

Il progetto della CTE di Matera con IVERT

A Matera, la tecnologia quantistica rende sicure le transazioni tra blockchain

Giampiero Pepe, Responsabile Scientifico della CTE di Matera: “La sfida è sviluppare le potenzialità della sicurezza quantistica e inserirle in contesti applicativi di grande interesse per il mercato”

L'ente

Il Comune di Matera, conosciuto in tutto il mondo per i suoi storici Sassi oggi patrimonio dell'umanità UNESCO, è l'Ente capofila della Casa delle Tecnologie Emergenti di Matera avviata nel 2019. Le CTE sono centri di ricerca, sperimentazione e trasferimento tecnologico, il cui obiettivo è promuovere lo sviluppo di soluzioni innovative e l'avanzamento delle piccole e medie imprese. In particolare, la CTE di Matera si concentra su AI, Blockchain, Quantum Technology, IoT, e 5G, applicate ai settori industrie culturali e creative, patrimonio culturale, comunicazione e servizi per la sostenibilità e turismo. La città si trasforma così in un laboratorio di innovazione aperto e partecipato, dove enti pubblici, imprese private, università e centri di ricerca collaborano per creare soluzioni innovative e sostenibili.

L'idea in breve

La CTE di Matera, in collaborazione con IVERT srl, ha promosso lo sviluppo di un sistema innovativo di protezione quantistica per la comunicazione tra blockchain. Il progetto affronta un tema centrale della cybersecurity applicato al settore finanziario, e mira a rafforzare la sicurezza e l'integrità dei dati nelle transazioni digitali.

L'innovazione e la collaborazione tra la CTE di Matera e IVERT

Il progetto si inserisce nel contesto del laboratorio *Blockchain e Quantum Key Distribution* della CTE di Matera, il cui obiettivo è unire tecnologie quantistiche, in particolare la sicurezza quantistica (QKD), con la blockchain, una delle tecnologie individuate dal MIMIT nelle attività delle Case delle Tecnologie Emergenti. Il laboratorio è dotato di strumenti avanzati, come un generatore di chiavi quantistiche accessibile anche da remoto e rivelatori superconduttivi di singolo fotone che portano le performances della trasmissione allo stato dell'arte. La collaborazione con IVERT è nata grazie a

una delle *Call for Ideas* della CTEMT, che ha messo a disposizione risorse per le PMI e le startup innovative. Il progetto di IVERT è stato selezionato e finanziato con 10.000 euro. L'idea nasce dall'esigenza di aumentare la sicurezza sulle transazioni cross-blockchain.

Transazioni blockchain sicure e interoperabili

L'aumento delle transazioni di crypto-asset ha fatto nascere l'esigenza di interoperabilità tra le diverse reti. Attualmente, lo scambio di dati tra blockchain indipendenti avviene tramite intermediari, uscendo però dal perimetro di sicurezza della blockchain stessa. Questo rende la zona di scambio particolarmente vulnerabile agli attacchi informatici. Per risolvere il problema, IVERT ha creato un canale parallelo tra le due blockchain con una soluzione che sfrutta la generazione di chiavi quantistiche per criptare le informazioni necessarie a sincronizzare le due catene di blocchi. Questi dati vengono trasferiti in modo bidirezionale, garantendo una comunicazione sicura, disintermediata e protetta. Il prototipo è stato realizzato su Hyperledger Fabric, un'infrastruttura di blockchain permissioned.

Benefici

Grazie all'utilizzo di tecnologie quantistiche emergenti, la soluzione rappresenta un importante passo avanti nella protezione delle informazioni sensibili, garantendo comunicazioni crittografiche avanzate per le applicazioni dell'Industria 4.0. La soluzione consente lo swap di asset tra blockchain differenti in modo sicuro, utilizzando uno smart contract cross-blockchain per gestire il deposito a garanzia. Il progetto ha un duplice impatto: da un lato dimostra come la tecnologia quantistica possa essere applicata a contesti industriali concreti, dall'altro evidenzia come la collaborazione tra pubblico e privato possa generare risultati tangibili e aprire nuove opportunità in settori ad alto potenziale. Le prospettive future puntano a superare la fase di prototipo ed estendere la funzionalità anche alle blockchain *permissionless*, come Ethereum, per accedere a un mercato molto più ampio e offrire benefici all'intera comunità.