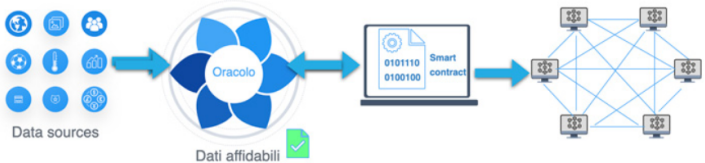
Politecnico di Torino
Dipartimento di Scienze Matematiche "G. L. Lagrange"

DISMA
ECCELLENZA 2018•2022

Presented By:
Attanasi Alessio
Buccelli Giorgia
Cannistrà Maria
El Amrani Rachid

Introduzione



- Gli smart contracts estendono la funzionalità di una blockchain ma sono in alcuni casi limitati, non potendo interagire con dati e sistemi esterni.
- Gli oracoli fanno da ponte tra mondo reale e blockchain.

Le tappe fondamentali

1. 2017: Primo whitepaper
2. 2019: Lancio ufficiale e registrazione del marchio
3. 2021: Chainlink 2.0

- Fondatori: Sergey Nazarov e Steve Ellis

Potenzialità e rischi

Potenzialità:

- Spina dorsale per l'intera tecnologia blockchain.
- È il primo operatore nonostante la concorrenza.
- Nessun limite alle possibili aree di applicazione.

Rischi:

- Non esiste una tabella di marcia fissa.
- Mantenere le partnership.
- Appiattimento dell'interesse per gli smart contract.

Architettura

- on-chain
- off-chain

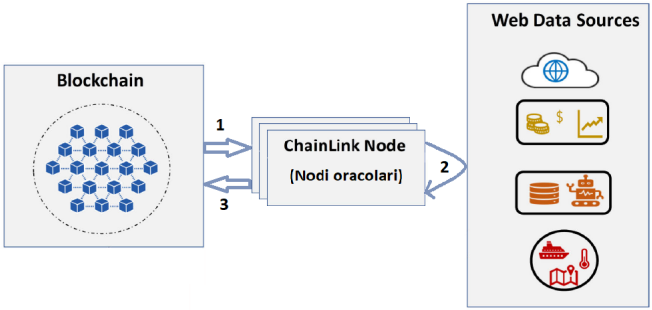


Figure: Esecuzione del flusso di lavoro

Architettura

On-chain

Smart contracts:

- USER-SC
  - *requesting contract*
- CHAINLINK-SC
  - *reputation contract*
  - *order-matching contract*
  - *aggregating contract*

Fasi di lavoro:

1. selezione oracolo/i
2. trasmissione dei dati
3. aggregazione dei risultati

Off-chain

Nodi oracolari:

- *Core adapters*
- *External adapters*

Flusso di lavoro

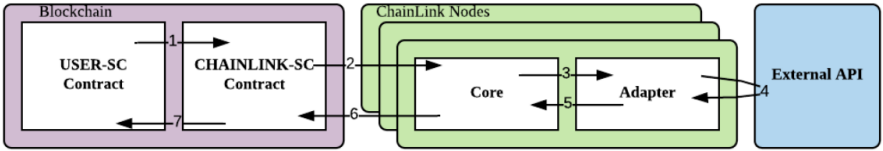


Figure: Flusso di lavoro ad alto livello

Off-Chain Reporting

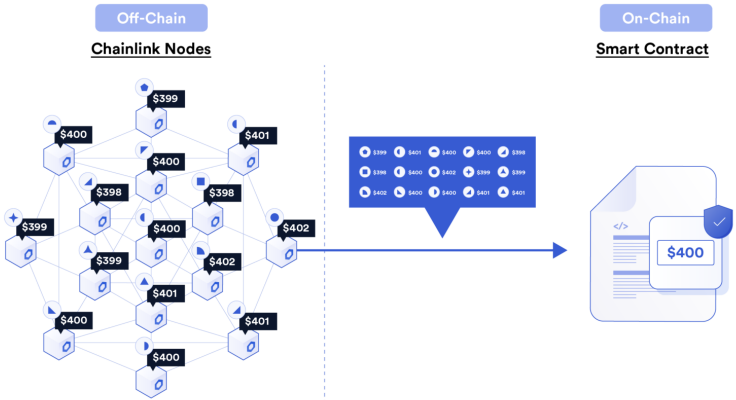


Figure: Chainlink off-chain reporting

Sicurezza dell'oracolo

Domanda: Perchè la sicurezza degli oracoli è così importante?

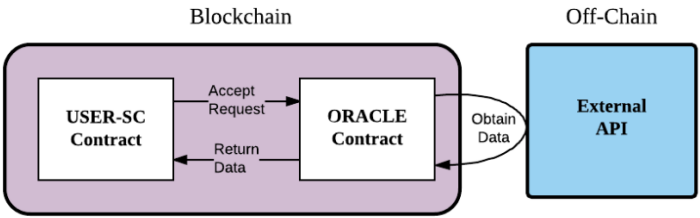
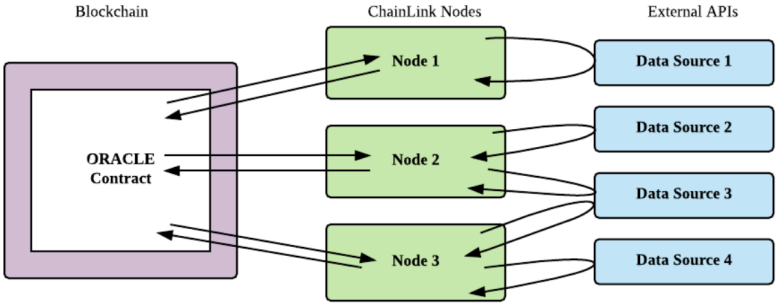


Figure: Comportamento di un oracolo ideale

Decentralizzazione

Si propongono due approcci complementari contro i nodi difettosi:

- Distribuzione delle sorgenti
- Distribuzione degli oracoli



ChainLink Security Services

ChainLink propone principalmente 3 key security services:

1. Validation System
   - *Monitoraggio On-Chain del comportamento dell'oracolo*
2. Reputation System
   - *Verifica integrità e controllo statistiche dell'oracolo*
3. Link (Token di ChainLink)
   - *funge da* ***token di utilità*** *per molteplici scopi sulla rete ed in particolare per premiare e pagare gli operatori dei nodi che convalidano le transazioni*

Grazie per l'attenzione

Politecnico di Torino