

## Tracciamento di filiere industriali tramite blockchain

La tecnologia della blockchain trova una delle sue applicazioni nel ruolo di "notaio digitale". Questo è possibile poiché l'algoritmo di validazione delle informazioni è autonomo e non influenzabile esternamente.

Nel caso d'uso in esame abbiamo un sistema che raccoglie informazioni sulle varie fasi di una filiera industriale su server privato, per poi tracciarne lo stato tramite transazioni sulla blockchain di Bitcoin. Il sistema inoltre implementa sia un metodo di report profilato dei tracciamenti eseguiti su blockchain, sia un metodo di verifica dei report, il quale fa riferimento unicamente alla blockchain e non dipende dal sistema privato che l'ha generato. È quindi possibile validare ogni step del processo industriale in maniera agnostica rispetto al sistema, garantendo un certo grado di trasparenza e affidabilità.

Il server privato che raccoglie i dati è un potenziale punto di vulnerabilità dell'architettura, la tesi consiste nello studio di una possibile evoluzione dell'attuale architettura, utilizzando una tecnologia chiamata sidechain privata, ovvero una blockchain "secondaria", affiancabile a quella principale (es. Bitcoin/Ethereum). L'introduzione della sidechain sarà a supporto (o sostituzione) del server privato per la raccolta dei dati.

Opzionalmente si realizzi un applicativo PoC che mostri quanto studiato.

## Studio sull'uso di smart contract nelle architetture a oracoli

Alcune implementazioni della tecnologia blockchain permettono l'esecuzione di smart contract, ovvero programmi eseguiti dai nodi della rete le cui operazioni sono transazioni della blockchain a tutti gli effetti. Essendo la blockchain un sistema isolato, è impossibile per uno smart contract comunicare con servizi o sistemi esterni. Per ovviare al problema si utilizzano gli oracoli, applicazioni che attingono informazioni da fonti affidabili e le iniettano nella blockchain.

Utilizzando smart contract e oracoli si vuole studiare un sistema di decision making applicato al turismo. Lo scenario prevede che sia possibile effettuare prenotazioni nel settore alberghiero, le quali verranno confermate o annullate in base al meteo della zona di interesse. La logica di conferma o annullamento delle prenotazioni è in questo caso incapsulata nello smart contract, ottenendo così una validazione autonoma e non influenzabile esternamente. Analogamente, le informazioni sul meteo verranno fornite tramite un oracolo, per far sì che siano attendibili e disponibili allo smart contract.

La tesi consiste nel definire l'architettura del sistema in esame a partire dal processo di prenotazione in essere. Opzionalmente si realizzi un applicativo PoC che mostri quanto studiato.

## Studio sul ledger distribuito IOTA

IOTA è un ledger distribuito progettato per registrare ed eseguire transazioni tra dispositivi nell'ecosistema IoT (Internet of Things). L'innovazione chiave di IOTA è il Tangle, un sistema di nodi su cui si basa tutta la logica della rete e che sostituisce la più nota blockchain.

La tesi consiste nel tracciare lo stato dell'arte del ledger distribuito IOTA.

In particolare, si richiede di:

- descriverne l'architettura (fondata sul concetto di tangle)
- evidenziare le principali e più significative differenze con altre DLT (distributed ledger technology) e blockchain
- riportare e schematizzare informazioni sui principali tool per lo sviluppo e l'integrazione di applicazioni (es. SDK)
- applicazioni note e casi d'uso (es. progetti su GitHub)

Opzionalmente si realizzi un applicativo PoC che permetta di connettersi a IOTA come client (effettuare/leggere transazioni).