

COME FUNZIONA IN PRATICA LA LIGHTNING NETWORK.

Alice, Bob e Zoe e la transazione Bitcoin.



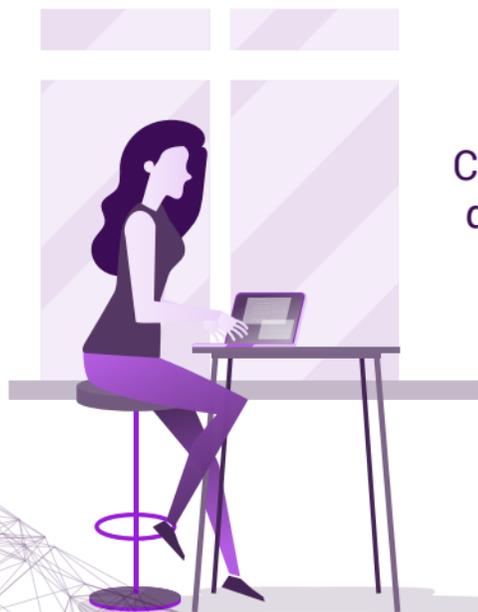


ALICE

BOB

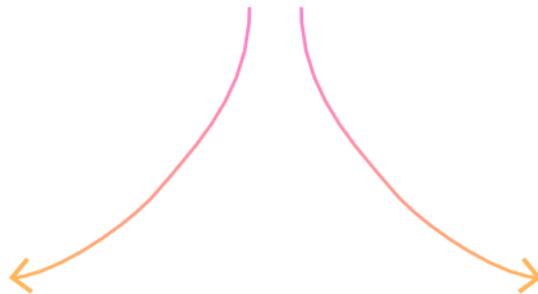
Supponiamo ci siano due nodi Lightning, Alice e Bob, che vogliono eseguire una transazione, facendo uso della Lightning Network. Come sappiamo, questa rete instrada transazioni per mezzo di canali creati tramite nodi.

ALICE HA DUE POSSIBILITÀ PER INVIARE 1 BITCOIN A BOB



1

Creare un canale diretto con Bob



2

Sfruttare Zoe, un altro nodo Lightning, al quale entrambi sono già collegati e con il quale hanno entrambi **5 bitcoin stanziati nei rispettivi canali**. Quindi, il canale tra **Alice e Zoe conterrà 10 bitcoin** (5 messi da Alice e 5 messi da Zoe) ed il canale tra **Zoe e Bob ne conterrà altrettanti 10** (5 messi da Bob e 5 messi da Zoe).



ESSI DECIDONO DI SFRUTTARE LA SECONDA POSSIBILITÀ, UTILIZZANDO ZOE.

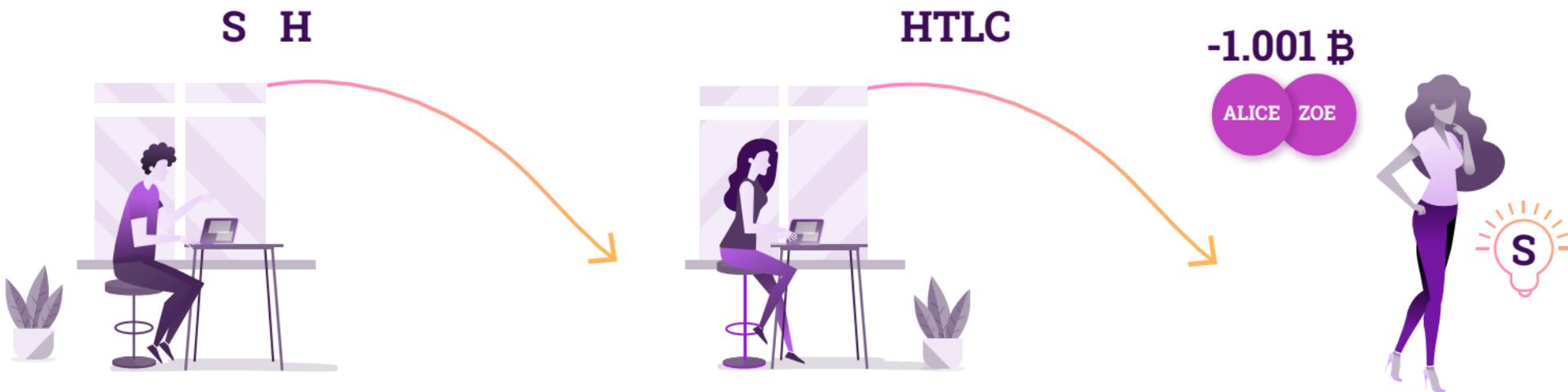


**Nodo Lightning
Alice e Zoe 10 bitcoin**
5 mesi da Alice e 5 mesi da Zoe



**Nodo Lightning
Bob e Zoe 10 bitcoin**
5 mesi da Bobe 5 mesi da Zoe

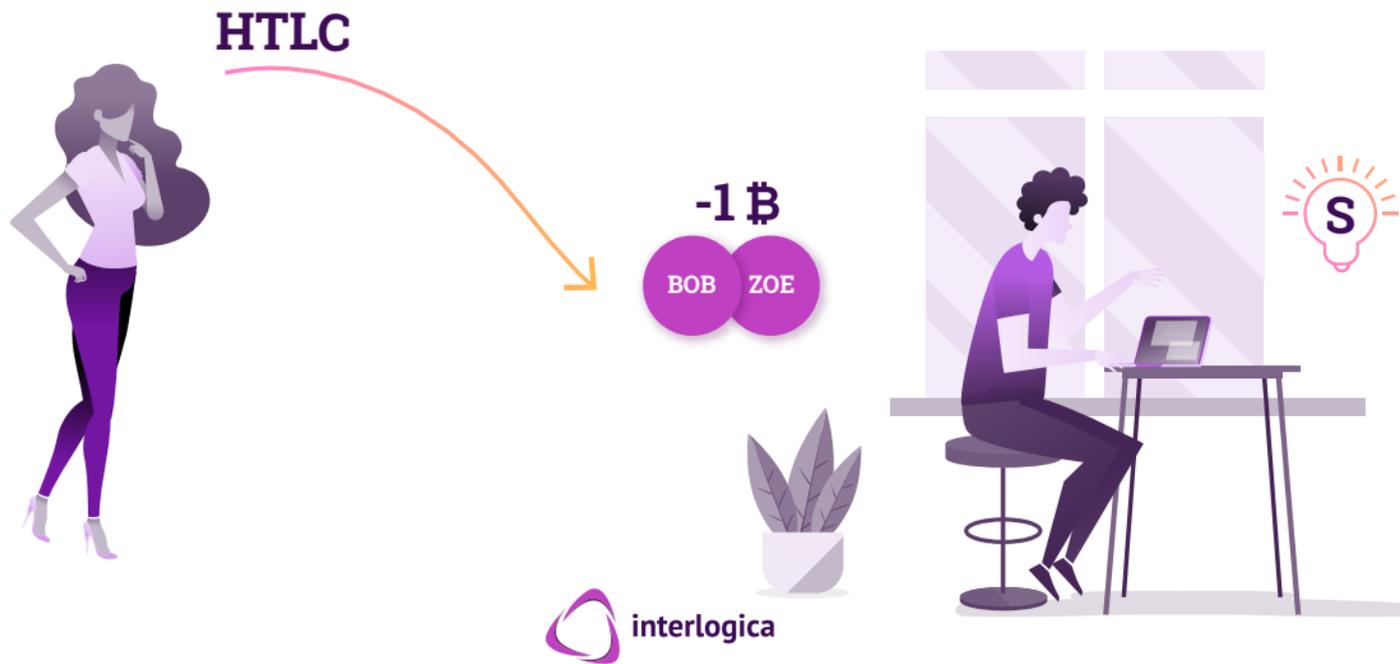
Bob, il destinatario, genera un segreto S e il suo relativo hash H ed invia quest'ultimo ad Alice.
Alice crea un HTLC "Alice sta sottraendo 1.001 bitcoin dal suo canale con Zoe, dandoli a Zoe, se Zoe conosce il segreto, altrimenti il pagamento ritorna indietro ad Alice se nel mentre vengono minati 10 blocchi".



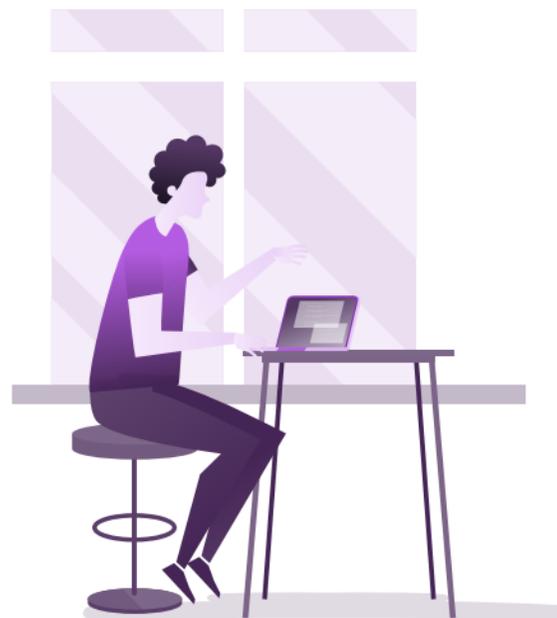
Il canale tra i due sarà quindi caratterizzato dall'aver 5 bitcoin posseduti da Zoe, 3.999 bitcoin posseduti da Alice e 1.001 bitcoin stanziati nell'HTLC.



A questo punto, Zoe costruisce un HTLC verso Bob "Zoe sta sottraendo 1 bitcoin dal suo canale con Bob, dandoli a Bob, se Bob conosce il segreto, altrimenti il pagamento ritorna indietro a Zoe se nel mentre vengono minati 9 blocchi".



Il canale tra i due sarà quindi caratterizzato dall'aver 5 bitcoin posseduti da Bob, 4 bitcoin posseduti da Zoe e 1 bitcoin stanziato nell'HTLC.



Bob, conoscendo il segreto, riscatta il pagamento programmato nell'HTLC di Zoe ed invia il segreto S a Zoe.
Zoe, a sua volta, riscatta il pagamento programmato nell'HTLC di Alice.



Il pagamento risulta così terminato con successo.



I canali sono quindi aggiornati in modo tale che il canale che Alice ha con Zoe contiene 3.999 bitcoin. Quello che Zoe ha con Alice contiene 6.001 bitcoin. Il canale tra Zoe e Bob è di 4 bitcoin e, infine, quello che Bob ha con Zoe è di 6 bitcoin.



Bob ha così ottenuto il suo pagamento di 1 bitcoin e Zoe, l'intermediario, ha ottenuto 0.001 bitcoin come "ricompensa" per aver partecipato al pagamento.

BOB



1



OTTENUTO

ZOE



0.001



**COME
RICOMPENSA**



**VUOI APPROFONDIRE?
CLICCA QUI!**

WWW.INTERLOGICA.IT