Integrazione di sistemi di Agentic AI in architetture basate su Distributed Ledger Technologies (DLT)

L'assegnista contribuirà alla progettazione, sviluppo e valutazione di metodologie e prototipi che integrano agenti AI autonomi (*agentic AI*) con infrastrutture distribuite basate su ledger, con un focus specifico su sicurezza, privacy, accountability e robustezza dei sistemi decentralizzati.

Il programma di formazione dell'assegno prevede le seguenti attività organizzate nel periodo di un anno:

1. **Analisi dello stato dell'arte**

- Studio delle architetture di *agentic AI*, con attenzione ai rischi di sicurezza (es. escalation autonoma, manipolazione del contesto, attacchi di poisoning) e alle implicazioni sulla privacy.
- Analisi delle tecnologie DLT e dei protocolli di consenso, valutandone proprietà di sicurezza, resistenza agli attacchi e capacità di preservare la privacy.
- Identificazione delle principali minacce nell'integrazione AI–DLT (Sybil attacks, data leakage, misuse degli smart contract, vulnerabilità degli oracoli).
- Studio delle specifiche del Model Context Protocol (MCP), con particolare attenzione ai meccanismi di sicurezza, autenticazione, autorizzazione e controllo degli accessi.

2. **Progettazione dell'architettura integrata**

- Definizione di modelli di interazione sicuri tra agenti AI e componenti DLT, includendo smart contract resilienti, oracoli verificabili e protocolli di governance robusti.
- Progettazione di interfacce MCP che garantiscano integrità, confidenzialità e tracciabilità delle operazioni degli agenti.
- Studio di meccanismi per assicurare privacy-by-design, come tecniche di anonimizzazione, zero-knowledge proofs, secure enclaves e gestione sicura delle identità digitali (DID).
- Definizione di un livello di interoperabilità che sfrutti MCP per garantire comunicazioni sicure, auditabili e resistenti a manipolazioni.

3. **Sviluppo di prototipi e strumenti software**

- Implementazione di agenti AI autonomi con capacità di interazione sicura con reti DLT tramite API, smart contract e protocolli MCP.
- Sviluppo di moduli MCP con controlli di sicurezza integrati (autenticazione forte, validazione delle richieste, logging verificabile).
- Realizzazione di sistemi per la gestione sicura delle identità e delle credenziali degli agenti, con attenzione alla protezione dei dati sensibili.
- Creazione di prototipi dimostrativi che evidenzino come sicurezza e privacy siano preservate anche in scenari complessi (supply chain, IoT, DeFi, governance distribuita).

4. **Sperimentazione e valutazione**

- Definizione di metriche per valutare sicurezza, privacy, robustezza e resilienza dell'integrazione AI–DLT.
- Esecuzione di test su reti di prova, includendo analisi di vulnerabilità, simulazioni di attacchi e valutazioni di leakage informativo.
- Validazione dell'efficacia dei meccanismi MCP nel prevenire accessi non autorizzati, manipolazioni del contesto e compromissioni dei dati.
- Analisi dei risultati e proposta di miglioramenti architetturali orientati alla sicurezza.

Sono inoltre previste attività di gruppo orientate alla predisposizione di materiali e prototipi. Saranno anche maturate esperienze significative relativamente a: redazione di documenti di carattere divulgativo e presentazione di risultati e prototipi alla comunità scientifica e ad aziende del territorio.

Digitally signed
by: Andrea Omicini,
on: 15 gennaio 2026