CENTRO REGIONALE
INFORMATION COMMUNICATION TECHNOLOGY
CERICT SCRL

Soluzione per la **Certificazione delle transazioni** adottata in ambito **Smart Mobility** per il progetto MyWay2Go di R&D

Tecnologia Blockchain

Argomenti trattati:

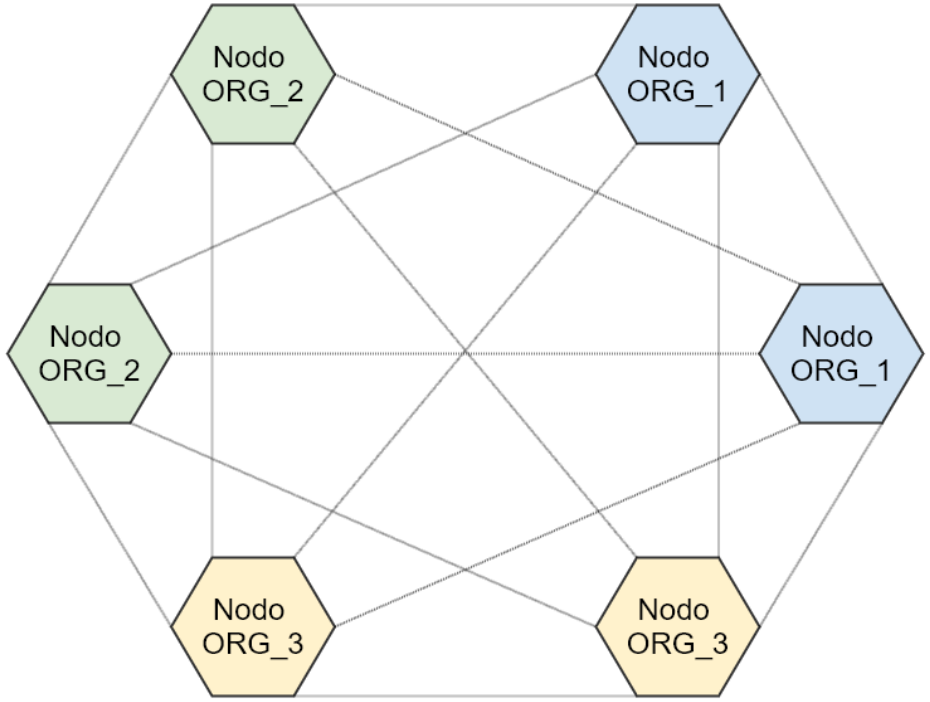
1. Introduzione alla **tecnologia BlockChain** ed ai suoi ambiti di utilizzo.
2. Introduzione alla problematica del progetto R&D **MyWay2Go** (tematiche di Smart City e **Mobility as a Service**)
3. Utilizzo di **Hyperledger Fabric** come soluzione adottata per la certificazione delle transazioni generate in MyWay2Go
4. **Analisi prestazionali** della soluzione individuata

Che cos’è una Blockchain

Una Blockchain (anche BT) è un sistema distribuito realizzato da una rete di nodi, che utilizzano un registro di record (ledger) condiviso. Tale sistema consente la memorizzazione permanente e la **certificazione di transazioni** di natura digitale.

Ognuno dei nodi della rete Blockchain memorizza una copia del ledger condiviso, e contribuisce all’aggiunta di nuove transazioni mediante **meccanismi di consenso** che utilizzano strumenti crittografici.

I nodi posso essere raggruppati in **organizzazioni** che includono le differenti tipologie di attori che partecipano al processo di certificazione delle transazioni memorizzate.



Proprietà delle transazioni certificate

La certificazione delle transazioni digitali riguardanti dati sensibili ottenuta adoperando un sistema come Blockchain, si realizza mediante il raggiungimento delle seguenti proprietà dei dati registrati nel ledger condiviso:

- **Non modificabilità**
- **Non ripudiabilità**
- **Nessuna possibilità di traslare nel tempo il verificarsi dell'evento**

Tali proprietà sono raggiunte mediante l'utilizzo di strumenti di crittografia e meccanismi di consenso e di memorizzazione. La certificazione ottenuta dall'utilizzo della BT, determina la **tracciabilità dei passi compiuti in un determinato processo**, e ne aumenta la **trasparenza**. Bisogna ricordare che i meccanismi di crittografia a chiave pubblica utilizzati, possono garantire **privatezza e riservatezza** del dato.

Come funziona (1/2): transazioni e blocchi

I **blocchi** sono insiemi di transazioni registrate nella rete Blockchain, che si collegano tra di loro formando una catena:

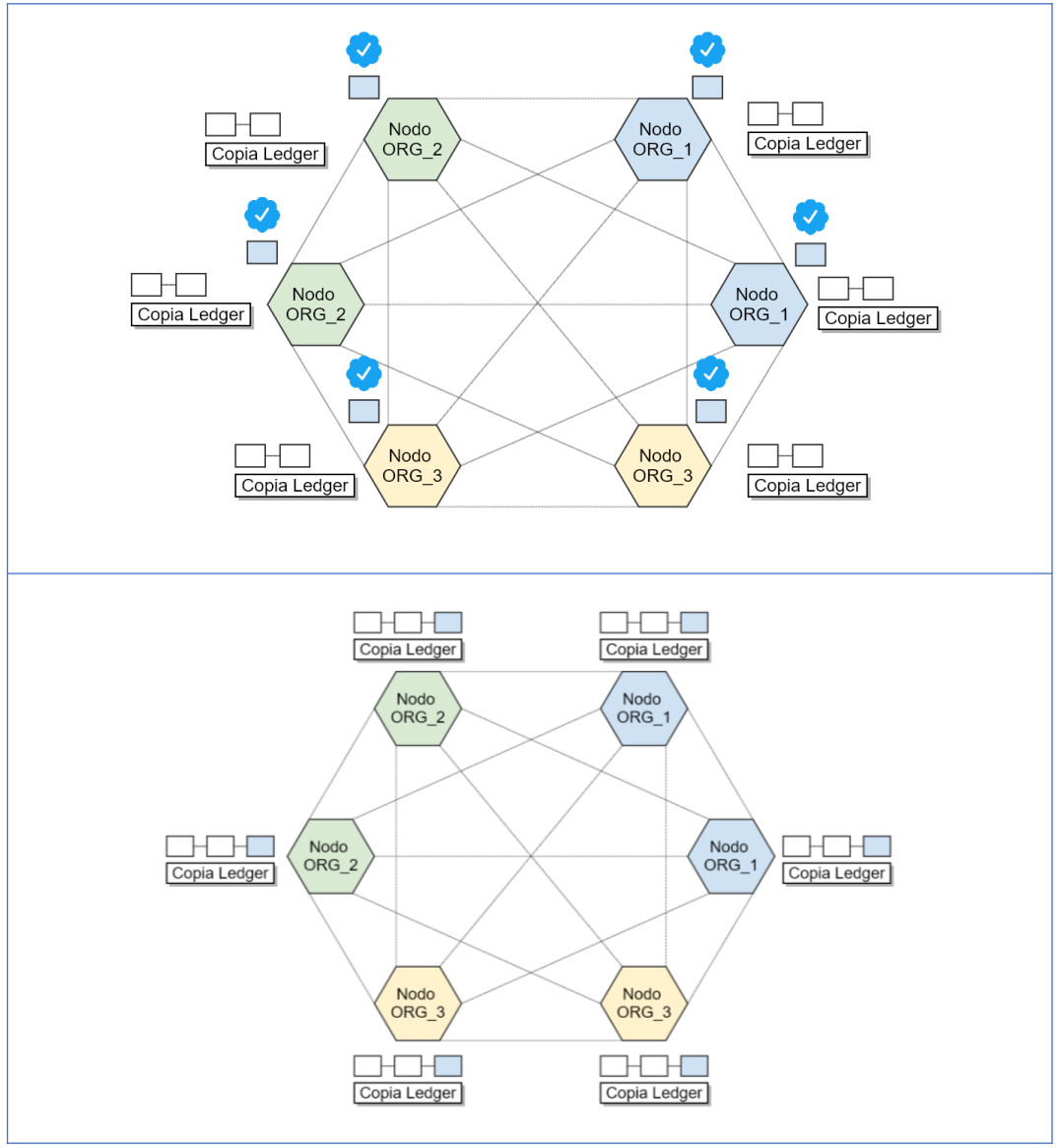
- Ogni blocco racchiude un certo numero di transazioni.
- Ogni blocco genera un'impronta digitale del proprio contenuto (hash).
- Ogni blocco si collega al precedente, mediante l'impronta digitale di quest'ultimo.

La catena di blocchi così costruita da luogo al registro distribuito (Ledger).

Come funziona (2/2): aggiunta del blocco

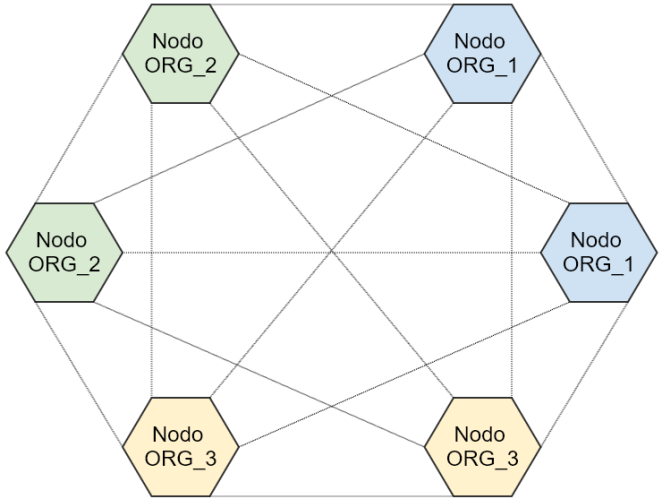
Quando viene creato un nuovo blocco, deve essere aggiunto correttamente al ledger distribuito della rete BT. Per far si che ciò avvenga c'è bisogno della **verifica** da parte dei nodi coinvolti e del raggiungimento del **consenso**.

- Il nuovo blocco di transazioni viene creato come visto al passo precedente.
- Il nuovo blocco viene inviato a tutti i nodi partecipanti alla rete.
- I nodi che ricevono il blocco possono effettuare verifiche sullo stesso.
- I nodi avviano il meccanismo di **consenso** (ad es. Proof-of-Work) che porterà ad accettare o rigettare il nodo.
- In caso di consenso raggiunto il nuovo nodo viene **aggiunto a tutte le copie del ledger** distribuite tra i nodi.

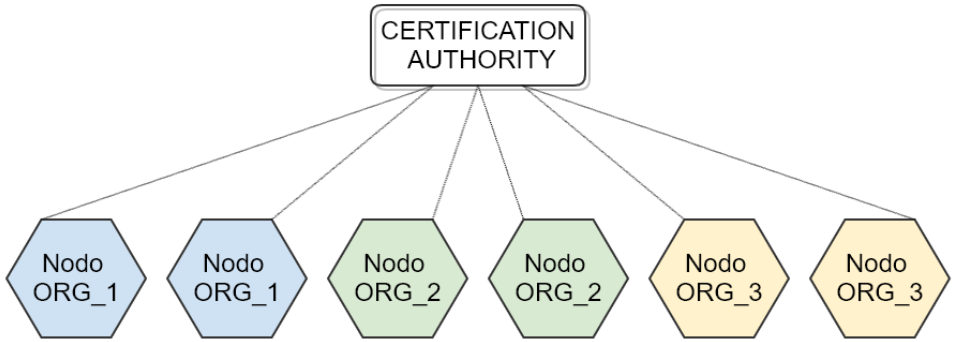


Approccio decentralizzato VS centralizzato

- Più economico
- Possibilità di introdurre nuove soluzioni per le community
- Fiducia nella rete dove ogni nodo contribuisce (controllo attivo)
- Possibilità di riutilizzare sottoinsiemi di informazioni generate da sistemi verticali (Silos)
- Realizzare applicazioni che richiedono Identità digitale.



- Costoso
- Necessità di fidarsi di una terza parte esterna (atto di fede)
- Unica copia centralizzata delle transazioni
- Performance più efficienti



Settori di applicazione

Gran parte delle industrie possono trarre benefici dall'impiego dei distributed ledger. Esistono parecchi casi di utilizzo commerciale delle blockchain, con transazioni che vengono automaticamente verificate e organizzate da una piattaforma decentralizzata che non richiede la supervisione di un ente o di un soggetto centrale (super partes), pur garantendo la resistenza a manomissioni e frodi.

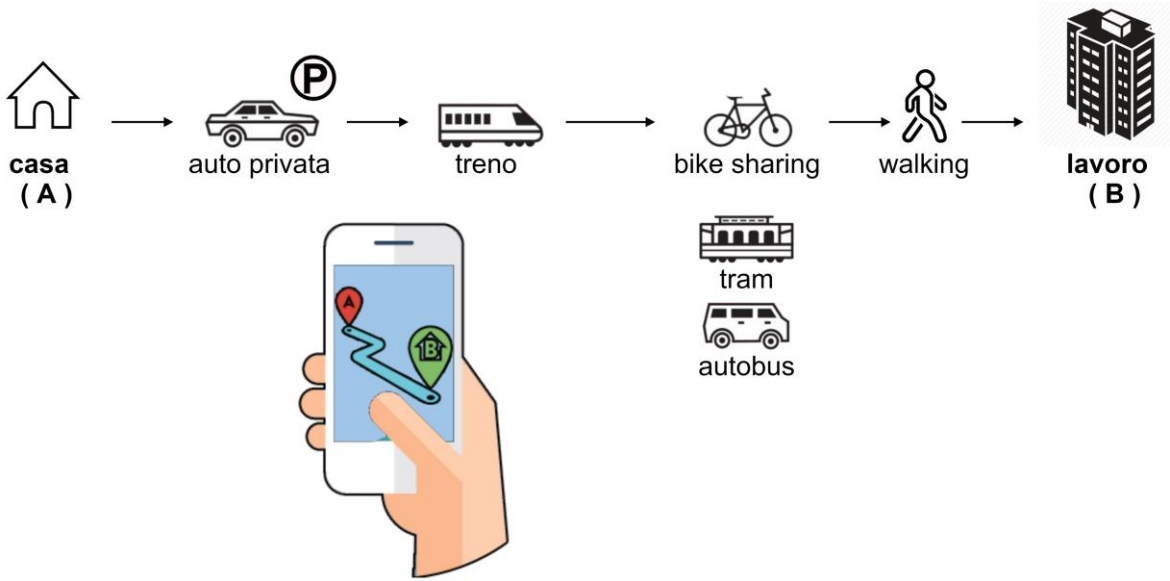
Banking e finance. Pagamenti e trasferimenti di denaro. Cybersecurity e Risk Management. Scuola e mondo accademico. Legittimazione del voto elettorale: e-voting. Leasing e compravendita di automobili. Networking e IoT. Analisi finanziarie, scommesse sportive e attività di previsione. Musica online.	Car sharing. Compravendita di azioni. Compravendita immobiliare. Assicurazioni. Sanità. Supply Chain. Management/Finance. Archiviazione di dati nel cloud. Gestione dell'energia. Sport.	Gift card e programmi di fidelizzazione. Enti governativi e pubblica amministrazione. Monitoraggio della compravendita di armi. Testamenti ed eredità. Vendita al dettaglio, mondo retail. Beneficienza e ONG. Forze dell'ordine e sicurezza. Gestione delle HR (risorse umane). Trasporti.

Fonte: https://www.blockchain4innovation.it/iot/blockchain-benefici-concreti-le-applicazioni-piu-promettenti-27-settori/

Il progetto MyWay2Go dell'aria R&D

MyWay2Go è una piattaforma tecnologica che affronta le tematiche dell'ambito **Smart Mobility** e che implementa un modello di tipo **MaaS (Mobility as a Service)** impiegando differenti servizi di mobilità offerti da differenti operatori.

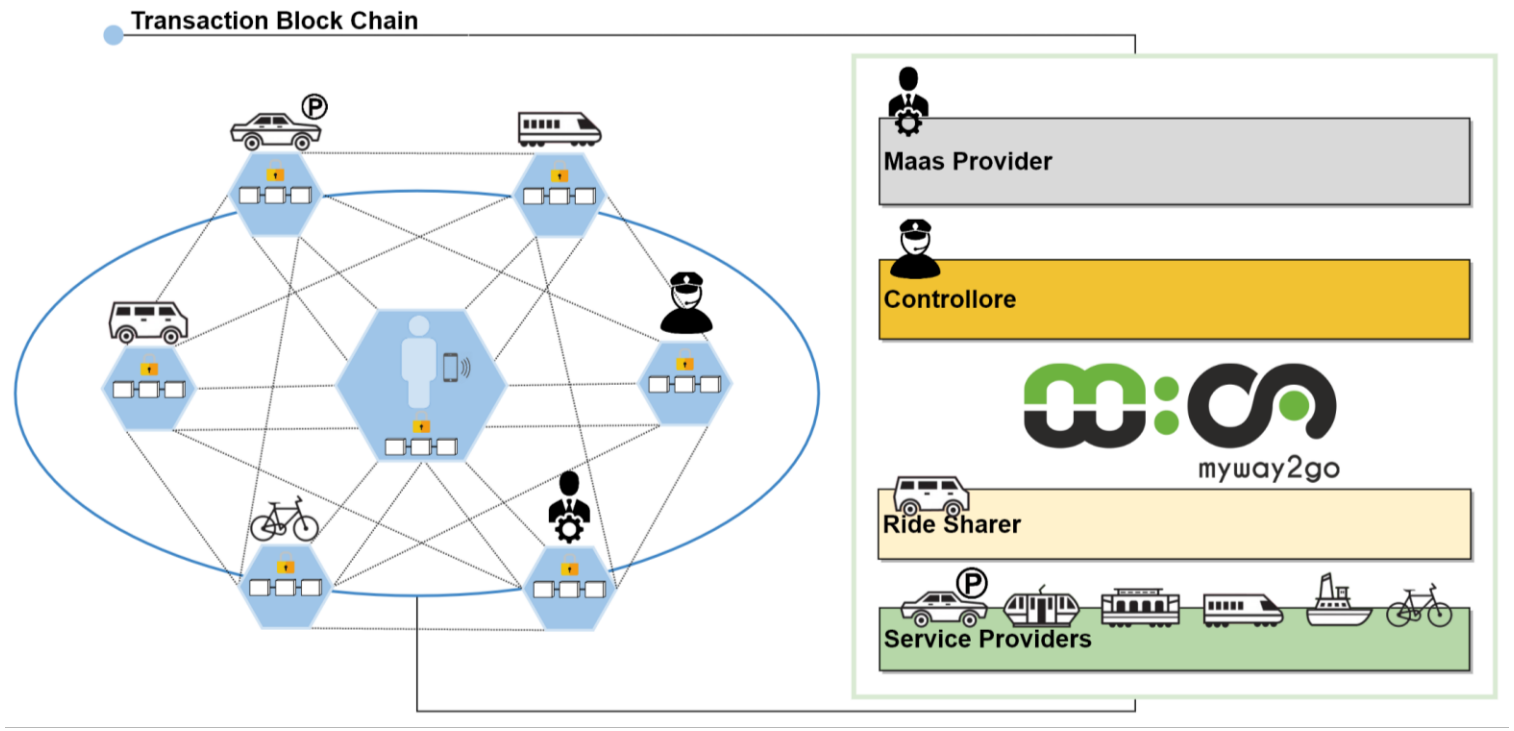
Il cittadino mediante l'utilizzo di **un'unica App mobile**, richiede alla piattaforma MyWay2Go di restituire un insieme di soluzioni intermodali per potersi spostare da un punto dipartenza ad un punto di destinazione. Il cittadino **fruisce dei servizi di mobilità che compongono il proprio itinerario e paga i titoli di viaggio corrispondenti** utilizzando sempre e solo l'applicazione mobile del sistema MyWay2Go. Tali dinamiche generano **movimenti finanziari** e la necessità di rendicontazioni tra le parti interessata, nonché la necessità per tutti gli attori coinvolti di avere la **certificazione degli eventi (transazioni) che generano tali movimenti**.



BT per la certificazione delle transazioni di MyWay2Go

Gli attori del sistema MyWay2Go coinvolti nelle dinamiche di un percorso intermodale sono:

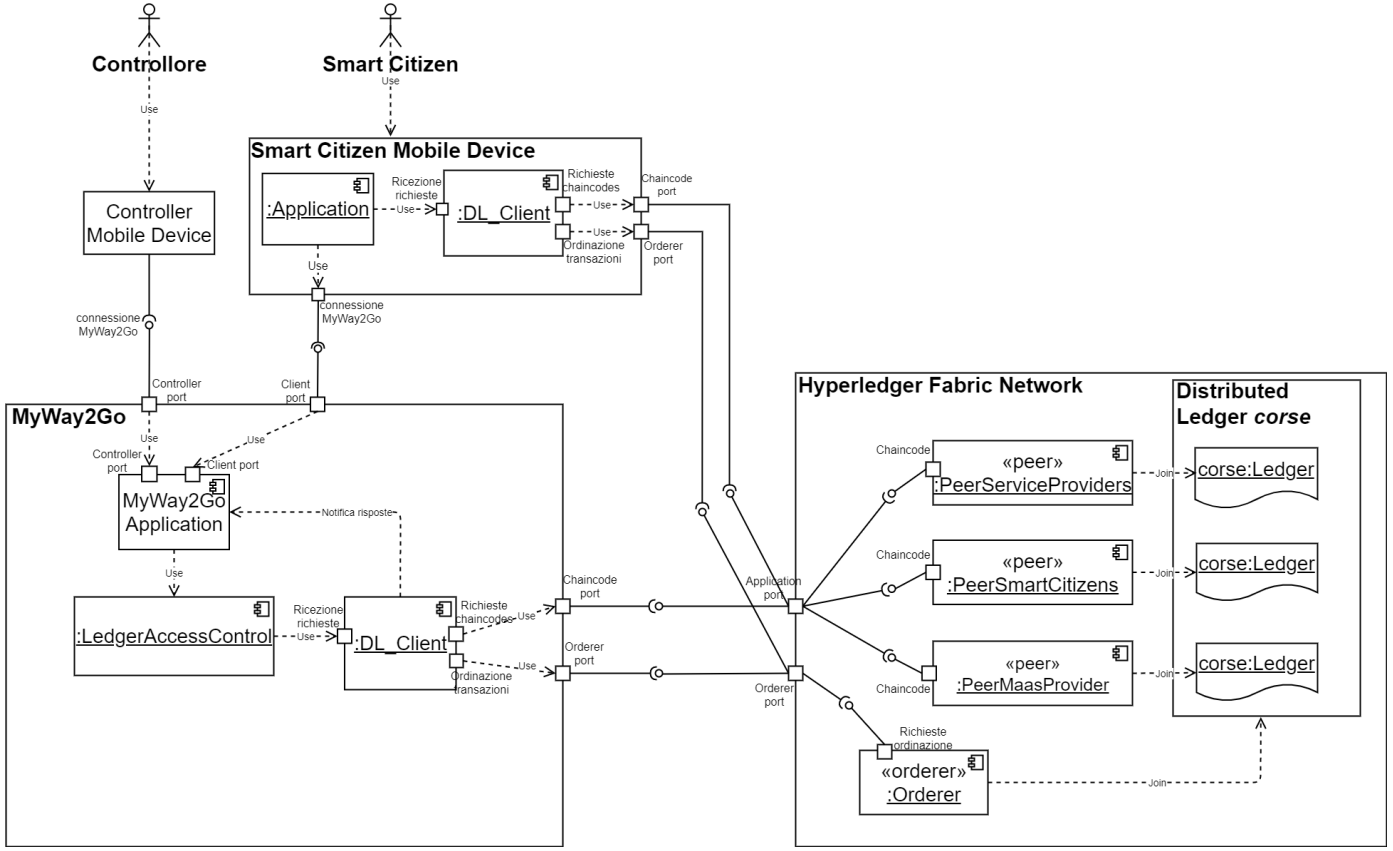
- Lo **Smart Citizen** che utilizza la app del sistema per i suoi spostamenti.
- I **Service Provider** che offrono i propri servizi di mobilità (bus, tram, parcheggio, car-sharing, ecc …)
- I **Ride Sharer** che offrono servizi di mobilità a chiamata (Taxi, Uber).
- Il **Controllore** che tramite app verifica il possesso dei titoli di utilizzo del servizio da parte dello Smart Citizen.
- Il **Maas Provider**, che gestisce la piattaforma di tipo MaaS, spesso coincide con le amministrazioni territoriali.



Soluzione tecnologica adottata in MyWay2Go

Hyperledger Fabric Network:

- 3 peers (**MaaSProvider, SmartCitizens e ServiceProviders**);
- Ogni peer ha una copia del ledger corse;
- Gli Smart Citizens inviano le richieste di **iniziaCorsa** e **fineCorsa**;
- Tutti i peers devono convalidare le richieste;
- Orderer rappresenta il servizio di ordinamento, composto da tre orderers (**crash fault tolerant**);
- **TLS** attivo per tutte le comunicazioni.



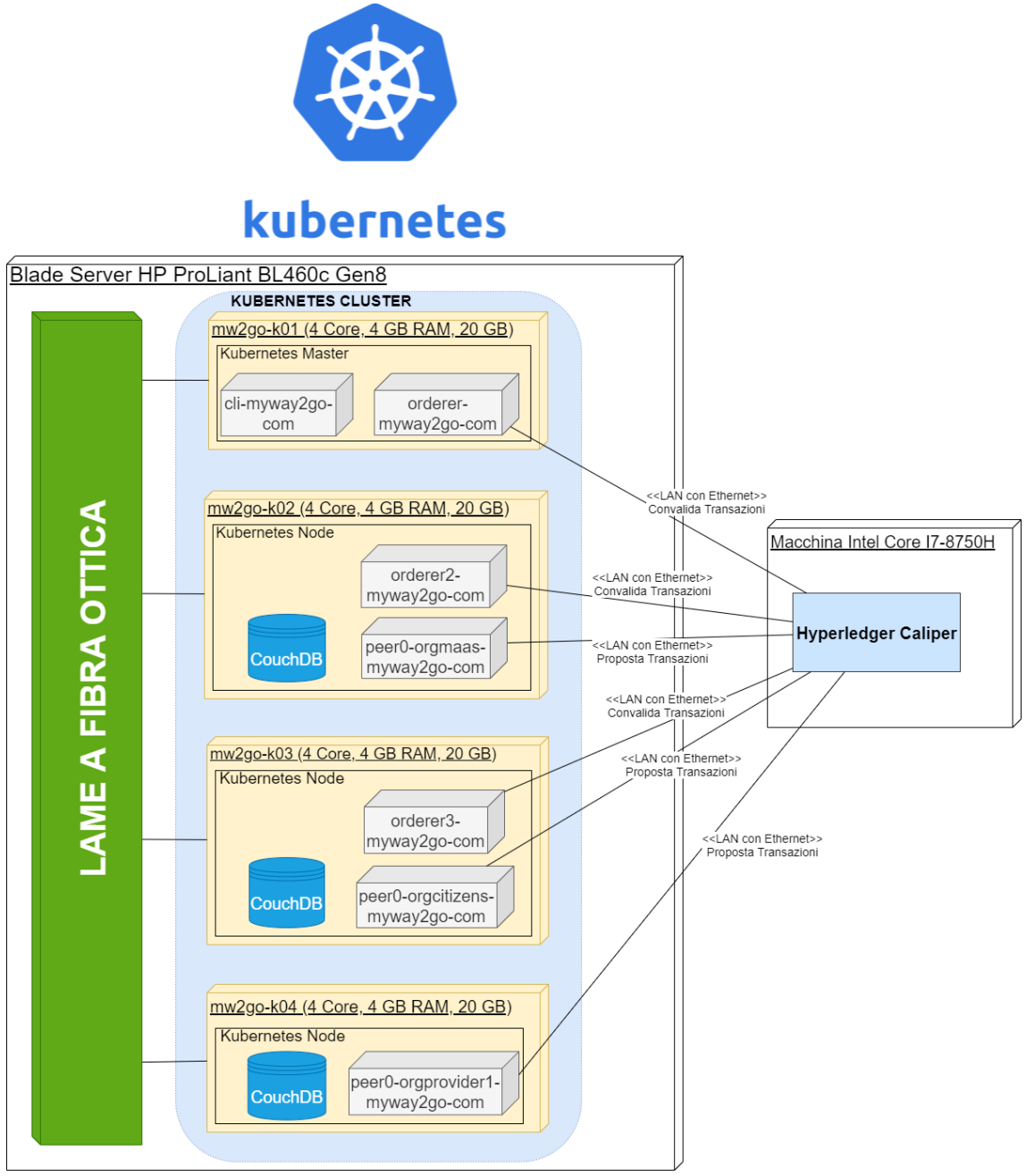
Deploy in Cloud della rete Hyperledger

È stata effettuao il deploy della soluzione utilizzando un cluster **Kubernetes**, soluzione adottata in molti casi industriali, composto da 4 macchine che ospitano la rete Hyperledger:

- mw2g0-k01 esegue un orderer e la command line interface (cli);
- mw2go-k02 e mw2go-k03 eseguono ciascuna un peer, il database associato per il world state e un orderer;
- mw2go-k04 esegue un peer e il database associato per il world state.

Caratteristiche delle macchine:

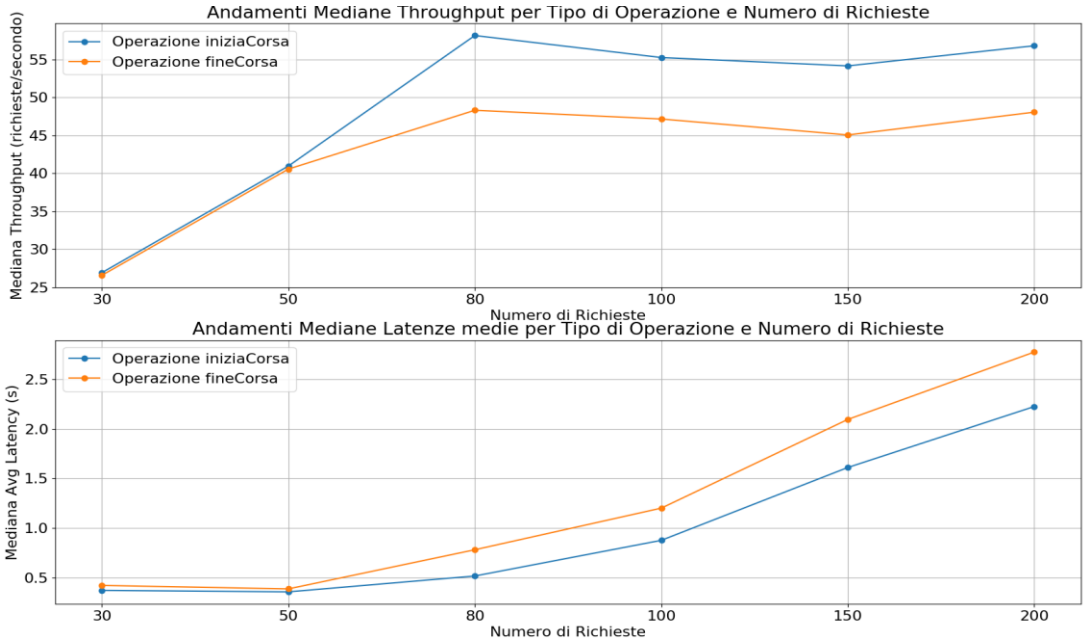
- Processore 4 core;
- RAM 4 GB;
- Disco 20 GB;
- Ubuntu 18.04 LTS.



Analisi delle prestazioni della rete Hyperledger: definizione dei parametri

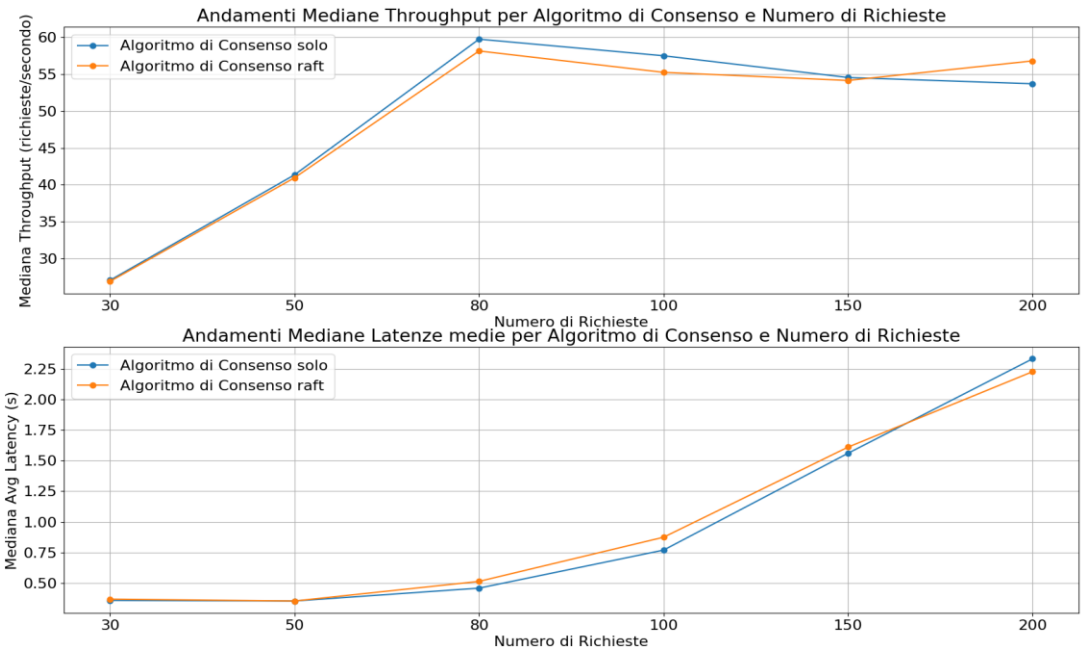
Parametro	**Valori**
Tipo di operazione	- Solo scrittura (richieste di tipo *iniziaCorsa*) - Lettura e scrittura (richieste di tipo *fineCorsa*)
Endorsement Policy	- AND (risposta da tutti i peers) - OR (risposta da un solo peer)
Algoritmo di consenso	- Solo - Raft
Database World State	- CouchDB - LevelDB
Dimensione blocchi	- 10 transazioni - 20 transazioni - 50 transazioni - 100 transazioni

Analisi delle prestazioni della rete Hyperledger: Latenze e Throughput per Tipo di Operazione e Algoritmo di Consenso



Mediane misurate all'aumentare del numero di richieste variando le operazioni in ingresso.

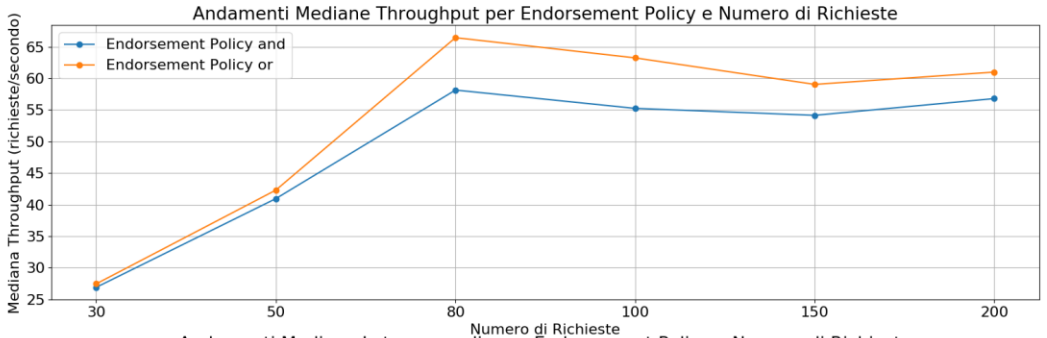
Operazione	Usable Capacity	Throughput	Latenza Media
iniziaCorsa (blu)	80 ric/s	58,15 ric/s	0,51 s
fineCorsa (arancione)	80 ric/s	48,3 ric/s	0,78 s

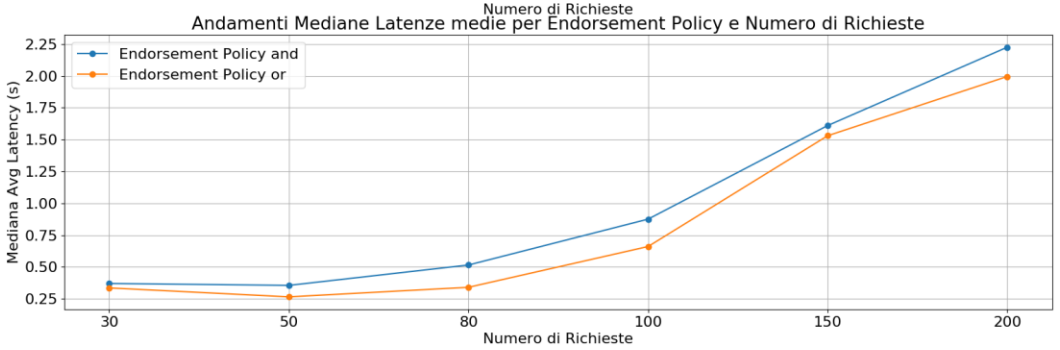


Mediane misurate all'aumentare del numero di richieste variando il numero di orderers.

Algoritmo di Consenso	Usable Capacity	Throughput	Latenza Media
Solo (blu)	80 ric/s	59,75 ric/s	0,46 s
Raft (arancione)	80 ric/s	58,15 ric/s	0,51 s

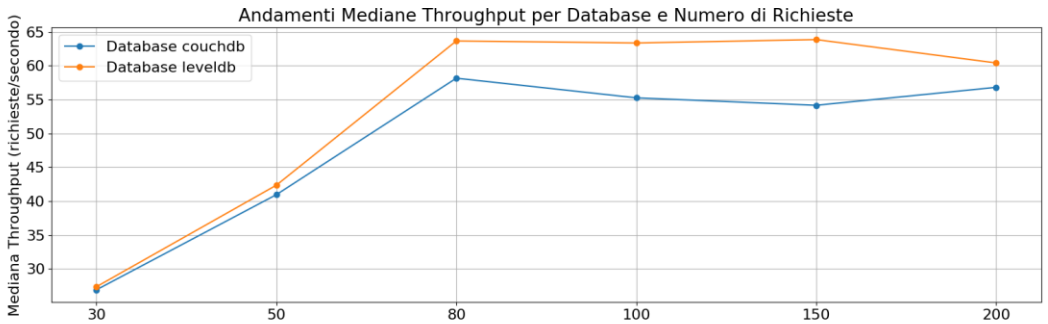
Analisi delle prestazioni della rete Hyperledger: Latenze e Throughput per Endorsement Policy e Database World State

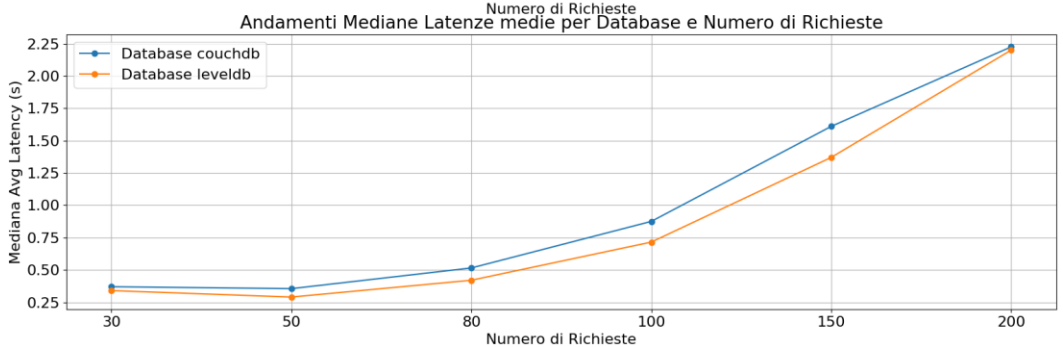




Mediane misurate all'aumentare del numero di richieste variando le operazioni in ingresso.

Operazione	Usable Capacity	Throughput	Latenza Media
AND (blu)	80 ric/s	58,15 ric/s	0,51 s
OR (arancione)	80 ric/s	66,45 ric/s	0,34 s

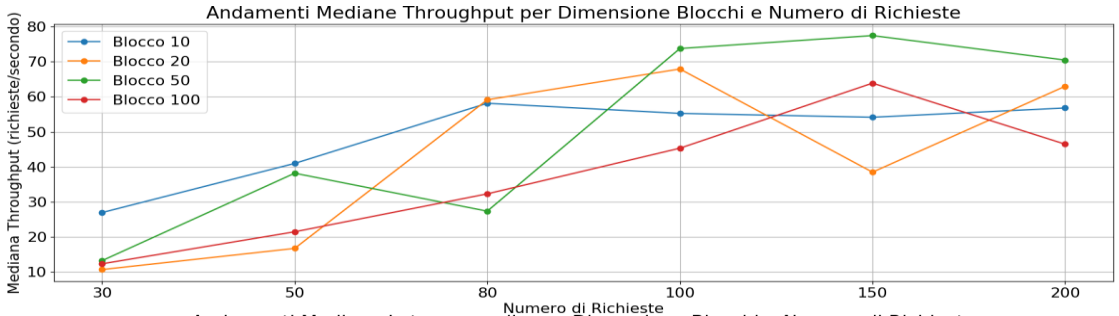


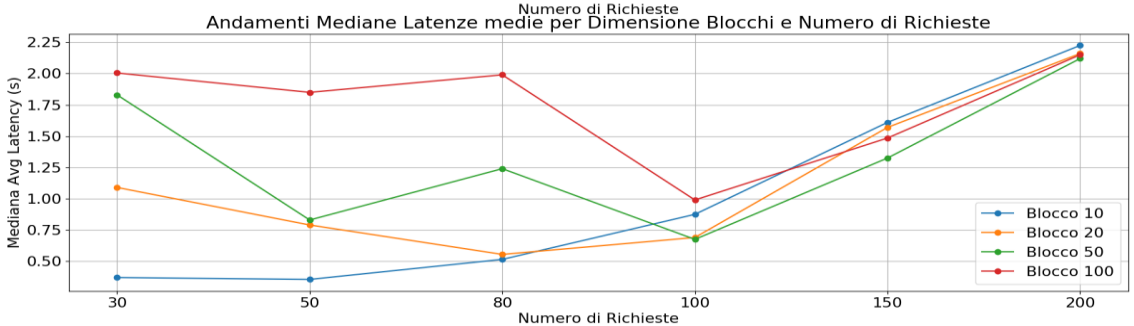


Mediane misurate all'aumentare del numero di richieste variando il database per il world state.

Algoritmo di Consenso	Usable Capacity	Throughput	Latenza Media
CouchDB (blu)	80 ric/s	58,15 ric/s	0,51 s
LevelDB (arancione)	80 ric/s	63,65 ric/s	0,42 s

Analisi delle prestazioni della rete Hyperledger: Latenze e Throughput per Dimensione Blocchi





Mediane misurate all'aumentare del numero di richieste variando il numero di transazioni per blocco.

- Con basso carico i blocchi di piccole dimensioni sono convalidati velocemente (se non ci sono abbastanza transazioni da riempire il blocco, l'ordering service attende un timeout che aumenta i tempi di risposta);
- All'aumentare del numero di richieste le prestazioni dei blocchi grandi migliorano.

Dimensione Blocco	Usable Capacity	Throughput	Latenza Media
10 (blu)	80 ric/s	58,15 ric/s	0,51 s
20 (arancione)	100 ric/s	67,95 ric/s	0,69 s
50 (verde)	100 ric/s	73,8 ric/s	0,67 s
100 (rosso)	150 ric/s	63,9 ric/s	1,48 s

Caso di studio città di Salerno (1/2): Dati degli spostamenti

Lo studio intitolato **Il Sistema di Trasporto della città di Salerno***, effettuato dal laboratorio di Analisi di Sistemi di Trasporto dell'Università di Salerno nel 2019, ha analizzato i dati degli spostamenti sistematici per motivi di studio o lavoro effettuati da e verso la città riportati nell'ultimo censimento ISTAT del 2011. In tabella sono riportati gli spostamenti divisi per orario:

Orari	Spostamenti Interni-Interni	Spostamenti Esterni-Interni	Spostamenti Interni-Esterni	Tutti gli Spostamenti
Prima delle 7:15	7015	16080	3936	27031
Dalle 7:15 alle 8:14	25387	12992	6318	44697
Dalle 8:15 alle 9:14	9910	2794	1584	14288
Dopo le 9:15	2421	1751	672	4844

Su un totale di 90860 spostamenti 44697 (circa il 49%) sono effettuati nell'ora di punta che va dalle 7:15 alle 8:14.

Nella soluzione MyWay2Go ad ogni spostamento sono associate le due richieste di inizio e fine corsa, nel caso peggiore in cui tutti gli spostamenti hanno una durata inferiore a 60 minuti il carico sottoposto al sistema è di 89394 richieste nell'ora di punta, che se distribuite uniformemente corrispondono a circa 25 richieste al secondo.

* http://www.comune.salerno.it/allegati/29791.pdf

Caso di studio città di Salerno (2/2): Confronto con prestazioni MyWay2Go

Come riportato dai grafici il cluster utilizzato riesce a gestire il carico presentato e può sopportare anche un numero maggiore di richieste al secondo in arrivo in quanto per tutte le configurazioni dei parametri considerate l'usable capacity è uguale o superiore a 80. In tabella sono riportati i risultati ottenuti con un carico di 30 richieste al secondo in ingresso usando la configurazione di default utilizzata per i test, avente le seguenti caratteristiche:

- **Endorsement Policy:** AND;
- **Algoritmo di Consenso:** Raft;
- **Database:** CouchDB;
- **Dimensione Blocchi**: 10 transazioni.

Operazione	Numero Richieste in Ingresso	Mediana Throughput	Mediana Latenza Media
iniziaCorsa	30 ric/s	26,9 ric/s	0,37 s
fineCorsa	30 ric/s	26,55 ric/s	0,42 s

Conclusioni

La soluzione proposta permette alle tre entità smart citizens, MaaS provider e service providers di raggiungere il consenso sugli eventi e di calcolare i costi in base ad essi in modo trasparente, semplificando il lavoro della piattaforma e rappresentando una garanzia sia per i cittadini che per gli operatori del trasporto.

I test mostrano che per la configurazione di rete utilizzata i risultati di latenza e di throughput sono abbastanza indipendenti dalla scelta di configurazione riguardante l'algoritmo di consenso, che il database per il world state e l'endorsement policy hanno un piccolo impatto, e che invece esiste una dipendenza dal dimensionamento del blocco e dal tipo di richieste inviate alla blockchain. È possibile migliorare le prestazioni modificando la configurazione della rete dinamicamente in funzione del carico partendo dalle analisi sul territorio effettuate, oppure aumentando la dimensione della rete ed includendo un numero maggiore di peers per organizzazione in modo da parallelizzare l'esecuzione delle richieste.