



## Muhamed Kharsany

**Consultant**

**Digital consulting**

**Tel:** +27 63 645 4839

**Email:** [muhamed.kharsany@kpmg.co.za](mailto:muhamed.kharsany@kpmg.co.za)



## Shaheed Petersen

**Accountant**

**Advisory services**

**Tel:** +27 63 645 4522

**Email:** [shaheed.petersen@kpmg.co.za](mailto:shaheed.petersen@kpmg.co.za)

# Insurance in the metaverse

## Introduction

**When it comes to technological revolution, nothing compares to the way the metaverse stormed onto the scene in late 2021. The metaverse is an amalgamation and intersection of virtual reality (VR), digital assets, and the utility provided by its developers. It promises the existence of virtual worlds parallel to the physical world – wherein you can spend your digital life, exist as a digital avatar, and enjoy digital experiences designed to simulate the physical world. Underpinning these vast new worlds and the promise of digital infinity is the distributed ledger and blockchain technology that birthed the now familiar concepts of cryptocurrencies and non-fungible tokens (NFTs). These concepts go hand in hand with the metaverse - with the cryptocurrencies serving as metaverse currency and tokenised, NFTs roleplaying as digital 'metaversal' assets. All of which is secured on a blockchain. These concepts deliver a completely new class of assets and valuables through the virtual property we own, the health of our avatars, and the data that is making all this possible. Like all other assets, these will need to be protected.**

With the NFT market holding a staggering valuation of USD15.7 billion in 2021, the metaverse offers virtual asset types ranging from digital art pieces to virtual real estate on one of the many metaverse platforms. Music, gaming consumables, collectibles, virtual fashion, and event tickets populate a towering list of assets that, whilst typically existing physically and sold for fiat currency, can be minted and sold as an NFT.

While the same assets existing in the physical world offer a tangibility unmatched, these virtual assets deliver benefit to both sellers and holders. Musicians can be compensated in full for the proceeds from their art, gamers are able to enjoy the uniqueness and non-fungibility of their in-game assets, and wearers of virtual clothing are able to benefit from an asset that undergoes no physical wear. If anything, early virtual assets are expected to appreciate, as their originality and collectability skyrockets with the influx of new NFT creators as the metaverse expands.

With blockchain technology enabling true ownership of digital assets and therefore creating significant utility, marketability and tradability, these digital assets now have a more distinct, inherent value. Naturally, owners of this value would want to protect it by implementing risk controls, one of them being the insurance of their digital assets. In this article, we will discuss the effect of the metaverse (a shared, virtual experience powered by blockchain technology) on the insurance industry.

## The impact of the metaverse on the insurance industry

Virtual assets, including cryptocurrencies and NFTs, and the underpinning digital data behind them, represent the metaverse's version of economic assets held by citizens of these virtual worlds. Just like physical economic assets, these virtual assets bring a need to be protected from events such as attacks, misplacement and in the case of digital data, accidental and malicious destruction. The oft-touted security and decentralisation presented by blockchain technology arrives with different classes of risks against which users of the metaverse, NFTs, and crypto-assets will seek insurance.

## Opportunities presented by the metaverse

**Marketing:** Experiences in the metaverse extend much farther from retail, entertainment, and leisure, as industries look towards capitalising on the reach and opportunity that virtual environments offer. With the digital infinity that blockchain technology and the metaverse offer, functional operations of the insurance landscape are poised to be bolstered and hosted in the metaverse and on the blockchain. The saturated quantities of data stored on the metaverse and which contain information such as consumer purchase history, financial behaviour and incident history, present a gold mine for insurance providers to deliver personalised value to virtual citizens. Virtual environments also create an entirely new and dynamic landscape for marketing opportunities and brand awareness, especially when geared towards the more youthful citizen, who presents the typical user of the metaverse. The metaverse creates an opportunity for sellers of insurance to host client-agent consultations in a virtual setting. This allows for, what is usually a haggle over a phone call, to become an immersive experience enriched by a face-to-face conversation and even virtual depictions and simulations of scenarios and incidents that could impact the insurance holder and their assets. These same virtual environments provide a platform for firms to train claims adjusters in simulated environments mimicking real-life damage inspections through digital replicas of such scenarios.

**Smart insurance contracts:** Metaverse technology brings much more than its face of immersive experiences and data-rich personal avatars suggests. The underpinning blockchain technology powering the metaverse and its assets presents even more use-cases for the insurance industry - tokenised and NFT-based contracts and policies. Whereas real-life contracts are currently digitised and document-based, the issuing of contracts as non-fungible tokens hints at protection from fraudulent activity through forged documents and tampered policies. Tokenised contracts promise traceable and secure documentation in full ownership and control by policyholders. On top of this, smart contracts utilised on the blockchain offer a secure means of premium payments by policyholders or claim settlements by insurance providers, all in cryptocurrency. In the real world, claims can take a significant amount of time to be verified, processed, and paid. Smart contracts may contain functionality that automatically determines whether a claim is valid and applicable, and could disburse payment instantaneously (e.g. travel insurance claims could be instantly paid out once it is verified on the blockchain that a flight was cancelled).

**Innovation:** The data-rich and complex nature of metaverse technology presents the biggest driver for digital transformation in firms looking to prepare for adoption. While no insurance firm benefits from a proprietary and in-house developed metaverse platform or blockchain, there is certainly a need for future-gearred firms to remain digitally dynamic. Synchronous internal IT departments and metaverse centres of excellence will help support the business landscape and employees to remain operational, efficient, and well-trained in handling the new environments, ways of work and products effected by a firm's metaverse adoption. Additionally, the risks and looming regulation of metaverse technology will require an enormous effort from risk, compliance, and governance teams to create risk management frameworks and controls to ensure that all aspects of "metaversal" ventures remain in compliance with regulation and business continuity protocols.

## Risks presented by the metaverse

It would be necessary to determine the main risks related to the unique environment which the metaverse presents. It is also noteworthy that every risk presents an opportunity to provide innovative insurance solutions. Insurance considerations of risks relating to the metaverse would include:

**Crypto wallets:** these are digital wallets/addresses existing on a blockchain where one can store cryptoassets. These wallets can be hot wallets or cold wallets, where the former is a wallet which is connected to the internet and cryptocurrency network (and in most cases, held on a trading exchange) while the latter is an offline wallet stored on a platform not connected to the internet and which is normally used for storage of cryptoassets for prolonged periods of inactivity. Naturally, hot wallets would be riskier from a security perspective and would result in higher insurance premiums for coverage than cold wallets as they would be more exposed to security breaches and/or losses incurred from active trading. Cold wallets are associated with long-term holdings of cryptoassets and are therefore less risky from an insurance perspective as they are not as exposed to vulnerabilities such as online hacks and crypto exchange hacks like hot wallets are.

**Crypto companies:** crypto companies themselves would also require insurance services to offset their risks. These could include policies relating to cybersecurity which are already provided by certain insurance providers and there is now a need to instil and facilitate cryptosecurity policies too. Even though blockchain technology is a technological advancement in digital security, it still will not guarantee its users or providers complete safety. Crypto exchange companies are susceptible to attack. Crypto.com lost \$30 million worth of cryptocurrency from 483 users' crypto wallets in a hack at the beginning of 2022. Additionally, as most crypto companies have user license agreements which result in them holding ownership over the keys to crypto wallets on their exchange, crypto companies could find themselves in potential lawsuits if the keys to these wallets are accidentally deleted or stolen.

**Hackers:** since the rise of the internet, hacking has been a constant security threat which companies have insured against, whether it be over the value of their servers or as a contingency plan in case of a distributed denial-of-service (DDoS) attack. However, the metaverse could intensify this threat. With access to the metaverse leaning toward virtual realities, hackers could access and create copies of your biological and personal data. With data such as your fingerprints and identity details, much damage can be done to financial arrangements and reputation. Hackers may even be able to hack virtual reality gear and execute simulations which could cause neurological and physical harm to users. Insurance companies would therefore have to create tailor-made policies for these virtual reality-related risks and others no one has even thought of yet.

**Cryptocurrency:** cryptocurrency holders and traders are creating an increasing demand for insurance policies relating to cryptocurrency itself. This would be tricky from an insurance perspective, as it would require an in-depth understanding relating to the nature of the currency at hand. For example, blockchains can be categorised into various levels, similarly to how our current networks can have various levels. Just like how the internet is one level, and the world wide web is built on top of the internet, and certain applications like Facebook are built on top of the web – similar instances occur for blockchain networks. Blockchains which have no scalability (the ability to build an app or software on top of a blockchain) are typically less risky than blockchains which do have scalability. This is because the more layers the cryptoasset is built on top of, the more vulnerabilities it is exposed to as it is exposed to the inherent risk of each layer.

Additionally, the nature of the cryptoasset itself could be risky. Luna was a cryptocurrency which instead of being backed by fiat money, was attempting to be backed by cryptocurrency itself to branch away from fiat dependency. As a result, it lost 99.9% of its value after falling victim to a wide-scale dilapidation because its stablecoin was de-pegged.

Insurance companies would therefore need an in-depth technological understanding of each cryptocurrency before drafting policies for them. Insurance companies may need to consider the curation of a one-size-fits-all cryptocurrency insurance policy as the due diligence required for unique cryptoassets may be cost-intensive. Offering unique, tailor-made insurance solutions may be possible if policyholders are willing to pay higher premiums for them. Insurance companies may choose to outsource the analysis of blockchain vulnerabilities and crypto-related risks to avoid capital-intensive investments.

**Rugpulls:** these are situations where the original creator(s) of a crypto project gather funding (whether cryptocurrency or fiat currency) through an initial offering in exchange for their created cryptoasset. This could be cryptocurrency or an NFT. The creators then disappear with the money received from investors, rendering the project an empty shell, causing its fair market value to nosedive, and essentially removing whatever solid foundation investors thought they had from underneath them. For centuries, people have fallen victim to ponzi schemes and fraudulent projects, and therefore insurance companies would need to perform extensive due diligence on a crypto project before being willing to create any policies for the investor or creator's benefit.

**Physical and mental health:** much like the increase of technological and social media adoption has had a correlative effect on the decreased mental and physical health of most developed societies, the mainstream adoption of a virtual reality-based metaverse is expected to have the same impact. With individuals spending more time in a virtual world, reduced physical movement would result in decreased quality of physical health. This, coupled with the concept of the real world being contrasted with a utopian virtual world could result in increased mental health issues. There is also a risk of physical injury – an India Times article notes that “many users who are already logged onto the metaverse are reporting injuries - ranging from benign fractures to more serious ones. According to the Wall Street Journal, virtual reality is sending people to emergency rooms.”<sup>1</sup> This is yet another opportunity for insurers to consider offering insurance to cover metaverse physical injury risk. This decrease in the quality of society's physical and mental health could result in insurance companies having to diversify their life and medical insurance product range.

<sup>1</sup> <https://www.indiatimes.com/technology/news/virtual-reality-injuries-rising-in-hospitals-561025.html>



## Future

The road to realising the possibilities and opportunities that the metaverse promises, is riddled with risks and undefined regulatory hurdles that need to be addressed before firms can begin to pilot associated programmes. Both the pace at which the technology evolves, and its mainstream adoption present even further challenges that CIOs and COOs will have to consider as they undertake their metaverse journey. Regardless, the insurance industry is poised to evolve as metaverse technology continues to accelerate in growth, scope, and adoption. While physical and real-life asset insurance will always be necessary, digital assets such as cryptocurrencies, NFTs, and virtual real estate usher in new classes of assets to be insured and protected. The metaverse's virtual environments will serve as platforms for immersive client-customer engagement with data-rich personal avatars providing a means for personalised policies and product offerings. Blockchain technology provides a means for a more secure, automated, and robust mechanism for the issuing of contracts and policies, while transactions facilitated by smart contracts hosted on the blockchain provide a means for settling of claims and payment of insurance premiums. Firms will need to gear towards digitally transforming their businesses to remain ever ready for the inevitable arrival of these revolutions to the insurance landscape, and to stay abreast of the risks, regulation, and impending legal implications.

Insurance entities should take the time to understand what the metaverse entails and what it is trending towards. Insurance laws may need to evolve as well, as End-User License Agreements (EULA) for participating in various metaverse platforms may become increasingly important for insurance purposes. Just as a drunk driver cannot claim for a car crash, individuals who sign up to participate in certain metaverse activities and agree to whatever was stated in the EULA without understanding the terms and conditions may not be able to claim from their insurance provider. A conversation will then have to be had regarding whether an everyday layperson would understand the concepts and clauses of the EULA they agreed to. People are becoming simpler, while the bounds of technology are becoming increasingly complex, and it is therefore the task for insurance companies to find a middle ground on which to base innovative insurance solutions.

It is extremely easy to get caught up in the hype and want to be the 'first' and 'ground-breaking' insurance company to branch into the metaverse, however the space is constantly evolving. We have not even begun to scratch the surface of what the impact of the metaverse, blockchain technology and NFT's will be on society at large. Innovative companies are not necessarily successful companies, and it may be worthwhile to sit back, obtain an evolving understanding, analyse the market, and determine what works before branching into the metaverse. Being the first to the market is exciting, however investing in a market too quickly could mean the difference between becoming the next Myspace, or the next Facebook.

### P.S. Note from the editor

If you are like me and are still grappling with coming to grips with the barrage of new technologies and the technical jargon that goes with it, on the next page we thought we would include a glossary of the technical terms used that might help you navigate this article.

Term	Definition	Reference source
Distributed ledger	A <b>distributed ledger</b> is a database that is consensually shared and synchronized across multiple sites, institutions, or geographies, accessible by multiple people. It allows transactions to have public "witnesses." The participant at each node of the network can access the recordings shared across that network and can own an identical copy of them. Any changes or additions made to the ledger are reflected and copied to all participants in a matter of seconds or minutes. A distributed ledger stands in contrast to a centralized ledger, which is the type of ledger that most companies use. A centralized ledger is more prone to cyber attacks and fraud, as it has a single point of failure.	<a href="https://www.investopedia.com/terms/d/distributed-ledgers.asp">https://www.investopedia.com/terms/d/distributed-ledgers.asp</a>
Blockchain	A <b>blockchain</b> is a distributed database or ledger that is shared among the nodes of a computer network. As a database, a blockchain stores information electronically in digital format. Blockchains are best known for their crucial role in cryptocurrency systems, such as Bitcoin, for maintaining a secure and decentralized record of transactions. The innovation in a blockchain is that it guarantees the fidelity and security of a record of data and generates trust without the need for a trusted third party. One key difference between a typical database and a blockchain is how the data is structured. A blockchain collects information together in groups, known as blocks, that hold sets of information. Blocks have certain storage capacities and, when filled, are closed and linked to the previously filled block, forming a chain of data known as the blockchain. All new information that follows that freshly added block is compiled into a newly formed block that will then also be added to the chain once filled. A database usually structures its data into tables, whereas a blockchain, as its name implies, structures its data into chunks (blocks) that are strung together. This data structure inherently makes an irreversible timeline of data when implemented in a decentralized nature. When a block is filled, it is set in stone and becomes a part of this timeline. Each block in the chain is given an exact timestamp when it is added to the chain.	<a href="https://www.investopedia.com/terms/b/blockchain.asp">https://www.investopedia.com/terms/b/blockchain.asp</a>
Cryptocurrency	A <b>cryptocurrency</b> is a digital or virtual currency that is secured by cryptography, which makes it nearly impossible to counterfeit or double-spend. Many cryptocurrencies are decentralized networks based on blockchain technology—a distributed ledger enforced by a disparate network of computers. A defining feature of cryptocurrencies is that they are generally not issued by any central authority, rendering them theoretically immune to government interference or manipulation.	<a href="https://www.investopedia.com/terms/c/cryptocurrency.asp">https://www.investopedia.com/terms/c/cryptocurrency.asp</a>
Non-fungible token (NFT)	A <b>non-fungible token (NFT)</b> is a financial security consisting of digital data stored in a blockchain. The ownership of a NFT is recorded in the blockchain, and can be transferred by the owner, allowing NFTs to be sold and traded. NFTs can be created by anybody, and require few or no coding skills to create. <sup>[1]</sup> NFTs typically contain references to digital files such as photos, videos, and audio. Because NFTs are uniquely identifiable assets, they differ from cryptocurrencies, which are fungible.	<a href="https://en.wikipedia.org/wiki/Non-fungible_token">https://en.wikipedia.org/wiki/Non-fungible_token</a>
Token/tokenized	Generally speaking, a token is a representation of a particular asset or utility. Within the context of blockchain technology, tokenization is the process of converting something of value into a digital token that's usable on a blockchain application. Assets tokenized on the blockchain come in two forms. They can represent <b>tangible</b> assets like gold, real estate, and art, or <b>intangible</b> assets like voting rights, ownership rights, or content licensing. Practically anything can be tokenized if it is considered an asset that can be owned and has value to someone, and can be incorporated into a larger asset market.	<a href="https://www.gemini.com/cryptopedia/what-is-tokenization-definition-crypto-token#section-security-tokens-utility-tokens-and-cryptocurrencies">https://www.gemini.com/cryptopedia/what-is-tokenization-definition-crypto-token#section-security-tokens-utility-tokens-and-cryptocurrencies</a>
DDoS attack	A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of internet traffic.	<a href="https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/">https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/</a>
Stablecoin	Stablecoins are cryptocurrencies the value of which is pegged, or tied, to that of another currency, commodity or financial instrument. Stablecoins aim to provide an alternative to the high volatility of the most popular cryptocurrencies including Bitcoin (BTC), which has made such investments less suitable for wide use in transactions.	<a href="https://www.investopedia.com/terms/s/stablecoin.asp">https://www.investopedia.com/terms/s/stablecoin.asp</a>

P.P.S. Further note from the editor – if, like me, you still don't understand, please feel free to call one of the authors at KPMG!

## References

<https://www.faegredrinker.com/en/insights/publications/2022/7/protecting-your-insurance-brands-in-the-metaverse>

<https://www.vertafore.com/resources/blog/insurance-metaverse>

<https://www.zurich.com/en/media/magazine/2022/can-we-work-in-the-metaverse>

<https://www.atlas-mag.net/en/category/tags/focus/digital-insurance-in-the-metaverse>

<https://next.ergo.com/en/Trends/2022/metaverse-meta-virtual-reality-opportunities-challenges-financial-insurance>

<https://www.lexology.com/library/detail.aspx?g=f4360185-b3fc-4421-ab31-dd5023f9e0a0>

<https://www.prweek.com/article/1790069/metaverse-insurance-ushering-new-class-assets>

<https://www.reuters.com/article/bc-finreg-metaverse-insurers-opportunity-idUSKCN2MQ1D3>

<https://open.spotify.com/episode/5CsPXddmENJ2M9aXTXuJtj?si=5bUfRcMpRTaEZTvnS73CAw>

<https://open.spotify.com/episode/0SIW6z7hXX6ohyFePijX12?si=00ecc825e5034489>

<https://open.spotify.com/episode/5FI15pDy305Gy5qwdAIJFM?si=10280a0f84324a48>

<https://youtu.be/tMAUYVfmhko>

<https://www.vertafore.com/resources/blog/understanding-metaverse-and-insurance>

<https://www.iamagazine.com/markets/nft-insurance-understanding-the-challenges-and-solutions>



