi, non rendere possibile affermare che vi sia stato scambio di denaro fra gli stessi (non tracciabilità – *untraceability*).

Il primo dei due obiettivi è ottenuto attraverso il concetto di firma digitale one-time. Il secondo grazie alla *ring signatures*. L'uso del plurale è legato al fatto che a livello teorico non esiste una sola soluzione di *ring signature*, ma più soluzioni di cui Monero ne implementa un tipo. Anche in *Monero* tuttavia sono riscontrabili storicamente due implementazioni di *ring signature*. La tecnica usata in origine è sta poi modificata nella *Ring confidential transaction* (RingCTs). Di seguito analizzeremo l'idea originaria per poi illustrare la RingCTs, introdotta nel gennaio 2017 e attualmente in fase sperimentale[27].

Gli utenti di Monero hanno delle coppie di chiavi private e pubbliche di lungo periodo. L'invio di denaro presuppone però la creazione, per ogni transazione, di chiavi pubbliche e private 'usa e getta' (firma digitale one-time). Per inviare dei fondi ad un'altra persona, un utente di Monero genera una chiave pubblica one-time di questa persona ed una chiave identificativa della transazione. A partire dalla chiave della transazione e della sua chiave privata di lungo periodo, il destinatario è in grado di capire di aver ricevuto dei soldi e di spenderli generando una chiave privata one-time.

In particolare chi vuole inviare del denaro chiede la chiave pubblica di lungo periodo del destinatario. A questo punto genera un'informazione randomica e crea due chiavi pubbliche: una per la transazione, ed una one-time per il destinatario. La chiave pubblica della transazione contiene sia l'informazione di tipo randomico appena creata che un'informazione di tipo deterministico. La chiave pubblica one-time del destinatario è prodotta a partire dall'informazione contenuta nella chiave pubblica della transazione e dalla sua chiave pubblica di lungo periodo. In questo modo anche il destinatario, conoscendo la chiave della transazione e la sua chiave pubblica di lungo periodo, sarà in grado di riprodurre la chiave pubblica one-time e quindi sapere di aver ricevuto dei soldi. Inoltre, usando la propria chiave privata di lungo periodo e la chiave della transazione, il destinatario sarà l'unico in grado di generare la chiave privata one-time che gli consentirà di spendere la valuta virtuale ricevuta.

Se una transazione contiene più output, cioè invii a più destinatari, anche se due dei destinatari sono in realtà la stessa persona, i due output avranno comunque chiavi pubbliche one-time diverse. In Monero quindi più invii di denaro ad una determinata persona sono in realtà fatti verso chiavi pubbliche differenti e per questo motivo, a partire dalle informazioni contenute nelle copie del registro contabile di Monero, non si è in grado di stabilire se, dati due invii di denaro, la valuta virtuale sia stata o meno spedita ad un'unica persona (*unlinkability*).

Se la firma digitale one-time serve per ottenere il risultato di *unlinkability*, l'obiettivo della non tracciabilità è perseguito attraverso la *ring signature*. Uno schema[28] di *ring signature* si basa su tre algoritmi[29]:

1. un algoritmo che crea una una coppia di chiavi, privata e pubblica;
2. un algoritmo che crea una firma digitale di un messaggio a partire dal messaggio stesso, dalla chiave privata di chi firma e da un insieme di chiavi pubbliche (detto *ring*) di cui fa parte anche la chiave pubblica del firmatario;

3. un algoritmo che, a partire dalla firma, dal messaggio originale e dal *ring*, restituisce 'vero' solo se la firma è stata creata, a partire dal messaggio, da un membro del *ring*.

L'utilizzo della *ring signature* permette quindi, ad un osservatore esterno, solo di poter affermare che un messaggio è stato firmato da uno dei membri del *ring*. Membri che sono scelti di volta per ogni messaggio da firmare.

Chi vuole inviare della valuta virtuale deve averla prima ricevuta su un suo conto: su una chiave pubblica one-time di cui è l'unica persona in grado di costruire la corrispondente chiave privata one-time. Nella rete Monero ci sono però altri conti one-time che hanno ricevuto la stessa quantità di soldi, è possibile quindi creare un *ring* composto, oltre che dal vero conto di origine della valuta da trasferire, anche da una serie di conti associati alla stessa quantità di denaro ma che servono solo a mascherare la vera origine dei fondi e per questo motivo sono chiamati mix-in.

In questo modo, oltre ad un osservatore esterno, anche i miner, cioè i nodi della rete incaricati di registrare le transazioni, non sono in grado di sapere da quale conto sono presi i soldi. Per evitare così la possibilità di avere doppi pagamenti, cioè di inviare dei soldi verso un indirizzo senza cancellarli da quello di origine, è necessario in qualche modo indicare da quale conto è preso effettivamente il denaro.

La possibilità di usare la valuta disponibile su una chiave pubblica one-time è testimoniata dalla capacità di creare una chiave privata one-time ad essa associata. Per i miner quindi i soldi da cancellare sono quelli del conto legato alla chiave privata one-time che si sta usando per la transazione. Solo l'effettivo proprietario del conto è in grado di creare ed usare questa chiave privata e se gli si chiede di generare una firma di un determinato messaggio e di includere la firma nella transazione, la chiave privata one-time può essere eliminata da parte dei nodi della rete dalle chiavi nuovamente utilizzabili per spedire dei soldi: se usata nuovamente genererebbe infatti la stessa firma, che i miner già conoscono.

Il messaggio firmato, chiamato key image, consente così di evitare la possibilità dei doppi pagamenti inibendo l'uso ripetuto di una chiave privata one-time. Il meccanismo descritto[30] è tuttavia tale da non fornire nessuna informazione che possa essere usata per risalire alla chiave pubblica one-time da cui proviene il denaro speso.

Di recente è stata introdotta una nuova modalità di *ring signature* all'interno di *Monero*. Questa modalità, chiamata *ring confidential transaction* (RingCTs) rende possibile includere in un *ring* anche chiavi pubbliche a cui è associato un ammontare differente rispetto a quello che si sta inviando. La RingCTs è fatta in modo da non fornire informazioni circa l'ammontare di ogni conto incluso nel ring pur rendendo possibile per i miner di verificare che l'ammontare dei soldi inviati combaci con quello dei soldi ricevuti.

6. Analisi della tracciabilità di Monero

Nell'articolo *A Traceability Analysis of Monero's Blockchain*[31] è analizzata la possibilità di tracciare, nonostante l'uso della *ring signature*, le transazioni effettuate con la piattaforma *Monero*.

In realtà una transazione può essere composta da più input e quindi da più conti di origine dei fondi. *Ring signature* e *key image* sono necessari per ogni input. Lo studio della tracciabilità è quindi a livello di ogni singolo input di una transazione.

Lo studio esplora le affermazioni che un osservatore esterno può fare analizzando le copie del registro delle transazioni sulla base di tre euristiche. La prima euristica si basa sulle seguenti considerazioni:

1. se una persona crea un *ring* composto da un solo conto (cioè non vi sono *mix-in*) allora il conto è quello da cui sono presi effettivamente i soldi e può essere considerato come speso;
2. l'efficacia di qualunque *ring* che usa dei *mix-in* è misurabile in termini di numero di conti che compongono il *ring* meno quelli che lo compongono e che sono stati individuati come spesi nel punto precedente (questo conteggio è chiamato *effective anonimity-set size*);
3. per un *ring* la cui *anonimity set size* è pari a uno è possibile affermare da quale conto sono presi i soldi usati.

Se una persona non inserisce dei *mix-in* non incide quindi solo sulla *effective anonimity-set size* dei propri input, ma anche su quella di altri input che usano i *mix-in*. Si ottiene così un effetto a cascata significativo. Gli autori dello studio evidenziano infatti come, nella propria analisi, nel 65% dei casi gli utenti non hanno usato dei *mix-in* e questo impatta sulla identificazione di un altro 22% di conti effettivamente spesi ma che gli utenti avevano provato a non rendere identificabili includendoli in dei *ring* accompagnati da *mix-in*. La percentuale di input tracciabili in questo modo è però diminuita dopo fine marzo 2016 in seguito all'introduzione del numero minimo richiesto di due *mix-in*, numero che dovrebbe passare a quattro[32].

La seconda euristica si basa su una considerazione di tipo probabilistico: se una transazione indica, come origine, alcuni conti che compaiono come destinazione in un'unica transazione già registrata, allora probabilmente questi conti appartengono alla stessa persona e quindi non sono usati presumibilmente come *mix-in*. Anche se l'informazione ricavabile in questo modo è solo di tipo probabilistico, è possibile usare questa conoscenza in combinazione con quella ottenuta grazie alla prima euristica per rafforzare o indebolire delle ipotesi sul conto effettivamente usato fra quelli che compongono un *ring* la cui *effective anonimity-set size* è stata già ridotta. Analizzando i conti identificati come probabilmente veri (cioè effettivamente spesi nella transazione) dalla seconda euristica con quelli indicati come effettivamente veri dalla prima, gli autori dello studio evidenziano come nell'87% dei casi l'assunto alla base della seconda euristica possa essere considerato vero.

Anche la terza euristica si basa su un'ipotesi di tipo probabilistico: più un conto esiste da molto tempo, più è probabile che i soldi siano già stati spesi. Quindi all'interno di un ring, più un conto è datato, più è probabile che sia un mix-in. Gli autori dello studio evidenziano come, nel dataset analizzato, nella quasi totalità dei casi i conti individuati come spesi nella prima euristica sono effettivamente quelli meno datati usati in un ring.

Le tre euristiche si basano così sul comportamento degli utenti, che può rendere inefficace la bontà di Monero nel rendere non tracciabili le transazioni. Per migliorare il grado di non tracciabilità è necessario così incidere su tale comportamento. Per quanto riguarda l'uso dei mix-in, da fine marzo

2016 è richiesto di indicarne almeno due. Relativamente alla terza euristica, gli autori dello studio suggeriscono che la scelta dei mix-in dovrebbe basarsi sugli effettivi comportamenti di spesa degli utenti e quindi essere fatta in funzione della probabilità che un conto con una data 'anzianità' sia stato già usato come vera origine di una transazione e non come mix-in.

7. Conclusioni

Nella rete Bitcoin, così come in Monero, la possibilità di spendere del denaro non è legata ad informazioni sull'identità di una persona, bensì ad una capacità, quella di essere gli unici in grado di eseguire un comportamento: usare la corretta chiave privata per Bitcoin e poter creare ed usare la corretta chiave privata one-time per Monero. Le uniche analisi che possono essere condotte su queste due reti sfruttano le interconnessioni fra comportamenti eseguiti (le transazioni) o informazioni recuperate al di fuori della rete, come in punti di scambio fra valuta virtuale ed altri beni.

Nel caso del Bitcoin l'analisi della tracciabilità è abbastanza semplice e per questo motivo sono nati dei servizi di mixing. Gli studi presentati in questo articolo evidenziano però che l'informazione nascosta è in un certo senso sostituita da quella relativa al comportamento dei servizi stessi: informazioni come la struttura dei conti, i ritardi temporali degli scambi e le quote di pagamento richieste.

A differenza del Bitcoin, la piattaforma Monero include al proprio interno il concetto di mixing in maniera nativa. In questo caso però, come evidenziato, l'informazione rintracciabile è legata al comportamento degli utenti: a come usano, spesso in maniera inefficace, la piattaforma.

Queste osservazioni fanno supporre che, in reti di scambi basate sul comportamento e non sull'identità, l'unica informazione recuperabile sia di tipo comportamentale e che un'informazione di questo tipo non possa essere del tutto eliminata, ma solo sostituita da informazione dello stesso tipo. Tuttavia affermazioni fatte su analisi comportamentali sono in genere probabilistiche e pertanto risultano indebolite quando i comportamenti sono randomici o tali da 'confondersi fra la folla'.

Note

(Ultimo accesso ai link indicati: 21 luglio 2017)

[1] O. CALZONE, *Bitcoin e distributed ledger technology*, Il Mondo dell'Intelligence – Sistema di Informazione per la sicurezza della Repubblica, Roma 2017, https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/02/Bitcoin-e-DLT-Calzone.pdf.

[2] NOVETTA, *Survey of Bitcoin Mixing Services: Tracing Anonymous Bitcoins,* McLeans (Virginia, USA), 2015, https://www.novetta.com/wp-content/uploads/2015/10/NovettaBiometrics_BitcoinCryptocurrency_WP-W_9182015.pdf.

[3] M. CHIRIATTI, *I nove (falsi) miti più comuni di bitcoin e della valute virtuali*, in «Il Sole 24 Ore», 3 febbraio 2016, http://www.ilsole24ore.com/art/tecnologie/2016-02-02/bitcoin-e-anonimo-171022.shtml?refresh_ce=1.

[4] Codice numerico che identifica un dispositivo collegato ad internet, https://it.wikipedia.org/wiki/Indirizzo_IP

[5] In genere si usa la l'iniziale maiuscola per indicare la tecnologia (es. *Bitcoin* o *Monero*) e l'iniziale minuscola per indicare la moneta virtuale (es. *bitcoin* e *monero*).

[6] LocalBitcoins, https://localbitcoins.net.

[7] TOR, https://www.torproject.org.

[8] Useremo la stessa logica anche per *Monero*.

[9] Elenco degli ATM in *bitcoin*, https://coinatmradar.com.

[10] Anche noti con il nome di servizi di *tumbling*.

[11] Un software di questo tipo è chiamato *ransomware*.

[12] Novetta, *Survey of Bitcoin Mixing Services*, cit.

[13] Bitmixer, https://bitmixer.io.

[14] Bit Launder, https://bitlaunder.com.

[15] Shared Coin, http://blockchatvqztbll.onion (indirizzo TOR che attualmente non risulterebbe più attivo).

[16] Bitcoin Blender, http://bitblendervrfkzr.onion (indirizzo TOR).

[17] A. DORI, *A Complex Web: Bitcoin Mixing Services*, 2016, http://blog.checkpoint.com/2016/11/23/complex-web-bitcoin-mixing-services.

[18] Blockchain.info, https://blockchain.info.

[19] P. DAL CHECCO, *Blockchain.info rimuove la funzione di taint analysis*, 6 febbraio 2017, http://www.bitcoinforensics.it/2017/02/blockchain-info-taint-analysis

[20] Dori, *A Complex Web*, cit.

[21] Sito ufficiale di Monero, https://getmonero.org.

[22] E. SPAGNUOLO, *Addio Bitcoin, nel deep web ora si paga con Monero e Zcash*, in «Wired», 26 aprile 2017, https://www.wired.it/economia/finanza/2017/04/26/bitcoin-monero-zcash.

[23] S. ARANZULLA, *Deep Web: cos'è e come entrare*, https://www.aranzulla.it/deep-web-cose-entrare-38651.html

[24] https://en.wikipedia.org/wiki/CryptoNote.

[25] https://coinmarketcap.com/currencies/monero.

[26] https://getmonero.org/getting-started/merchants.

[27] Fase che dovrebbe concludersi a settembre 2017.

[28] S. MEIKLEJOHN, *An Exploration of Group and Ring Signatures*, 2011, https://cseweb.ucsd.edu/~smeiklejohn/files/researchexam.pdf.

[29] In realtà l'articolo evidenzia la necessità solo degli algoritmi di firma e di verifica.

[30] Se ci sono più input, *ring signature* e *key image* sono necessari per ogni input.

[31] A. KUMAR, C. FISCHER, S. TOPLE, P. SAXENA, *A Traceability Analysis of Monero's Blockchain*, 2017, https://eprint.iacr.org/2017/338.pdf.

[32] https://www.reddit.com/r/Monero/comments/5gewer/the_default_mixin_number.

Bibliografia

O. CALZONE, *Bitcoin e distributed ledger technology*, Il Mondo dell'intelligence – Sistema di Informazione per la sicurezza della Repubblica, Roma 2017, https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/02/Bitcoin-e-DLT-Calzone.pdf

A. DORI, *A Complex Web: Bitcoin Mixing Services*, 2016, http://blog.checkpoint.com/2016/11/23/complex-web-bitcoin-mixing-services.

A. KUMAR, C. FISCHER, S. TOPLE, P. SAXENA, *A Traceability Analysis of Monero's Blockchain*, 2017, https://eprint.iacr.org/2017/338.pdf

S. MEIKLEJOHN, *An Exploration of Group and Ring Signatures*, 2011, https://cseweb.ucsd.edu/~smeiklejohn/files/researchexam.pdf

NOVETTA, *Survey of Bitcoin Mixing Services: Tracing Anonymous Bitcoins*, McLean, Virginia, USA 2015, https://www.novetta.com/wpcontent/uploads/2015/10/NovettaBiometrics_BitcoinCryptocurrency_WP-W_9182015.pdf