B2B ORACLE MIDDLEWARE ▪ EVENT ATTESTATION ▪ NO-CUSTODY

Oracle-PM: Attestazione Verificabile per Mercati Predittivi Regolati

Attesta l'esito di eventi reali e consegna payload firmati e verificabili ai contratti di settlement EVM dei licenziatari, senza gestire il mercato e senza custodire fondi: consenso multi-fonte e quorum di firme M-di-N (EIP-712).



02

Cos'è Oracle-PM & Value Proposition

Panoramica

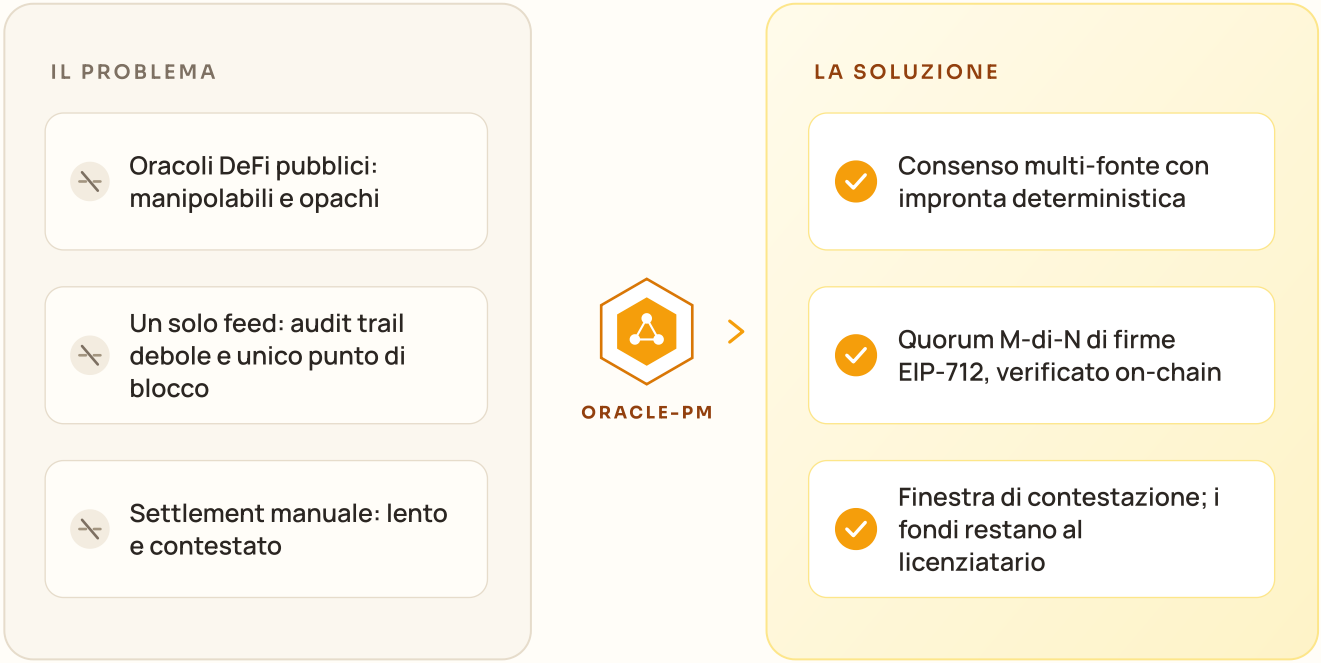
Oracle-PM è un middleware B2B di attestazione eventi, erogato in modalità Technology-as-a-Service: raccoglie dati da più fonti indipendenti, li porta a consenso in una rete di nodi oracolo autorizzati (Consensus Oracle Network, CON) e consegna l'esito firmato ai contratti di settlement controllati dal licenziatario. È un fornitore tecnologico: non è un operatore di scommesse, un exchange, un assicuratore né un custode.

Il Problema che Risolve

Gli oracoli DeFi pubblici sono manipolabili e opachi per operatori vigilati; un feed centralizzato unico ha un audit trail debole e, se si ferma, mette in crisi la credibilità del settlement; il settlement manuale è lento e contestato.

La Soluzione

Ingestione multi-fonte, impronta deterministica del consenso (consensusHash) e quorum M-di-N di firme EIP-712 verificato on-chain dal contratto del licenziatario, con una finestra di contestazione prima della finalizzazione. Fondi e decisioni di mercato restano al licenziatario.



Dal problema alla soluzione.

03

Architettura & Moduli Chiave

01

Consensus Oracle Network (CON)

Adapter modulari e isolati raccolgono e normalizzano i dati di più fonti: se una fonte cade, il ciclo prosegue con le altre. Il motore di consenso sceglie l'esito per maggioranza (per Predict è raccomandato un accordo di almeno il 66% delle fonti), in caso di pareggio non produce alcun esito e calcola un'impronta deterministica (consensusHash), riproducibile offline.

02

Attestazione EIP-712 & Registro dei Validatori

Ogni nodo autorizzato firma lo stesso payload EIP-712: marketId, outcome, timestamp, roundId, consensusHash. Il contratto OracleValidatorRegistry verifica on-chain il quorum M-di-N e rifiuta firme non autorizzate, duplicate o fuori ordine. Oracle-PM non gestisce liquidità: nessun AMM, nessun pool, nessun market making.

03

Dispute Time-Lock

Superato il quorum, l'esito passa in stato «Proposed» e resta bloccato per una finestra programmabile (tipicamente 24 ore). In questo intervallo solo il resolver designato dal licenziatario può annullare il mercato per emergenza o forza maggiore; allo scadere chiunque può finalizzare. È un time-lock di sicurezza, non un arbitrato: nessuno staking, nessuno slashing.

04

Integrazione B2B & Suite Modulari

API REST con chiave dedicata e template Solidity di riferimento (interfaccia IOracleConsumer), che il licenziatario distribuisce e controlla. Si attivano solo le suite per cui si è autorizzati: Predict (prototipo attivo, pronto per il pilota); Insur, Gaming e Structured (scaffold con specifica definita). Feed WebSocket e KMS/HSM sono in roadmap Enterprise.



03 · ARCHITETTURA

Dal dato al settlement: il flusso di attestazione

PERIMETRO ORACLE-PM · TaaS
Ingestione, consenso e firma: software e nodi oracolo autorizzati

LICENZIATARIO
Mercato e fondi

01

Fonti dati

Più fonti indipendenti: dati macro, tassi delle banche centrali, risultati elettorali ufficiali

02

Normalizzazione

Adapter isolati per fonte; il guasto di una fonte non blocca il ciclo

03

Consenso CON

Esito a maggioranza, pareggio = nessun esito; impronta consensusHash

04

Firma M-di-N

Ogni nodo autorizzato firma lo stesso payload EIP-712

05

Contratto del licenziatario

Verifica del quorum on-chain, poi time-lock prima della finalizzazione

Proposed · time-lock · Finalized

oppure Voided (resolver)

NO-CUSTODY
Fondi, puntate e premi restano nei contratti del licenziatario, che opera con la propria licenza

Sintesi visiva dei moduli descritti nella sezione 03 (Predict, la suite oggi pronta per il pilota).

04

Vantaggi Strategici

Perché Scegliere Oracle-PM

Integrità del Dato

Nessun singolo adapter e nessun singolo validatore può chiudere un mercato: servono consenso tra le fonti, quorum di firme e finestra di contestazione. Se i dati non bastano o non concordano, il ciclo si ferma e non inventa valori.

Zero Custodia, Perimetro Chiaro

Oracle-PM attesta i fatti. Mercato, collaterale, rapporto con l'utente e autorizzazione restano al licenziatario: un confine netto tra attestazione e amministrazione del mercato.

Audit Trail On-Chain

Ogni attestazione porta le firme EIP-712 dei validatori ed è verificata dal registro on-chain; l'impronta consensusHash si può ricalcolare offline. Dopo la finalizzazione, gli aventi diritto riscuotono dal contratto del licenziatario.

05

Pronto a integrare attestazioni verificabili nei tuoi contratti di settlement?

Contatta il Team di Ingegneria DLT

Prova il simulatore → oracle.globalconsultant.eu

GLOBAL CONSULTANT di Roberto Bonadies

E-MAIL info@globalconsultant.eu

WEB globalconsultant.eu

TELEFONO +39 393 5756044



Oracle-PM è un fornitore tecnologico B2B No-Custody: non è un operatore di scommesse, un exchange, un assicuratore né un custode, e non detiene licenze di operatore. Il licenziatario opera con la propria autorizzazione. Oracle-PM è una tecnologia di GLOBAL CONSULTANT di Roberto Bonadies.