

CONSENSO NELLE BLOCKCHAIN

ALGORITMI DI CONSENSO DISTRIBUITO:

1. TERMINAZIONE
2. ACCORDO
3. INTEGRITÀ

ALGORITMI DI CONSENSO DISTRIBUITO PER LE BLOCKCHAIN:

1. TERMINAZIONE
2. ACCORDO
3. VALIDITÀ
4. INTEGRITÀ

Il consenso nelle blockchain è influenzato da 3 fattori:

1. COME VENGONO SELEZIONATI I PARTECIPANTI
2. ALGORITMO SCELTO PER IL CONSENSO
3. STRUTTURA DATI USATA NELLA BLOCKCHAIN

*struttura di un algo.
di consenso per le
blockchain:*

1. PROPOSTA DI UN BLOCCO
2. PROPAGAZIONE DELLE INFORMAZIONI
3. VALIDAZIONE DEI BLOCCHI
4. FINALIZZAZIONE DEI BLOCCHI
5. MECCANISMO DI INCENTIVAZIONE

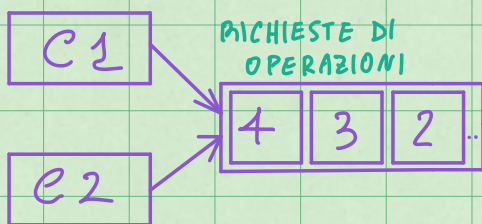
STATE MACHINE REPLICATION

Il consenso su B.C. si ispira allo state machine replication, infatti sussistono i seguenti parallelismi:

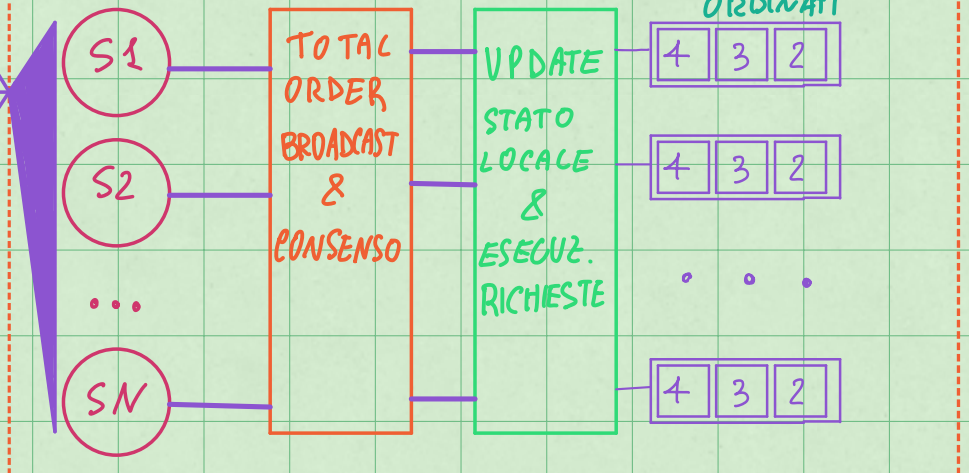
STATE MACHINE REPLICATION

1. PROPOSTA DI UN BLOCCO / richiesta di op. da parte dei CLIENT
2. PROPAGAZIONE DELLE INFORMAZIONI / reliable broadcast delle richieste
3. VALIDAZIONE DEI BLOCCHI / verifica firme ed ecc. richieste
4. FINALIZZAZIONE DEI BLOCCHI / consenso dei server sullo stato cor.
5. MECCANISMO DI INCENTIVAZIONE / non c'è un parallelismo.

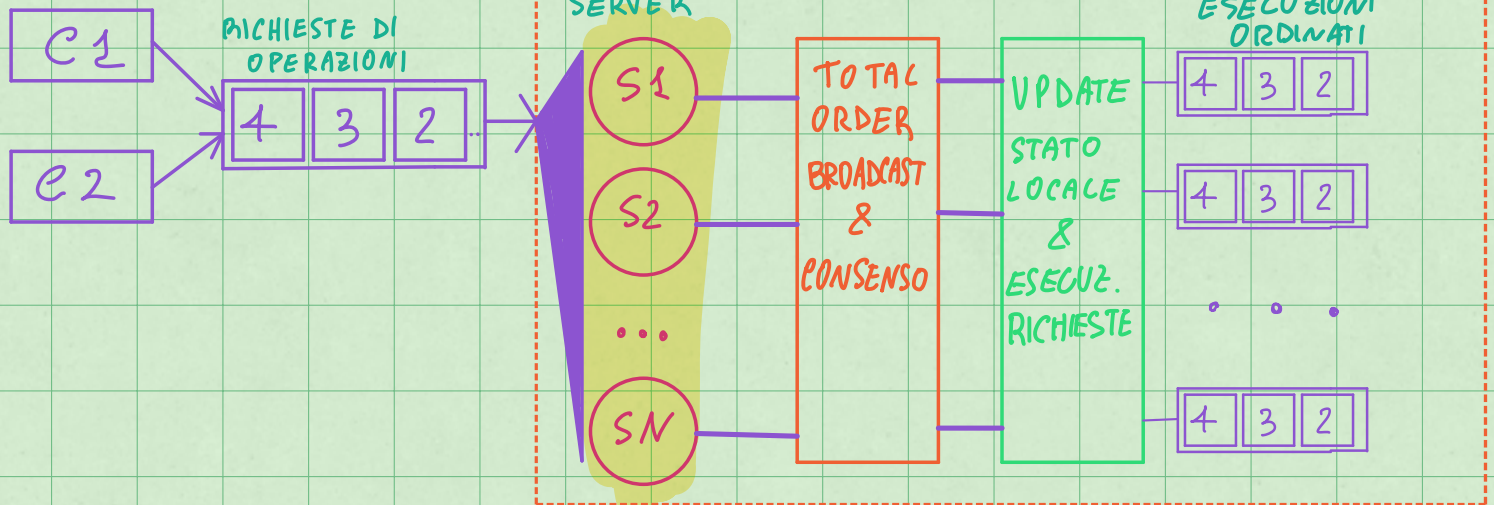
GRUPPO CLIENT



CONSORZIO SERVER

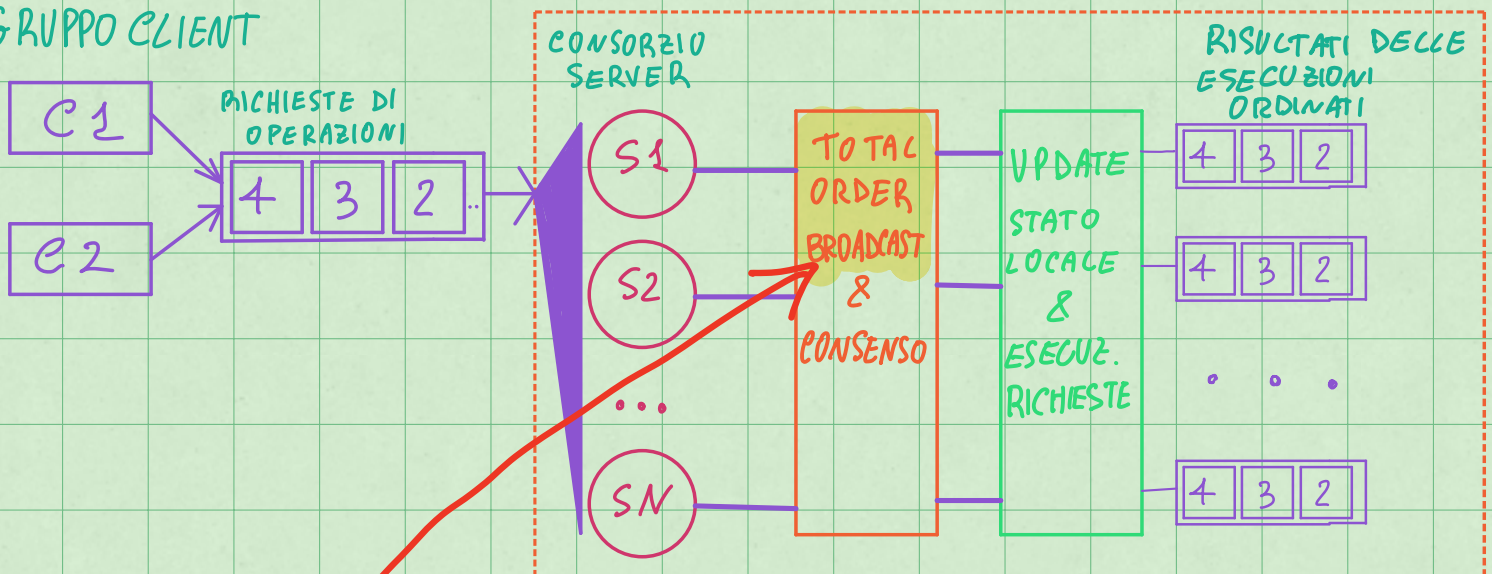


GRUPPO CLIENT



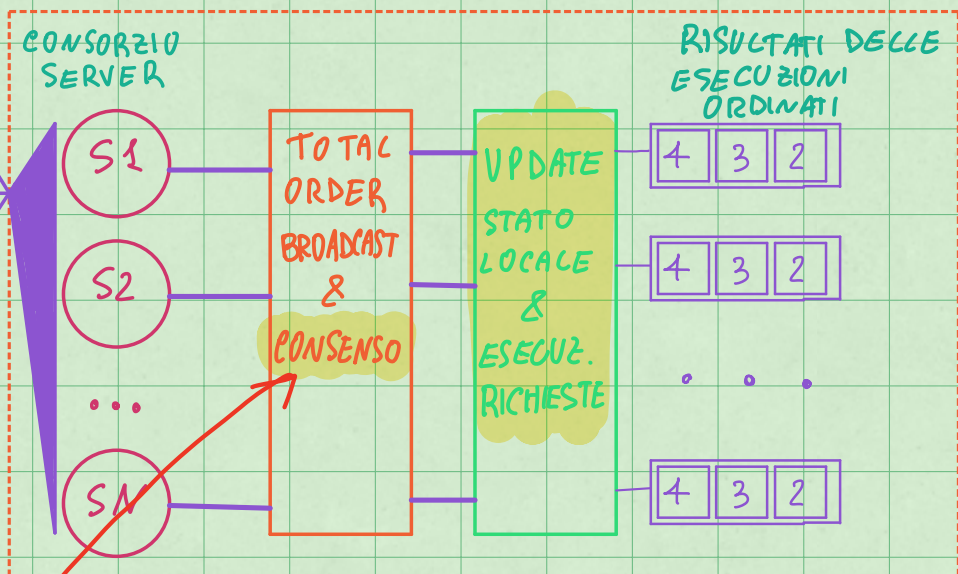
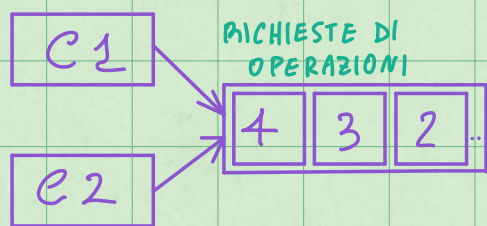
Tutti i Server iniziano con lo stesso stato iniziale

GRUPPO CLIENT



l'invio delle richieste di operazioni viene fatto in ordinamento Totale. In questo modo tutti i server ricevono le richieste nello stesso ordine con le quali le riceve un altro server.

GRUPPO CLIENT



Tutti i server prima di eseguire le richieste devono arrivare a consenso sull'ordine delle richieste di operazione per come le hanno ricevute, una volta ottenuto i server aggiornano il loro stato locale ed eseguono le richieste.

Conclusioni:

Se Tutti i server hanno ricevuto le stesse richieste, nello stesso ordine, allora eseguendole, tutti otterranno gli stessi risultati.