Multichannel factories – lightning network

scritto da Alberto De Luigi | 17 Marzo 2020
Questo articolo è un focus sulle channel factories di lightning network, estratto da questo trattato precedente.

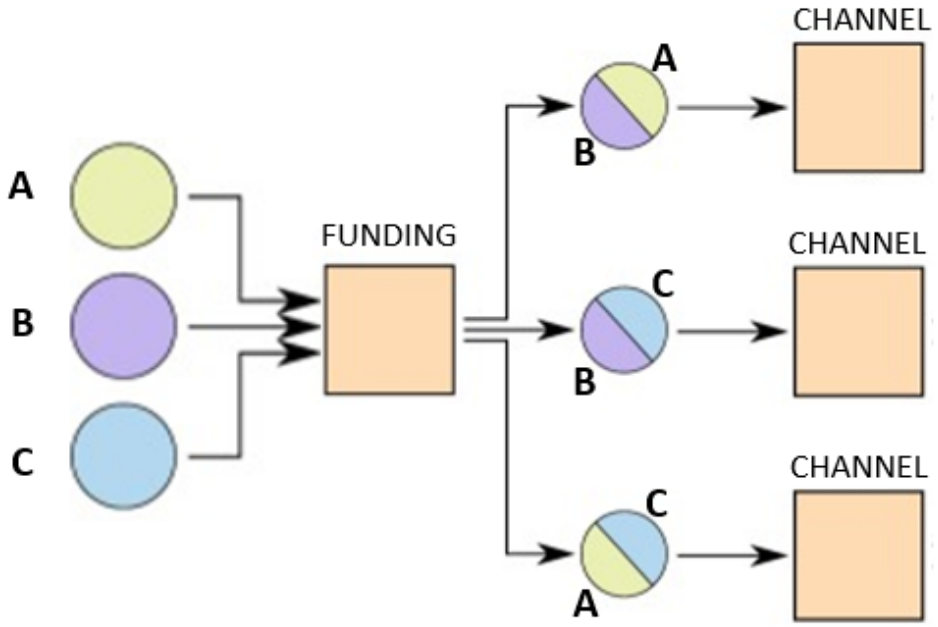
Le transazioni Lightning di apertura dei canali potranno essere "aggregate", in un meccanismo che si chiama Multi-party funded channels. Questo concetto è comparso per la prima volta nel paper *Scalable Lightning Factories for Bitcoin* e poi affinato in *Scalable Funding of Bitcoin Micropayment Channel Network* che è un paper incredibilmente semplice e chiaro dal punto di vista grafico.

Anticipiamo già che le channel factories sono la vera killer application, quella che fa sperare ai puristi del blocco piccolo che il parametro blocksize possa addirittura non essere mai più modificato.

Il meccanismo di funzionamento è molto semplice: anziché aprire un canale fra due soli utenti, più utenti mettono in comune i fondi in un "recipiente" (funding), che è in effetti l'unico output di un'unica grande transazione, contenente come input i bitcoin provenienti dai wallet di ogni utente. Nessun utente si deve fidare degli altri poiché in qualsiasi momento può decidere di sbloccare autonomamente quei fondi, essendo la transazione creata con lo stesso meccanismo di multisig e checksequence tipico di Lightning Network, semplicemente esteso a più persone.

A partire da questo output bloccato onchain, offchain vengono costruiti tutti i canali fra gli utenti: è possibile, ma non necessario, che ogni partecipante apra un canale con ogni altro utente (come nel grafico esemplificativo qui sotto, con soli tre utenti). Questi canali possono essere chiusi e riaperti senza mai tornare onchain, a patto ovviamente che i

movimenti di denaro non oltrepassino le quantità immesse nella funding originaria. In poche parole, la funding è un canale Lightning Network di layer 2, mentre i canali bilaterali veri e propri tipici di Lightning sono una sorta di layer 3 che vi viene costruito sopra.



channel factories – lightning network

Nell'esempio in figura, ipotizziamo che A, B e C mettano in comune nella funding 1 bitcoin a testa, per un totale di 3 btc (le tre palline colorate). Ogni canale sarà aperto con 0,5 bitcoin su ogni lato, perciò ad esempio 1 bitcoin di A (la pallina verde chiaro) verrà diviso in modo da creare un canale con B e uno con C.

A avrà 0,5btc nel canale con C e gli altri 0,5 btc nel canale con B. Ogni canale avrà una capacità totale di 1btc, quindi la capacità del canale AC sarà 1 btc, di cui mezzo appartentente ad A e mezzo a C:

AC: 0,5 | 0,5

Se A paga a C mezzo bitcoin, il balance nel canale passerà ad essere:

AC: 0 | 1

Normalmente in Lightning Network, questo significa che domani A non potrà più pagare altri 0,5 btc a C, poiché significherebbe passare sul lato di C del canale ben 1,5 btc, il che sarebbe impossibile per due ragioni:

- A non ha quella disponibiltà nel canale con C
- La capacità massima del canale, calcolata sommando i fondi di A e C in AC, è già stata raggiunta, poiché limitata a 1btc

Eppure A possiede 0,5 btc disponibili nel canale con B. Grazie al fatto che tutti questi canali si trovano su un "layer 3", A può chiudere il canale con B e C e questa operazione rimane offchain, poiché l'output onchain della FUNDING non viene toccato. I fondi nella FUNDING vengono solo "rimescolati" nella creazione di nuovi canali, in modo che A possa aprire un nuovo canale AC utilizzando quanto prima possedeva nel canale AB. Il risultato sarà:

AB: canale chiuso (non è richiesta transazione onchain)
AC: 0 | 1,5 (riaperto con 0,5btc di capacità in più, senza transazioni onchain)

Questo sistema è ottimo per tre ragioni:

1. **Si possono aprire e chiudere infinite volte i canali su layer 3 senza mai transare onchain**
2. **Le commissioni di transazione per la creazione onchain della funding originaria vengono divise fra tutti i partecipanti alla channel factory**
3. **La funding originaria aggrega le transzioni di "apertura di canale" di molti utenti, risparmiando una quantità incredibile di spazio sulla blockchain**

Pensiamo a 10 utenti che uniscono i loro fondi in un'unica funding e da qui creano 45 canali fra loro, facendo sì che ogni utente abbia un canale diretto con tutti gli altri e che

possa chiudere e riaprire i canali, in base alle necessità, con qualsiasi altro di questi 10 utenti.

Nota: per 10 utenti (da A di Alice a L di Leorio) il numero minimo di canali diretti è 45, in base alla formula matematica m = n(n-1)/2; con m = numero canali e n = numero utenti. Per contarli in modo un po' meno elegante, ma più intuitivo, si procederebbe come segue:

A apre un canale con **B**,**C**,D,E,F,G,H,I,L (9 canali)

B apre un canale con **C**,D,E,F,G,H,I,L (AB esiste già, vengono aperti quindi altri 8 canali)

C apre con D,E,F,G,H,I,L (AC e BC esistono già, vengono aperti quindi altri 7 canali)

…e così via

Se analizziamo il peso di una channel factory che riunisce 10 utenti rispetto alla creazione di 45 canali bilaterali, ognuno con un'apposita transazoine onchain, notiamo che il risparmio di spazio sulla blockchain è del 90%. Se si usasse Schnorr, sarebbe addirittura il 96%.

Questo significa che le channel factories aumentano la possibilità della blockchain di ospitare canali Lightning di oltre <u>20 volte</u> a parità di spazio occupato (solo di 10 volte senza Schnorr)

Inoltre i canali di layer 3 costruiti in una factory sono molto più "utili" dei tipici canali Lightning, poiché possono essere ricombinati a piacimento, aprendo nuove opzioni di scambio fra tutti gli utenti coinvolti

Users (n)	Channels (m)	LN vbytes	Factories vbytes	Savings (%)
3	3	720	320	55.56%
4	6	1440	415	71.18%
5	10	2400	510	78.75%
6	15	3600	605	83.19%
7	21	5040	700	86.11%
8	28	6720	795	88.17%
9	36	8640	890	89.70%
10	45	10800	985	90.88%

Il problema di questa soluzione è uno solo: maggiore è il numero di utenti che partecipano e più probabile è che uno solo di essi voglia chiudere la factory. Se uno solo sceglie di chiudere (o se si vuole aggiungere anche un solo utente ad una factory già esistente) è necessario transare onchain, e ogni canale di layer 3 va chiuso. La bella notizia è che tutti i partecipanti che rimangono nella factory possono ricostruire i canali di layer 3 con la stessa transazione di chiusura del canale (che chiude la factory escludendo l'utente che vuole abbandonare, riaprendola per tutti gli altri).

Dall'altro lato, è anche vero che, maggiore è il numero di partecipanti (più grande è il canale e la sua capacità), maggiore sarà l'incentivo a rimanere in esso per ogni partecipante, poiché i bitcoin in Lightning sono più liquidi (spendibili a minor costi in termini di tempo e commissioni) rispetto ai Bitcoin onchain. Si può immaginare un network Bitcoin del futuro che sia fatto quasi interamente da channel factories di gruppi di utenti, ove tutti i principali movimenti di bitcoin avvengano quasi esclusivamente su un terzo layer di canali Lightning.

Maggiore il numero di utenti, maggiore il risparmio. Ma anche soltanto con 10 utenti, una channel factory pesa 985 bytes, con Schnorr 435bytes (tutti i numeri hanno buone approssimazioni). Significa che in 1mb di blocco si possono creare 2.300 transazioni di questo tipo, ovvero 23 mila utenti che creano 103 mila canali. Contando 6 blocchi in un'ora e 144

al giorno, significa che ogni giorno 3 milioni di persone possono creare quasi 15 milioni di canali.