ABSTRACT

Rendere una città più intelligente ha lo scopo di migliorare numerosi aspetti della stessa: gestione delle risorse, efficienza nel caso di interventi, qualità dei servizi offerti ai cittadini, sicurezza delle infrastrutture e molto altro.
La realizzazione di questo paradigma richiede l'utilizzo di diverse tipologie di sensori elettronici IoT che si occupano di acquisire dati inerenti a: traffico stradale, inquinamento, temperatura e così via.
L'insieme di questi sensori non è gestito da una singola entità (es. il comune), bensì ogni organizzazione facente parte della città si occupa di gestire il proprio sottoinsieme di questi dispositivi, condividendo poi i dati raccolti col comune.
L'approccio è quindi multi-tenant e federato , non centralizzato.
Il comune funge da decision maker centrale, il quale ottiene i dati raccolti dalle varie organizzazioni ed ha lo scopo di inferire conoscenza utile al fine di migliorare le politiche ed i servizi offerti nell'ambito della città, ad esempio migliorando l'efficienza con cui le forze dell'ordine intervengono in caso di necessità, monitorare la sicurezza dei parchi e delle strade, controllare il traffico ed intervenire istantaneamente in caso di incidenti.
Realizzare questo paradigma porta numerose sfide: i dati devono essere protetti da accessi non autorizzati e da usi maliziosi, è necessario introdurre politiche di controllo degli accessi utili per definire chi può accedere a quali dati.
Prima dell'avvento della tecnologia Blockchain l'utilizzo di database per memorizzare i dati e le politiche di accesso portava il problema di dover mantenere la consistenza di queste informazioni in un sistema distribuito asincrono quale è Internet, problema che mira ad essere risolto dalla tecnologia Blockchain.
In questo lavoro di tesi si illustrano le tradizionali soluzioni adottate per realizzare il paradigma di città smart e di tutti i problemi derivanti da queste prima dell'avvento della tecnologia Blockchain, per poi introdurre una nuova soluzione che faccia uso della Blockchain e del paradigma della Self Sovereign Identity(SSI) al fine di risolvere questi problemi.
Si spiegano nel dettaglio i componenti che insieme rendono possibile la realizzazione della SSI, le funzioni crittografiche necessarie, i protocolli di comunicazione, la tecnologia Blockchain ed i progetti Hyperledger per realizzare applicazioni basate su queste tecnologie.
La soluzione così proposta viene poi implementata utilizzando Hyperledger Aries (tool per la creazione di applicazioni basate sul paradigma della SSI) ed Arduino (scheda elettronica programmabile utilizzata per simulare un sensore elettronico) e spiegata nel dettaglio mostrando le interazioni tra le entità partecipanti al sistema.