Principles of Cryptocurrency Design

Appunti ed Esercizi

Francesco Pasquale

28 maggio 2026

La Lightning Network [2] come rete di canali di pagamento può essere formalizzata come un grafo non-diretto $G = (V, E)$ con archi pesati, gli archi sono i *canali* e i pesi $c : E \to \mathbb{N}$ le *capacità*. La capacità $c(e)$ di un canale $e = \{u, v\}$ è condivisa fra i due nodi estremi del canale, ognuno dei quali in ogni momento ne detiene una parte $\{b_e(u), b_e(v)\}$ con $b_e(u), b_e(v) \in \{0, 1, \ldots, c(e)\}$ e $b_e(u) + b_e(v) = c(e)$, chiamata *bilancio* del canale. Per comodità, dato un canale $e = \{u, v\}$, qui definiamo anche $b_{\min}(e) = \min\{b_e(u), b_e(v)\}$ e diciamo che il canale "e" è *vuoto in una direzione* se $b_{\min}(e) = 0$.

Un *pagamento* tra due nodi adiacenti u e v consiste in un aggiornamento del bilancio dell'arco $e = \{u, v\}$; ad esempio, se il bilancio corrente tra u e v è $\{b_e(u), b_e(v)\}$ e il nodo u esegue un pagamento $\texttt{pay}(u, v, x)$ verso il nodo v di *importo* $x \in \{1, \ldots, b_e(u)\}$, allora il nuovo bilancio $\{b'_e(u), b'_e(v)\}$ dell'arco sarà dato da $b'_e(u) = b_e(u) - x$ e $b'_e(v) = b_e(v) + x$.

I pagamenti possono essere *instradati* attraverso la rete: un nodo u che desidera inviare un importo x a un nodo non adiacente v può cercare un cammino $\mathcal{P} = (u = u_0, u_1, \ldots, u_h = v)$ nel grafo tra i nodi u e v e, se un tale cammino esiste, eseguire un pagamento $\texttt{pay}_{\mathcal{P}}(u, v, x)$ verso il nodo v lungo il cammino $\mathcal{P}$ di importo x, a condizione che $x \leqslant b_{e_i}(u_i)$ per ogni canale $e_i = \{u_i, u_{i+1}\}$ appartenente al cammino. Un tale pagamento aggiorna di conseguenza i bilanciamenti di tutti i canali in $\mathcal{P}$; cioè, per ogni canale $e_i = u_i, u_{i+1}$ nel cammino, il nuovo bilancio $\left(b'_{e_i}(u_i), b'_{e_i}(u_{i+1})\right)$ dopo il pagamento sarà[1]

$$\begin{cases} b'_{e_i}(u_i) &= b_{e_i}(u_i) - x \\ b'_{e_i}(u_{i+1}) &= b_{e_i}(u_{i+1}) + x \end{cases}$$

Mentre il grafo $G = (V, E)$ e le capacità dei canali $c, :, E \to \mathbb{N}$ sono note a tutti i nodi della rete, il bilancio $b_e(u), b_e(v)$ di un canale $e = u, v$ è noto soltanto ai suoi estremi u e v. Pertanto, è possibile (e ciò accade frequentemente nella Lightning Network reale) che, quando un nodo u cerca di effettuare un pagamento di importo x verso un nodo

[1] Nella Lightning Network reale, per ciascun canale intermedio è prevista una piccola *commissione* (*fee*) che il nodo incaricato di inoltrare il pagamento sottrae all'importo. Pertanto, se v deve ricevere un importo x, il nodo u deve inviare un importo maggiore, ad esempio $x + \varepsilon$, dove ε rappresenta la commissione totale trattenuta dai nodi intermedi $u_1, \ldots, u_{k-1}$ lungo il cammino. Per mantenere il nostro modello semplice e concentrarlo sul principale problema di teoria dei grafi che intendiamo affrontare, trascuriamo questo dettaglio (così come diversi altri aspetti) del reale processo di instradamento dei pagamenti nella Lightning Network.

non adiacente v utilizzando un cammino $\mathcal{P} = (u = u_0, u_1, \ldots, u_k = v)$, il pagamento non possa essere eseguito perché, per qualche canale del cammino, il bilancio non è sufficiente a supportare il pagamento. Ciò si verifica quando esiste un canale $e_i = (u_i, u_{i+1})$ nel cammino con bilancio $(b_{e_i}(u_i), b_{e_i}(u_{i+1}))$ tale che $b_{e_i}(u_i) < x$. In tal caso diciamo che si verifica un *fallimento del pagamento* (*payment failure*) e il nodo u deve scegliere un altro cammino per effettuare il pagamento verso il nodo v.

In [1] abbiamo sudiato il seguente processo aleatorio.

Algorithm 1 Tempo di primo fallimento

Require: Un grafo non-diretto, connesso e pesato $G = (V, E)$;
Capacità degli archi $c(e) = 2k_e$ per ogni $e \in E$;
Bilancio iniziale $b_e(u) = b_e(v) = k_e$, per ogni arco $e = \{u, v\}$.

1: **while** $b_{\min}(e) > 0$ per ogni $e \in E$ **do**
2: Scegli un nodo sorgente u in V, u.a.r.
3: Scegli un nodo destinatario v in V, u.a.r.
4: Scegli un cammino minimo $\mathcal{P} = (u = u_0, u_1, \ldots, u_h = v)$,
u.a.r. fra tutti i cammini minimi fra u e v;
5: **for** $i = 0, \ldots, h-1$ **do**
6: $b_{\{u_i,u_{i+1}\}}(u_i) = b_{\{u_i,u_{i+1}\}}(u_i) - 1$
7: $b_{\{u_i,u_{i+1}\}}(u_{i+1}) = b_{\{u_i,u_{i+1}\}}(u_{i+1}) + 1$
8: **return** Il numero di iterazioni del ciclo WHILE

Per analizzare un tale processo, è necessario familiarizzare con le *catene di Markov*.

Una *birth-and-death chain* finita con bordo assorbente è una catena di Markov $\{X_t : t \in \mathbb{N}\}$ con spazio degli stati

$$\Omega = \{-k, -k+1, \ldots, -1, 0, 1, \ldots, k-1, k\}$$

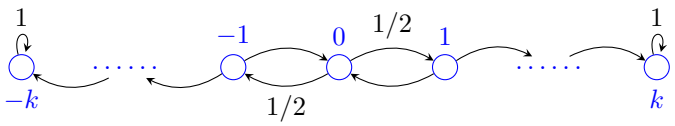
per qualche $k \in \mathbb{N}$, dove

$$\mathbf{P}(X_{t+1} = -k \,|\, X_t = -k) = \mathbf{P}(X_{t+1} = k \,|\, X_t = k) = 1$$

e per ogni $j = -k+1, \ldots, -1, 0, 1, \ldots, k-1$,

$$\begin{aligned} \mathbf{P}(X_{t+1} = j+1 \,|\, X_t = j) &= p \\ \mathbf{P}(X_{t+1} = j-1 \,|\, X_t = j) &= q \\ \mathbf{P}(X_{t+1} = j \,|\, X_t = j) &= 1 - (p+q) \end{aligned}$$

con p e q non-negativi e tali che $p + q < 1$. Quando $p = q = 1/2$ la catena si dice *unbiased*.



Esercizio 1. Sia $\tau = \inf\{t \in \mathbb{N} : X_t = \pm k\}$ la variabile aleatoria che indica il primo istante in cui la catena si trova nello stato k o nello stato $-k$. Dimostrare che il valore atteso di τ per la catena che parte da uno stato arbitrario $j \in \Omega$ è

$$\mathbf{E}\left[\tau \mid X_0 = j\right] = k^2 - j^2$$

Per dare una stima della probabilità che una catena finita raggiunga il bordo prima o dopo un certo valore, a volte è conveniente considerare catene infinite.

Esercizio 2. Sia $\{X_t : t \in \mathbb{N}\}$ una catena di nascita e morte *unbiased* con spazio degli stati $\Omega = \mathbb{Z}$. Per ogni istante $t \in \mathbb{N}$ e per ogni *target state* $k \in \mathbb{N}$ si ha che

$$\mathbf{P}\left(|X_t| \geqslant k \mid X_0 = 0\right) \leqslant \mathbf{P}\left(\max_{i=1,\dots,t} |X_i| \geqslant k \mid X_0 = 0\right) \leqslant 2\mathbf{P}\left(|X_t| \geqslant k \mid X_0 = 0\right)$$

Esercizio 3. Si provi a vedere l'analisi del processo aleatorio in [1].

Riferimenti bibliografici

[1] Taki E.M. Abedesselam, Fabio Giacomelli, Francesco Pasquale, and Michele Salvi. Payment-failure times for random lightning paths. In *Proc. of 7th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS'25)*, pages 1–10. IEEE, 2025. `https://ieeexplore.ieee.org/iel8/11302407/11302901/11302927.pdf`.

[2] Joseph Poon and Thaddeus Dryja. The bitcoin lightning network: Scalable off-chain instant payments. `https://lightning.network/lightning-network-paper.pdf`, 2016.