Come ottenere Bitcoin Cash gratis in poche semplici mosse

In questo articolo vedremo come tutti i possessori di Bitcoin possono ottenere Bitcoin Cash gratuitamente entro il 1 agosto. La prima parte dell'articolo spiega cosa sono i bitcoin cash e perché sono "distribuiti" a qualsiasi possessore di Bitcoin. La seconda parte indica le operazioni pratiche da compiere per ottenerli.

Cos'è Bitcoin Cash (BCH)?

Bitcoin Cash è una nuova moneta creata con un hard fork di Bitcoin. La blockchain Bitcoin e quella Bitcoin Cash sono comuni fino alle ore 14.20 italiane (12.20 UTC). Ogni utente che possiede dei bitcoin entro le 14.20 del primo agosto è intitolato ad un eguale ammontare di bitcoin cash, a patto di eseguire semplici operazioni, più avanti descritte.

Qual è la ragion d'essere di Bitcoin Cash?

A fine agosto si attiverà l'upgrade a SegWit su Bitcoin, permettendo tecnologie di scalabilità offchain. Bitcoin Cash rifiuta SegWit e punta a scalare onchain, aumentando la dimensione dei blocchi e appesantendo così la blockchain. Secondo i promotori di questa visione, il progresso tecnologico garantirà uno sviluppo di hardware e banda sufficienti a gestire una blockchain molto più pesante di quella attuale, senza particolari rischi di sicurezza, mentre SegWit non sarebbe la scelta più sicura perché darebbe più potere ad aziende che forniranno intermediazione nel mercato offchain, accentrando quindi la rete nelle mani di intermediari. Bitcoin Cash si chiama proprio cash (contante) perché vuole rimanere una soluzione disintermediata. Il tema SegWit vs Big Blocks è stato analizzato in altri articoli sul

blog e non ci si dilungherà qui oltre.

È Bitcoin Cash il tanto temuto fork del 1 agosto?

No, il temuto fork del primo agosto era BIP148 UASF, ed è stato scongiurato grazie a BIP91, la prima parte dell'upgrade SegWit2x. Bitcoin Cash non è un pericolo, poiché è la semplice creazione di una nuova moneta, esattamente come se venisse lanciata sul mercato una diversa altcoin. L'UASF invece costituiva una minaccia perché sarebbe potuto risultare in un chain split, dove vi sarebbe stata incertezza su quale delle due catene fosse il vero Bitcoin, con enormi disservizi e perdite per utenti, aziende e miners.

Chi sostiene Bitcoin Cash?

Bitcoin Cash era la soluzione di ripiego proposta dall'azienda Bitmain, produttrice di mining hardware, qualora SegWit2x fosse fallito e il primo agosto UASF avesse dato via al fork. I miners contrari a UASF, creando una nuova moneta grazie a questo hard fork, avrebbero potuto proteggersi dal reorg di UASF, la cui catena, se avesse ottenuto la maggioranza di potenza di calcolo, avrebbe inghiottito la vecchia catena legacy. Oggi, SegWit2x è stato un successo quasi plebiscitario, perciò nessun miner, nemmeno Bitmain, ufficialmente sostiene Bitcoin Cash. Non è difficile prevedere che comunque qualcuno dedichi una piccola parte di potenza di calcolo, anche a soli fini sperimentali, per la creazione della catena BCH.

Come avviene tecnicamente il fork?

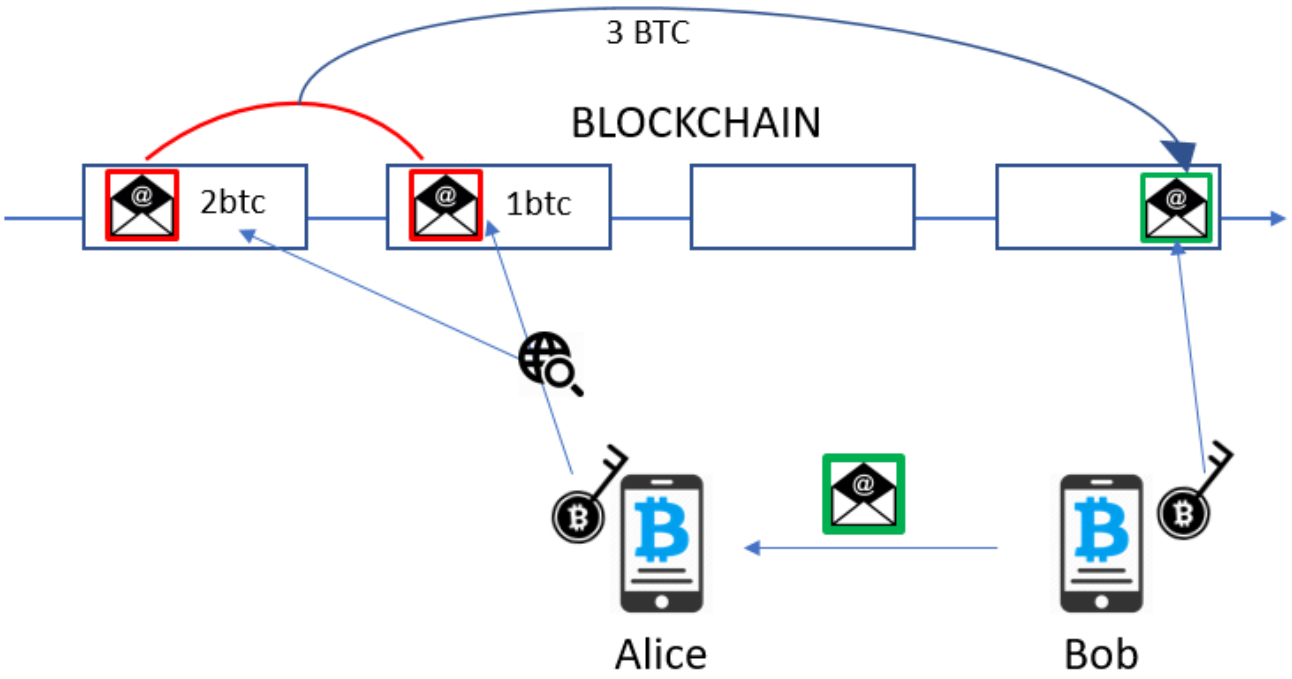
Per dare via al fork, la catena Bitcoin Cash accetterà soltanto un blocco più grande di 1mb dopo le 14.20 del 1 agosto. Il fork avverrà esattamente al primo blocco creato sulla catena Bitcoin dopo le 14.20, poiché quel blocco, seguendo il protocollo originario Bitcoin della catena legacy, avrà una dimensione pari o inferiore a 1mb, venendo quindi rifiutato dai client e miners Bitcoin Cash. Da quel momento, i

miners dedicati a Bitcoin Cash lavoreranno per creare il primo blocco BCH, di dimensione necessariamente maggiore a 1mb. Dato che la difficoltà di mining sulla catena BCH è inizialmente pari a quella del Bitcoin, ma la potenza di calcolo che lavorerà sulla catena sarà molto inferiore, potrebbero volerci ore perché venga creato il primo blocco BCH. Per questa ragione le transazioni BCH saranno inizialmente lentissime: senza un blocco che le scriva nel registro blockchain, nessuna transazione sarà mai confermata. Col tempo, la difficoltà di mining diminuirà fino a normalizzare la situazione, ma a patto che la catena BCH rimanga in vita e sostenuta da qualche miner.

Come è possibile che ogni utente "duplichi" i propri bitcoin in Bitcoin e Bitcoin Cash?

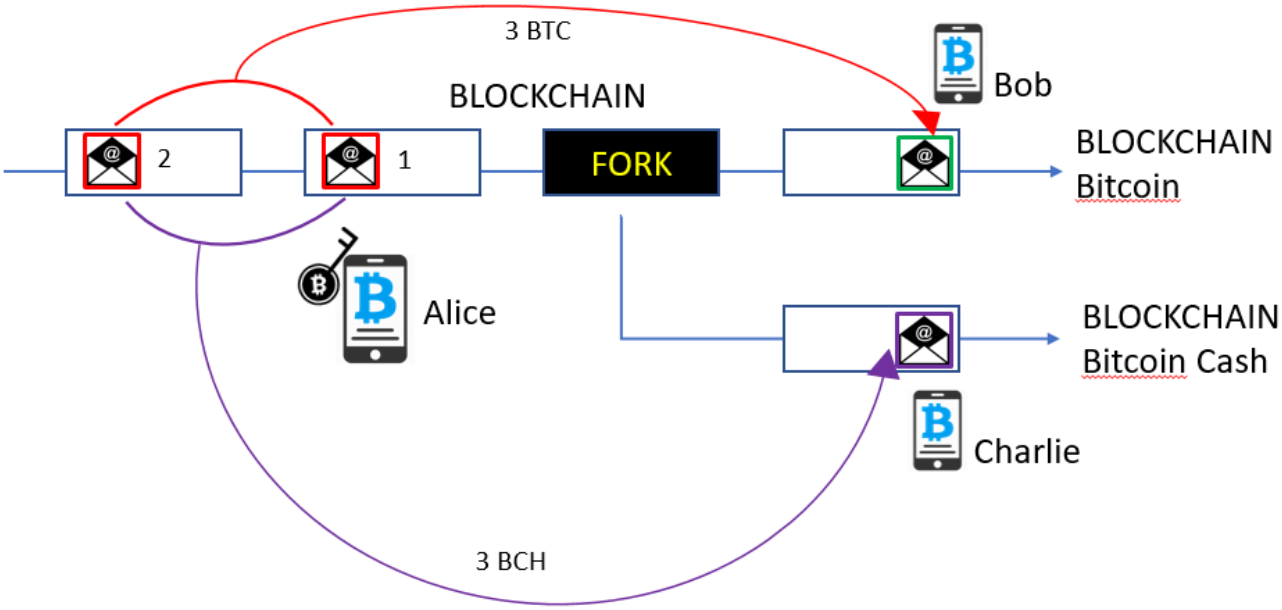
Una breve e semplice premessa teorica è necessaria per capire questo fatto: la blockchain è fatta di blocchi che registrano le transazioni. Quando vogliamo ricevere una transazione Bitcoin, il nostro client wallet produce una coppia di chiavi, quella pubblica e quella privata. Immaginiamo che Bob voglia 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, 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. Dalle ore 14.20 (fuso italiano) il primo blocco creato sulla catena legacy non sarà accettato dai clients e miners Bitcoin Cash. Alice potrà quindi trasferire i 3btc a Bob, che ha un client Bitcoin tradizionale (catena legacy), ma Charlie, che invece ha un client BitcoinABC, o Electroncash, o altri client che supportano Bitcoin Cash, non vedrà come valido il blocco appena creato, quindi non riconoscerà la transazione fatta da Alice 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 Cash. Alice

quindi a tutti gli effetti potrà vendere due volte i suoi coin.



Come conservare sia Bitcoin che Bitcoin Cash?

SOLUZIONE 1: L'EXCHANGE

Alcuni exchange garantiscono il supporto di Bitcoin Cash. Ciò significa che automaticamente accrediteranno all'utente una somma di BCH pari ai BTC che l'utente mantiene in deposito sull'exchange fino al momento del fork. Vi sono vari exchange elencati nella sezione apposita del sito https://www.bitcoincash.org/ che accreditano i BCH, ma ne consiglierei tuttavia uno soltanto: Kraken.com. Il motivo è che non solo Kraken è uno dei migliori exchange che accredita all'utente i BCH, ma ha espressamente dichiarato che permetterà di tradarli con EUR, USD e BTC.

PRO:

– Ci si affida a Kraken per la gestione e la "duplicazione" dei propri coin in BTC e BCH senza dover installare wallets ed esportare o importare alcuna chiave o seed

– Kraken permetterà non solo di conservare e trasferire i BCH, ma di venderli e comprarli sulla piattaforma in cambio di Bitcoin, Euro o Dollari. Il vantaggio fondamentale è che i BCH saranno già sulla piattaforma e pronti ad essere scambiati nei primissimi momenti successivi al fork. Questa situazione è ben diversa rispetto al caso in cui teniamo i BTC (e di conseguenza i BCH) su un wallet personale al momento del fork. Infatti per inviare i BCH ad un exchange e poi venderli impiegheremmo moltissimo tempo, poiché la convalida della transazione verso l'indirizzo dell'exchange sarebbe lentissima da parte dei miners. Come spiegato, la potenza di calcolo della catena BCH sarà molto inferiore a quella BTC e il primo blocco potrebbe essere creato solo dopo molte ore il fork.

CONTRO:

– Bisogna fidarsi di Kraken. Storicamente abbiamo visto che vari exchange sono stati hackerati o sono falliti (o forse hanno inscenato un fallimento) con conseguente perdita di denaro degli utenti

– Bisogna verificarsi al Tier 1 di Kraken per poter trasferire BTC sulla piattaforma: è cioè richiesto l'inserimento di Nome, Cognome, Data di nascita, Paese e Telefono. Fortunatamente per tradare e fare withdrawal di crypto è sufficiente il Tier 1, senza dover procedere a ulteriori verifiche o registrare un documento di identità.

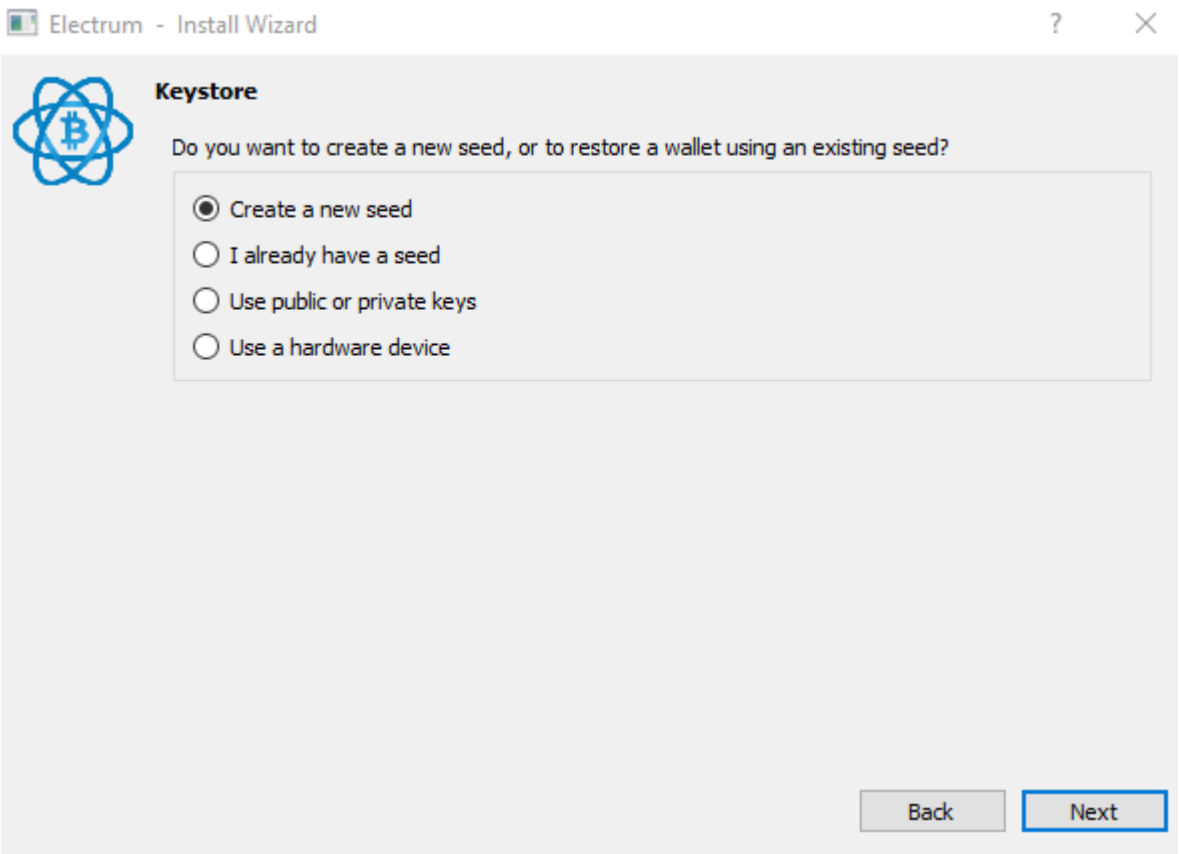
SOLUZIONE 2: IL WALLET CON CHIAVI PRIVATE

A) Inviare tutto su un nuovo portafoglio Electrum

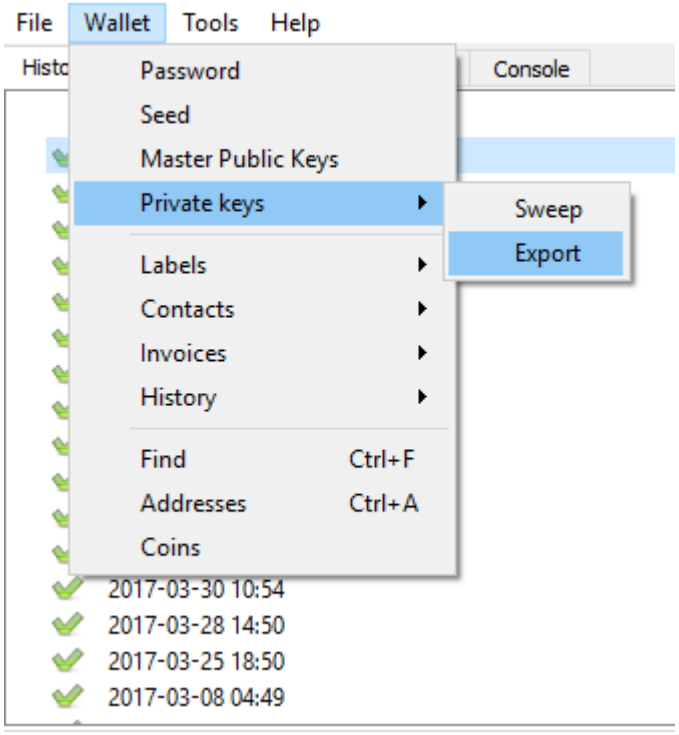
Se controlliamo le chiavi private o il seed (che non è altro che una passphrase che il wallet usa per generare a cascata tutte le chiavi private) relativi alle chiavi pubbliche su cui sono conservati i nostri bitcoin, allora siamo anche in grado di utilizzare queste chiavi/seed per ottenere i bitcoin cash.

Se detenete i fondi su un wallet come Coinbase che non dà in

mano all'utente il seed o la possibilità di esportare le chiavi private, i fondi vanno trasferiti su un nuovo wallet. Consiglio di usare Electrum https://electrum.org/#download perché 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 da Coinbase (o comunque il wallet che avevate in precedenza) e portateli su Electrum. Come scrupolo aggiuntivo, esportate le chiavi private da Electrum. Questo vi permetterà di importare sul wallet di Bitcoin Cash i coin con due diversi metodi, il che può essere conveniente, dato che potrebbero uscire release di wallets BCH che supportano solo alcune tipologie di import.



Attenzione perché se muovete i vostri Bitcoin dopo l'export delle chiavi private, queste ultime risulteranno "vuote", ovvero non associate ad alcuna chiave pubblica con dei bitcoin/bitcoin cash.

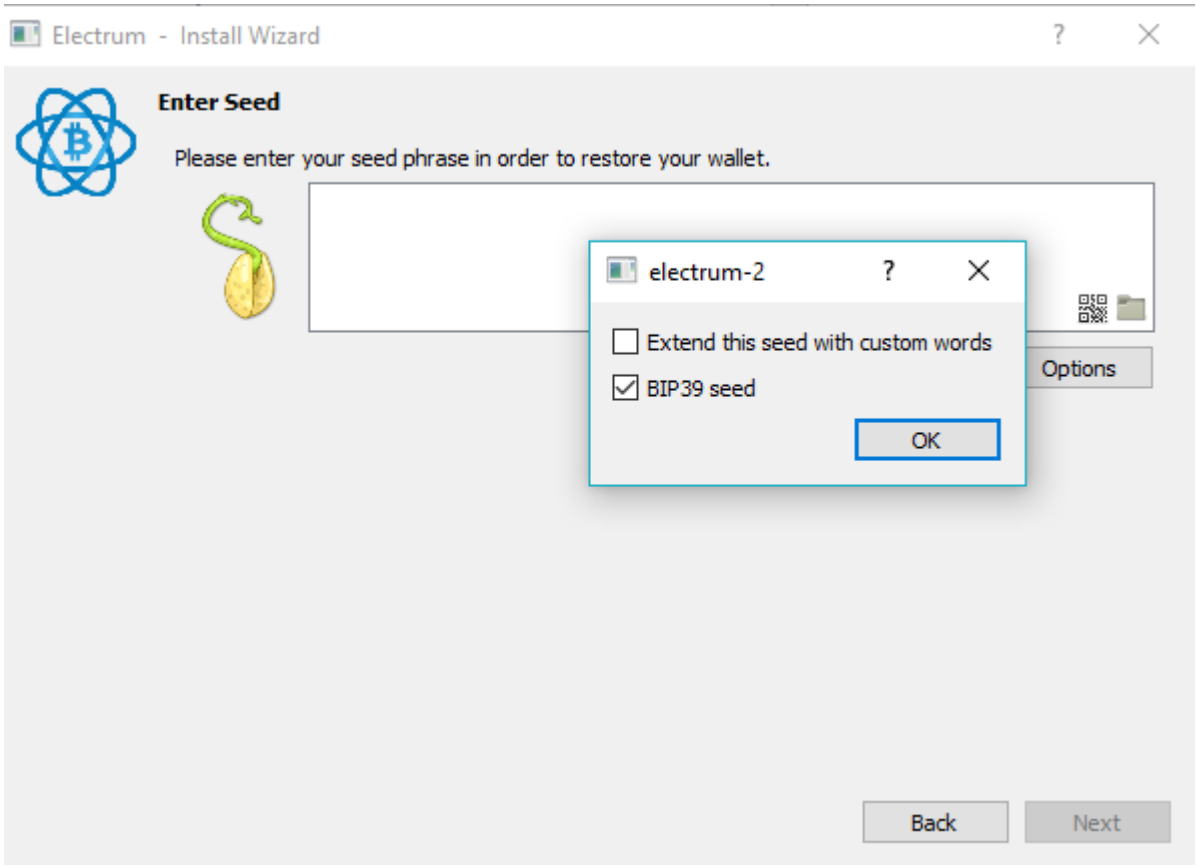
Sarà ovvio, ma è bene ricordare che una volta fatto l'export delle chiavi, non bisogna più muovere i bitcoin fino al fork, attendendo quindi almeno il primo blocco legacy dopo le 14.20, che dovrebbe avvenire all'incirca intorno alle 14.30. Al seguente link potete controllare l'avvento del fork, ovvero quando il numero "Current Height" (del blocco) sarà inferiore per Bitcoin ABC (Bitcoin Cash) rispetto alla catena legacy, anziché pari come in questo momento: https://www.btcforkmonitor.info/ Se il numero è inferiore, significa che sulla blockchain Bitcoin Cash ci sono meno blocchi validi, ovvero Bitcoin Cash sta rifiutando alcuni blocchi creati dalla legacy chain.

B) Importare il portafoglio su Electrum

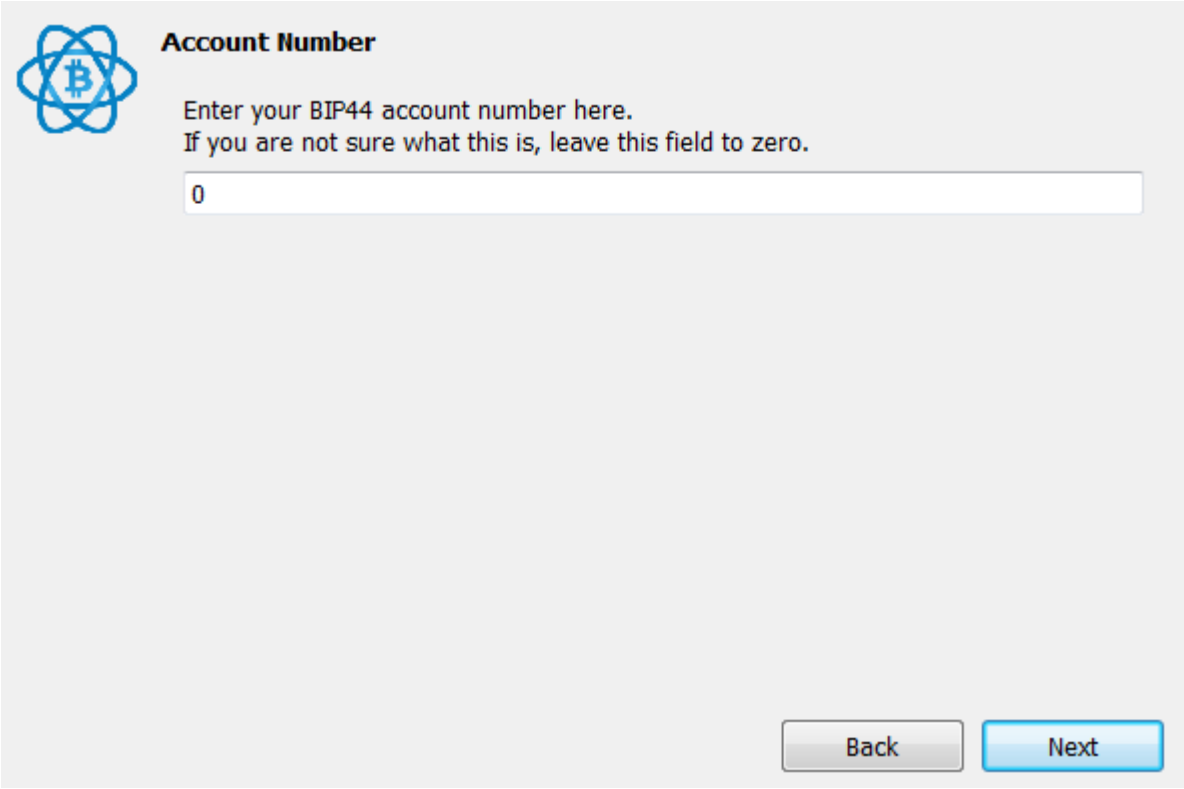
In alternativa al punto A), Se avete già i BTC su un wallet con seed o che permette l'export di chiavi private,

assicuratevi di essere in grado di riuscire a importare i coin anche su Electrum. Questo vi darà la sicurezza che dopo il fork sarete anche in grado di fare l'import su un wallet Bitcoin Cash come http://www.electroncash.org/

Quindi scaricate Electrum per Bitcoin e 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.



Ricordate che se avete problemi con l'import su Electrum e quindi avete dubbi che riuscirete a utilizzare il vostro seed o le vostre chiavi private dopo il fork, prima del fork potete effettuare una semplice transazione verso Electrum, pagando dei costi di commissione ai miners, ma almeno starete tranquilli che riuscirete a recuperare i Bitcoin Cash.

Infine: Importare il portafoglio su un client Bitcoin Cash

Dopo il fork, sarà disponibile al download Electroncash. È un fork di Electrum, perciò non dovreste avere alcun problema a importare il seed o le chiavi private, esattamente come fareste se fosse la versione Electrum per Bitcoin. Selezionate quindi "I already have a seed" oppure, se volete usare le chiavi private precedentemente esportate, "Use public or private keys". Quindi incollate all'interno le vostre chiavi o seed e il gioco è fatto, avrete un wallet coi vostri BCH.

Se non vi fidate del software Electroncash, prima di importare seed e chiavi private lì, assicuratevi di aver spostato i Bitcoin su un altro wallet, quindi sotto a un diverso seed e chiavi private (nota: ovviamente è un'operazione da fare solo

dopo il fork, o non avrete più i BCH!).

Potrebbero uscire dei wallet alternativi a Electroncash. Potrete provare anche lì l'import o l'export delle chiavi o seed. Infine, ovviamente si potrà anche usare il client ufficiale fullnode di Bitcoin Cash, ovvero BitcoinABC. Tuttavia questa scelta richiede il download dell'intera blockchain, ovvero circa 120gb. Non è possibile scaricare la blockchain in 3 giorni da qui al 1 agosto, perciò escludo sia un'opzione. Se già avete scaricato l'intera blockchain e fate girare un fullnode, si presume siate utenti esperti, quindi non avete bisogno di questa guida. Ad ogni modo, assicuratevi di copiare la blockchain in una directory differente rispetto alla vostra versione di Bitcoin Core o di btc1, dove andrete a installare BitcoinABC, per evitare che l'installazione sovrascriva il client Core.

Subito dopo il fork potrete spostare i vostri bitcoin dal wallet/chiavi private in cui erano conservati. Una volta importati i BCH sul relativo client, potrete scambiarli o inviarli su un exchange, se deciderete di venderli. Si ricordi soltanto che la rete Bitcoin Cash potrebbe essere molto lenta, specie i primi giorni, quindi anche se il trading dei relativi token su exchange avverrà alla stessa velocità di tutte le altre monete sull'exchange, depositi e withdrawal potrebbero impiegare ore (o giorni?).

Infine, non è detto che i Bitcoin Cash avranno alcun valore. Se lo avranno, forse sarà soltanto per i primi minuti o ore di trading, finché le vendite porteranno il prezzo a zero. Non è nemmeno detto che ci sia l'hard fork: qualora l'hashing power a sostegno della catena fosse irrisorio, anche i pochi miners potrebbero rinunciare e abbandonare la catena nei primissimi blocchi. Viceversa, BCH potrebbe stupirci ed avere molto più supporto di quanto previsto. Staremo a vedere!

momento, cliccando sul link presente in calce ad ogni mail ricevuta! Clicca qui: **SUBSCRIBE**