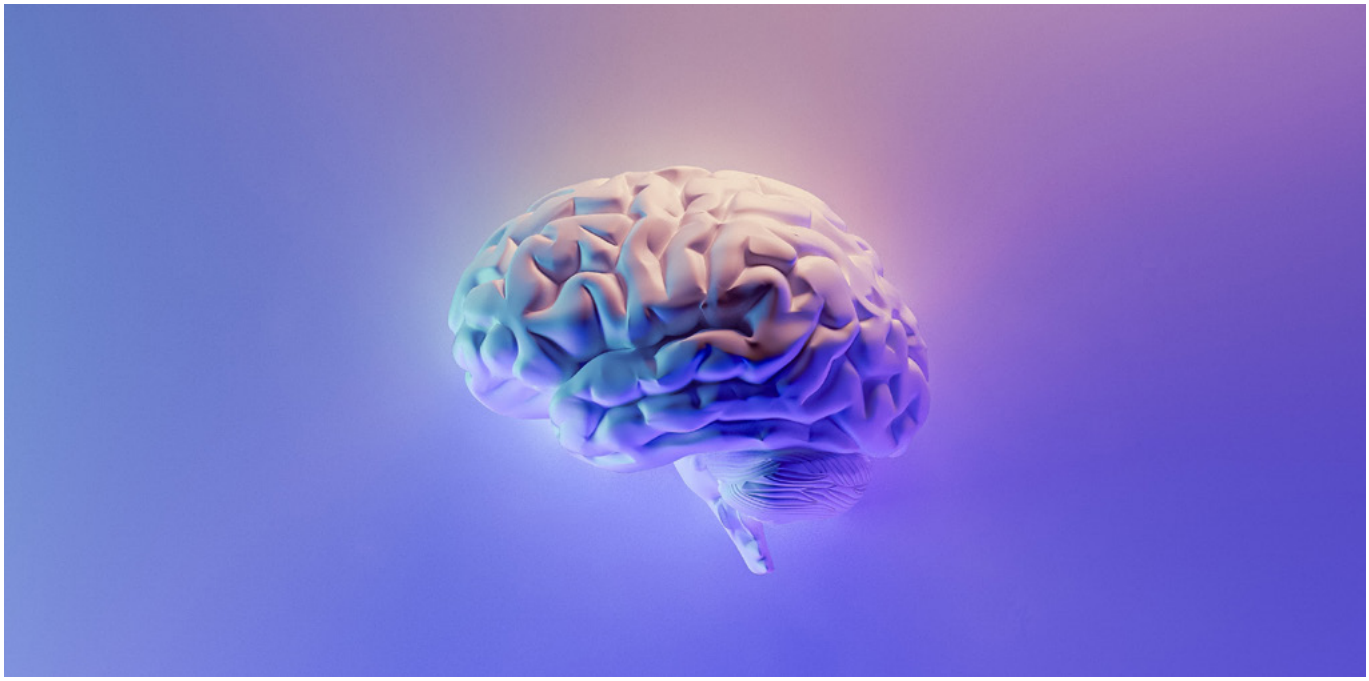
OPPORTUNITY #36

What if we secured our digital identities using quantum encryption?

QUANTUM AVATAR

Quantum encryption protects the integrity of avatars in digital realities, creating an environment of trust that uplifts creativity, commerce and security.



MEGATREND
Technological Vulnerabilities

TRENDS
Cybersecurity
Digital Art & Design
Metaverse
Virtual Reality

SECTORS AFFECTED
Cyber & Information Security
Data Science, AI & Machine Learning
Immersive Technologies

WHY IT MATTERS TODAY

As the digital reality universe grows, so does the use of avatars to navigate them. Every interaction an avatar has in a virtual environment leaves a trail of data points. Estimates suggest that a 20-minute virtual reality session with a headset can generate up to 2 million data points about an individual's body language, which can reveal both mental and physical health conditions.[627] Linking such data to financial, communication and contact data gathered in digital realities mean avatars could become prime targets for cyberattacks. The more active avatars are, the more they are at risk of data fraud and misrepresentation and even full avatar identity theft (known as cybersquatting).[628]

Today, avatars are second nature in gaming, which today boasts nearly 3 billion players worldwide.[629] Video games revenues rose 32% between 2019 and 2021 and are estimated to rise at a compound annual growth rate (CAGR) of just over 8% through to 2026, creating a $321 billion industry.[630]

In addition, avatars are core to augmented reality (AR) and virtual reality (VR). The AR and VR market was valued at $15 billion in 2020 and is projected to reach $454 billion by 2030 with a CAGR of 40.7%.[631] AR and VR have the potential to add $4 billion to the United Arab Emirates' economy by 2030.[632]

There are nearly

3 BILLION

gamers worldwide

THE OPPORTUNITY

An avatar is a virtual self-representation.[633] Protecting it from harm and from harming others will be key in the future, particularly in digital realities, where the lack of the possibility of physical harm may reduce people's perceptions of the importance of harms suffered and caused. Additionally, in such spaces, avatars can themselves be separate legal personalities who can be controlled by Artificial Intelligence (AI) as opposed to a human.[634]

Quantum encryption could allow people to protect their avatars (i.e. their identity and data) from malicious attacks and accidental breaches. Ensuring complete avatar security would create a high-trust environment that enabled the growth and success of new social and business models in digital reality spaces. Agreements, purchases and expressions of opinion or creativity could each be verified, reducing costs and the risk of misrepresentation or falsification.

Together with a legal review – and possibly new laws and regulations relating to avatars covering fraud, identity theft, defamation and other crimes – quantum-secured avatars could provide greater confidence to individuals and society in digital realities.[635]

BENEFITS

Safer, lower-cost transactions and improved social interactions, contributing to the growth and stability of digital realities.

RISKS

Unnoticed quantum encryption breaches, enabling avatar doubles to infiltrate sensitive situations for criminal or espionage purposes. Slow evolution of legal systems, meaning they fall out of sync with the quantum approach to encryption, making enforcement challenging.

Estimates suggest that
a **20-minute virtual reality session**
with a headset can generate up to

2 MILLION

data points about an individual's body language