ORACLE-PM

Oracle-PM: Architettura Tecnica

Panoramica pubblica dell'architettura

Un middleware B2B che attesta l'esito di eventi reali e consegna payload verificati ai contratti di settlement EVM dei licenziatari, senza gestire il mercato, senza custodire fondi e senza raccogliere puntate.

Categoria: *middleware di attestazione eventi multi-fonte*, erogato in modalità Technology-as-a-Service (TaaS). Prodotto: Oracle-PM · Consensus Oracle Network (CON). Maturità: Predict è un prototipo attivo, pronto per il pilota (*Active prototype / Pilot ready*).

Oracle-PM è un fornitore tecnologico: **non è** un operatore di scommesse, un exchange, un bookmaker, un assicuratore né un custode. Il mercato lo gestisce la controparte autorizzata, con la propria licenza.



1. Cosa fa e cosa non fa

ORACLE-PM FA	ORACLE-PM NON FA
Aggrega fonti dati verificate tramite adapter modulari	Toccare fondi o raccogliere puntate
Gestisce il consenso tra nodi oracolo autorizzati	Custodire chiavi private di utenti finali o operatori
Firma gli esiti secondo lo standard EIP-712	Detenere asset di terzi on-chain
Consegna payload attestati ai contratti del licenziatario	Fare da pool di liquidità, da banco o da market maker

I contratti di escrow e di settlement sono **template di riferimento**: li distribuisce, li configura e li controlla il licenziatario.

2. Architettura a tre livelli



Architettura a tre livelli (fonti: README.md, 00_MASTER_PROTOCOL_SPEC.md)

Livello 1 — Runtime off-chain. Pipeline dei nodi in TypeScript con API Fastify (REST): ingestione → consenso → firma. I moduli sono separati per regola: gli adapter non firmano, il consenso non contiene logiche specifiche delle fonti, la firma non decide il settlement.

Livello 2 — Core on-chain. `OracleValidatorRegistry` (Solidity, Foundry) custodisce l'insieme dei validatori autorizzati e verifica il quorum M-di-N delle firme EIP-712. È il `verifyingContract` del dominio EIP-712, non l'escrow.

Livello 3 — Consumo del licenziatario. Il contratto di settlement del licenziatario implementa l'interfaccia `IOracleConsumer` (più l'interfaccia della suite) e accetta un esito solo dopo `verifyQuorum`. I fondi, se presenti, restano sotto le chiavi e nel perimetro regolamentare del licenziatario.

3. Pipeline del nodo

1. **Ingestione**: adapter senza stato per famiglia di fonte; raccolgono e interpretano i dati, senza firmare né regolare nulla.
2. **Normalizzazione**: ogni risultato diventa un'osservazione canonica (`queryId` , `value` , `timestamp` , metadati) con l'impronta dei metadati della fonte.
3. **Consenso**: vince l'esito con più voti; con un pareggio il ciclo fallisce e non viene emesso alcun esito. L'impronta `consensusHash` è il keccak256 delle impronte dei metadati ordinate: non dipende dall'ordine delle fonti ed è ricalcolabile offline.
4. **Firma**: ogni validatore autorizzato firma in modo indipendente lo stesso digest EIP-712 (ECDSA secp256k1).
5. **Consegna**: l'attestazione e le firme, ordinate per indirizzo crescente, vengono impacchettate per l'invio on-chain dal licenziatario o da un relayer.

In ogni caso dubbio la pipeline si ferma (*fail closed*): una fonte che non risponde viene scartata, nessun valore viene inventato, e senza abbastanza osservazioni o firme il ciclo si interrompe.

4. Attestazione EIP-712

CAMPO	SIGNIFICATO
`marketId`	Identificativo del mercato o dell'evento
`outcome`	Esito canonico (es. SÌ/NO, candidato, fascia di tasso), con tabella di codifica concordata
`timestamp`	Momento dell'attestazione (secondi Unix)
`roundId`	Ciclo di consenso o di rilevazione
`consensusHash`	Impronta vincolante delle osservazioni aggregate

Dominio EIP-712: nome `Oracle-PM` , versione `1` , chain di destinazione, `verifyingContract` = `OracleValidatorRegistry` .

La verifica on-chain recupera ogni firmatario dal digest, rifiuta firme non autorizzate, duplicate o di lunghezza errata, richiede firmatari in ordine strettamente crescente e un numero di firme valide almeno pari alla soglia di quorum.

5. Dispute time-lock

STATO	COSA SUCCEDE
Active / Open	Il mercato è aperto; nessun esito
Proposed	Il quorum ha attestato un esito; parte la finestra di contestazione (tipicamente 24 ore)
Finalized / Resolved	Finestra scaduta: chiunque può finalizzare; gli aventi diritto riscuotono dal contratto (modalità *pull*)
Voided	Durante la finestra, il resolver designato dal licenziatario ha annullato il mercato (emergenza, forza maggiore); rimborso 1:1

Il time-lock è un **meccanismo di sicurezza, non un tribunale decentralizzato**. Non c'è staking né slashing; il resolver è un indirizzo del licenziatario (tipicamente un multisig), mai di Oracle-PM.

6. Suite verticali

SUITE	STATO	SEGMENTO	SETTLEMENT
Predict	Prototipo attivo, pronto per il pilota	Prediction market ed event contract regolati: dati macro, tassi delle banche centrali, risultati elettorali ufficiali	*Pull* dopo quorum e time-lock
Insur	Scaffold, specifica definita	Assicurazione parametrica: meteo / agricoltura, ritardi cargo e voli	*Pull* dell'importo parametrico dopo il trigger (roadmap)
Gaming	Scaffold, specifica definita	Scommesse sportive B2B e in-play per operatori autorizzati	*Pull* o settlement a lotti dopo il cut-off (roadmap)
Structured	Scaffold, interoperabilità architetturale	Green bond, SAL, eventi di default	Approvazione a quattro occhi: l'attestazione non muove mai i pagamenti da sola

Si attivano solo le suite per cui il licenziatario è autorizzato. Per Gaming la latenza inferiore a 1,5 s è un obiettivo da definire nel contratto, non un valore misurato in produzione.

7. Interoperabilità con Valoris

Oracle-PM e Valoris sono **due prodotti distinti**, con repository e brand separati. Oracle-PM non importa logiche di Valoris (registro ERC-3643, compliance, vIBAN, NAV) e non è «l'oracolo di Valoris».

L'unico ponte previsto è logico: un modulo Valoris, nel proprio codice, può implementare `IOracleConsumer` e ricevere attestazioni generiche (`queryId` , `value` , dati ausiliari). L'interpretazione di quei dati resta interamente in Valoris.

8. Cosa è vero oggi

Implementato

- Pipeline off-chain (TypeScript, Fastify), `OracleValidatorRegistry` e template di escrow Predict (Solidity, Foundry).
- Formula del consenso e ordinamento dei firmatari coperti da 51 test automatici (32 Vitest + 19 Foundry).
- **Prova il simulatore:** oracle.globalconsultant.eu, simulatore interattivo pubblico. La verifica dal simulatore non invia transazioni on-chain.

In roadmap Enterprise (solo a contratto)

- Ingestione WebSocket a bassa latenza.
- Firma con KMS/HSM hardware (oggi stub modulari e multi-firma locale).
- Compressione del quorum con firme a soglia (TSS) o aggregate (BLS).

9. Avvertenze

Questa panoramica è un documento tecnico informativo. Non è un parere legale né un'offerta. Oracle-PM non detiene licenze di operatore (GFSC o altre) e non è approvato da alcuna autorità: l'autorizzazione all'attività di mercato resta in capo al licenziatario. Il veicolo societario previsto a Gibilterra è in costituzione: non è operativo e non è parte contraente.

Oracle-PM è una tecnologia di GLOBAL CONSULTANT di Roberto Bonadies.

Contatti · GLOBAL CONSULTANT di Roberto Bonadies · info@globalconsultant.eu · +39 393 5756044 · globalconsultant.eu