Bitcoin Foundation

Introduzione a Bitcoin

Comitato per l'Educazione della Fondazione Bitcoin

Che cos'è Bitcoin e perché dovrei preoccuparmi?

Quando la maggior parte della persone sentono parlare per la prima volta di Bitcoin, la prima domanda che si pongono è "Che cos'è?" Questa guida fornisce una risposta concisa a questa domanda e spiega alcuni dei termini che di solito si sentono in relazione a Bitcoin.

In termini concreti, Bitcoin può essere soltanto pensato come due cose: (1) un circuito di pagamento e (2) una valuta che viene utilizzato nel circuito di pagamento Bitcoin. Spesso ci riferiamo alla valuta come BTC, ad esempio "per favore mi paghi 3.1 BTC".

Ma perché il mondo ha necessità di un'altra moneta e di un altro circuito di pagamento? Per rispondere a questa domanda dobbiamo vedere come Bitcoin differisca da valute esistenti e come Bitcoin si differenzi dai circuiti di pagamento esistenti.

La **valuta bitcoin** è esclusivamente digitale. Non è emessa o garantita da un governo, un'organizzazione o un' azienda. Non ci saranno mai più di 21 milioni di bitcoin, e la disponibilità di moneta aumenta con un tasso predefinito e decrescente fino a raggiungere il suddetto limite. Tali caratteristiche sono quasi completamente antitetiche se paragonate a quelle delle valute locali. Ad esempio, il dollaro USA ha una forma fisica (le banconote da un dollaro), è emessa e garantita dalla banca centrale degli Stati Uniti, non vi è alcun limite al numero di dollari che potrà mai esistere e la velocità di generazione, anche detta "stampa", del dollaro è sconosciuta.

La **rete Bitcoin°° è una rete di computer peer-to -peer decentralizzata, in cui i computer possono scambiare informazioni tra di loro senza la mediazione di un server centrale. La rete Bitcoin è quindi neutra perché nessun computer centrale può vietare ad un altro computer di essere parte della rete. La sicurezza dei messaggi scambiati nella rete Bitcoin è garantita dall'utilizzo di crittografia a chiave pubblica e la validità delle transazioni è garantita da complessi calcoli matematici che i computer della rete devono eseguire in un processo chiamato "mining". Infine, i costi delle transazioni della rete Bitcoin sono o gratuiti o estremamente bassi.

Facciamo un confronto tra la rete Bitcoin e SWIFT, il circuito di pagamento utilizzato da molte banche nel mondo. Il circuito SWIFT dipende da un numero selezionato di server ed è una rete centralizzata. Analogamente alla rete Bitcoin, i messaggi nella rete di SWIFT sono protetti da crittografia, ma le transazioni sono convalidate da un database centrale. Infine, le transazioni con il circuito SWIFT possono essere molto costose.

Fino ad ora avete scoperto che:

- La moneta bitcoin è esclusivamente digitale, indipendente da qualsiasi autorità centrale di emissione, senza confini, con un disponibilità di valuta che è limitato e predeterminato.
- La rete Bitcoin è una decentralizzata e neutrale , rete di computer peer-to -peer, che è protetta da crittografia e ha addebita zero costi o commissioni molto ridotte.

Bene, vediamo ora alcuni casi in cui Bitcoin e la rete Bitcoin si dimostrano superiori alle valute e ai circuiti di pagamento che già esistono.

- Se siete uno dei 2,5 miliardi di persone in questo mondo che non hanno un conto in banca o se avete amici e parenti che vivono in altri paesi, è possibile utilizzare la rete Bitcoin per scambiare bitcoin con persone provenienti da tutto il mondo immediatamente con poca o nessuna spesa.
- Se disponete di risparmi e siete preoccupati che il vostro governo potrebbe confiscarne una parte, come il governo di Cipro ha fatto nel marzo del 2013, potreste voler trasferire una parte dei vostri risparmi in bitcoin per proteggerli.
- Utilizzando la rete Bitcoin è possibile scambiare bitcoin con persone che non avete mai incontrato pur essendo assolutamente sicuri che i vostri bitcoin arriveranno al legittimo proprietario. Tutto questo senza la necessità che una banca faccia come intermediario.
- Le rimesse, i pagamenti che di solito un membro di una famiglia straniera invia ad altri familiari nel paese di origine possono avere elevati costi di transazione. Bitcoin permette tali pagamenti con tariffe molto più basse.

Infine, ricordate che Bitcoin è una nuova tecnologia che può avere molte nuove applicazioni in futuro. In maniera simile al modo in cui Internet nei primi anni '90 è stata considerata quasi sinonimo di e-mail, Bitcoin oggi è considerato, dai più, sia circuito di pagamento Bitcoin che la valuta bitcoin.

Proprio come Internet oggi non è solo posta elettronica, ma World Wide Web, video e telefonia, allo stesso modo Bitcoin domani sarà più di quanto non lo sia già oggi.

Quindi preparatevi al futuro imparando di più su Bitcoin. Si può iniziare imparando il significato di alcuni termini importanti che sono contenuti nelle domande frequenti qui sotto:

Che cosa è un Bitcoin Indirizzo?

Un indirizzo Bitcoin è simile ai numeri di conto in banca. È possibile inviare denaro bitcoin a qualsiasi indirizzo, proprio come è possibile inviare denaro a qualsiasi conto bancario, se si conosce il suo numero e si possono spendere bitcoin solamente da un indirizzo che si controlla. È possibile controllare il vostro indirizzo Bitcoin tramite una chiave segreta, detta chiave privata. A differenza di un conto in una banca, però, si può facilmente avere tanti indirizzi Bitcoin quanti se ne desidera.

Che cosa è un portafoglio Bitcoin?

Un portafoglio Bitcoin è un programma per computer che contiene le chiavi private dei vostri indirizzi Bitcoin e rende i trasferimenti da e verso tali indirizzi facile e sicuro. Il portafoglio mostra anche il bilancio di tutti i bitcoin che ci sono negli indirizzi Bitcoin che lo stesso contiene. Consigliamo di proteggere il portafoglio con una password e assicurarsi che nessun altro vi abbia . Questo è molto importante e deve essere ripetuto: Non si dovrebbe mai dare la chiave privata associata a un indirizzo Bitcoin! Se lasciate che qualcun' altro entri in possesso di una vostra chiave privata, quest'ultimo avrà la possibilità di spendere i vostri Bitcoins dal vostro indirizzo bitcoin. Può spaventare un pochino all'inizio, ma una volta fatto non sarà più un grosso problema, dovete solo proteggere le chiavi cifrandole, cosa che il vostro portafoglio renderà comodo.

Perche tanta crittografia e sicurezza?

Si potrebbe leggere un sacco di descrizioni di Bitcoin che parlano di crittografia, funzioni hash, chiavi pubbliche e private e tutti i tipi di termini dal suono molto tecnicistico. Per cominciare l'unica cosa che dovete davvero capire è che Bitcoin funziona e che i vostri Bitcoin sono sicuri proprio grazie a complessi calcoli matematici. Questi calcoli complessi permettono di condurre affari e scambiare denaro con persone su Internet che non conoscete e di cui non dovete necessariamente avere fiducia. Tutto questo è davvero fantastico!