

# **Sicurezza nel Metaverso: nuove frontiere della cybersecurity nell'era degli ambienti virtuali immersivi**



Il metaverso rappresenta una delle evoluzioni più significative dell'internet contemporaneo, configurandosi come uno spazio virtuale condiviso dove utenti, rappresentati da avatar digitali, possono comunicare, collaborare e socializzare tra loro e interagire con oggetti digitali in mondi virtuali generati dal computer. Questa convergenza tecnologica, che integra realtà virtuale (VR), realtà aumentata (AR), intelligenza artificiale (AI) e blockchain, sta creando un ecosistema digitale di complessità senza precedenti, caratterizzato da vulnerabilità di sicurezza emergenti e sfide crittografiche inedite.

L'espansione accelerata degli ambienti virtuali ha comportato l'emergere di rischi multidimensionali che trascendono i tradizionali paradigmi di cybersecurity. Con l'espansione degli ambienti virtuali, emergono rischi legati alla proprietà digitale (NFT), alla contraffazione di avatar e agli attacchi cross-platform, richiedendo approcci innovativi per la protezione delle transazioni e dell'identità digitale.

## **Tassonomia delle vulnerabilità nel Metaverso**

### **Minacce alla proprietà digitale e NFT**

Il paradigma degli NFT (Non-Fungible Tokens) nel metaverso ha introdotto nuove dimensioni di vulnerabilità relative alla

proprietà intellettuale digitale. Gli NFT sono più che semplici collezioni – sono la spina dorsale dell'economia del metaverso, consentendo la creazione e lo scambio di valore in forma puramente digitale. Tuttavia, questa rivoluzione porta con sé rischi significativi:

**Violazioni del copyright digitale:** Artisti come Banksy e Lois van Baarle hanno avuto i loro nomi impersonati o le loro opere “rubate” e trasformate in NFT per la vendita su piattaforme di trading famose come OpenSea. Questo fenomeno evidenzia la necessità di meccanismi robusti di autenticazione e verifica della proprietà intellettuale.

**Falsificazione di contenuti digitali:** Le blockchain sono sicure per progettazione, ma le applicazioni costruite sopra di esse possono essere vulnerabili a hack, phishing o difetti nel codice dei contratti intelligenti. La natura immutabile della blockchain, paradossalmente, può perpetuare frodi se contenuti falsificati vengono registrati permanentemente.

## **Impersonificazione di avatar e minacce all'identità digitale**

L'autenticazione dell'identità negli ambienti virtuali presenta sfide uniche che richiedono approcci crittografici avanzati:

**Spoofing e identity theft:** Nel metaverso, è possibile per un individuo creare un avatar o un account utente che assomigli a qualcun altro, per ottenere accesso ad aree riservate o informazioni. Questo tipo di attacco può essere utilizzato per scopi malevoli, come il furto di informazioni sensibili o il danneggiamento della reputazione della persona impersonata.

**Clonazione comportamentale:** Gli attaccanti possono impersonare le vittime nel metaverso sfruttando i dati comportamentali e biologici raccolti dai dispositivi AR/VR per creare un avatar falso per uso criminale. Questa forma sofisticata di impersonificazione sfrutta algoritmi di machine learning per

replicare pattern comportamentali specifici.

**Vulnerabilità cross-platform:** Nel metaverso, gli utenti possono accedere ai mondi virtuali da una varietà di piattaforme e dispositivi diversi, come computer, smartphone e visori per realtà virtuale. Questo può creare sfide per l'autenticazione, poiché piattaforme diverse possono avere meccanismi di autenticazione diversi.

## **Attacchi Cross-Platform e interoperabilità**

La natura interconnessa del Metaverso introduce vulnerabilità sistemiche che possono propagarsi attraverso multiple piattaforme:

**Man-in-the-Room (MitR) attacks:** L'attacco Man-in-the-Room (MitR), realizzato da un'applicazione di social networking vulnerabile, ha portato a capacità sia di worm che di botnet adattate per VR con potenziali impatti critici che interessano milioni di utenti.

**Propagazione di malware in ambienti immersivi:** Il malware ha colpito tutti i consumatori della stanza immersiva. L'esecuzione JavaScript e altre vulnerabilità nel meccanismo di autenticazione portano a diversi altri attacchi come phishing, intercettazioni, condivisione desktop illegittima, attacco man-in-the-room (MITR) e denial of service.

## **Standard crittografici post-quantistici per il Metaverso**

### **La minaccia quantistica agli attuali paradigmi crittografici**

L'avvento del quantum computing rappresenta una minaccia esistenziale per gli attuali standard crittografici utilizzati nel Metaverso. La maggior parte degli algoritmi di chiave pubblica ampiamente utilizzati si basa sulla difficoltà di uno

di tre problemi matematici: il problema della fattorizzazione degli interi, il problema del logaritmo discreto o il problema del logaritmo discreto della curva ellittica. Tutti questi problemi potrebbero essere facilmente risolti su un computer quantistico sufficientemente potente che esegue l'algoritmo di Shor.

**Impatto sulle transazioni blockchain:** È previsto che entro il 2035 circa, i computer quantistici raggiungeranno un livello di sofisticazione tale da poter efficacemente frantumare algoritmi di sicurezza come RSA-2048. Questo scenario minaccia direttamente la sicurezza delle transazioni NFT e delle criptovalute utilizzate nel metaverso.

## **Crittografia Lattice-Based per ambienti virtuali**

I sistemi crittografici basati su reticoli rappresentano una delle soluzioni più promettenti per la sicurezza post-quantistica nel Metaverso:

**CRYSTALS-Kyber e CRYSTALS-Dilithium:** FIPS 203, FIPS 204 e FIPS 205, che specificano algoritmi derivati da CRYSTALS-Dilithium, CRYSTALS-KYBER e SPHINCS+, sono stati pubblicati il 13 agosto 2024. Questi standard NIST rappresentano la frontiera della crittografia resistente ai quantum per applicazioni ad alta sicurezza.

**Implementazioni ottimizzate per IoT:** La ricerca ha dimostrato implementazioni efficienti di algoritmi post-quantistici su dispositivi a risorse limitate. L'implementazione di Kyber su processori ARM64 a 64 bit mostra che la loro implementazione raggiunge un buon equilibrio tra prestazioni e utilizzo della memoria, rendendola adatta per dispositivi con risorse limitate.

## **Blockchain quantistico per il Metaverso**

L'integrazione di tecnologie quantistiche nelle infrastrutture blockchain del Metaverso offre soluzioni innovative:

**Quantum Multiparty Secret Computation (QMSC):** Il documento propone Multiparty Space Sharing and Authentication (MSSA), un approccio innovativo per il login sicuro degli utenti e il controllo degli accessi alla posizione all'interno di piattaforme metaverso specializzate. MSSA sfrutta Quantum Multiparty Secret Computation (QMSC) integrato con una rete blockchain quantistica.

**Delegated Proof-of-Stake quantistico:** La blockchain quantistica sottostante impiega un meccanismo di consenso Delegated Proof-of-Stake (DPoS) con uno schema di voto Borda per la selezione dei nodi autorità, offrendo resistenza sia agli attacchi classici che a quelli quantistici futuri.

## **Architetture di sicurezza avanzate**

### **Sistemi di autenticazione continua biometrica**

L'autenticazione nel Metaverso richiede approcci multi-dimensionali che sfruttano le caratteristiche uniche degli ambienti immersivi:

**Autenticazione biometrica multimodale:** I ricercatori hanno proposto vari tipi di autenticazione continua utilizzando dispositivi indossabili, inclusa la misurazione delle onde sonore nell'orecchio e dei segnali pulsatili da un sensore di fotoplethysmografia (PPG).

**Crittografia a curva ellittica e blockchain:** Ryu et al. hanno proposto uno schema di autenticazione reciproca per il metaverso utilizzando informazioni biometriche, crittografia a curva ellittica e tecnologia blockchain, combinando multiple tecnologie per una sicurezza robusta.

### **Protezione della privacy comportamentale**

La raccolta massiva di dati comportamentali nel Metaverso richiede framework di privacy sofisticati:

**Biometric Psychography Protection:** La psicografia biometrica è un tipo di informazione centrata sul corpo che può rivelare dettagli intimi sui gusti, antipatie, preferenze e interessi degli utenti. La protezione di questi dati richiede tecniche crittografiche avanzate e protocolli di consenso granulari.

**Anonimato differenziale:** L'autenticazione è la verifica dell'identità e non implica il conferimento dell'identità o il contenuto dell'identità di per sé. L'autenticazione ha le sue radici nei meccanismi di fiducia nello spazio virtuale. A differenza del mondo fisico, l'identità digitale si basa sulla fiducia crittografica piuttosto che sulla fiducia umanistica.

## **Sicurezza delle transazioni in realtà virtuale**

Le transazioni economiche nel Metaverso richiedono protocolli crittografici specifici che garantiscano integrità e non-ripudiabilità:

**Smart contracts quantum-resistant:** I contratti intelligenti abilitano pagamenti automatici di royalty e verifica della proprietà, garantendo una gestione senza soluzione di continuità dell'asset durante tutto il suo ciclo di vita. L'implementazione di algoritmi post-quantistici in questi contratti è essenziale per la sicurezza a lungo termine.

**Hybrid NFTs con NFC sicuro:** Gli NFT ibridi combinano token digitali con asset del mondo reale, segnando un passo trasformativo nella tecnologia blockchain. Gli articoli fisici incorporano chip NFC collegati a token digitali unici, garantendo una connessione ininterrotta tra i due.

## **Governance e compliance normativa**

### **Framework normativi emergenti**

La regolamentazione del Metaverso richiede approcci innovativi che bilancino innovazione e protezione:

**Standards tecnici per la governance:** TS-MG dovrebbe abilitare il vantaggio del first-mover della formulazione di standard per le organizzazioni di standardizzazione. Include anche politiche di governance per fasi che bilanciano la compatibilità e la sicurezza degli standard nelle fasi iniziali, di crescita e mature del metaverso.

**Interoperabilità regolamentata:** I sub-universi, le piattaforme virtuali formeranno gradualmente un set completo di standard e protocolli nei prossimi 15 anni (2035-2050) per realizzare l'aggregazione dei sub-universi e formare un metaverso.

## **Ethical AI e controllo algoritmico**

L'integrazione di sistemi AI nel Metaverso solleva questioni etiche che richiedono governance tecnica:

**Trasparenza algoritmica:** Per esempio, il metaverso potrebbe essere usato per manipolare l'opinione pubblica o interferire con le elezioni diffondendo disinformazione o propaganda, specialmente se manca la trasparenza rispetto agli account automatizzati (bot/AI) e agli avatar.

**Audit di sicurezza AI:** I sistemi AI affrontano due minacce di sicurezza: sicurezza del modello e privacy del modello/dati. La sicurezza del modello riguarda le minacce affrontate dai modelli AI durante i loro cicli di vita, inclusi potenziali attacchi e problemi di robustezza intrinseci.

## **Implementazioni pratiche e case studies**

### **Architetture di riferimento**

**Metaverse Security Center:** Il Metaverse Security Center offre informazioni sulla formazione di sicurezza del metaverso e la certificazione Certified Metaverse Security Consultant (CMSC). Questo rappresenta un approccio sistematico alla formazione

professionale nella cybersecurity del metaverso.

**Implementazioni blockchain:** Algorand è il leader nella resilienza quantistica blockchain, proteggendo già l'intera storia della catena contro le minacce future dei computer quantistici attraverso l'implementazione delle firme FALCON, uno standard di crittografia post-quantistica riconosciuto globalmente basato su reticoli.

## **Metriche di sicurezza e KPI**

La valutazione della sicurezza nel Metaverso richiede metriche specifiche che tengano conto della natura immersiva degli ambienti:

**Presenza e sicurezza:** La misurazione della presenza negli ambienti virtuali è una sfida significativa nello sviluppo del metaverso. La presenza, o la sensazione di essere presenti in un ambiente virtuale, è un aspetto critico dell'immersione e del godimento dell'esperienza virtuale.

**Validazione multi-dimensionale:** È cruciale per i creatori del metaverso utilizzare una combinazione di misure soggettive e oggettive, così come condurre studi utente e sondaggi, per ottenere una comprensione completa del senso di presenza dell'utente negli ambienti virtuali.

## **Prospettive future e raccomandazioni tecniche**

### **Roadmap tecnologica**

**Transizione post-quantistica:** Ethereum riconosce la minaccia quantistica e ha preso misure proattive per integrare la resistenza quantistica nella sua roadmap. Questa transizione rappresenta un modello per altre piattaforme blockchain nel metaverso.

**zk-STARKs per la privacy:** Gli zk-STARK utilizzano un sistema di prova a conoscenza zero per abilitare la verifica di dati crittografati senza rivelare alcuna informazione sottostante. Gli STARK offrono miglioramenti rispetto agli zk-SNARK basandosi su funzioni hash resistenti alle collisioni piuttosto che su curve ellittiche e setup fidati.

## **Raccomandazioni per professionisti della sicurezza**

**Implementazione graduale:** I professionisti dovrebbero adottare un approccio graduale nell'implementazione di soluzioni post-quantistiche, iniziando con sistemi ibridi che combinano algoritmi classici e post-quantistici.

**Formazione continua:** Gli esperti del settore saranno preoccupati per i rischi di sicurezza emergenti del metaverso che includeranno nuove forme di minacce alla sicurezza e alla protezione dei dati, furto di identità e frode. La formazione continua è essenziale per mantenere competenze aggiornate.

**Collaborazione inter-industriale:** La sicurezza del metaverso richiede collaborazione tra settori tecnologici, finanziari e normativi per sviluppare standard condivisi e best practices efficaci. mi classici e post-quantistici.

**Formazione Continua:** Gli esperti del settore saranno preoccupati per i rischi di sicurezza emergenti del metaverso che includeranno nuove forme di minacce alla sicurezza e alla protezione dei dati, furto di identità e frode. La formazione continua è essenziale per mantenere competenze aggiornate.

**Collaborazione Inter-industriale:** La sicurezza del Metaverso richiede collaborazione tra settori tecnologici, finanziari e normativi per sviluppare standard condivisi e best practices efficaci.

# Conclusioni

Il Metaverso rappresenta una frontiera tecnologica che ridefinisce i paradigmi tradizionali della cybersecurity. L'emergere di minacce legate alla proprietà digitale, all'impersonificazione di avatar e agli attacchi cross-platform richiede l'adozione di standard crittografici post-quantistici e architetture di sicurezza innovative.

La transizione verso sistemi resistenti ai quantum computing non è più una questione di "se" ma di "quando". Le organizzazioni che operano nel Metaverso devono iniziare immediatamente l'implementazione di soluzioni crittografiche avanzate, con particolare attenzione agli algoritmi lattice-based e alle tecnologie blockchain quantistiche.

L'integrazione di sistemi di autenticazione biometrica continua, la protezione della privacy comportamentale e l'implementazione di smart contracts quantum-resistant rappresentano gli elementi fondamentali per un ecosistema Metaverso sicuro e resiliente.

La collaborazione tra ricerca accademica, industria e organismi di standardizzazione sarà cruciale per sviluppare framework normativi adeguati e garantire che l'evoluzione del Metaverso proceda in modo sicuro e sostenibile, proteggendo gli utenti e preservando l'integrità dell'ecosistema digitale globale.

## Fonti

Dong, Y., & Wang, C. (2023). Copyright protection on NFT digital works in the Metaverse. *Security and Safety (S&S)*. [https://sands.edpsciences.org/articles/sands/full\\_html/2023/01/sands20220012/sands20220012.html](https://sands.edpsciences.org/articles/sands/full_html/2023/01/sands20220012/sands20220012.html)

NFT News Today. (2025). NFTs in 2025: Key Trends, Innovations, and Market Shifts.

<https://nftnewstoday.com/2024/12/24/nfts-in-2025-key-trends-innovations-and-market-shifts/>

Identity Management Institute. (2022). Metaverse Security and Privacy Threats. <https://identitymanagementinstitute.org/metaverse-security-and-privacy-threats/>

World Economic Forum. (2022). Here's how to prevent crime in the metaverse. <https://www.weforum.org/stories/2022/08/crime-punishment-metaverse/>

NIST Computer Security Resource Center. (2024). Post-Quantum Cryptography Standardization. <https://csrc.nist.gov/projects/post-quantum-cryptography>

Nature Scientific Reports. (2024). Leveraging quantum blockchain for secure multiparty space sharing and authentication on specialized metaverse platform. <https://www.nature.com/articles/s41598-024-74213-x>

Frontiers in Big Data. (2023). The metaverse digital environments: a scoping review of the challenges, privacy and security issues. <https://www.frontiersin.org/journals/big-data/articles/10.3389/fdata.2023.1301812/full>

Algorand Foundation. (2024). Algorand's post-quantum blockchain technology. <https://algorand.co/technology/post-quantum>

Metaverse Security Center. (2024). Metaverse in 2040 – Extensive Report. <https://metaversesecuritycenter.org/metaverse-security-center/f/metaverse-in-2040-extensive-report>

Condividi sui Social Network:  
<https://www.ictsecuritymagazine.com/articoli/metaverso/>