Cos’è Bitcoin Gold? Chi lo ha voluto? Come guadagnare grazie al fork del 25 ottobre?

Il prezzo di Bitcoin si è impennato negli ultimi giorni, forse anche grazie alle aspettative per il fork di Bitcoin Gold (BTG) previsto il 25 ottobre. Infatti, dopo l’esperienza con Bitcoin Cash del primo agosto, gli utenti di Bitcoin hanno ormai imparato che un fork volto a generare una nuova moneta non è un pericolo, quanto piuttosto un’opportunità. Vediamo cos’è Bitcoin Gold e chi lo ha voluto, cosa comporta il fork e come fare per cogliere al meglio questa opportunità di guadagno.

Perché Bitcoin Gold?

Bitcoin Gold è molto simile al Bitcoin originale, con una differenza fondamentale: il cambio di POW (Proof of Work). In sostanza, viene cambiato l’algoritmo con cui si effettua il mining. Tramite il mining vengono creati bitcoin e vengono validate le transazioni degli utenti, inserendole nella blockchain. Questo processo richiede molta energia che viene spesa in potenza computazionale dei computer, nel calcolo della funzione crittografica SHA256. Per effettuare questa operazione, inizialmente venivano usate semplici CPU (processori di PC tradizionali), oggi invece si usano gli ASIC, apparecchi hardware specializzati che hanno come unico utilizzo il mining mediante SHA256. Il fatto che sia necessario un hardware specializzato, pena la totale inefficienza, rende il mining centralizzato nelle mani dei pochi che riescono a essere più competitivi (con miglior hardware e minore spesa energetica). Cambiando la POW invece,

il mining sarebbe accessibile a chiunque possieda delle comuni schede video, esattamente quelle che utilizzano i videogiocatori.

Possiamo quindi supporre che uno dei motivi "ideologici" per cui Bitcoin Gold è nato sia quello di avere un mining più decentralizzato. Si pensa che questo possa dare una sicurezza maggiore qualora delle entità molto potenti, come gli Stati nazionali, volessero prendere il controllo di Bitcoin, oppure qualora i miners stessi dovessero tentare manovre contrarie all'interesse del resto della rete.

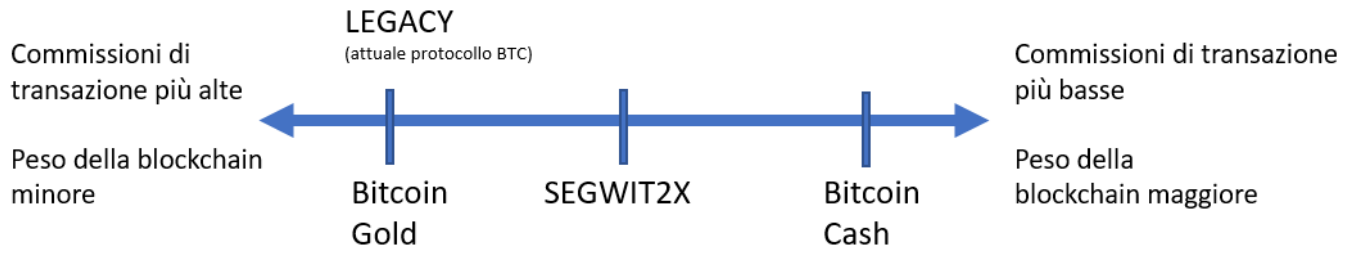
Per comprendere davvero Bitcoin Gold e quale sia la nicchia di utenti cui si rivolge è necessaria una visione complessiva dell'ecosistema Bitcoin, in particolare nel quadro dello "scaling debate". Infatti le tempistiche con cui Bitcoin Gold è stato promosso e ha suscitato interesse nei media e sui social, nonché il nome scelto, non sono affatto casuali. Per capirlo, dobbiamo ripassare un po' di storia.

Ad agosto è stato approvato SegWit, uno degli upgrade più attesi di Bitcoin, ma anche un upgrade a lungo dibattuto e controverso, che ha apportato modifiche importanti al protocollo. Alcuni utenti erano diffidenti nei confronti delle conseguenze di SegWit, specialmente considerando le implicazioni dell'upgrade sul futuro di Bitcoin. Per la "fazione" dei big blockers infatti, approvare SegWit significava dare primaria importanza alla scalabilità off-chain (tramite tecnologie come Lightning Network) evitando il più possibile uno scaling onchain, che ha il vantaggio di essere immediato, anche se appesantisce la blockchain. Perciò il primo di agosto, in anticipo sul deployment di SegWit, è nato Bitcoin Cash, con un protocollo più simile a quello originario di Bitcoin e pensato per evitare un'eccessiva congestione di transazioni sulla blockchain. Bitcoin Cash aumenta progressivamente la dimensione dei blocchi con l'obiettivo di poter sempre contenere tutte le transazioni fatte dalla rete. L'idea è che si mantengano sempre il più

possibile bassi i costi di transazione per gli utenti. Ho trattato altrove i pro e i contro relativi alla scelta di scalare onchain o offchain, e non mi ripeterò qui.

Ad ogni modo, il nome Bitcoin Cash (BCH) è pensato proprio perché l'obiettivo è quello di avere sempre un basso costo di transazione, proprio come il contante (Cash) che viene scambiato di mano in mano senza frizioni. Il nome richiama anche simbolicamente il White Paper di Satoshi Nakamoto: "Bitcoin: A Peer-to-Peer Electronic Cash System". Infatti, come spesso ricordato dai big blockers, Bitcoin Cash è più simile al protocollo originario rispetto all'attuale Bitcoin.

Oggi Bitcoin (BTC) vede costi di transazione maggiori, poiché gli utenti sono in numero sempre crescente e finché le tecnologie di scalabilità off-chain non saranno pronte, il blocco di dimensioni ridotte permette solo circa 3 transazioni al secondo. Se si vuole la propria transazione confermata in un blocco, è quindi necessario pagare di più, per scavalcare le altre transazioni in coda. Questo fa sì che attualmente Bitcoin sia poco adatto come moneta di scambio e più simile ad un asset finanziario, buono come riserva di valore o investimento (finché appunto il trend del prezzo è positivo). La proposta di novembre SegWit2x intende aumentare moderatamente la dimensione del blocco (blocksize a 2mb). Da qui, si comprende anche il significato della proposta Bitcoin Gold: se la "fazione" SegWit2x vincerà, il protocollo Bitcoin verrà modificato, muovendo verso destra (nel grafico sotto), quindi mostrando di non disdegnare anche soluzioni onchain più immediate, mentre si lavora allo sviluppo di tecnologie offchain.



I più strenui oppositori di un aumento dei blocchi potrebbero vedere in Bitcoin Gold una soluzione di ripiego, più vicina alle loro preferenze. Attualmente SegWit2x è sostenuto da circa il 90% dei miners, perciò spostarsi su moneta con un'altra POW (su cui gli attuali miners non hanno un vantaggio competitivo) significherebbe proprio volersi smarcare dalla loro influenza, in chiaro segno di rappresaglia.

Bitcoin Gold, proprio come l'oro, sarà più difficile da spostare e utilizzare come moneta di scambio rispetto al "contante" di Bitcoin Cash, perciò concettualmente sarà più simile a un asset, rappresentando un modo di conservare al sicuro i propri valori, come le riserve auree. Se la speranza dei supporter di Bitcoin Gold è che i migliori sviluppatori si spostino lì, forse il termine Gold può anche stare a indicare una tecnologia di pregio, rispetto alle alternative. In effetti, in un'ottica di lungo periodo tutti i bitcoiners, indipendentemente da quale "versione di bitcoin" preferiscano, sperano in un mondo in cui le cryptomonete siano in grado di sostituire completamente la moneta fiat. Perciò, anche chi rifiuta le attuali soluzioni onchain vede il Bitcoin come "asset" solo momentaneamente.

Se con il fork di novembre SegWit2x vincerà e la legacy chain morirà, è probabile che alcuni utenti perderanno interesse in Bitcoin Cash, vedendo la soluzione più mainstream SegWit2x comunque vicina alle loro preferenze. Al contrario Bitcoin Gold potrebbe attirare più attenzioni. Nell'ipotesi invece in cui SegWit2x fallisse, Bitcoin Cash potrebbe tornare alla ribalta, e Bitcoin Gold venire dimenticato.

L'ipotesi per cui BTG possa essere una soluzione di ripiego in caso di vittoria di SegWit2x è anche confermata dalle frasi di alcuni accaniti avversari di Bitcoin Cash e 2x, fra cui l'italiano Giacomo Zucco: "se veramente riescono a uccidere la Legacy chain, economia e dev si spostano su bgold che è fatto in modo onesto, lasciando bcash e B2X al loro destino di altcoin inutili" (vedi fonte)

Personalmente, dissento da Zucco su tutta la linea:

1. trovo assurdo che l'economia e gli sviluppatori si spostino su Bitcoin Gold

2. sono da sempre sostenitore dell'upgrade di Bitcoin chiamato SegWit2x e non credo affatto sia inutile, tanto meno che sarà un'altcoin

3. Soprattutto però, non si può proprio dire che Bitcoin Gold sia fatto in modo molto "onesto".

Chi c'è dietro Bitcoin Gold?

Il progetto di Bitcoin Gold è supportato principalmente da Jack Liao, CEO a capo dell'azienda di mining LightningASIC. Non solo è un miner, ma anche un produttore di hardware per il mining.

Abbiamo detto che il cambio di POW permetterà il mining mediante le più comuni GPU (schede video), tuttavia è probabile che LightningASIC produca anche degli ASIC specifici per il mining di Bitcoin Gold e che ovviamente questi siano più efficienti delle GPU.

Un altro dettaglio che fa insospettire è il "pre-mine". Ovvero, ci sarà un periodo in cui sarà possibile minare 8000 blocchi in pochissimo tempo. Questo consentirà agli sviluppatori di accaparrarsi fino a 100.000 Bitcoin Gold. Se BTG dovesse valere anche solo pochi euro, si può facilmente calcolare che ricchezza potrebbero ottenere Jack Liao e soci in poco tempo. Ma finché sarà il libero mercato a concedergliela, buon per loro….

È curioso però notare che gli sviluppatori avessero diramato un comunicato per dichiarare che non ci fosse pre-mine, eppure alla fine l'hanno lasciato nel codice, con un comportamento al limite della truffa. Ancora più bizzarro è il fatto che lo sviluppo sembra stato fatto in estremo ritardo e con poca

efficienza: 3 giorni ci sono voluti per cambiare una label testuale aggiungendo la scritta “Gold”. La chat pubblica per fare domande agli sviluppatori pare chiusa e tutte le informazioni sono vacanti e imprecise, persino su argomenti fondamentali come la data del fork e la replay protection. Ciononostante, una cosa sembra che l’abbiano pensata attentamente: come fare a non farsi soffiare i BTG pre-minati. Il meccanismo infatti prevederà un sistema di whitelisting hardcoded degli indirizzi di output della transazione coinbase del pre-mine, ovvero la transazione con cui il miner che scopre il blocco “vince” la ricompensa di n. bitcoin: le ricompense potranno essere inviate solo ad alcuni indirizzi prestabiliti, perciò se alcuni miners concorrenti sovrascrivessero i blocchi pre-minati, tentando di riscrivere la storia della blockchain BTG, dovranno comunque indirizzare le ricompense verso gli indirizzi degli sviluppatori. (nota: grazie a Gianluigi Crimi per i suggerimenti)

Come guadagnare grazie al fork del 25 ottobre?

Nonostante tutti i difetti, sembra che Bitcoin Gold abbia già un piccolo mercato. Su Bitstar i futures vengono scambiati per 0.04BTC, ovvero il 4% di un Bitcoin. Se mantenessero questo prezzo dopo il fork, col Bitcoin a circa 5000€, significa che per ogni Bitcoin avremo “vinto” circa 200€.

Forse queste stime sono troppo ottimistiche. Personalmente, penso che venderò i Bitcoin Gold sul primo exchange che li accetta, sempre che varranno qualcosa. Avevo fatto un errore a vendere immediatamente i Bitcoin Cash (vedi articolo http://www.albertodeluigi.com/2017/09/01/bitcoin-vs-bitcoin-cash/#3), ma in questo caso il fork è molto diverso rispetto a BCH; la base di utenti (e early adopter) a supporto è di gran lunga inferiore (forse inesistente) e non c’è una difficoltà di mining iniziale che impedisca agli utenti di depositare velocemente sugli exchange. Per queste ragioni, è difficile che si verifichino le stesse condizioni descritte

relativamente a BCH nell'articolo linkato.

Per quanto riguarda le piattaforme su sui scambiare Bitcoin Gold, al momento purtroppo, forse anche per via della natura semi-truffaldina di BTG, non ci sono molte informazioni. Lo stesso vale per i wallet a supporto. Perciò l'unica operazione da fare è conservare al sicuro le chiavi private relative ai propri Bitcoin e non muoverli fino al momento del fork. Dopo il fork, potremo muovere BTC, conservando sempre seed o le chiavi private in cui li tenevamo prima del fork. Non appena sarà uscito un wallet compatibile con BTG e utilizzabile anche da utenti senza particolari abilità informatiche, chiunqe potrà in qualsiasi momento decidere di riscattare i propri BTG. Iscrivetevi alla **newsletter** per rimanere informati.

Come unico segnale di trading, avviso che in questi giorni prima del fork, oltre alla salita del prezzo del Bitcoin, c'è stata una leggera flessione delle altcoin. È quindi possibile che alcuni utenti siano passati su Bitcoin vendendo le alt solo per ottenere i BTG "gratis". Questo potrebbe significare un rinculo del prezzo di BTC dopo il fork, se questi utenti intendono rientrare sulle alt. Il mio consiglio spassionato è comunque quello di non shortare mai Bitcoin.

Come sempre, per conservare i propri BTC, anche in vista del fork, consiglio di usare **Electrum**, per i seguenti motivi:

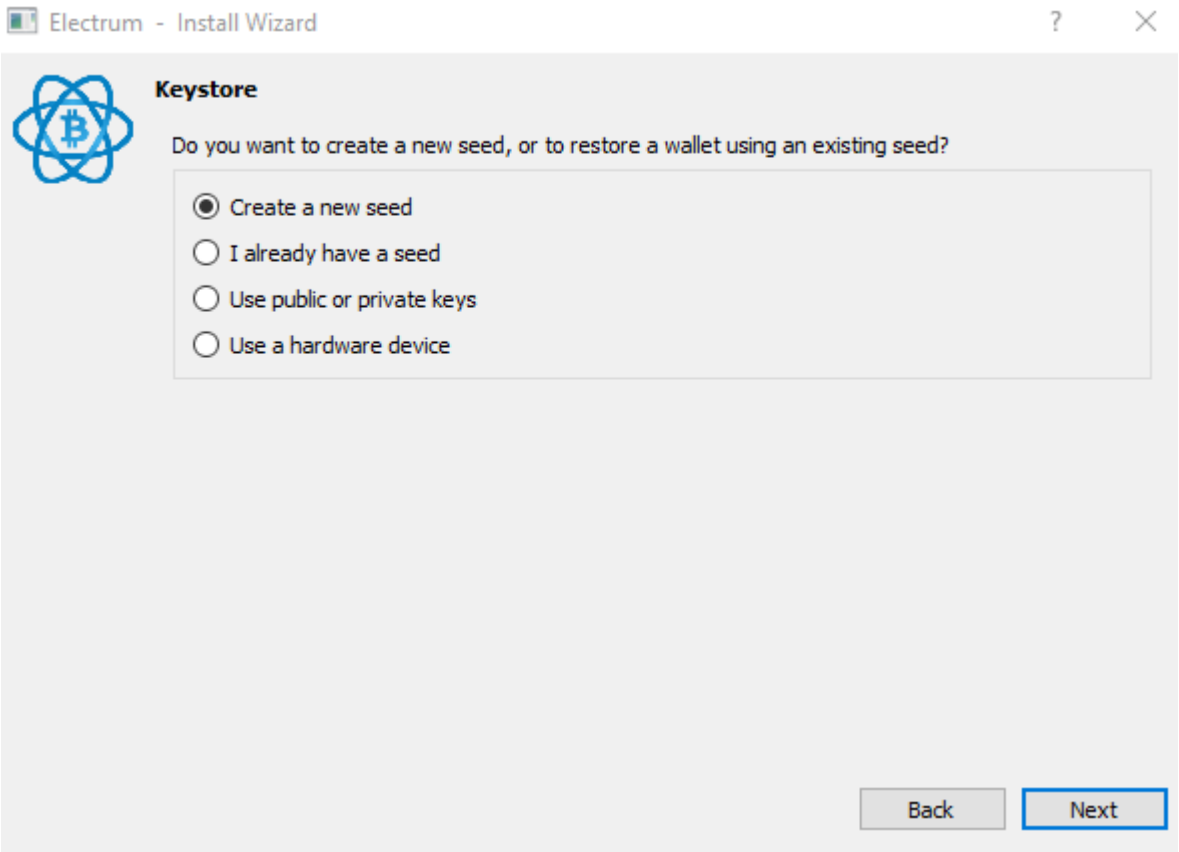
1) è sicuro e open source

2) si possono impostare fee dinamiche e vengono suggerite fee adatte al mercato,

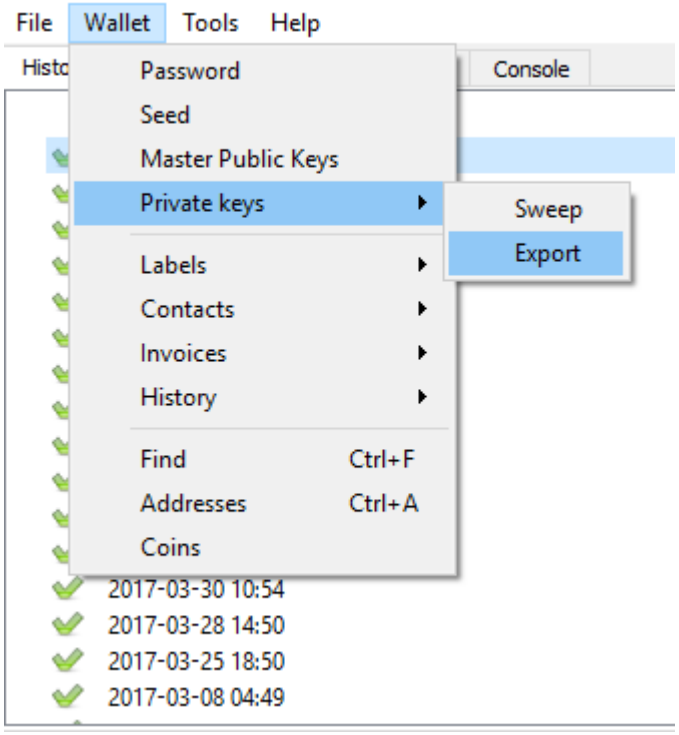
3) per velocizzare le transazioni ancora pending è disponibile il meccanismo RBP (replace by fee), ovvero aumentare la commissione per avere la transazione validata il prima possibile

4) permette di importare ed esportare con facilità sia seed che chiavi private.

Installato Electrum, create un nuovo seed e salvatelo.

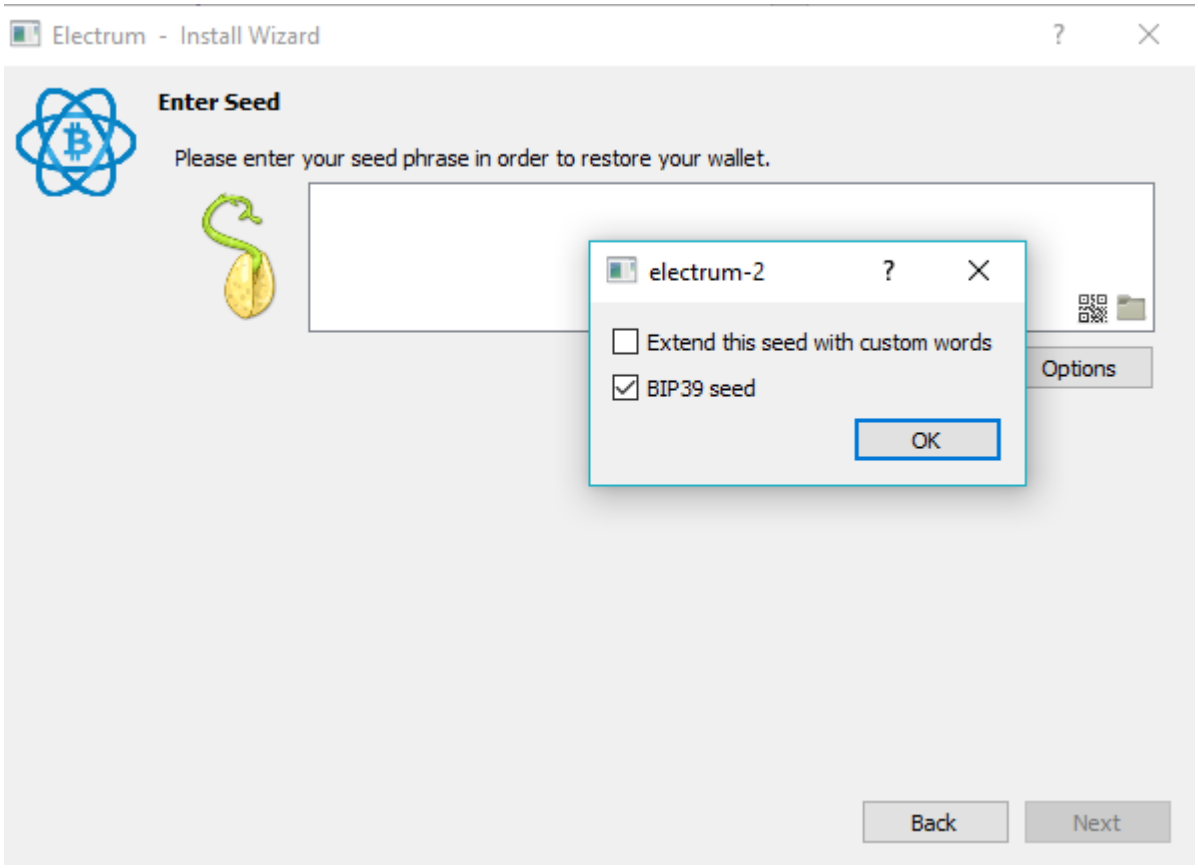


Quindi trasferite tutti i vostri fondi lì. A questo punto, basterebbe il seed, ma come scrupolo aggiuntivo, esportate le chiavi private da Electrum. Questo vi permetterà di importare sul wallet di Bitcoin Gold i coin con due diversi metodi, il che può essere conveniente, dato che potrebbero uscire release di wallets BTG che supportano solo alcune tipologie di import

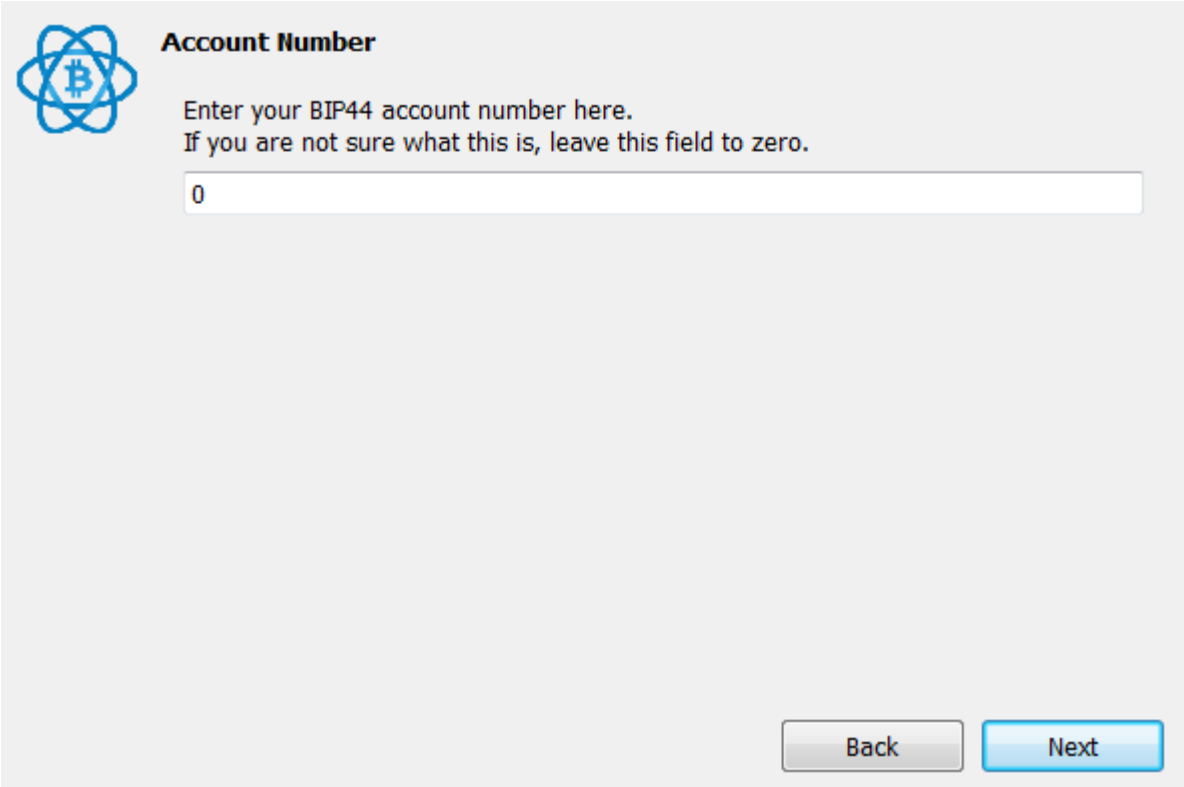


Attenzione perché se muovete i vostri Bitcoin dopo l'export delle chiavi private, ma prima del fork (ovvero della creazione del primo blocco di Bitcoin Gold) queste ultime risulteranno "vuote", ovvero non associate ad alcuna chiave pubblica con dei bitcoin/bitcoin gold.

Se avete già i BTC su un wallet con seed o che permette l'export di chiavi private, assicuratevi di essere in grado di riuscire a importare i coin anche su Electrum. In quel caso selezionate "I already have a seed" anziché generare un nuovo seed. Perché Electrum riconosca il seed, potrebbe essere necessario selezionare Options -> BIP39 seed (la maggior parte dei wallet usa passphrase mnemoniche di tipo BIP39).



Se il wallet da cui importate è un multi-account BIP44, dovrete ripetere la procedura importando un account per volta. Se per esempio avete 3 account, nel pop-up “Account number” selezionate prima 0, poi 1 e poi 2. In questo modo avrete importato tutti e 3 gli account.

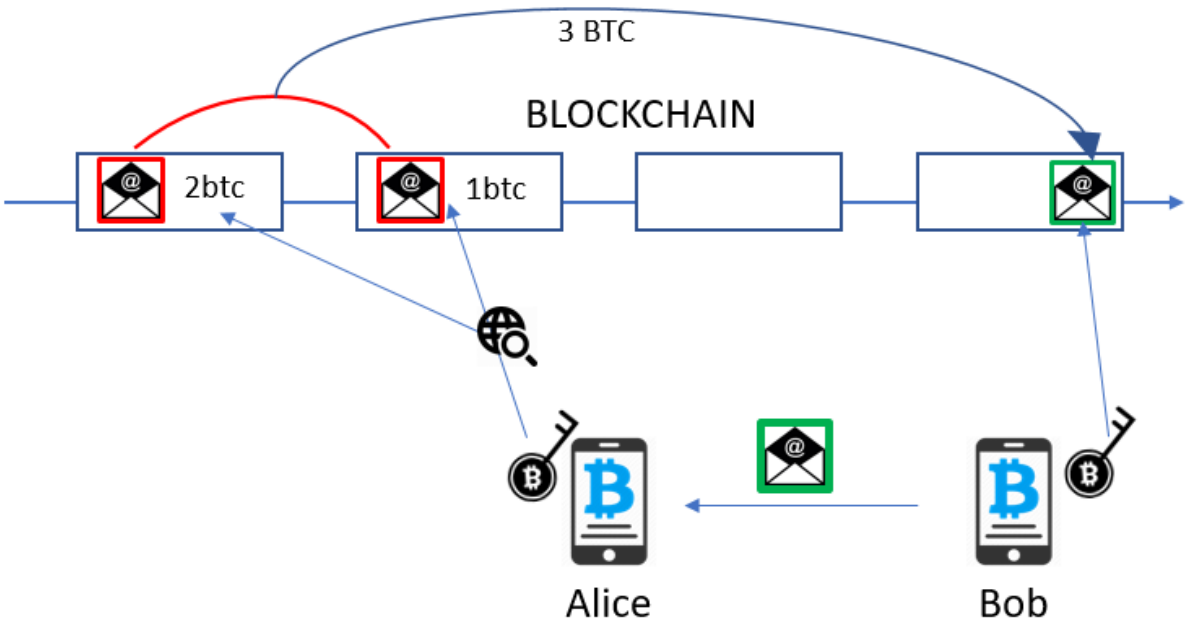


Come è possibile che i miei coin vengano duplicati (Bitcoin + Bitcoin Gold)?

Quando avviene un fork, la blockchain di Bitcoin prende due direzioni, una è la catena legacy, ovvero il Bitcoin originale, l'altra la nuova catena, che ha un protocollo di regole differenti. L'utente che al momento del fork aveva il controllo delle chiavi private dei propri Bitcoin, avrà un eguale ammontare anche di Bitcoin Gold.

Una breve premessa teorica è necessaria per capire questo fatto: la blockchain è fatta di blocchi che registrano le transazioni. Quando vogliamo ricevere una transazione Bitcoin, il nostro client wallet produce una coppia di chiavi, quella pubblica e quella privata. Immaginiamo che Bob voglia vendere ad Alice una fiat Panda che costa 3 btc: il wallet di Bob in automatico genera una chiave privata e una chiave pubblica. Quest'ultima viene trasmessa in forma di indirizzo (riquadro verde) ad Alice, mentre il wallet di Bob conserva in segreto la chiave privata. Alice sa che deve pagare 3btc all'indirizzo che ha ricevuto da Bob, quindi il suo wallet scansiona la

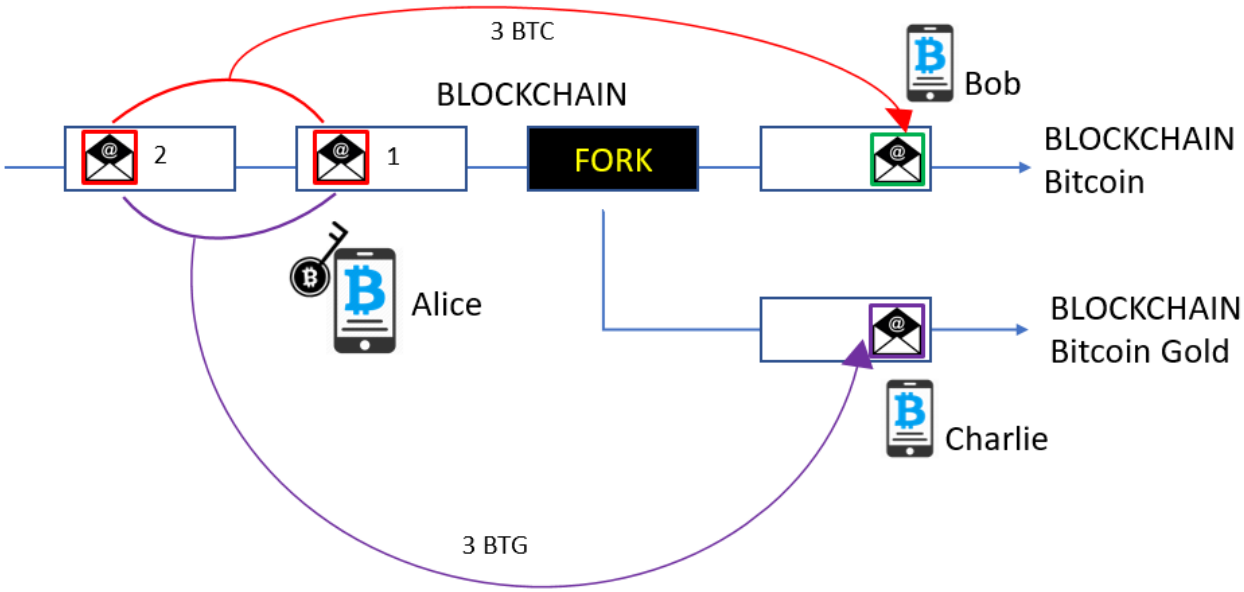
blockchain alla ricerca dei bitcoin da inviare. Un wallet Bitcoin non è altro che una repository di chiavi private, utilizzate per scansionare le chiavi pubbliche presenti sulla blockchain e visualizzare quindi quali di queste sono “sbloccabili” con la corrispondente chiave privata. In questo modo il wallet calcola quanti bitcoin registrati sulla blockchain l’utente è potenzialmente in grado di spostare, determinando quindi l’ammontare nel proprio “balance”, o “conto”. Nell’esempio, Alice con le sue chiavi private può spostare 3 bitcoin presenti in diverse chiavi pubbliche registrate sulla blockchain. Alice esegue quindi la transazione, firmando con le chiavi private e inviando a Bob. Dal momento in cui la transazione viene inserita dai miners nel blocco successivo della blockchain, sarà Bob a poter muovere quei bitcoin con la sua chiave privata, perché è l’unico a poter sbloccare i bitcoin trasferiti nella nuova chiave pubblica (riquadro verde).



Ora vediamo cosa succede in caso di Hard Fork con creazione di una seconda moneta. Il 25 ottobre verrà creato un blocco X con un protocollo diverso, che non sarà accettato dai clients e

miners del Bitcoin originale. Questo sarà il primo blocco di Bitcoin Gold. Se alcuni miners che accettano le nuove regole, e non quelle vecchie, proseguono spendendo la propria potenza di calcolo creando blocchi compatibili con il blocco X, contribuiscono a creare una nuova catena, la blockchain di Bitcoin Gold.

In questo modo esisteranno due catene che hanno una storia comune. Alice potrà trasferire 3btc a Bob, che ha un client Bitcoin tradizionale (catena legacy), ma Charlie, che invece ha un wallet client che supporta Bitcoin Gold, non vedrà come valido il blocco appena creato con la transazione di Alice, quindi non la riconoscerà come valida. Se la transazione non è valida, significa che Alice potrà inviare gli stessi 3 bitcoin nuovamente come input per una transazione verso Charlie e quest'ultimo accetterà i coin, che verranno registrati dai miners nella nuova catena Bitcoin Gold. Alice quindi a tutti gli effetti potrà vendere due volte i suoi coin.



Nei prossimi articoli: tutto quello che c'è da sapere sul fork di Novembre SegWit2x

Iscriviti alla **newsletter** per ricevere una notifica ad ogni

nuovo articolo!