Guida completa al wallet Bitcoin, con Lightning Network

Questo articolo è una guida pratica alla creazione di un wallet Bitcoin e al suo utilizzo, comprensivo di Lightning Network. Scoprirete che è tutto tanto semplice da essere alla portata di grandi e piccini. Se avete in voi un forte desiderio di anarchia, pronti via! Ma mi raccomando, solo con forbici a punta arrotondata!

> ***Nota preliminare:*** *nella precedente guida al wallet Bitcoin, datata 2018, consigliavo di utilizzare Electrum SegWit con indirizzi non nativi (non bech32), poiché lo standard bech32 era ancora poco adottato nella community, Oggi questo approccio è superato: se un servizio o exchange ancora non riconoscesse gli indirizzi bech32, fareste meglio ad abbandonarlo. Usando bech32, le vostre transazioni saranno un po' più leggere (circa il 10% in meno) rispetto a transazioni SegWit, le quali già permettono un risparmio, quindi pagheranno ancor meno commissioni al miner.*
>
> ***Ringraziamenti:*** *i bitcoin utilizzati per questa guida sono stati donati al blog albertodeluigi.com da Alessio Ferraro. Come vedi Alessio, per l'intera guida ho speso pochissime commissioni di transazione, così posso investire il restante in qualche altra attività di divulgazione!*

Indice:

A – Nozioni di base

        - Focus teorico: a cosa è dovuto il diverso peso di una transazione
    4. Velocizzare una transazione che state inviando (Replace-by-fee o RBF)
    5. Velocizzare una transazione che state ricevendo (Child-Pays-For-Parent o CPFP)

B – Lightning Network

    6. Aprire un canale LN
        - Focus teorico: capienza dei canali Lightning Network
    7. Inviare e ricevere su LN
    8. Aumentare la capacità di ricezione o invio del canale LN (submarine swap)
    9. Chiudere un canale LN
    10. Backup dei canali LN e migrazione del wallet su altro computer

C- Gestione del seed e chiavi private

D – Portafogli multifirma

APPENDICE: Lightning Network da mobile, il modello Breez

> *tl;dr – la guida in breve:*
>
> *1-Installate Electrum e create il vostro wallet*
> *2-Inviate dei bitcoin onchain a Electrum*
> *3-Aprite un canale LN con un grosso nodo della rete*
> *4-Installate l'app Breez su smartphone*
> *5-Inviate dei bitcoin da Electrum LN all'app mobile Breez, così da liberare la capacità in ricezione sul vostro wallet desktop ed al contempo avere dei bitcoin su smartphone pronti per pagare*
> *6-Accedete ai wallet almeno 1 volta ogni due settimane e fate backup dei canali LN*

Nozioni di base:

La **blockchain** è il registro pubblico di tutte le transazioni Bitcoin, che chiunque può scaricare sul proprio computer o consultare online. Ogni transazione registrata sulla blockchain riporta almeno un **indirizzo** di destinazione e una cifra che rappresenta il numero di *bitcoin* trasferiti (o per la precisione di ***satoshi***, l'unità decimale più piccola di Bitcoin). I *bitcoin* (o *satoshi*, a seconda dell'unità di misura) non sono altro che quel numero associato alla transazione scritta nel registro pubblico: sono quindi un dato esistente soltanto nella blockchain e **non sono fisicamente né logicamente nel wallet** di nessuno.

Il wallet custodisce le chiavi necessarie a muovere i bitcoin da un output all'altro registrati in blockchain. Per questa ragione, è utile immaginare il wallet più come un portachiavi che un portamonete che contiene bitcoin. Inoltre, il wallet può non avere consistenza fisica, poiché la chiave può essere conservata sui supporti più disparati:

- scritta su carta (**paper wallet**) o qualsiasi altro materiale adatto alla scrittura o incisione;
- in un software (**software wallet**, come Electrum) che può essere installato su supporti diversi (PC Windows, Linux o iOS, smartphone etc.);
- in hardware dedicato come chiavette usb speciali (**hardware wallet**);
- ricordata a memoria (**brain wallet**).

Per potere muovere dei bitcoin da un indirizzo è necessario conoscere la relativa chiave privata. Per motivi di privacy, è consigliato utilizzare un indirizzo nuovo per ogni pagamento ricevuto, perciò **ogni singolo utente potrebbe avere molteplici indirizzi e molteplici chiavi private**. Un wallet dovrebbe quindi raggruppare tutte queste chiavi nel modo più semplice e comodo possibile. La soluzione adottata per la maggiore, fra gli sviluppatori di wallet Bitcoin, è stata quella di

introdurre un’unica “**master public key**”, da cui l’utente deriva tutti gli indirizzi, e la relativa “**master private key”,** da cui l’utente deriva tutte le chiavi private relative a quegli indirizzi.

Poiché la master private key (talvolta chiamata anche “account extended key”) è lunga e complicata da ricordare o digitare, per facilitare l’essere umano è generalmente convertita in una sequenza di parole, solitamente 12 o più, detta “seed” o “seme**”. Il seed non è altro che un modo diverso, più “umano” di scrivere la “master private key”**,

Per **possedere dei bitcoin, ma anche per riceverli in pagamento,** non è necessario avere un pc, uno smartphone o un qualsiasi altro apparecchio elettronico. Vi basterà soltanto mostrare un vostro indirizzo Bitcoin, magari in versione QR Code stampato su carta, del quale conoscete la chiave privata. Per esempio, andando su https://www.bitaddress.org/ potrete creare un wallet Bitcoin in pochi secondi semplicemente generando l’indirizzo e relativa chiave privata:

Anziché la chiave privata potete **imparare a memoria un seed** di 12 parole in grado di derivarla. Potreste impararne a memoria solo alcune delle 12 parole e scrivere le altre su un supporto fisico, così che un eventuale ladro, impossessandosi dei vostri appunti, risalirebbe soltanto a una parte del seed, insufficiente a rubarvi i fondi.

Inserendo quindi il seed in qualsiasi wallet Bitcoin scaricabile online, quest’ultimo deriverà tutti i vostri indirizzi attivi e relative chiavi private, quindi si collegherà online per **scansionare la blockchain al fine di calcolare quanti soldi “possedete”**, ovvero quanti bitcoin ancora spendibili compaiono a quegli indirizzi presenti nel registro pubblico, di cui soltanto voi avete la chiave privata. Quando ricevete un pagamento, per verificare che i

bitcoin siano stati ricevuti, anche senza possedere un wallet è possibile cercare il proprio indirizzo su un sito internet come un "**block explorer**", da cui è possibile osservare i movimenti su blockchain.

La maggior parte dei wallet non è solo un mezzo per custodire le chiavi, ma abilita all'invio di bitcoin, ovvero permette di utilizzare le chiavi per firmare digitalmente le transazioni da spedire alla rete. Una transazione inviata online però non deve solo essere firmata, ma anche **inclusa nella blockchain da un miner**, al fine di essere riconosciuta come valida dagli altri utenti.

I **miner** creano i blocchi della blockchain, che possiamo considerare come delle "pagine" del registro su cui scrivere le transazioni, con frequenza media di circa 10 minuti per ogni nuova pagina. Ogni pagina ha una dimensione massima (un po' più di 1mb), volutamente limitata dal protocollo Bitcoin al fine di mantenere la blockchain leggera, processabile da hardware alla portata chiunque (come un pc di basse prestazioni). Poiché però c'è un limite allo spazio, anche il **numero di transazioni validabili in un dato momento è limitato**. Se c'è molto traffico, i miner scelgono di inserire con priorità le transazioni che pagano commissioni più elevate, perché nel momento in cui un miner riesce a costruire un blocco Bitcoin (è a tutti gli effetti una gara) cercherà di massimizzare il profitto, riempiendo il blocco fino al limite con tutte le transazioni che pagano commissioni più alte.

La **commissione (o fee)** è un parametro che ogni utente stabilisce quando genera un pagamento dal proprio wallet. Software wallet come Electrum scandagliano la rete per valutare quanto sia trafficata, quindi suggeriscono una commissione della transazione adeguata alle esigenze impostate dall'utente, che a seconda delle situazioni può preferire pagare di più per avere transazioni più veloci, o viceversa fare transazioni economiche ma lente.

La blockchain non è immutabile nel breve/brevissimo periodo, poiché possono capitare (anche se molto di rado) **blocchi "orfani"** che vengono creati da un miner, ma poi scartati dal resto della rete. Se quindi la vostra transazione è inclusa in uno di quei blocchi viene "confermata" solo apparentemente, per alcuni secondi o minuti. Per avere quindi certezza che un pagamento sia andato a buon fine, è buona usanza attendere che, a valle del blocco in cui un miner ha incluso la vostra transazione, altri miner abbiano già creato ulteriori blocchi. **Generalmente, i wallet mostrano una transazione come "definitiva" quando sono stati creati 3 blocchi**: si dice in gergo che la transazione ha ottenuto **3 "conferme".**

Le transazioni che non ottengono velocemente la prima conferma **possono essere velocizzate anche dopo essere state inviate**, sfruttando sistemi come Child Pays For Parent o Replace By Fee (approfonditi in seguito). In alternativa, **per transare alla velocità di un "fulmine" e a commissioni prossime allo zero, si può partecipare alla rete "Lightning"**, che permette di trasferire bitcoin direttamente da wallet a wallet (in via privata e anonima) senza ricorrere alla blockchain. Sostanzialmente, Lightning Network è uno smart contract che prevede, per ogni transazione, uno scambio di "chiavi" diretto da utente a utente, le quali permettono di trasferire un output presente sulla blockchain. Il trasferimento su blockchain però non avviene: è sufficiente la "possibilità di trasferire" per renderti effettivamente in possesso di quei bitcoin. È possibile effettuare o ricevere pagamenti Lightning con qualunque utente nel mondo che sia collegato al Lightning Network senza doversi fidare di nessuno, se non del proprio wallet, proprio come avviene per le normali transazioni Bitcoin.

Questa guida pratica illustra come muoversi al meglio nell'utilizzo pratico dei wallet, sia per quanto riguarda la sua creazione che l'effettivo utilizzo nell'inviare, ricevere o velocizzare transazioni, senza fare errori o pagare più

commissioni del dovuto. Principalmente si vedrà l'utilizzo del software Electrum su PC, ma anche di wallet mobile (Breez). A scanso di equivoci, va detto che Coinbase, Binance, Crypto.com e altri siti o exchange non sono dei wallet propriamente detti, ma dei "**custodian**", ovvero servizi o banche che custodiscono per voi (nei loro wallet) i "vostri" bitcoin. Un sito internet è un sito internet, non è un wallet. Se non conoscete il seed o la chiave privata, non avete reale possesso dei vostri soldi.

1. **Installazione e creazione del wallet**

Se non avete ancora il wallet Electrum, scaricatelo dal sito ufficiale https://electrum.org/#download (per windows: "Windows installer"), quindi create il vostro wallet Bitcoin in pochi passaggi. Non appena installato e lanciato il software:

1. Nella prima schermata di creazione del wallet, scegliete un nome a piacere da dare al wallet. Il nome serve a identificare quel particolare wallet Electrum, poiché potrete avere wallet diversi sullo stesso pc. Digitato il nome, cliccate next.
2. Schermata "Create new wallet": selezionate "standard wallet" e cliccate avanti/next
3. Schermata "Keystore": selezionate "Create a new seed" e cliccate next
4. Schermata "Seed type": selezionate "segwit" e cliccate next
5. Quindi copiate il seed (le 12 parole) e scrivetelo anche su un supporto diverso dal computer che state usando. Ad esempio, un foglio di carta da tenere al sicuro (il così detto paper wallet). Ricordate che non dovrete mai perdere per nessun motivo quelle 12 parole, né mostrarle

a nessuno. Quelle parole **sono** il wallet, chiunque le possiede, possiede i vostri bitcoin.

6. Infine, nell'ultima schermata potete inserire una password. Questo passaggio è facoltativo, potete anche non inserire niente e cliccare su next. Questa password verrà richiesta ogni qual volta che lancerete l'applicazione Electrum sul pc.

Chi avesse già dei bitcoin in altro wallet, può importare il seed su Electrum, così da non dover fare una transazione onchain per trasferire lì i soldi. In fase di creazione del wallet è sufficiente scegliere l'opzione "I already have a seed/possiedo già un seed" nella schermata "Keystore". Normalmente, quando un seed viene importato si visualizzerà il proprio saldo non appena Electrum si è sincronizzato con la rete. Se non fosse così, si veda la sezione **Chiavi private** di questo articolo. Infatti, in alcuni casi il derivation path standard utilizzato da Electrum potrebbe essere diverso da quello del wallet che utilizzavate prima. È importante però specificare che soltanto un wallet SegWit (non multifirma) può funzionare con Lightning Network, che è a dir poco fondamentale nell'ecosistema Bitcoin, specie per gli anni a venire. Quindi se avete un wallet datato, consiglio di procedere con la creazione di un seed nuovo e trasferire tutti i vostri fondi sul nuovo wallet SegWit bech32 con Lightning Network.

2. **Ricevere bitcoin (onchain).**

Una volta che avrete il vostro wallet, la prima cosa da fare è ricevere dei Bitcoin. Senza che possediate dei Bitcoin non potete ovviamente inviarne, ma neanche aprire canali Lightning Network.

Andante quindi sul tab “ricevi/receive”, cliccate su New Address e copiate l’indirizzo che vi verrà mostrato. Cliccando su QR Code invece visualizzerete l’indirizzo Bitcoin nel formato scansionabile da fotocamera.

Quando un utente vi pagherà, vedrete immediatamente la transazione nella schermata “Cronologia”. La transazione non sarà ancora confermata però, bisognerà attendere che venga inserita in un blocco e, successivamente, che i miner generino ulteriori blocchi sopra di quello (per 3 conferme).

Se volete scegliere un qualsiasi altro indirizzo del vostro wallet anziché quello presentato nella schermata “Ricevi”, potete andare nel tab “Indirizzi” e copiare uno qualsiasi degli indirizzi lì presenti. Riceverete comunque su questo wallet i bitcoin. Gli indirizzi sono quei codici che iniziano per bc1, ad esempio “bc1q46zj4ww04hfz2jegympwfkd09wxe3nptchegk6”. Il formato che inizia con “bc1” (Native Segwit Bech32) è il più efficiente e permette di risparmiare commissioni di transazione, ma esistono anche indirizzi bitcoin più datati che iniziano con il numero 1 o il numero 3. Se un vostro amico vi mostra un indirizzo con l’1 o il 3, prendetelo per il culo perché è vecchio e ditegli che è pure stronzo, perché intasa la blockchain più del dovuto coi suoi indirizzi antiquati (la blockchain è di tutti, lasciate pulito quando passate!).

Non dovete essere online per ricevere un pagamento. Potrete controllare di aver ricevuto i bitcoin anche giorni, mesi o anni dopo. Conoscendo l’indirizzo/i che avete mostrato a terzi, potete risalire ai bitcoin ricevuti anche senza aprire il vostro wallet. Si può per esempio andare su un block explorer online e controllare, ad esempio su: https://www.blockchain.com/explorer

Nel caso d’esempio, l’indirizzo ha ricevuto nel tempo 0.0306 BTC e ne ha spediti poi 0.0306, per cui il saldo finale è zero.

3. **Inviare bitcoin pagando basse commissioni (onchain)**

Ci sono due modi per inviare Bitcoin dal proprio wallet: onchain oppure offchain tramite Lightning Network. L’invio onchain è il sistema tradizionale, richiede tempo e costa di più, ma è sempre possibile. Lightning Network invece è istantaneo e praticamente gratuito, ma richiede l’apertura di un canale, come si vedrà in seguito. Onchain si paga a degli “indirizzi” Bitcoin, su Lightning Network si paga invece a degli “Invoice”.

Per pagare onchain, sotto al tab “Invia” inserite l’indirizzo a cui volete spedire i soldi e l’importo (a fianco comparirà anche il corrispettivo in euro, o in qualsiasi altra valuta che impostate sotto a strumenti -> preferenze).

Cliccate quindi su “Paga” e comparirà una schermata ove impostare la commissione di mining. Siamo noi a dover impostare la commissione più alta o più bassa in base all’urgenza che abbiamo di inviare i soldi. Lasciando il mouse sulla barretta blu (nera in mouse over), il wallet vi mostrerà la commissione da pagare espressa in satoshi per byte. Si noterà che se impostiamo la commissione a 10 satoshi per byte si sborseranno 0.24 euro a fronte di una transazione da 159.88 euro. Quei 0.24 euro, ovvero 0.000015 BTC, si ottengono moltiplicando i satoshi che decidiamo di pagare per il peso in byte che possiamo trovare nella schermata di dettaglio (cliccare su “Progredito” per vederla).

La transazione è misurata in byte proprio perché il blocco su blockchain in cui verrà inserita ha un limite di spazio di poco più di un megabyte, di conseguenza maggiore è il peso della transazione, più in proporzione pagherete.

La cosa più interessante del wallet è che vi può suggerire la commissione da pagare. A fianco della barra per impostare il "Tasso di commissione" c'è un menu in cui potete selezionare l'opzione "**Tempo stimato di arrivo**". Cliccandola e muovendo la barra, il wallet vi suggerirà una commissione appetibile per i miner così da avere la transazione confermata entro *n* blocchi (è solo una stima, non una certezza).

Per ottenere la stima, il wallet guarderà al traffico di transazioni nella **mempool**, che è la memoria in cui vengono salvate tutte le transazioni intercettate nella rete, oltre che le commissioni pagate da quelle transazioni. In questi giorni in cui scrivo Bitcoin è appena tornato ai massimi storici e c'è traffico nella rete, perciò le commissioni di transazione sono medio-alte. Per inviare entro 25 blocchi (entro 4 ore circa) Electrum mi suggerise 61.8 satoshi per byte (circa 1.40 euro), per inviare entro i prossimi 2 blocchi (mediamente 15 minuti) suggerisce quasi 3 euro.

Salvo urgenze, il mio consiglio è quello di impostare una commissione bassa ed eventualmente aumentarla successivamente con l'opzione "replace by fee" se la transazione non venisse confermata per troppo tempo.

Nella schermata di dettaglio della transazione (cliccare su "Progredito"), oltre a vedere il peso della stessa in alto a destra (i questo caso "Dimensione: 141 bytes"), si può anche digitare l'esatto importo in satoshi per byte che volete

spendere, nel campo “Commissione obiettivo”.

Onde evitare di impostare una commissione esageratamente bassa, per i meno esperti è consigliato usare l’opzione del wallet “Tempo stimato di arrivo” anziché “Statico”. Infatti, se ci fosse molto traffico a tutte le ore del giorno, sette giorni su sette, può accadere che la transazione non venga mai confermata. Alcuni miner scartano le transazioni più vecchie di due settimane, quindi può essere che, anche se la mempool fosse vuota, nessun miner mantenga più nella propria memoria locale (mempool) traccia del vostro pagamento, che non verrà mai quindi inserito in blockchain. In ogni caso, si può sempre rimediare utilizzando “replace-by-fee” o “child-pays-for-parent” (approfonditi ai paragrafi sucessivi).

Ora, se vi sentite pronti a fare la prima transazione Bitcoin dal vostro bel wallet, fatela verso questo indirizzo: **bc1qlr9kf0vkxyutwaem6qrwjrurwh2y9ryx3gwmwv**. Potreste vincere magici premi e nuove guide pratiche su Bitcoin… e non solo! Inviarli lì è anche il modo più sicuro per accertarvi che quei soldi non finiscano mai all’Agenzia delle Entrate. Magari finiranno nel regalo di Natale a mia moglie (se sono sfortunato) o a Polina Malinovskaya (se sono fortunato), ma in ogni caso, di sicuro non all’Agenzia delle Entrate, promesso.

Focus teorico: a cosa è dovuta la variazione di peso di una transazione

Il peso di una transazione Bitcoin è variabile a seconda dei seguenti parametri:

- **Il numero di input**: più sono gli input che utilizzate per pagare, maggiore sarà il peso della transazione.

Immaginiamo per esempio di avere 2 bitcoin, ottenuti grazie a 2 transazioni: la prima da 1,3 BTC e la seconda da 0,7BTC. Queste due transazioni, anche se ricevute ad un nostro stesso indirizzo, hanno prodotto 2 output. Se quindi vogliamo spedire 1,5 Bitcoin dovremo attingere da entrambi questi output e utilizzarli come input, spendendo completamente il primo da 1,3 e ulteriori 0,2 dal secondo. La transazione avrà così 2 input anziché 1 soltanto. Se avessimo speso una qualsiasi cifra uguale o inferiore a 1,3, avremmo usato 1 solo input.

- **Il numero di output**: più output, maggiore è il peso. Generalmente una transazione Bitcoin ha 2 output: l'indirizzo del destinatario e un nostro indirizzo a cui ricevere "il resto". Tornando all'esempio fatto sopra, se inviamo 1,5 Bitcoin dovremo spendere completamente 1,3 BTC da un input e soltanto 0,2 dal secondo input che ammonta a 0,7 BTC. Quest'ultimo input viene necessariamente "spostato" nella sua interezza e i restanti 0,5 devono tornare al mittente. Le uniche transazioni con 1 solo output sono quelle in cui spendiamo interamente l'input e quindi non c'è bisogno di resto. Ci sono poi transazioni con molteplici output, ad esempio se abbiamo molti destinatari. In questi casi è conveniente fare una transazione unica che invia un pagamento a molti piuttosto che eseguire ogni transazione indipendentemente, poiché tutte insieme sommate peserebbero di più (questa pratica si chiama batching ed è molto utilizzata da exchange e servizi). Electrum permette di pagare a più destinatari: si veda la sezione strumenti->paga a molti (tools->pay to many).
- **Il tipo di indirizzo** in invio e ricezione: bech32 comporta commissioni inferiori rispetto a SegWit o indirizzi legacy, ovvero quelli prima dell'upgrade di Bitcoin approvato nell'agosto 2017
- **L'uso di SegWit**: l'utilizzo di indirizzi SegWit permette di "spalmare" il peso della propria transazione su due distinte parti del blocco Bitcoin: il blocksize e il

blockweight. Per questo motivo risulteranno meno costose rispetto a transazioni non segwit, che caricano tutto il peso sul blocksize, che è limitato a 1mb ed è più "affollato". Da notare che gli indirizzi bech32 che iniziano con bc1 sono SegWit, così come quelli che iniziano con il "3". Per quanto raro, si possono incontrare indirizzi che iniziano con il 3 che non siano segwit: si tratta dei multi-signature. Gli indirizzi sicuramente non SegWit sono quelli che iniziano con l'1.

- **Gli account multi-signature** (multi-firma): inviare da tali indirizzi costa di più perché la transazione richiederà due o più firme anziché una sola, e quindi peserà di più. La firma è l'elemento di peso maggiore in una transazione (circa 100bytes, contro circa 20bytes per un input o un output)
- **Le transazioni di smart contract** pesano di più, come i suddetti multi-signature, i locktime (non puoi spendere l'output ricevuto fino al bloco x) e altri script, fra cui le transazioni di apertura dei canali di Lightning Network.

Esempi di peso in byte di transazioni (bech32):

- Transazione standard senza resto (1 input, 1 output): 110 byte
- Transazione standard con resto (1 input, 2 output): 141 byte
- Apertura canale LN con 1 input, 2 output: 153 byte
- Apertura canale LN con 4 input, 2 output: 356 byte
- Chiusura del canale LN con 2 input, 2 output: 180 byte

4. **Velocizzare una transazione che state inviando (Replace By Fee o RBF)**

Anzitutto, assicuratevi di avere l'opzione "replace-by-fee"

abilitata nel wallet. Andate su “Strumenti/tool” -> “Preferenze/Preferences” e controllate che vi sia il flag sul campo “Usa Replace-by-fee/Use Replace-By-Fee”)

Questo consente di rimpiazzare (replace) una transazione con una identica, ma che paga commissioni maggiori. Non dovrete “cancellare” in alcun modo la transazione precedente (non potete farlo, ormai è stata trasmessa alla rete), ma potete stare certi che solo una delle due transazioni identiche che avete spedito online potrà essere inclusa nella blockchain. Infatti, una volta che una delle due transazioni è confermata in blockchain, se un miner includesse anche l’altra nel blocco che va a creare, quel blocco verrebbe scartato da tutti gli altri nodi del network Bitcoin, poiché presenterebbe un “double-spending”.

Un altro campo può essere molto utile da tenere flaggato: “Batch RBF Transactions” (la pessima traduzione italiana è “Transazioni partita RBF”). Qualora aveste più di una transazione in attesa di conferma, quest’ultima opzione permette di aggregare fra loro le transazioni (il già citato batching)

Invio quindi dei bitcoin impostando una fee fee troppo bassa: 1,4 satoshi per byte. La transazione appare subito nella cronologia del wallet, ma solo per miracolo la vedremo confermata in blockchain. Faccio quindi un **replace-by-fee** cliccando col destro sulla transazione e quindi su “aumenta commissione/increase fee”

Il wallet mi mostra l’interfaccia in cui impostare la nuova fee (commissione). Selezionando “tempo stimato di arrivo” e trascinando la barra al minimo, il wallet suggerisce 53 satoshi/byte. Secondo Electrum, guardando alla stato attuale

della mempool, quell'importo dovrebbe bastare per ottenere una conferma entro 25 blocchi.

Siccome però a me piace fare lo sborone e sono pure un tirchio di merda, gioco a battere in intelligenza l'algoritmo di Electrum e imposto una fee più bassa, a 25 satoshi per byte anziché 53, che mi sembrano troppi (guai a spendere quei 0.70$ in più!). Per farlo, semplicemente digito manualmente la cifra nel riquadro e poi clicco OK. Nella schermata successiva, mi viene mostrato il dettaglio della transazione:

Come vedete la commissione totale ammonta a 0,000036BTC, ovvero circa 70 centesimi di euro. Mi può andar bene. Clicco su **"Firma"** (Sign), quindi su **"Trasmissione"** (Broadcast) per mandare alla rete. Ora tornando nella cronologia delle transazioni vedrete la transazione ancora Unconfirmed, ma il valore di fee impostato che potete vedere a fianco è cresciuto.

Vi chiederete la ragione per cui ho impostato 25 satoshi per byte e il ragionamento che ho seguito. Ebbene, ci sono siti internet che ci permettono di osservare lo status della mempool. In particolare, a me piace questo (lo trovate fra i primi risultati su google digitando "mempool bitcoin": https://jochen-hoenicke.de/queue/#0,24h

Fra i grafici presentati nel sito, vedete il seguente che raggruppa le transazioni in colori diversi in base a quante commissioni pagano. In questo momento una transazione da 25 satoshi per byte è nel gruppo verde chiaro. Si può notare che in questo momento (l'1.00 di notte circa) ci sono circa 28 mila transazioni in attesa, ma di queste poche che pagano di più rispetto a quelle nel gruppo verde chiaro. C'è qualche transazione nella fascia gialla in attesa (che paga 80-100

satoshi per byte), ma non appena quelle entreranno in un blocco, ci sarà spazio anche per la mia. Un blocco mediamente contiene più di 2 mila transazioni, quindi ho abbastanza fiducia di avere una conferma presto, salvo ovviamente che non arrivino in questi minuti una serie di altre transazioni a priorità maggiore.

Di fatto, la transazione è stata inclusa quasi subito, nel blocco bitcoin numero 659.984 delle ore 01.07. Non sono stato solo bravo, ma anche fortunato. La trovate inserendo l'id su qualsiasi block explorer, ad esempio: https://blockstream.info/tx/27a35525d76c47f2bd3b049ef2662faded0709f5e8582374209341ef9f20d1d4

In genere, non fatevi scoraggiare troppo da transazioni molto alte. Spesso le commissioni si possono abbassare repentinamente anche soltanto nell'arco di due blocchi. Qui un caso d'esempio in cui il sito mempool.space suggerisce dapprima 1.22$ per una transazione ad alta priorità e solo 5 minuti dopo l'importo suggerito scende a 0.24$.

Se comunque non avete dimestichezza con la mempool e/o non volete perdere tempo per risparmiare pochi centesimi e rischiare un ritardo nelle transazioni, fidatevi di Electrum che andate sul sicuro.

5. **Velocizzare una transazione che state ricevendo con Child Pays For Parent (CPFP)**

Abbiamo visto come si può velocizzare una transazione che

stiamo inviando, ma per quelle che riceviamo come si può fare? Ci sono tre modi per ricevere più in fretta Bitcoin: comunemente detti la soluzione Charmender, la soluzione Squirtle e la soluzione Bulbasaur. Chiamate così in onore dei tre veri supercattivi dietro allo pseudonimo Dread Pirate Roberts (l'FBI ha fatto un grave errore col povero Ross Ulbricht, per cui ricordiamo sempre di lasciare una firma per la sua scarcerazione su change.org).

1. La soluzione Charmender è più una punizione che soluzione, di tipo corporale per giunta, e prevede di bruciare vivo il mittente taccagno finché non paga commissioni più alte o fa un Replace-by-fee. È un sistema efficace. Purtroppo però, soltanto di rado avrete fisicamente a portata di mano il mittente per seviziarlo. In ogni caso, mi raccomando bambini: nell'appiccare il fuoco fatevi assistere da un adulto.

2. La soluzione Squirtle è invece più pacifica e punta tutto sull'altissima liquidità: ci si fa pagare su Lightning Network anziché su blockchain (vedasi il capitolo dedicato). La transazione risulterà immediata, a zero fee e non inquina la blockchain con inutili dati, che eleganza! Ma non sempre la nostra controparte avrà un canale Lightning pronto in cui navigare, perciò anche in questo caso, la soluzione è applicabile solo in situazioni circostanziate.

C'è per fortuna una terza via, applicabile in ogni circostanza e per cui sarete del tutto autonomi:

3. La soluzione Bulbasaur, anche detta **Child-pays-for-parent**. Per godere dei frutti del Bitcoin, devi curare la tua piantina e farla crescere in equilibrio con l'universo. Vediamo come.

Per tenere duro nella spiegazione teorica che segue, pensate al musetto sorridente di Bulbasaur (ve la devo indorare così, altrimenti mi skippate il paragrafo, maledette nuove generazioni). Ebbene, Child-pays-for-parent (CPFP) consiste nell'effettuare una transazione "figlia" della transazione che

state per ricevere. Immaginiamo che il mittente stia trasferendo i bitcoin dal suo indirizzo A al vostro indirizzo B. La sua transazione (che chiamiamo M per “madre”) non è ancora confermata in blockchain, eppure voi potrete comunque trasmettere online una transazione F (“figlia”) che trasferisce l’output della madre dall’indirizzo B all’indirizzo B stesso. F non potrà essere inclusa in blockchain da un miner senza che sia confermata anche M, altrimenti spenderebbe un output inesistente in blockchain. Tuttavia, il miner potrà includere in un singolo blocco sia F che M, incamerando le commissioni pagate da entrambe. Lo farà perché la somma delle fee pagate dalle due transazioni gli risulta appetibile, in rapporto al peso aggregato in byte di F e M. In poche parole, la transazione F dovrà pagare commissioni un po’ più alte della media, per compensare quelle base pagate con M.

Se non avete capito una mazza non importa, **all’atto pratico è semplicissimo**.

Tutte le transazioni non confermate in ricezione possono essere velocizzate, anche le transazioni di chiusura dei canali Lightning Network. Nel caso d’esempio, velocizzeremo proprio la transazione di chiusura del canale (il procedimento comunque non cambia per qualsiasi altro tipo di transazione).

Nella schermata della cronologia, **cliccate col destro sulla transazione che volete velocizzare**. Selezionate quindi “**Child pays for parent**” e impostate una commissione secondo le logiche già descritte nel capitolo dedicato al replace-by-fee. In questo caso, il wallet calcolerà in automatico il rapporto satoshi/byte considerando il peso aggregato di entrambe le transazioni (madre e figlia).

Cliccate quindi su “OK” lanciando così in rete la vostra transazione figlia.

Come noterete, le fee erano già abbastanza alte per la madre (79 s/b), ma stanotte ho particolarmente fretta di finire la guida perché ho sonno, quindi dilapiderò ogni mio avere pagando ben 149 s/b con la CPFP, per un totale di oltre 30 mila satoshi pagati per transazione madre e figlia.

Nella cronologia vediamo quindi entrambe le transazioni, di cui la figlia presenta l'icona di "attenzione" perché la relativa transazione madre non è confermata. La madre invece presenta la solita iconcina con le rotelle, a indicare che è in elaborazione (o meglio, in attesa di essere confermata in blockchain). In pochi minuti, le due transazioni sono state inserite nel primo blocco creato (ci mancherebbe, con le fee che ho pagato!). Come per ogni transazione Bitcoin, la prima conferma è mostrata in rosso, poi l'icona diventa verde quando nuovi blocchi vengono aggiunti sopra la transazione.

Un'ultima cosa da notare: se siete in dubbio sulla commissione da pagare per una transazione CPFP, potete prima impostarla più bassa e poi fare un RBF su di essa! *Pure magic*!

Se siete tristi perché avete dovuto pagare una commissione di transazione altina, ricordate sempre il motto:

B – Lightning Network

L'idea fondamentale dietro agli sviluppi di Bitcoin degli ultimi 5 anni[1] – e che lo contraddistingue rispetto a tutte le altcoin – è che la blockchain vada utilizzata principalmente per aprire e chiudere "canali di pagamento" da

wallet a wallet che processeranno offchain la gran parte delle transazioni, anziché ingolfare la blockchain, che è limitata in termini di scalabilità. Lightning Network permette a un nodo/wallet di connettersi con un altro nodo e, tramite questo che ci farà da ponte, all'intera rete. Per capire il principio per cui riusciremo così a transare con chiunque altro nella rete, ci possiamo rifare alla famosa regola dei 6 gradi di sperazione di Karinthy: ognuno al mondo è collegato con qualunque altra persona attraverso una catena di conoscenze e relazioni con non più di 5 intermediari. Questo vale per persone connesse in modo del tutto casuale, tanto più per una rete informatica col preciso scopo di connettere tutti, per cui non scegliamo i nodi router in maniera casuale.

Il nostro nodo Electrum non sarà un nodo che fa routing, cioè non convoglierà i pagamenti di altre persone verso altri nodi. Quell'attività, seppur non così complicata (qualunque smanettone può farlo senza fatica), esula dallo scopo di questa guida per bambini. Il wallet sarà un così detto light client ("leggero") o light wallet, che non deve essere sempre online come i nodi Lightning che fanno routing. E non è necessaria alcuna fiducia verso il nodo con cui abbiamo aperto un canale, quantomeno **non se accediamo al wallet almeno una volta ogni 2 settimane**, così che possa sincronizzarsi con la rete per controllare eventuali tentativi di frode e bloccarli istantaneamente, tramite la chiusura forzata del canale che scatta automaticamente.

I light wallet non fanno routing, si possono solo connettere a uno o più nodi che fanno loro da ponte per partecipare alla rete LN. Hanno però il grande vantaggio di non dover rimanere sempre online e richiedono risorse hardware risibili. Alcuni dei più noti wallet mobile sono invece custodial, perciò bisognerà fidarsi del provider.

6. **Aprire un canale LN**

Prima di continuare, un breve inserzione promozionale. Sto progettando e sviluppando una sidechain di Bitcoin per la creazione di asset digitali come security token e stablecoin, chiamata Mintlayer. Vi invito a visitare il relativo sito internet, leggere le Q&A degli utenti su Reddit e unirvi ai gruppi telegram inglese e italiano. Se non fate nessuna di queste azioni, koffing vi apparirà in stanza di notte spruzzando covid ovunque.

E babbo natale non vi porterà i regali.

Proseguendo con la guida: premesso che abbiate dei Bitcoin nel wallet, spostatevi nella **schermata "Canali"** e cliccate su **Apri canale**.

Cliccate quindi su "Suggest peer", Electrum vi suggerirà un fullnode router che ha individuato in questo momento come ottimo punto per allacciarsi al network di canali Lightning. Inoltre, inserite la quantità di Bitcoin che volete inviare nel canale. **I soldi che state caricando sul canale rimarranno vostri** finché non deciderete di inviarli a qualcuno tramite una transazione Lightning Network. Attraverso il canale, **non potrete mai inviare e ricevere un numero di bitcoin maggiore dell'ammontare che state caricando** ora sul canale.

Ogni volta che ripeterete questa operazione, Electrum potrebbe suggerire un nodo diverso. Potete decidere di connettervi a quel nodo o sceglierne un altro, inserendo voi l'ID di un nodo a piacere che conoscete o che avete trovato in rete. A scopo dimostrativo, opterò per questo primo nodo scelto per noi da Electrum, ma comunque curiosiamo online per vedere qualche informazione in più. Andiamo quindi su un sito piuttosto comune per monitorare l'attività su Lightning Network:

https://1ml.com/

Quindi inseriamo l'ID del nodo nella barra di ricerca principale e premiamo invio. Potete cercarlo anche voi ora incollando il **node id, ovvero la "public key" del nodo**: 0384417e479afb21bff425f467382f9c064ac08bd422ea36542fa6799e026d77e6.
Il proprietario ha nominato il nodo "Maxjuwil", che gira su software LND (Lightning Network Daemon, il più comune fullnode).

Nel momento in cui ho preso lo screenshot, il nodo ha 49 canali connessi con una capacità totale di circa 0,74 bitcoin totali ed è attivo da ben 2 anni. Come vedete dal **Node Rank** a centro pagina, ci sono almeno 2058 nodi attivi da più tempo di questo, almeno 334 con maggiore capacità, almeno 218 con un numero di connessioni maggiore, ma non importa. È giusto che non tutti gli utenti si connettano soltanto ai nodi Lightning più grossi, così da aumentare la resilienza della rete. Infatti, se tutti fossero connessi a pochissimi grossi hub e un attacco riuscisse a colpirli, l'intera rete sarebbe rallentata: ogni utente dovrebbe chiudere e riaprire i canali aperti con quei grossi nodi.

Fra i maggiori hub della rete LN, oggi vediamo ACINQ, Bitfinex, Bitrefill, OpenNode, CoinGate, LNBIG, Wallet of Satoshi e altri. Volendo, potete scegliere anche di connettervi a uno qualsiasi di quei nodi, basta copiare la relativa public key su **1ml.com** e incollarla nel campo node id di Electrum quando create il canale. Non potete invece connettervi direttamente con un altro wallet Electurm come il vostro o con un wallet LN mobile come Breez, Bluewallet o Wallet of Satoshi. Tutti questi sono "light wallet" e hanno bisogno di connettersi con un fullnode router per funzionare nella rete LN, in maniera analoga a come un wallet SPV onchain si appoggia alla blockchain.

Ad ogni modo, le statistiche del nodo Maxjuwil mi sembrano più che accettabili a garantirmi una connessione con chiunque abbia un nodo Lightning nel mondo. Quindi procedo cliccando "OK". Electrum mi chiede di impostare una commissione per la transazione di apertura del canale.

Imposto una commissione bassa perché non ho fretta: 5 satoshi/byte. Al cambio attuale sono in totale 27 centesimi di euro, un quinto rispetto al costo suggerito in quel momento dal sito https://mempool.space per le transazioni a bassa priorità. Il wallet mi dà immediata conferma dell'apertura del canale, anche se non è ancora agibile (status: OPENING). **Servono tre conferme su blockchain prima che Electrum ci permetta di transare su Lightning Network.**

Nella finestra "Cronologia" vedremo la transazione di apertura. Finché non è confermata, il nostro saldo onchain figura ancora intatto (come se non avessimo ancora i soldi su LN), ma il saldo sul canale Lightning appare già, anche se il canale è ancora inagibile.

In attesa delle conferme spengo il pc e vado a dormire: non c'è bisogno che il pc rimanga online. L'indomani mattina noto che la transazione è stata confermata a circa 3 ore dalla sua esecuzione. Ora il mio canale è agibile e il saldo onchain è sceso. Trovate la transazione di apertura del canale qui (il blockexplorer di Blockstream riporta fieramente che la transazione, essendo SegWit bech32, ha speso il 47% in meno rispetto alle vecchie transazioni): https://blockstream.info/tx/f64d173ed5448d4e1f930ecad2d71d2d2312c1cb800849fdf101f41079078946

Osserviamo quindi il nostro canale nella finestra **Canali**. Qui

constato che ho una capacità di invio ma non di ricezione. Inoltre, il canale **ci permette di inviare una quantità di bitcoin leggermente inferiore rispetto al nostro saldo totale** su LN: infatti **poco meno di 0.0005 BTC devono rimanere a vostra disposizione per pagare i miner qualora vogliate chiudere il canale** con una transazione onchain. Questo è anche il motivo per cui **Electrum non ti permette di aprire un canale di importo inferiore a 0,0002 BTC**, che ad oggi sono un po' più di 30 euro. Dopotutto, non saprei a cosa possa servirvi un canale più piccolo di quella cifra.

Il fatto che, **nonostante aver aperto il canale, non potete ancora ricevere alcun Bitcoin tramite LN**, è la prima questione da dirimere. Questa sarà la situazione in cui vi ritroverete sempre con Electrum nel momento di apertura di un canale. Il motivo lo spieghiamo nel focus teorico di seguito.

Focus teorico: capienza dei canali Lightning Network

Dobbiamo pensare al canale come un'asta di **un abaco** e i bitcoin nel canale i suoi **anelli.** Non è possibile aggiungere o rimuovere anelli, soltanto spostarli da un'estremità all'altra dell'asta. Immaginiamo che Alberto (A) abbia appena aperto un canale da 0.005 bitcoin con Bulbasaur (B)[2]. Rappresentiamo ogni 0.001 BTC con un anello blu che scorre da un'estremità all'altra dell'asta quando viene trasferito da A a B o viceversa.

Tutto ciò che è trasferibile su un canale è soltanto quanto avete caricato alla sua apertura. Bulbasaur non potrà trasferire anelli blu ad Alberto, perché al momento sono tutti dalla parte di Alberto. Per abilitare quindi il canale anche in ricezione, Alberto dovrà spostare degli anelli blu verso Bulbasaur. Per farlo, deve eseguire almeno una di queste tre

azioni:

PRIMO: Pagare effettivamente qualcuno tramite Lightning Network

SECONDO: Effettuare un submarine swap

TERZO: Inviare a se stesso dei bitcoin su Lightning Network

Illustriamo punto per punto.

PRIMO: Aumentare capacità in ricezione pagando qualcuno

ipotizziamo che Bulbasaur abbia già dei canali aperti con Squirtle e Charmender. Bulbasaur è in questo caso un po' come il nodo router di Maxjuwil con cui abbiamo aperto il canale nella guida pratica e che, avendo molti canali aperti, può farci da tramite nelle transazioni con vari utenti. Il portafoglio totale di Alberto su LN è di 0,005BTC, quello di Bulbasaur anche, mentre Squirtle e Charmender possiedono rispettivamente 0,002 e 0,003 BTC.

Per ipotesi, Alberto deve ricevere 0.001BTC da Squirtle, ma in questo momento non ha alcuna capacità in ricezione su LN. Per fortuna però, deve anche pagare Charmender 0.002BTC.

A invia quindi 0.002 BTC a Charmender tramite Bulbasaur (**Fase 1**), così che può poi ricevere da Squirtle 0.001 BTC (**Fase 2**). Si noti che il portafoglio totale di Bulbasaur non è mai variato fra la fase 0, 1 e 2, se si sommano i bitcoin che possiede su tutti i vari canali. Bulbasaur è quindi in questo caso soltanto un nodo passivo che fa da tramite.

SECONDO: Effettuare un submarine swap

Nel momento in cui un canale è appena stato aperto, o se dopo

varie transazioni dovesse esaurire la sua capacità in ricezione (perché avete incassato tanto e speso poco) o in invio (perché avete speso tanto e incassato poco), si può "riequilibrare" il canale tramite un submarine swap[3].

Se vogliamo quindi aumentare la nostra capacità in ricezione sul canale, nello scambio si cedono dei bitcoin su LN in cambio di un'equivalente cifra che riceviamo da un altro utente con una transazione onchain (ovviamente pagando una fee al miner per quella transazione).

Nel caso d'esempio, Alberto manda 0.002BTC a Squirtle offchain, che restituisce ad Alberto 0.002BTC onchain.

In caso di submarine swap, il saldo totale di tutti gli attori in gioco non è cambiato:

- Alberto ha sempre 0.011BTC (11 anelli blu, se si somma saldo offchain e onchain), ma se prima ne aveva 0,005 su LN e 0,006 onchain, ora sono 0,003 LN e 0,008 onchain.
- Bulbasaur fa solo da tramite e ha sempre 0.003 BTC LN
- Squirtle ha sempre 0,008 BTC, prima solo 0,002 LN, ora 0,004. Il suo saldo onchain è invece sceso da 0.006 a 0.004 BTC

Ovviamente, un submarine swap può essere visto anche al contrario, ovvero non è solo Alberto ad aver bisogno di aumentare la sua capacità di ricezione, ma Squirtle a voler aumentare quella in invio. A seconda delle circostanze infatti, un utente potrebbe voler riequilibrare il proprio canale aumentando e diminuendo a piacere il potere di ricezione e invio.

Generalmente, ci sono nodi che si occupano specificamente di offrirti liquidità effettuando submarine swap in cambio di una piccola fee (nel caso del nodo a cui si appoggia Electrum per queste operazioni, la commissione è dello 0,01%).

TERZO: Inviare dei bitcoin a se stessi su Lightning Network

Per riequilibrare i propri canali c'è un secondo modo, più furbetto, che permette di evitare i submarine swap e la relativa commissione. Immaginate che, come nella situazione descritta al punto 1, Squirtle vi debba inviare dei bitcoin su LN, ma non c'è nessun utente come Charmender a cui dovete dei soldi e che, pagando, vi permette di liberare il vostro canale. Miei cari bimbi, non preoccupatevi, perché potete tranquillamente trasferire dei soldi a voi stessi!

Nella fase 1 sopra, immaginate di rimpiazzare Charmender con Alberto e il gioco è fatto. Voi direte che mi sono rincretinito: "ma se questo è il primo canale che ho aperto su Electrum, come faccio ad averne già uno a disposizione con capacità anche in ricezione, verso cui inviare bitcoin?". In realtà, come vedremo nel seguito della guida pratica, possiamo sfruttare dei wallet LN custodial o, ancor meglio, **il wallet non-custodial di Breez verso cui il nodo della società Breez crea in automatico un canale a spese loro**. Come questo sia per la società Breez un'attività economicamente sostenibile, lo spiego in appendice. Il canale che Breez creerà per noi può gestire **fino a 4 milioni di satoshi**, ad oggi circa 700 euro, quindi **non dovremo preocuparci della capacità in ricezione** finché non superiamo quelle cifre (ed è difficile che su smartphone vi servano più di 700 euro via LN). **Combinando Breez su smartphone ed Electrum su desktop, avrete la combo perfetta telefono+PC pronti sia a inviare che ricevere.** Potrete finalmente sentirvi fieramente bimbi nerd.

7. **Inviare e ricevere bitcoin su LN**

Appena aperto il canale su Electurm non possiamo ancora ricevere denaro, quindi inviamo dei bitcoin LN al wallet mobile Breez, per liberare la capacità in entrata di Electrum. Prima però, siccome Breez usa come unità di misura i satoshi, modifico anche l'unità di misura su Electrum. Almeno ci

liberiamo anche di degli “zero virgola” dalle cifre.

Una volta fatto, vedremo il nostro saldo del canale come 500.000 (satoshi) anziché 0.005 (bitcoin).

Apriamo quindi sul nostro smartphone **iOS o Android il wallet Breez**. Non c’è bisogno di una guida su come configurarlo in partenza, poiché la procedura guidata dell’app è estremamente semplice. Una volta fatto, **dalla schermata principale** dell’app Breez vediamo il pulsante “**Receive**”. Clicchiamo lì per creare una richiesta di pagamento, che in gergo è detta “**Invoice**”. Ovviamente, il primo requisito per una qualsiasi transazione è sapere chi dobbiamo pagare, lo stesso dunque vale per una transazione Lightning con la creazione dell’invoice da parte del ricevente. Nell’invoice è inclusa la public key (chi pagare) e l’ammontare (quanto pagare), perciò su breez specifichiamo anche la somma. Poiché su Electrum ho 500 mila satoshi, decido di spedirne 200 mila a Breez. Digito quindi 200000 nel campo “amount in sats” e clicco **Create**.

Dobbiamo quindi portare il codice dell’invoice su Electrum. Presupponendo che il vostro computer non abbia una fotocamera comoda per scansionare il QR code, copiamo il codice testuale da Breez, che ha questo aspetto:

Inviamolo al pc con Electrum in qualunque maniera. Possiamo anche rendere pubblico questo invoice mettendolo online. Incollo quindi l’invoice dentro Electrum nel campo “Paga a”, sotto al tab Invia/Send.

Non preoccupatevi se sotto “Paga a” l’invoice preso da Breez

assume un aspetto diverso su Electrum. Semplicemente tutte le informazioni contenute nell'invoice vengono "spacchettate" in node id, descrizione e quantità.

Dopo aver cliccato su "Paga…" Electrum vi chiederà un'ultima conferma. **Assicuratevi che il wallet di Breez sia online (il telefono non deve essere bloccato o sconnesso)**, quindi su Electrum cliccare su Yes. Se entrambi i wallet non sono online il pagamento fallirà e dovrete riprovare, incollando nuovamente l'invoice in Electrum e cliccando nuovamente su Paga. Questa è una grossa **differenza fra Bitcoin onchain e Lightning Network: quest'ultimo è istantaneo e "gratuito", ma ha lo svantaggio che mittente e destinatario devono essere connessi nello stesso momento** (in teoria, anche tramite connessioni alternative rispetto alla rete internet).

Possiamo notare nella schermata cronologia il nostro pagamento, contraddistinto rispetto alle normali transazioni onchain dall'icona del fulmine.

Ricordate che abbiamo inserito come unità di misura i satoshi. Dalla quantità spesa, possiamo vedere come il pagamento non sia del tutto "gratuito"… abbiamo speso ben 1,7 satoshi, che al cambio odierno ammontano alla bellezza di 0,00025 euro, ovvero 2 centesimi di centesimi di euro!! Per spendere 1 euro con queste transazioni, dovrei farne 10 mila. Su questa commissione e su chi se la intasca torneremo a breve.

Come piccola parentesi teorica, riporto una mappa del viaggio che hanno fatto i nostri satoshi per arrivare al wallet di Breez. Si noti che tutti i nodi intermedi (Maxjuwil, il dittatore coreano e l'azienda Breez) sono soltanto passivi, ovvero non hanno un cambiamento nel proprio saldo contabile. Infatti, ciascuno di essi ha due canali e guadagna 200 mila satoshi su un canale, perdendone 200 mila sull'altro.

La cosa interessante è che i nodi intermedi potrebbero non avere la più pallida idea di quale transazione stiano effettivamente processando. Soltanto Alberto (PC) e Alberto (mobile) sanno chi sia mittente e destinatario (sempre Alberto, lol). Per esempio, il dittatore coreano al centro (o chi per lui) non sa quanto lunga sia la catena di passaggi, vede soltanto un pagamento in ricezione da Maxjuwil e uno in uscita verso Breez. Inoltre, qualsiasi utente che non è intermediario della transazione fra Alberto e Alberto non ne saprà mai nulla: questa transazione infatti non è scritta su blockchain, ma è registrata soltanto nei singoli wallet degli utenti coinvolti. Se pensavate di essere già di buonumore con queste informazioni, ora vi svolto proprio la giornata con la seguente rivelazione, che vi faccio in totale confidenza: i cosi blu che si muovono sull'abaco, nella figura sopra, non sono anelli o perline qualsiasi, ma si tratta di ovetti di cioccolato pasquali! Ora che vi ho rivelato questo magico segreto di felicità, proseguiamo con la guida.

A questo punto, come buon esercizio per far pratica di LN spediremo i 200 mila satoshi ad un terzo wallet che è Bluewallet (un wallet custodial che **NON** vi consiglio di usare e vedremo perché) e da qui li rimanderemo a Electrum. Ci sono un paio di **nozioni sulla capacità dei canali di cui tenere conto** che è più utile imparare con la pratica che nella teoria.

Una volta installato Bluewallet, **creo l'invoice** digitando 200000 (sats), lo copio (cliccando su **share**) e apro Breez. Avrei potuto scansionare con Breez l'invoice direttamente dall'app di Bluewallet tramite QR code, ma siccome ho installato entrambe le app sullo stesso telefono, mi tocca copiare la stringa testuale dall'app Bluewallet, quindi chiuderla e aprire Breez. Non appena aperto Breez, l'app mi riconosce immediatamente che il mio smartphone ha in memoria

(in clipboard) l’invoice appena copiato e, senza che io abbia fatto alcuna azione, mi chiede se voglio pagare quell’invoice. Do quindi la conferma e la transazione avviene istantaneamente su entrambe le app, in uscita per Breez, in entrata per Bluewallet.

Il mio saldo su Breez era 201.500, ma ora che abbiamo spedito a Bluewallet quei 200.000, su Breez non abbiamo 1.500 satoshi, ma soltanto 1.497. I 3 satoshi mancanti sono infatti stati pagati come commissione di transazione ai nodi intermedi fra Breez e Bluewallet. Evidentemente, nella transazione fra Electrum e Breez, dove abbiamo pagato solo 1,7 satoshi anziché 3, c’erano meno nodi intermedi, oppure i nodi intermedi ci caricavano una commissione di transazione minore rispetto a quelli fra Breez e Bluewallet. Quando parliamo di **transazioni “quasi” gratuite su LN** facciamo proprio riferimento a questa commissione, che se non abbiamo ancora menzionato finora è soltanto perché effettivamente è quasi irrilevante, dato che ha ordini di grandezza del tutto sotto-scala rispetto alle commissioni di mining.

Ora come ultimo esercizio effettuiamo il passaggio finale, ovvero da Bluewallet a Electrum. Garantisco che sarà un’esperienza altamente formativa.

Anzitutto, la prima cosa da controllare è la nostra capacità in ricezione su Electrum. Curiosamente, **Electrum ha appena inviato 200 mila satoshi a Breez, eppure adesso non può riceverne 200 mila, ma soltanto 195.000.** La nostra prima transazione effettuata da Electrum verso Breez aveva infatti comportato che, nel nostro canale aperto, ora noi abbiamo 200 mila satoshi in meno, mentre Maxjuwil è passato da 0 a 200.001 esatti. Quel singolo satoshi aggiuntivo è la commissione di transazione che si è guadagnato il buon Max quando abbiamo trasferito i fondi tramite il suo nodo.

La nostra capacità massima di ricezione sul canale (inbound) dovrebbe corrispondere al saldo della nostra controparte del canale (200.001s), eppure come vediamo è leggermente inferiore (195.001s). Questo avviene perché non possiamo azzerare completamente il saldo della nostra controparte. Infatti, **i wallet trattengono in via preventiva una certa quantità di satoshi sul canale** (in questo caso 5.000 satoshi, cioè **meno di 1 euro**), che servirà per pagare le commissioni di transazione: entrambi gli utenti infatti (Alberto o Maxjuwil), devono mantenere la possibilità di chiudere il canale in qualsiasi momento e riportare il proprio saldo onchain, effettuando una transazione che deve pagare i miner.

Se provo a trasferire per esempio 198.000 sats a Electrum, cioè più di 195.000, il pagamento fallirà e Bluewallet riporterà il seguente messaggio di errore: “Il destinatario ha abbastanza capacità in ricezione?”. Ho provato a fare lo stesso anche con Breez e lì dà un errore generico senza dettagliare le motivazioni del fallimento (confido che aggiorneranno in futuro).

Se invece provo a inviare 200.000 satoshi da Bluewallet, prima ancora di ricevere il messaggio di errore già visto, Bluewallet mi blocca. Infatti, il mio saldo su Bluewallet ammonta proprio a 200.000, e non posso trasferirli tutti perché l’azienda Bluewallet ha deciso che devo mantenere una riserva minima dell’1% per coprire le fee che pagherò a loro quando trasferisco i miei satoshi (ricordiamo che si tratta di un wallet custodial e quindi fiduciario). Essendo l’1% proprio 2000 satoshi, Bluewallet mi permette di inviare 198.000, ma non 200.000. Mi decido quindi a creare l’invoice per 195001 satoshi, ovvero il massimo ricevibile da Electrum.

Questa volta, avendo creato l’invoice sul PC desktop, posso

scansionare il qr code col mio telefono. Apro quindi l'app di Bluewallet e clicco sull'iconcina del QR Code, si accende la fotocamera, inquadro ed è fatta. Nel creare la transazione, Bluewallet specifica che potrei pagare commissioni fino a **1951 satoshi**! Si tratterebbe di circa 30 centesimi di euro, praticamente come una transazione onchain. Maledetti ladri.

A transazione fatta, vedo che Bluewallet mi ha caricato **606 satoshi** (fortunatamente non 1951). Voi direte: "relax, sono solo 10 centesimi, che ti costa!". Ma 10 centesimi ADESSO! Ma per mio nipote sarà uno stipendio. E io non ci tengo a dare a Bluewallet lo stipendio di mio nipote.

Per farla breve, ecco una scheda comparativa dei tre wallet presentati:

Wallet	**Funzionalità**	**Trustless**	**Semplicità d'uso**	**Costo di transazione LN**	**Voto**
Electrum	Avanzate	Si	Così così	1-3 satoshi = 0,000..€	Top
Breez	Base	Si	Molto semplice	1-3 satoshi = 0,000..€	Cool
Bluewallet	Base	No (custodial)	Molto Semplice	606 satoshi = 0,10 €	Ouch

8. **Aumentare la capacità di ricezione o invio del canale LN (submarine swap)**

Ora vediamo un'ultimo passaggio su Electrum, ovvero aumentare la capacità in ricezione o invio del proprio canale senza appoggiarsi a un altro wallet di cui siamo proprietari (ipotizzando quindi di non avere un Breez a supporto).

Nel caso in questione, ho un canale aperto col nodo LNBIG.com per un totale di 0,005 BTC. Non posso ricevere nemmeno un satoshi, quindi voglio aumentare la mia capacità inbound. **Nella schermata Canali seleziono la riga corrispondente al canale e quindi clicco sul pulsante Swap.**

Nella schermata che si apre, **cliccando sull'icona** lightning gialla o sull'icona di Bitcoin blu (quest'ultima rappresenta la transazione onchain) **possiamo modificare la tipologia di Swap che vogliamo effettuare**. Qui in figura sono mostrate entrambe le finestre popup una sotto all'altra, ma in realtà l'interfaccia di Electrum le mostra come alternative quando clicchiamo sulle suddette icone. Tramite la prima opzione, che è detta ***Reverse Swap***, possiamo aumentare la nostra capacità in ricezione su LN. La seconda, detta semplicemente ***Swap***, permette di aumentare la nostra capacità di invio su LN.

Alcuni secondi dopo aver effettuato il ***reverse swap,*** vediamo immediatamente il canale LN riequilibrato, con una buona capacità sia in invio che in ricezione, anche se la transazione onchain ancora non ha avuto la prima conferma.

9. **Chiudere un canale LN**

Chiudere un canale è semplicissimo, basta entrare nell'interfaccia "Canali", cliccare sul destro sul canale e selezionare "Chiudi canale". La richiesta verrà inoltrata alla controparte. Normalmente la controparte è d'accordo sulla chiusura bilaterale e firmerà la transazione, che verrà spedita in rete per l'inclusione da parte dei miner in blockchain.

Si ricorda che, qualora avessimo un saldo disponibile basso sul canale, per cui la transazione di chiusura è molto lenta o addirittura, nella peggiore delle situazioni, non viene inclusa in blockchain per giorni, potrete sempre fare un Child-pays-for-parent come descritto nel relativo capitolo.

Nel raro caso in cui il nodo con cui abbiamo aperto un canale non rispondesse, dobbiamo forzare la chiusura ("Chiusura forzata canale/ Force-close channel"). Di default, quando uno dei due nodi avvia la chiusura forzata può recuperare i propri fondi solo dopo 2016 blocchi Bitcoin dalla conferma della transazione di chiusura in blockchain. Questo ritardo (2016 blocchi corrispondono a circa 14 giorni) permette alla controparte del canale di avere due settimane di tempo per intervenire, qualora la chiusura forzata fosse fraudolenta.

Questa è anche la ragione per cui **è altamente consigliato aprire il wallet LN connesso a internet almeno 1 volta ogni 2 settimane. Appena connesso, se il nodo riconosce un'anomalia chiude il canale**. Ci sono altri modi più sofisticati per assicurarsi di non essere frodati, ad esempio configurando una **watchtower**, ovvero un server "torre di guardia" che monitora eventuali transazioni di chiusura. In generale comunque, i nodi LN a cui vi connetterete suggeriti da Electrum sono nodi pubblici che operano da molto tempo (anche anni) sulla rete, per cui è piuttosto improbabile che possano tentare di frodarvi. È bene comunque difendersi anche soltanto da eventuali errori tecnici da parte della nostra controparte, colme chiusure involontarie (ad esempio una migrazione errata del wallet), che anche se non sono deliberatamente una frode, all'atto pratico potrebbero portare allo stesso risultato. Insomma, non tenete canali aperti con quantità di bitcoin elevate se non ve ne fate nulla e non accedete al wallet per settimane.

Se vivete in bitcoin invece, è probabile che usiate abbastanza di frequente il vostro wallet, perciò non incorrete nel rischio di non monitorare a sufficienza il canale. In quel

caso quindi, è **bene tenere sui canali una quantità di bitcoin sufficiente a coprire tutte le vostre transazioni ordinarie in entrata e uscita, incluso lo stipendio**. Al termine di un mio precedente lungo articolo ho illustrato i calcoli per cui un ecosistema Bitcoin, **con singoli canali di dimensioni medio-grandi (volumi pari all'incirca ad uno stipendio mensile per canale)** può reggere circa 15 miliardi di transazioni annue in Bitcoin (Visa ne processa 55 miliardi), senza però considerare tutti i movimenti effettuati tramite custodian/banche, quindi non-trustless. Coi nuovi sviluppi su Bitcoin (in particolare **le multichannel factories**) senza aumentare le dimensioni dei blocchi e quindi della blockchain, **è possibile invece creare circa 2,5 miliardi di canali Lightning**: ipotizzando per ciascuno una frequenza di utilizzo di 40 transazioni al mese, arriviamo a **circa 1.200 miliardi di transazioni all'anno. Sufficienti per coprire il fabbisogno dell'intero pianeta.** Lightning Network è il cuore della scalabilità Bitcoin.

Grazie ai **multi-path payments**, che nel momento in cui scrivo non sono ancora implementati su Electrum LN, non dovrete necessariamente tenere su un singolo canale una capacità totale pari o superiore a uno stipendio sia in entrata che in uscita. Potrete invece suddivedere la liquidità in più canali aperti con nodi diversi, così da diminuire la vostra esposizione anche qualora non accedeste per molto tempo ai canali.

Ad ogni modo, sono certo che in futuro ci saranno molti servizi di watchtower a cui agganciarsi con un semplice click, probabilmente anche gratuiti (magari inclusi in "pacchetti" di gestione e ribilanciamento dei nodi, offerti da società specializzate), così da azzerare ogni rischio.

10. **Backup dei canali LN e migrazione del wallet su altro computer**

È possibile trasferire un wallet Lightning Network su un diverso computer, tuttavia **non è possibile utilizzare lo stesso wallet LN contemporaneamente su due computer o device diversi**. Questa è una differenza fondamentale rispetto ad un wallet utilizzato esclusivamente onchain, che può invece essere installato contemporaneamente su più dispositivi.

Se infatti portiamo il wallet Electrum su un secondo computer e qui effettuiamo una transazione LN, questa viene registrata solo su quest'ultimo pc, poiché le transazioni LN avvengono direttamente da wallet a wallet, da device a device. Se a quel punto aprissimo sul primo pc il vecchio wallet, questo riscontrerebbe un'anomalia, poiché il suo saldo non corrisponderebbe a quanto riportato dalla controparte del canale. In quel caso il nostro primo wallet penserà a un tentativo di frode e di conseguenza chiuderà in automatico il canale, trasferendo i fondi al proprio indirizzo onchain (ho fatto un test per verificarlo).

Una chiusura sbagliata del canale può portarvi a perdere i bitcoin, come vediamo in questo scenario ipotetico:

1. Alberto sul canale ha 3 btc, Bulbasaur 0 btc.
2. Alberto migra il proprio wallet, compreso il canale LN, sul secondo pc. Qui trasferisce 1btc a Bulbasaur. Il nuovo saldo è Alberto: 2, Bulbasaur 1
3. Alberto apre il vecchio wallet che nota un saldo anomalo (avendo in memoria ancora A:3, B:0), riscontrando che manca ad Alberto 1btc. Il wallet chiude il canale trasmettendo onchain un saldo pari a Alberto: 3, Bulbasaur: 0. Questo saldo però è sbagliato!
4. Il wallet di Bulbasaur vede una chiusura fraudolenta del canale, perché B aveva legittimamente ricevuto 1btc da A nella transazione avvenuta col secondo wallet. B quindi applica una "breach remedy transaction" appropriandosi di tutti e 3 i bitcoin di A presenti nel canale. Alberto ha quindi perso tutti i fondi sul proprio canale.

Nonostante questo rischio, in cui si incorre se si migra un wallet senza prestare le dovute attenzioni, è comprensibile che non si voglia fare affidamento a un unico PC per i propri bitcoin, per via dei rischi di "hardware failure", specialmente se il valore sui vostri canali è elevato. Le casistiche possono essere tante: furti, si brucia la memoria del pc, un terremoto vi distrugge casa, avviene l'ecatombe nucleare. In tutti questi casi, i vostri bitcoin dovrebbero rimanere saldamente al sicuro. Quindi un backup del wallet è fondamentale.

Ci sono due vie: **l'export dell'intero wallet** (**onchain + i canali lightning** che rimarranno **attivi** anche sul secondo pc) oppure un **backup** che permette di **recuperare il proprio saldo sul canale, ma non l'operatività del canale, che viene chiuso.**

Migrare il wallet Electrum LN su altro dispositivo

Vediamo anzitutto l'export dell'intero wallet, con migrazione su nuovo PC con backup dell'intero database dei canali. Fate molta attenzione a procedere correttamente, poiché una migrazione sbagliata può portare alla chiusura dei vostri canali LN, eventualmente anche con una perdita del vostro saldo sul canale.

I passaggi sono molto semplici, ma nei seguenti 6 punti della guida è bene non confondersi fra PC1, che è quello in cui è presente il wallet, e PC2, che è il computer su cui volete trasferire il wallet, rimuovendolo dal PC1.

- Sul **PC1** Accedete alla cartella "wallets" che contiene il file con estensione ".dat" e il nome che avete attribuito al vostro wallet. Nel mio caso è "wallet_8".
    - **Su Windows:** per raggiungere questa cartella andate al path: **\Users*TuoUserName*\AppData\Roaming\Electrum** Oppure, per trovare la cartella velocemente, cliccate sul pulsante windows per aprire la

ricerca di windows e digitate: **%APPDATA%\Electrum**
    - **Su Mac:** Aprite il Finder -> Go to folder (shift+cmd+G) e digitate ~/.electrum
    - **Su Linux:** Home Folder -> Go to Location e digitate ~/.electrum

- Copiate il file del wallet (nel mio caso “wallet_8”, nel vostro caso avrà il nome che gli avete attribuito in fase di creazione) e portatelo su una chiavetta USB o un qualsiasi altro supporto sicuro per trasferirlo sul **PC2**. Potreste anche trasferirvelo via internet, ma soltanto se crittato, perché chiunque riuscisse ad appropriarsi di quel file potrebbe sottrarvi tutti i bitcoin.
- Sul **PC1** Chiudete l’applicazione Electrum, spegnete il computer o sconnettetelo dalla rete. Assicuratevi di non aprire più Electrum sul **PC1**, almeno finché non avete eseguito e terminato il punto 6.
- Spostatevi sul **PC2**, quello su cui volete migrare il wallet, installate qui Electrum e aprite la cartella wallets, quindi trascinatevi all’interno il file (“wallet_8”) copiato dal PC1
- Aprite l’applicazione Electrum sul **PC2**, connesso alla rete, e controllate che il vostro saldo appia sia onchain che offchain. Ora che vi siete assicurati che la migrazione del wallet è andata a buon fine, potete procedere col punto 6.
- Tornate al **PC1** e, senza aprire Electrum, cancellate dalla cartella wallets il file (“wallet_8”) che avevate esportato. In questo modo **evitate di aprire per errore il vechio wallet Electrum sul PC1**, evitando chiusure forzate del canale. Una volta cancellato il wallet che avete migrato, potete continuare ad usare tanquillamente Electrum anche sul PC1, ma soltanto per wallet LN diversi da quello che avete ora su **PC2**.

Questo tipo di migrazione dei canali è possibile poiché non è l’IP, ma la public key il campo chiave su cui si basa

l’associazione fra i nodi LN. Perciò, nel momento in cui avrete migrato i canali sul wallet del PC2, questo invierà un messaggio di “node_announcement” comunicando il nuovo IP alla controparte.

Backup dei fondi di Electrum tramite interfaccia dell’applicazione:

Questo tipo di backup è detto in gergo “Static Channel Backup” https://wiki.ion.radar.tech/tutorials/troubleshooting/static-channel-backups e per ogni canale che abbiamo può essere fatto una sola volta, appena abbiamo aperto il canale. Importando il backup su un nuovo wallet permette di recuperare i propri fondi su LN **tramite la chiusura dei canali**. Prerequisito del backup è, anzitutto, il fatto di conservare il seed del proprio wallet. **Il seed** permette di ripristinare il proprio saldo onchain su qualsiasi dispositivo (anche sull’app Electrum per android), ma **non è sufficiente a ripristinare anche il saldo che abbiamo caricato sul canale LN**. Oltre al seed quindi, dobbiamo anche salvarci la stringa di testo che rappresenta il **backup del canale LN**. Se abbiamo **più canali** aperti, dovremo fare manualmente il **backup di tutti**.

Immaginiamo di aver bruciato o perso l’hard disk del vecchio computer dove era installato il wallet Electrum. Per fortuna abbiamo conservato sia il seed che un backup del canale. Ora abbiamo un pc nuovo e, come prima cosa, installiamo Electrum e importiamo il il seed (nella creazione del wallet selezionate “I already have a seed”/ possiedo già un seed). Fatto ciò, dovremo importare il canale LN. Come già detto, l’operazione non ristabilirà il canale attivo, come nel caso della migrazione del wallet tramite copincolla del file “ .dat” illustrata al punto precedente della guida, bensì innescherà la chiusura del canale, così che il saldo su Lightning venga recuperato onchain.

All’atto pratico, da **File** selezionare **Salva backup** (oppure cliccate col destro sulla riga corrispondente al canale nella

finestra “Canali” ed esportate il canale). In entrambi i casi, vedremo una finestra di popup come la seguente:

È possibile salvare li canale in formato file, o anche soltanto salvarsi il QR code o il testo della string di backup. Il testo risulterà simile al seguente:

Qualora volessi utilizzare questo backup per importare il saldo LN **nel nuovo wallet** (che dovrà avere lo stesso seed del vecchio), apriamo la schermata “**Canali**”, quindi **clicchiamo sul destro nel grande spazio bianco vuoto del riquadro principale,** dove normalmente vengono mostrati i canali, e seleziono “**importare il backup del canale**”. Si aprirà un popup dove possiamo incollare l’intera stringa di backup:

Una volta importato il canale non è agibile (non abbiamo capacità in inbound né outbound). L’unica cosa che possiamo fare è riportare il saldo presente sul canale al nostro indirizzo onchain, tramite una chiusura forzata. Lo status del canale che vedremo sarà “RECOVERED”, termine con cui si intende che la connessione con la controparte del canale è stata ristabilita e il nostro saldo su LN sta per essere trasferito onchain.

A differenza del seed, **il backup può essere salvato in chiaro anche in una vostra repository online/cloud** (benché non sia proprio la pratica più elegante, ma è meglio esporlo un po’ troppo che perderlo), poiché è comunque necessario il seed per poter accedere a quei fondi. Il seed invece è bene custodirlo offline.

Se importate il canale su un nuovo wallet, ma state continuando a usare anche **il pc vecchio col suo wallet**, sappiate che **il canale verrà chiuso su entrambi i wallet**, poiché si tratta a tutti gli effetti di un wallet solo presente su due pc diversi.

Cosa potrebbe succedere se state importando su un nuovo wallet il backup di un canale che non è aggiornato all'ultima transazione? Tecnicamente, quando importiamo il backup sul nuovo wallet, questo proverà a riconnettersi ai nodi precedenti e verrà inviata alla controparte una richiesta di chiusura del canale, così che sia questa a procedere nella chiusura del canale, anziché noi. In questo modo, si evita di trasmettere erroneamente uno stato anteriore rispetto a quello attuale. La controparte non può inventarsi uno stato che non è mai esistito (il vostro wallet lo riconoscerebbe come non valido), tuttavia potrebbe mentirvi trasmettendo uno stato antecedente, con un saldo a voi più sfavorevole. Si tratterebbe però di un tentativo di frode molto rischioso, perché la controparte non può sapere se avete veramente perso lo stato precedente del canale oppure se state solo fingendo di averlo perso. Se non l'avete perso davvero e provano a frodarvi, il vostro wallet potrà inviare alla rete una breach remedy transaction che vi farà guadagnare tutti i bitcoin all'interno del canale, azzerando il saldo del truffatore.

In poche parole, se perdete l'accesso al vostro wallet e avete soltanto un backup statico del canale **che non è aggiornato all'ultima transazione fatta**, non sarete sicuri al 100% di essere a prova di frode, ma avete ottime probabilità che la vostra controparte non tenti di frodarvi per due motivi:

- Probabilmente si tratterà di un nodo importante che ha una certa reputazione da mantenere
- Rischia di perdere tutti i fondi che ha sul canale, poiché non può sapere se realmente possedete o meno l'ultimo stato aggiornato. Questo meccanismo di "game theory" è detto in gergo "data loss protection"

C – Gestione del seed e chiavi private

Un bitcoiner esperto dovrebbe poter essere in grado di usare software wallet diversi spostando i propri fondi su qualsiasi wallet. Per poterlo fare, è bene sapere alcune nozioni fondamentali riguardanti il seed e le chiavi private. Le impariamo insieme utilizzando il tool di Iancoleman, un pokemon leggendario molto potente.

Anziché far generare al wallet Electrum il seed come descritto nella primissima parte di questa guida, potremmo usare questo metodo alternativo (più sofisticato e personalizzabile) di creazione del seed, dopodiché importare il seed o la master private key su Electrum.

Creiamo quindi il seed o "frase mnemonica" che sta alla base del wallet. Per farlo, aprite il **generatore di seed BIP39** (è un tool web open source). Potete scaricarlo qui (link diretto al download), o aprire la pagina web dal sito iancoleman.io/bip39 .

Per una maggiore sicurezza, se non volete usare il tool online, potete scaricare la pagina in html (cliccate col destro -> salva con nome) e aprire il file in browser quando siete disconnessi da internet, o addirittura da un pc che non è mai stato connesso a internet.

Una volta aperta la pagina, selezionate "12 words" e generate il vostro seed cliccando su "Generate". Apparirà quindi la vostra mnemonica nel campo nominato "BIP39 Mnemonic". Quella frase è il vostro wallet, abbiatene cura.

È a vostra discrezione come salvarla. Potete memorizzarla (brain wallet) oppure scriverla su un foglio (paper wallet) o inciderla da qualche parte. Potete scriverne solo una parte e ricordarvi il resto, oppure scrivere metà in un luogo e metà altrove. Se avete paura che qualcuno possa trovare la frase, è possibile scriverla modificando alcune parole o lettere o invertirle di posto, a patto che poi vi ricordiate quella originale. Sono tutti metodi che, qualora qualcuno riuscisse a fare breccia in casa vostra o nel vostro computer, vi possono dare il tempo di trasferire i fondi altrove, prima che lo faccia il "ladro".

In qualunque modo decidiate di conservare il seed, ricordate sempre che il numero di coloro che perde i propri bitcoin perché messi "troppo in sicurezza" e non più accessibili, è molto più grande rispetto al numero di quanti vengono effettivamente derubati. Insomma, non complicatevi troppo la vita e, soprattutto, se iniziate ad avere un discreto gruzzolo, pensate anche a come i vostri eredi possano reuperarlo anche senza il vostro aiuto diretto (non si sa mai).

Come ricevere bitcoin sul proprio paper/brain wallet? Nel tool di iancoleman, scorrete nella pagina verso il basso, fino a "Derivation Path", quindi **selezionate BIP84 per generare indirizzi e chiavi private SegWit bech32 (quelli che iniziano con "bc" consigliati in questa guida, perché più efficienti). Se invece voleste creare degli indirizzi non-nativi SegWit (che iniziano col "3"), dovrete selezioare BIP49**.. Si sconsiglia di non usare BIP32 o BIP44, perché si tratta dei vecchi indirizzi legacy (quelli che iniziano con "1") e i rispettivi multisignature (per wallet multi-account).

Evidenziata in figura è l'account **Extended Private Key**, che sarà la vostra "**master key**" ovvero il seed "declinato" nel derivation path BIP84. Più sotto, sono mostrati gli indirizzi

derivati da quella master key. Potete ricevere bitcoin a uno qualsiasi di quegli indirizzi. Potrete copiare il primo della lista e utilizzarlo come vostro indirizzo primario e mostrarlo a chiunque per ricevere pagamenti. L'importante è non mostrare a nessuno il seed, né la private key corrispondente a ciascun indirizzo.

Se importate la master key su Electrum (in italiano "**Usa una chiave principale**"), noterete che gli stessi indirizzi che avevate ottenuto su Iancoleman sono quelli mostrati da Electrum.

Alternativamente, potete importare il seed, il risultato finale sarà identico (ricordate di **flaggare il campo BIP39** quando inserite il seed):

Sull'applicazione mobile consiglio di importare direttamente la **master key**, pociché non è possibile impostare i vari derivation path come da desktop.

Dal tool di Iancoleman, quando generate seed e chiavi private, potete anche scegliere di encrittare le vostre chiavi con BIP38.

Per importare una chiave privata BIP38 su un qualsiasi wallet è necessario prima de-crittarla utilizzando la passhprase, qui è spiegato come fare.

Se volete monitorare quanti soldi sono stati inviati ai vostri indirizzi anche senza utilizzare Electrum, potete incollare l'indirizzo in un qualsiasi blockexplorer come blockchain.info, quindi cliccare su "Search"

Da qui è possibile vedere quanti btc sono su quell'indirizzo e anche il QR code, che si può usare per ricevere pagamenti come alternativa all'invio della stringa di testo.

È possibile monitorare uno o più indirizzi anche su Electrum, creando un watch only wallet. In quel caso, quando installate Electrum create un nuovo wallet, selezionate "Importa gli indirizzi Bitcoin o le chiavi private/Import bitcoin addressess or private keys", quindi incollate l'indirizzo all'interno:

Ogni volta che aprirete il wallet Electrum watch only potrete quindi controllare quanti soldi avete ricevuto. Un wallet di questo tipo può essere comodo per esempio da tenere su un device secondario, o sullo smartphone che abbiamo sempre con noi per controllare il nostro saldo. Se però volete anche spendere i vostri soldi, è necessario creare un wallet vero e proprio con tutte le sue funzionalità in invio e ricezione. Dovrete quindi importare il seed o la master key, non solo l'indirizzo.

D – Portafogli multifirma

I portafogli multifirma su Electrum non sono compatibili con Lightning Network, perciò è possibile fare solo tradizionali trasferimenti onchain. Il multifirma può essere come un tradizionale conto "cointestato" fra marito e moglie, dove serve l'autorizzazione di entrambi per effettuare un pagamento (transazione onchain in uscita). In realtà, il "conto

cointestato” sarebbe semplicemente un “2 firme su 2”, dove sono richieste le firme di due persone (marito e moglie) su due totali, ma è possibile configurare un portafoglio che chiede un numero a piacere di n firme su m totali (con m minore di 15).

Nel caso d’esempio, creiamo un portafoglio con 2 firme richieste su 3 possibili, e noi deteniamo una firma.

Dopo averci mostrato il seed, Electrum ci mostra la nostra **master public key**

Dovremo condividere questa chiave con gli altri 2 firmatari che eseguiranno dal principio la stessa nostra operazione (creazione nuovo portafoglio multifirma, selezionando 3 cofirmatari con 2 firme richieste).

Nello step successivo, dovremo inserire le master public key che ci vengono passate dai cofirmatari (gli altri due faranno lo stesso con la nostra):

APPENDICE: Lightning Network da mobile, il modello Breez

Breez è un wallet Lightning Network per mobile incredibilmente user friendly e innovativo. Appena installata l’applicazione sul nostro smartphone (iOS o Android), possiamo creare un invoice senza aspettare di avere un canale aperto. L’utente non dovrà mai preoccuparsi di aprire canali o attendere, farà tutto Breez automaticamente lontano dai nostri occhi.

Nel momento in cui creiamo un invoice per ricevere un pagamento, quello che farà Breez sarà creare istantaneamente un canale con la quantità necessaria a ricevere il pagamento, più 100.000 satoshi di ulteriore capacità (ad oggi 100k s sono circa 15€). Ovviamente, un canale non può avere conferma istantanea su blockchain, quindi nel momento in cui l'utente ci pagherà dovremo fidarci che Breez non trattenga il pagamento. Tuttavia, la fiducia verso Breez sarà necessaria solo fintanto che il canale non è confermato. Se dopo 10 minuti la transazione di apertura del canale è inserita dai miner in blockchain, tutte le transazioni che faremo saranno trustless come in qualsiasi nodo Lightning Network indipendente da parti terze.

Tecnicamente, per permettere un flusso automatico di questo tipo, il processo è il seguente:

- Alberto sul proprio wallet mobile Breez (che chiamiamo **nodo A**) vuole ricevere un pagamento dal wallet di Bulbasaur, che chiamiamo **nodo B**
- La società Breez (**nodo S**) crea un canale verso **A** con capacità pari all'importo del pagamento richiesto a Bulbasaur, più 100 mila sats.
- Un invoice viene inviato a **B** con l'importo da pagare a **S** (anziché al nostro wallet personale **A**). Bulbasaur paga.
- Contemporaneamente è creato un secondo invoice da **A** verso **S** in cui la stessa somma pagata da **B** viene trasferita da **S** ad **A**, meno una **commissione che tiene la società Breez per coprire l'apertura del canale** (e i costi del servizio), fissa allo **0,1%** dell'importo totale, ovvero 1 € su mille.

Poiché **questa somma è trasferita su un canale non ancora confermato** in blockchain, se dovesse esserci una frode da parte di Breez (o un errore tecnico) non potremo proteggerci trasferendo onchain i fondi. In poche parole, **finché il canale non è confermato, dovremo fidarci della società Breez**. Si tratta quindi di operare in un "**zero-confirmation channel**"

aperto con un’entità “di fiducia”, per alcuni minuti

Qualora in futuro dovessimo ricevere altri pagamenti che superano la capacità del canale, Breez aprirà altri canali aggiuntivi, sempre con lo stesso metodo istantaneo (zero-confirmation), per la capacità necessaria + 100 mila sats.

Breez usa **Multi-path payments (MPP),** non ancora implementato da Electrum, che permette di dividere un pagamento su più canali. Per esempio, se Bulbasaur ci ha spedito 30€, Breez avrà aperto un canale con noi da 45€ circa (30 + 100k s). Ipotizziamo che in seguito abbiamo speso completamente quei 30€, così da avere una capacità di ricezione (inbound) di 45€ totali sul canale. A quel punto, se Charmender dovesse inviarci 90€, 45 di questi fluirebbero al nostro wallet attraverso il canale che abbiamo già aperto (non dobbiamo quindi fidarci della società Breez per la ricezione di questi 45€, siccome il canale è già stato confermato), per gli altri 45 invece servirà aprire un nuovo canale. **Ogni qual volta che non c’è sufficiente capacità, la società Breez aprirà un canale aggiuntivo con noi**, in questo caso di circa 60 € (45€ + 100 mila sats, che sono circa 15€). Quando anche questo canale sarà confermato, avremo quindi 2 canali aperti con Breez, uno da 45€ e l’altro da 60€. Se dovessimo pagare Squirtle, potremo inviare il nostro pagamento sfruttando la capacità di invio di entrambi con un’unica transazione.

Se dovesse servire, Breez aprirà con noi uno o più canali per permetterci di ricevere fino a 4 milioni di satoshi, che ad oggi sono circa 700€. Tutto ciò in modo gratuito eccetto la commissione dello 0,1% sull’importo di ogni transazione di apertura canale (se quindi abbiamo aperto 1 solo canale, pagheremo questa commissione soltanto una volta). Una altro elemento interessantissimo è che **Breez non richiede di trattenere nel canale alcuna quantità di satoshi come riserva (channel reserve) per chiudere il canale.** Se ricevete 100, potete inviare 100! Magnifico no? **La chiusura del canale sarà quindi a carico della società Breez**, verosimilmente coperta

dalla fee di apertura del canale che abbiamo pagato in apertura.

Ho chiesto personalmente a Roy Sheinfeld, co-fondatore di Breez, **come possa essere sostenibile il loro modello**. La sua risposta è stata che i costi di apertura del canalea caricod i Breez sono minimizzati grazie al batching delle transazioni (aggregano le transazioni di apertura dei canali di più utenti), mentre l'importo dello 0,1% non è l'unica entrata, poiché il loro business model punta anche ad una vasta adozione dell'app da parte di molti utenti, attratti proprio per via dei vantaggi di questo wallet. Una parte di questi utenti potrebbero quindi anche sfruttare il marketplace presente in app, dove si possono acquistano bitcoin (già su LN) con carta di credito ("fiat on-ramp") e dove ovviamente Breez carica delle fee:

First, channels are not free. We charge 0.1% of the tx. There are several more factors to take into account: we have other ways of monetization other than routing fees (e.g. fiat on-ramp, marketplace, off-ramp) so your CLV is off, on-chain fees can be low with zero-conf and optimized with batching and the inbound liquidity provided to users is mainly coming from users. We're happy with the current numbers and already made some adjustments as business models are constantly evolving. I can tell you from my experience with other SaaS businesses, it's not so different than any other SaaS startup.

Tanto di cappello a questi ragazzi, che non solo sono tecnicamente molto bravi, ma sembra proprio che abbiano un'ottima vision. Non c'è dubbio che stiano seriamente innovando nel mondo di Lightning Network, sempre più verso un'adozione di massa.

Ricordo che il codice di Breez è open source e potete fare review del loro codice alla repository pubblica: https://github.com/breez/breezmobile

Qui alcune fonti sul funzionamento del loro wallet: https://medium.com/breez-technology/the-breez-release-candidate-getting-lightning-ready-for-the-global-takeover-b5d1f9756229

Se volete ringraziare per lo sbatti immenso di aver fatto la guida, rendetemi ricco:

bc1q46zj4ww04hfz2jegympwfkd09wxe3nptchegk6

[1] Nel corso del 2015 viene concepita l'idea di Lightning Network, il cui white paper è pubblicato nel gennaio 2016. Il 14 Dicembre 2015 avviene il fork upgrade di Bitcoin "check lock time verify", che dà la possibilità di creare canali Lightning Network in modo sicuro. Il 4 Luglio 2016 viene introdotto con altro fork upgrade il "check sequence verify, che permette a Lightning Network di tenere i canali creati aperti a tempo indeterminato. Infine, il 24 Agosto 2017 è il momento di SegWit, l'ultimo degli upgrade che erano necessari per l'utilizzo di Lightning Network, con il fix al malleability bug.

[2] Perché mai in informatica e crittografia dovreste usare Alice e Bob per A e B, quando potete usare Alberto in versione Giovanni Mucciaccia e Bulbasaur?

[3] È chiamato "scambio sottomarino" perché il canale Lightning Network è considerato uno strato ("layer") superiore alla blockchain di Bitcoin, e il submarine swap avviene "al di sotto" del canale LN, coinvolgendo proprio la blockchain