UNIVERSITÀ
POLITECNICA
DELLE MARCHE

DII
Dipartimento di Ingegneria
dell'Informazione

unimc

Vulnerabilità nella comunicazione tra Blockchain e mondo esterno

Sara Maraschio

Martedì 19 Luglio 2022

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

Cosa è la Blockchain

Cosa è la Blockchain

La Blockchain è un **registro distribuito**, strutturato come una catena di blocchi contenenti le transazioni, validate tramite un **meccanismo di consenso**, disponibile a tutti i nodi della rete.

L'**immutabilità** del registro, la **trasparenza**, la **sicurezza** basata su tecniche crittografiche e la **tracciabilità** delle transazioni sono le caratteristiche principali della tecnologia Blockchain.

L'obiettivo finale è la possibilità per i partecipanti alla rete di inserire e condividere dati, garantendo l'**autenticità** di questi, senza la presenza di un'autorità centrale (o intermediario).

Vulnerabilità

- ❑ Attacchi phishing
- ❑ Attacchi routing
- ❑ Attacchi Sybil
- ❑ Attacchi 51%

C’è tuttavia dell’altro…

Blockchain: sistema chiuso?

Blockchain: rete isolata

La Blockchain è una **rete isolata**.

L’isolamento di una Blockchain è la proprietà che la rende estremamente sicura e affidabile.

La rete deve solo fornire il consenso su una serie molto semplice di domande vero/falso utilizzando i dati già memorizzati al suo interno.

A volte però gli Smart Contract necessitano di informazioni esterne…

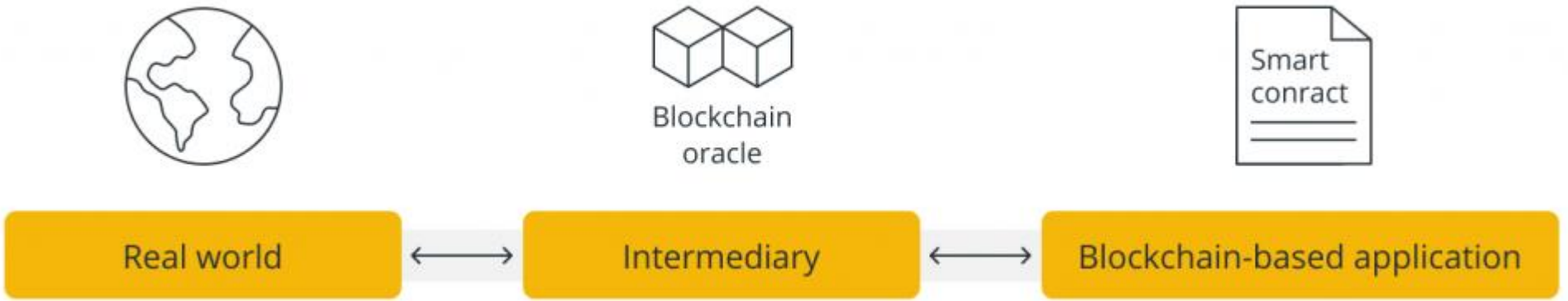
Problema dell'oracolo

Gli oracoli Blockchain sono uno degli strumenti per interagire con il mondo fisico e consentono di creare un ponte tra il mondo crittografico e quello fisico.

Un oracolo ha come funzione principale quella di essere un servizio attraverso il quale una Blockchain o uno Smart Contract attinge a informazioni esterne alla Blockchain su cui viene eseguito.

La sfida centrale nella progettazione di oracoli è il fatto che **se un oracolo viene compromesso, anche lo smart contract che si basa su di esso è compromesso.**

Problema dell’oracolo



Tipologie di Oracoli

- In entrata e in uscita
- Software e Hardware
- **Centralizzati e Decentralizzati**

Chainlink

Chainlink

Chainlink (rete decentralizzata di oracoli) è stato ideato con l’obiettivo di risolvere o mitigare al massimo il problema dell’oracolo.

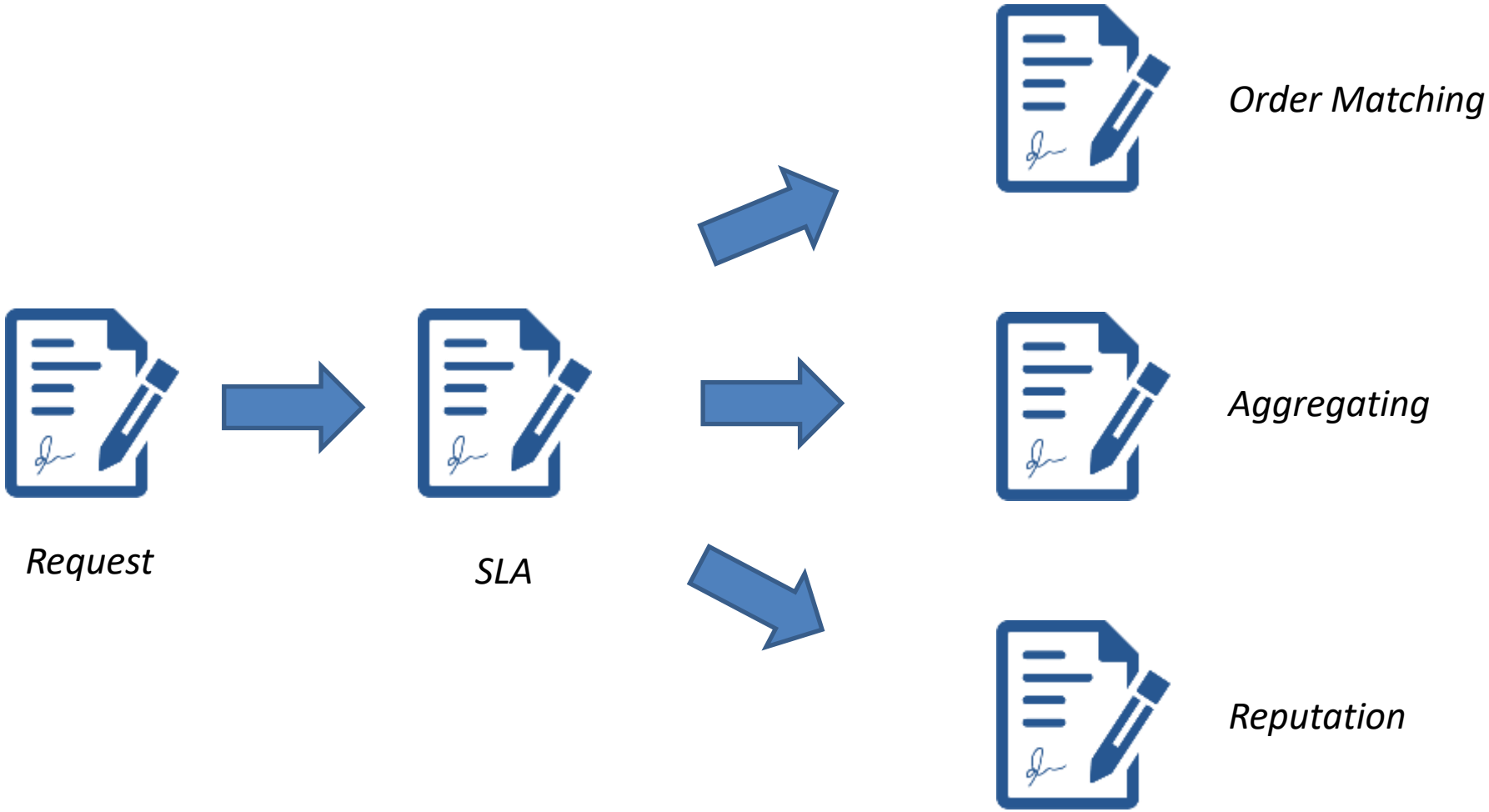
È un middleware tra sistemi on-chain e off-chain che fornisce agli smart contract l'accesso a risorse off-chain.

Chainlink

La componente on chain di Chainlink consiste di tre principali smart contract:

- **ORDER-MATCHING CONTRACT**: per l'abbinamento delle richieste
- **AGGREGATING CONTRACT**: per l'aggregazione dei risultati
- **REPUTATION CONTRACT**: per la misurazione della reputazione degli oracoli

Chainlink



Chainlink

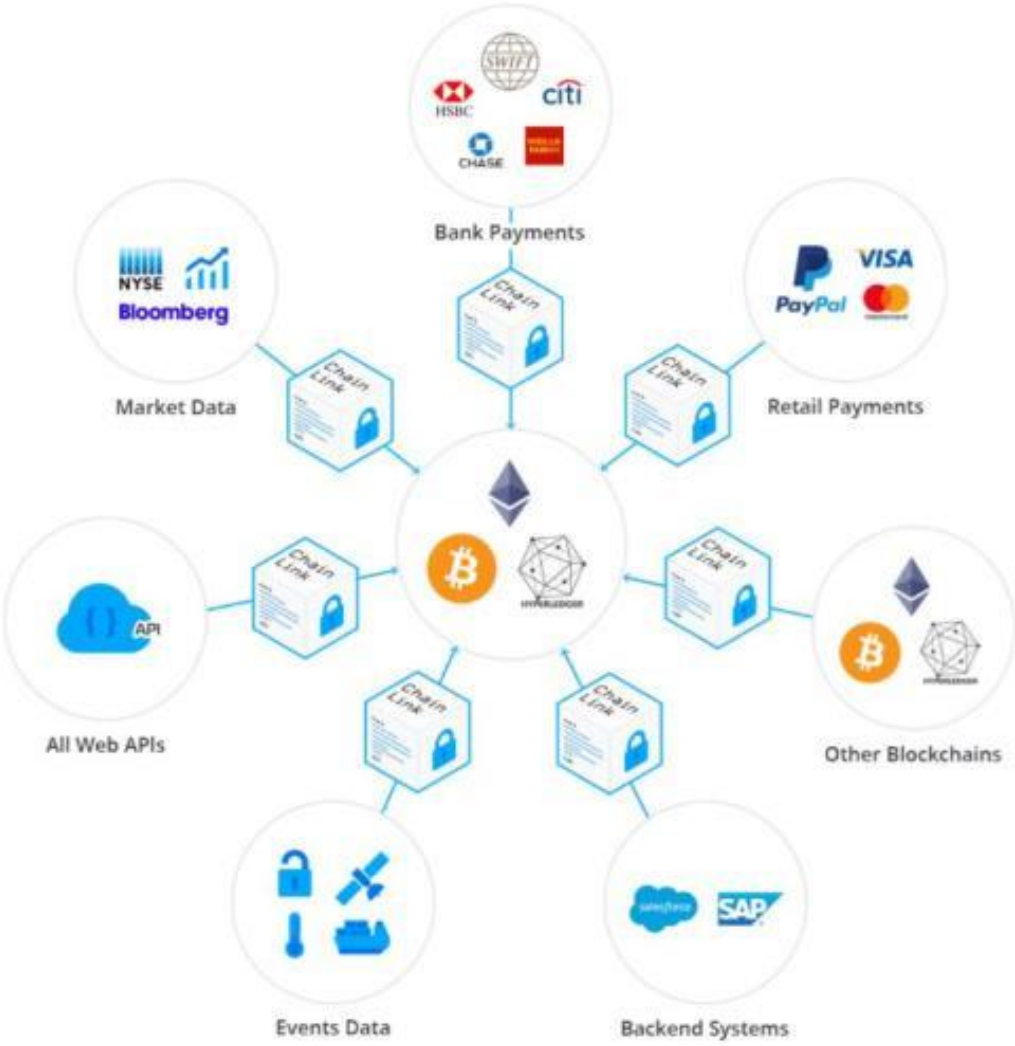
I punti principali su cui fa leva Chainlink sono:

- Molteplicità delle fonti di dati
- Pluralità di oracoli
- Aggregazione dei risultati (media aritmetica, media pesata, eliminazione dei risultati estremi dalla media)

Per favorire la presenza sulla rete di soli **oracoli onesti** vengono usati

- sistema di reputazione
- servizi di certificazione
- incentivi e disincentivi economici per gli oracoli (**LINK**)

Chainlink


Bank Payments
Market Data
Retail Payments
All Web APIs
Other Blockchains
Events Data
Backend Systems

Caso d’uso

AccuWeather

- **AccuWeather** sta sfruttando Chainlink per portare i dati meteorologici più accurati alle Blockchain.
- Il nodo di AccuWeather trasmette i dati attraverso Blockchain, firmandoli crittograficamente, consentendo agli utenti di sapere che provengono da loro.
- Gli sviluppatori possono quindi creare Smart Contract che eseguono il ping del nodo Chainlink di AccuWeather per i dati meteorologici.
- L'API funziona con Etherum ed è sviluppata in linguaggio di programmazione Solidity.

Caso d'uso

AccuWeather

Nodo Chainlink AccuWeather

Blockchain

E la privacy?

- Una delle principali sfide per gli oracoli Blockchain è proteggere la privacy dei suoi utenti

Privacy

Chainlink ha sviluppato delle tecnologie per garantire la privacy dei dati:

- DECO
- MIXICLES
- TOWN CRIER

Con l'uso della tecnologia Blockchain e degli oracoli Chainlink, i **rischi sulla nostra identità digitale** possono essere mitigati consentendo alle piattaforme l'accesso ai dati off-chain in modo sicuro, o eliminando completamente l'identità off-chain al posto dei dati on-chain verificati da reti di oracoli di Chainlink.

Grazie per l’attenzione