Come usare **Lightning Network** in 21’

Ing. Walter Maffione - Aprile 2023

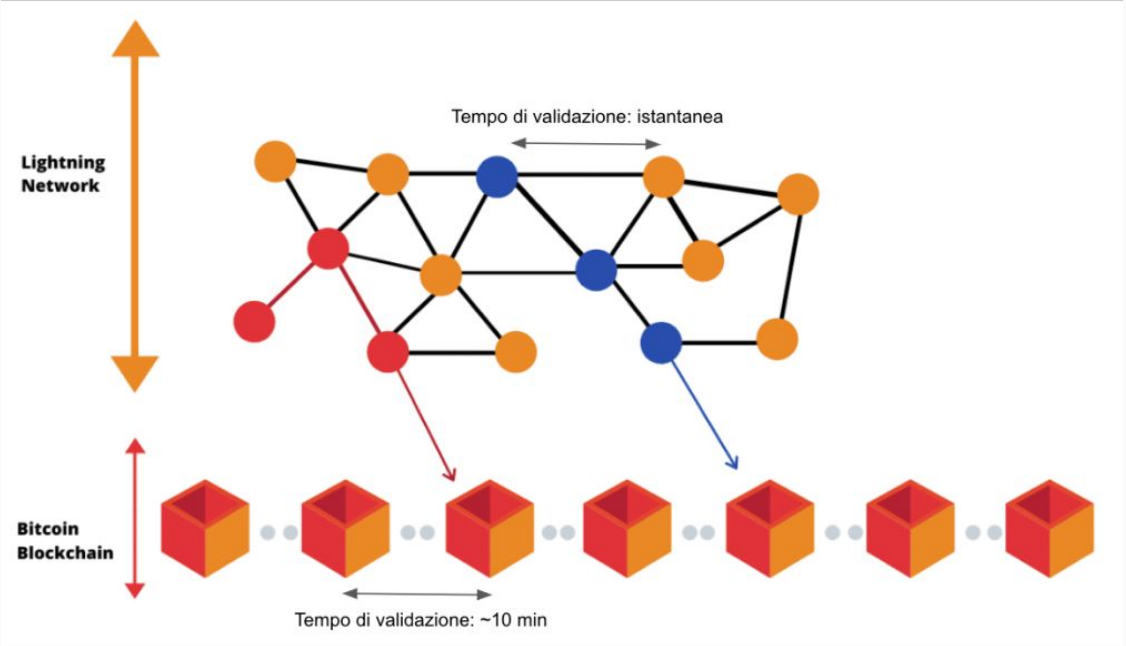
Introduzione

- Lightning Network
  - Recap
  - Canali di pagamento
  - Nodi LN
  - Liquidità
  - Pagamenti
- Wallet Lightning
  - Differenze
  - Variabili
- Confronto Wallet LN
- Conclusioni

Lightning Network - Recap

Modo più intelligente di usare Bitcoin

- Lightning Network è una rete di pagamento peer-to-peer che si basa sulla blockchain di Bitcoin
- Sfrutta i **canali di pagamento** per aumentare la capacità di elaborazione delle transazioni sulla rete
- Consente di effettuare transazioni **veloci** e a **basso costo**
- Contribuisce alla **scalabilità** e alla **privacy** di Bitcoin



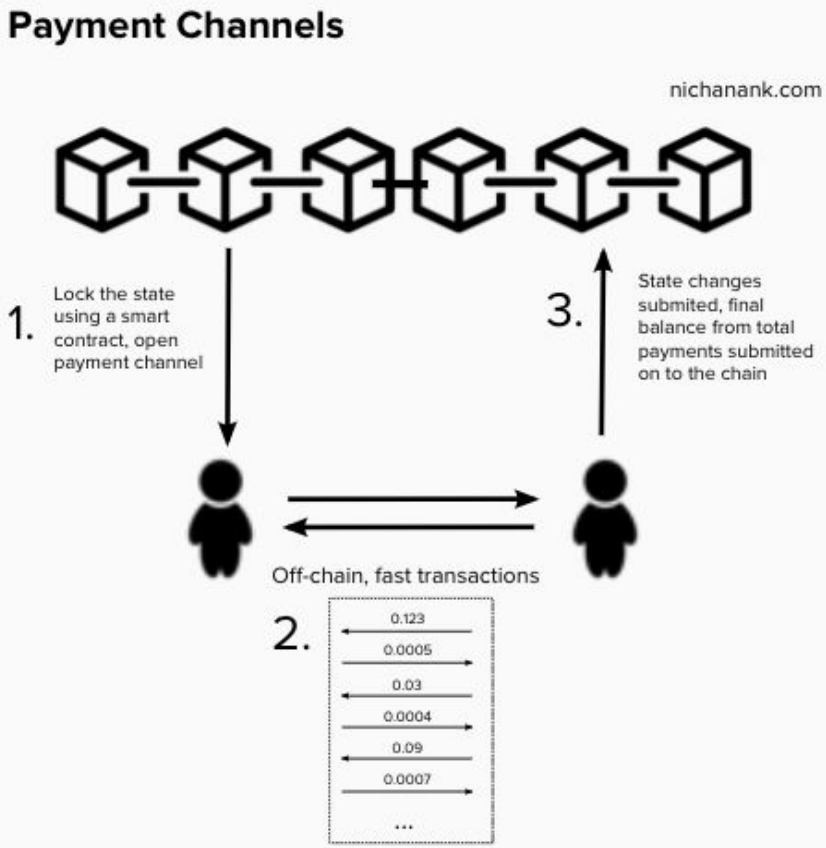
Canali di Pagamento

I canali di pagamento sono degli script (contratti) che permettono di scambiare **transazioni bitcoin valide** senza la necessità di propagarle immediatamente on-chain.

Viene scritta nella blockchain di Bitcoin solo la transazione di **apertura** e quella di **chiusura**

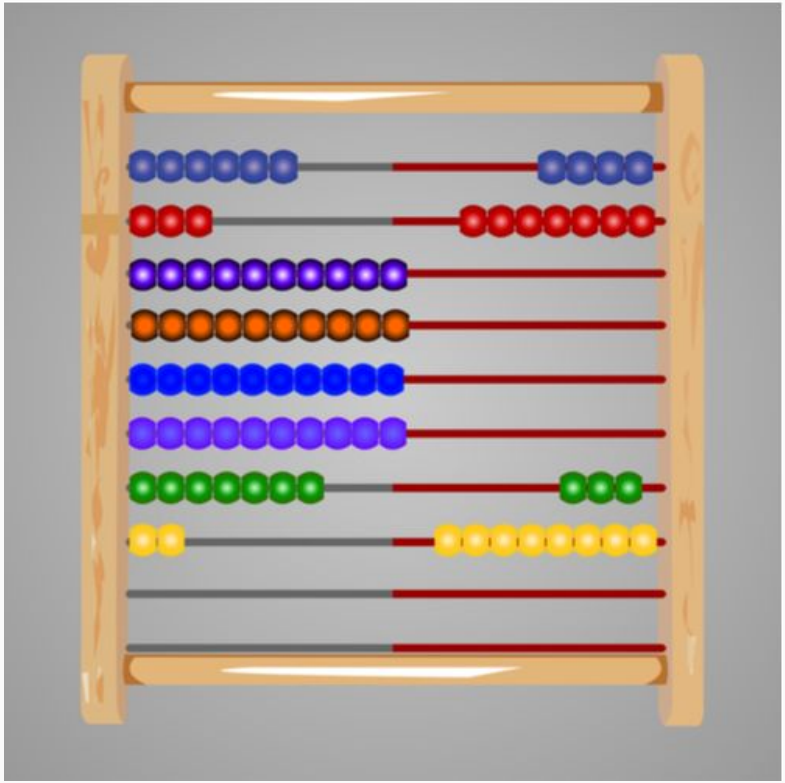
La creazione di un canale avviene tramite il deposito di una somma di bitcoin verso un indirizzo multi-sig 2-di-2 (Funding Transaction).

L'importo depositato nel canale rappresenta la **capacità** del canale e l'importo **massimo trasferibile**.

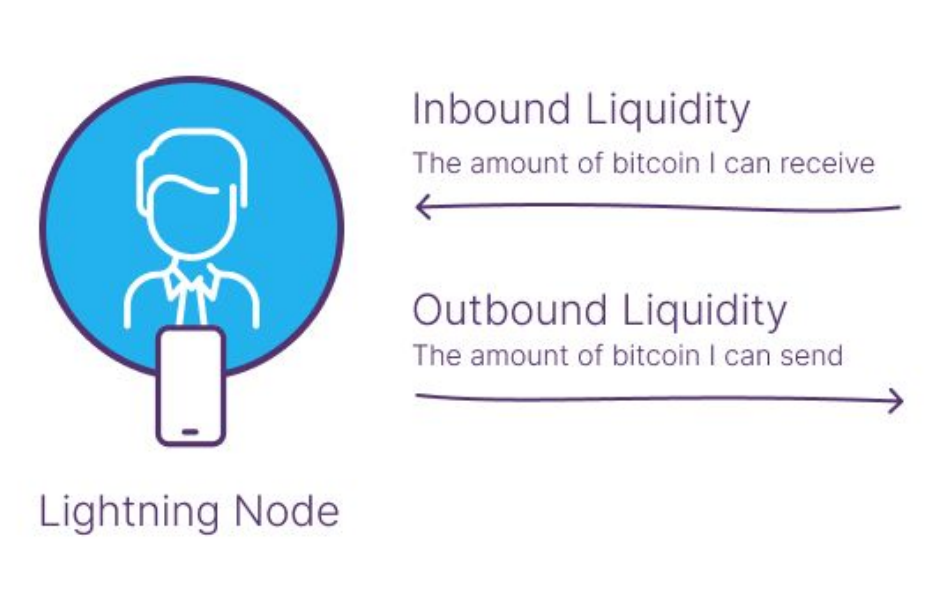


Canali di Pagamento

Le perline di un **abaco** per analogia possono rappresentare i **bitcoin** all'interno di un canale di pagamento.



Liquidità su Lightning



Senza liquidità in entrata (**inbound**) non posso ricevere

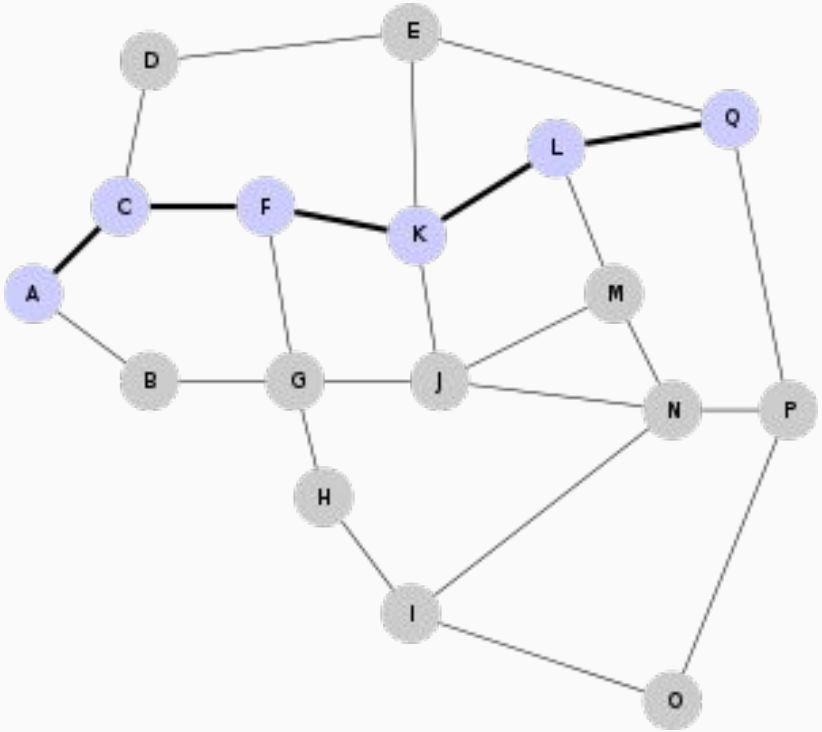
Senza liquidità in uscita (**outbound**) non posso inviare

https://bitcoin.design/guide/how-it-works/liquidity/

Routing

Annunciare i canali permette al nodo collegarsi ad altri nodi e costruire un grafo della rete, salvandolo in memoria

Due nodi **non devono** necessariamente **avere un canale** fra di loro **per poter fare un pagament**o, basta che sia presente un **percorso** che li colleghi e che tutti i canali intermedi abbiano abbastanza liquidità



Nodo Lightning

Software che gira su un server, PC o mobile, **scambia messaggi p2p** con altri nodi della rete parlando il **protocollo Lightning** descritto dai (BOLT)

Implementazione	Azienda	Linguaggio
Core Lightning	Blockstream	C
LND	Lightning Labs	Go
Eclair	ACINQ	Scala
LDK	Spiral	Rust

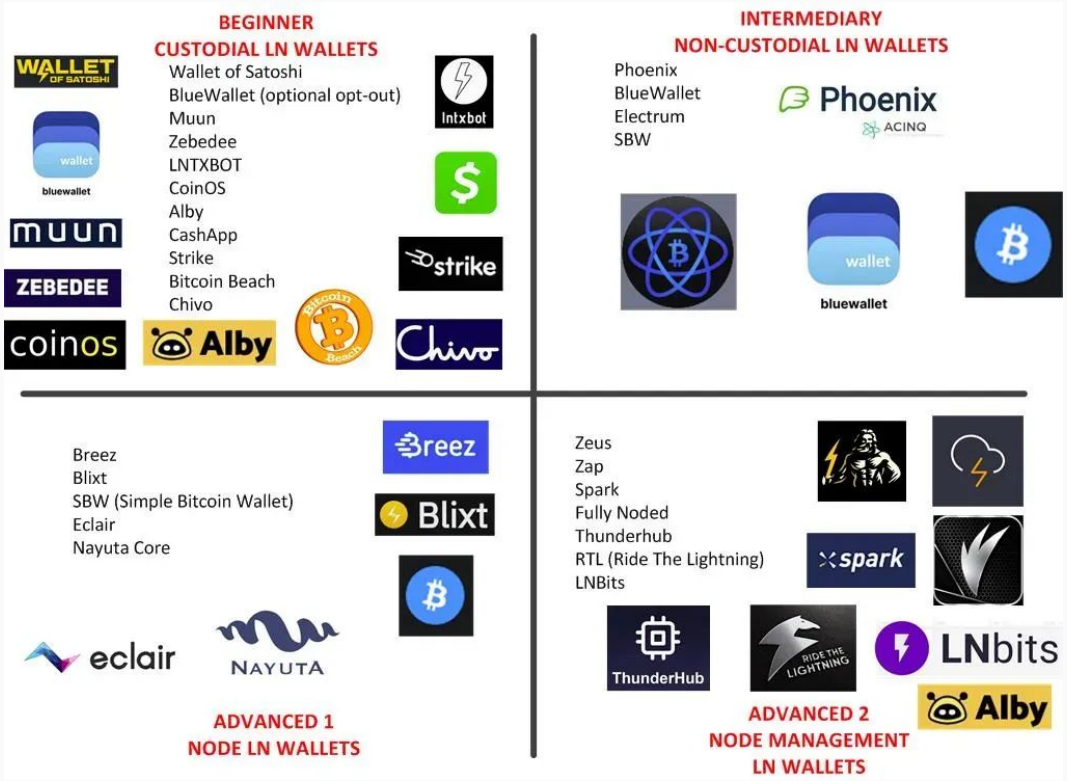
Lightning “Wallet”

App di pagamento mobile/web che permettono di ricevere e inviare bitcoin sulla rete Lightning

Si dividono principalmente in **custodial** o **non-custodial**

Non esiste il wallet migliore, ma dipende dalle **esigenze** ed **esperienza** di ognuno

È chiaramente preferibile **usare sempre wallet open-source**



Pagamenti

INVOICE (*BOLT11*):

Stringa generata dal ricevente **per poter essere pagato**, utilizzabile una sola volta e con un periodo di scadenza.

Codifica: Importo, Data di scadenza, Pubkey, etc

LNURL:

Protocollo proposto per migliorare l'UX dei pagamenti su Lightning. Aggiungendo ad esempio metodi per prelievo automatico o link di pagamento statici.
Presenta alcune criticità ma si sta sviluppando una soluzione migliore (BOLT12)

Come scegliere un app Lightning ?

Ci sono diverse variabili da tenere in considerazione

- **Hai un nodo?**
- **Custodial / Non Custodial**
- **Commissioni**
- **Affidabilità**
- **Semplicità / User Experience**
- **Velocità**
- **Funzionalità (es. POS, Podcast, App)**

Custodial Wallet

Soluzioni **account based,** come avere un conto in banca.

Il gestore del wallet ha un nodo Lighting, **ha lui le chiavi private che custodiscono i tuoi bitcoin**, gestisce lui canali e liquidità e ne ha sempre il controllo in qualsiasi momento.

Soluzioni come LndHub permettono di creare diversi account indipendenti su un unico nodo LN.
Possibile quindi condividere un nodo tra più persone, fidandosi del gestore.

Es. Wallet of Satoshi, Alby, lnbits, BlueWallet(✞), BTCPayServer di terzi

Non Custodial Wallet - (Your node, your coins)

Nodo Lightning in cui la custodia delle chiavi è in mano all'utente.

Diverse soluzioni possibili:

- Server Cloud (AWS, GCloud, Voltage)
- Server casalingo (PC, Workstation)
- Raspberry Pi (Umbrel, Raspiblits)
- Mobile (lndsync, LDK, eclair)

La gestione dei canali può essere gestita manualmente oppure affidata a tool automatici.
Nel caso di app mobile **l'azienda dietro il wallet gestisce i canali** facendo pagare piccole commissioni

Wallet of Satoshi

Wallet che gestisce oggi una grande parte dei pagamenti che avvengono su Lightning Network.

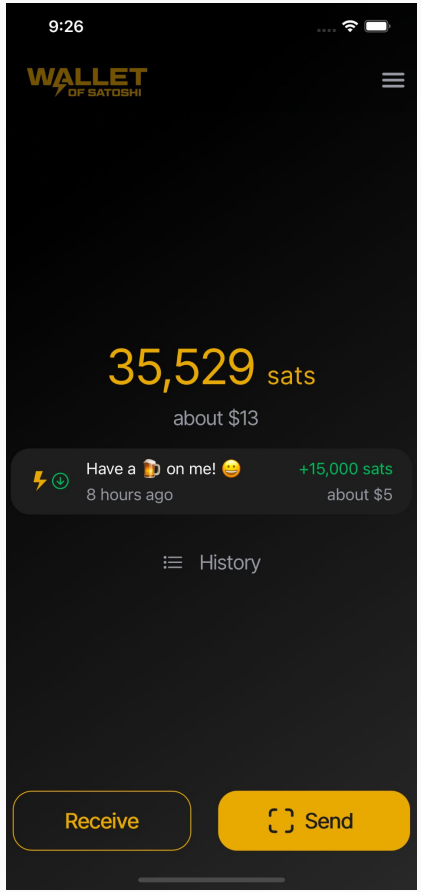
Soluzione **custodial** e **closed source,** in qualsiasi momento l'azienda potrebbe sparire coi fondi degli utenti.

Pro:

- Semplice
- Veloce
- Commissioni basse
- Non ci dobbiamo preoccupare dei canali

Contro:

- Custodial
- Closed source
- Brutto



Breez

Ottima app di pagamento Lightning che aggiunge POS per commercianti, Podcast player e altre applicazioni.

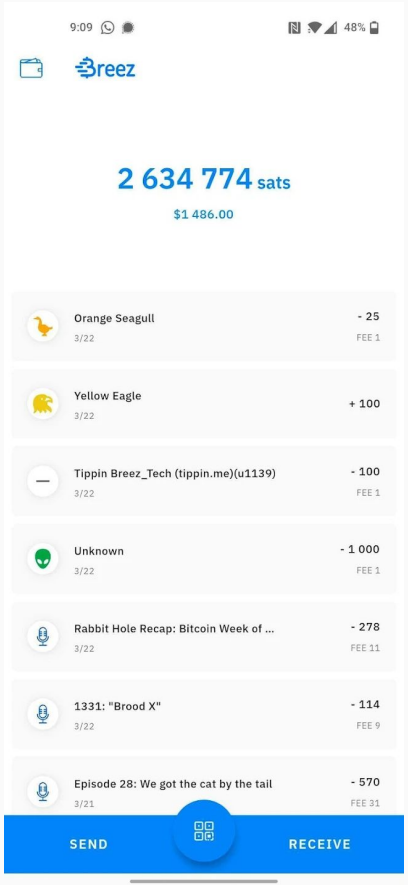
Soluzione **non-custodial** e **open source,** buona esperienza utente

Pro:

- Semplicità d'uso
- Buone commissioni
- Non custodial
- Possibile ricevere e inviare on-chain
- POS e altre app

Contro:

- Un po' lento
- Meno affidabile su importi elevati
- Limite di 4 mln di sats



Phoenix

Attualmente uno dei migliori wallet Lighting mobile

Soluzione **non-custodial**, integra anche un wallet on-chain.

A differenza di Breez, si dedica **solo** ai pagamenti

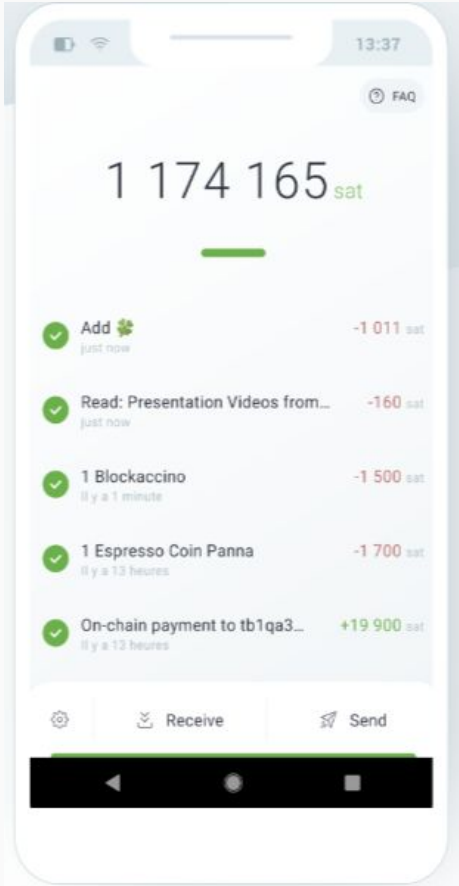
Pro:

- Facile da usare
- Affidabile nei pagamenti
- Privacy (usa tor e trampoline node)
- Non custodial
- Possibile ricevere e inviare on-chain

Contro:

- Alcune fee sono “nascoste”
- Apre canali più frequentemente

Icona app



Muun

Ottimo wallet **on-chain** ma non è un vero wallet Lightning.
L'utente non se ne accorge ma loro in background fanno degli swap LN/BTC.
Fee più alte anche per chi ci paga.

Ottimo strumento per migliorare la privacy on-chain

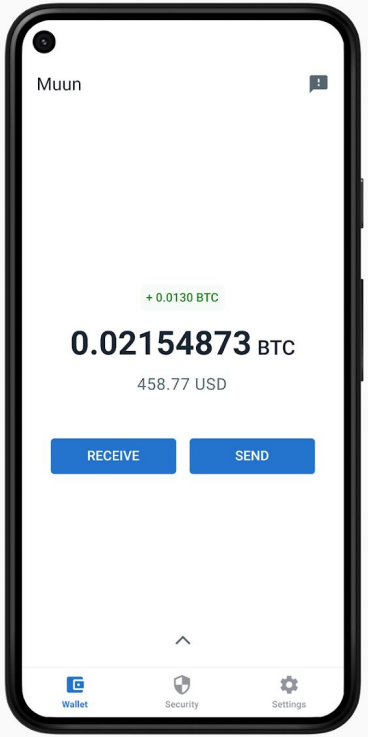
Pro:

- Non custodial
- Semplice
- Privacy

Contro:

- Molto lento (è on-chain)
- Fee più alte

Icona app



BitKit

Nuovo wallet ancora in beta ma con alcune features interessanti.
Rubrica di contatti per pagare su Lightning senza inquadrare QR code o copiare invoice (grazie a slashtags)
Interfaccia grafica di un altro livello rispetto ai competitor.
Non custodial, basato su **LDK**

Pro:

- User Experience
- Semplice
- Privacy

Contro:

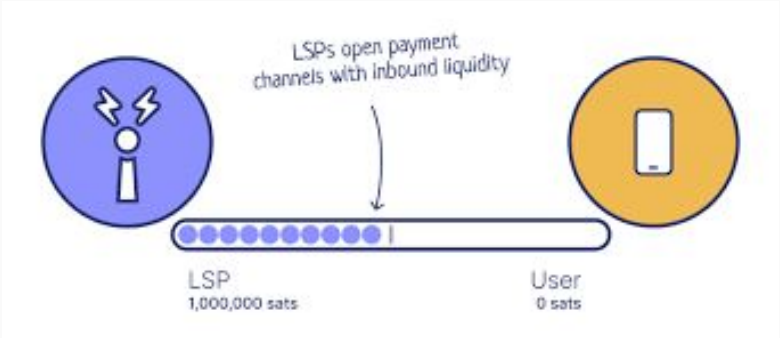
- Ancora in beta
- Fee più alte

Ricevere su Lightning - Commercianti

Chi riceve spesso su Lightning Network (es. commerciante) ha bisogno di avere **liquidità in entrata (inbound)** sempre disponibile.

Nel caso di una gestione **manuale** del nodo dobbiamo provvedere noi a questo problema.

- **Ribilanciamento**: Pagamenti a me stesso (LN o on-chain) passando dal canale che vogliamo ribilanciare
- **Chiedere o pagare qualcuno per fare aprire a lui un canale** verso il nostro nodo.



Utilizzando un wallet Lightning tipo Breez o Phoenix, il loro nodo si occupa di questo problema, facendo pagare una commissione.

Wallet di nuova generazione (GreenLight)

Greenlight di Blockstream fornirà nodi CLN on-demand, gestiti a basso costo, garantendo agli utenti il pieno controllo dei propri fondi.

Strumenti come **Breez-SDK** costruiti sopra Greenlight, permettono a qualsiasi tipo di sviluppatore, di integrare pagamenti in bitcoin su Lightning Network nelle proprie applicazioni, con minimo sforzo

Conclusioni

- Oggi, soluzioni come **Breez** e **Phoenix** sono ottime scelte
- **Evitare wallet custodial** se non volete rischiare di perdere fondi
- Preferibile non tenere grosse somme su un wallet Lighting (come un portafoglio)
- Nuove app di pagamento più innovative, semplici e belle stanno arrivando

References

- Mastering Lightning Network - Andreas M. Antonopoulos et al.
- Test of Bitcoin lightning wallets - Juraj Bednar
- Lightning liquidity | Bitcoin Design
- There Is No Such Thing as a “Lightning Wallet” - Roy Sheinfeld

Fine

Grazie per l’attenzione

Sentitevi liberi di donare qualche sats ;)