

CREATING
RISK
INTELLIGENT
PROFESSIONALS



GRMI

**GLOBAL RISK
MANAGEMENT
INSTITUTE**

METaverse / *Srijan Ghosh (Batch 10); guided by Saurav Nath*

PROGRAMME
ENDORSED BY



ASSOCIATE
PARTNER



STRATEGIC
PARTNER



ASSOCIATE
MEMBER

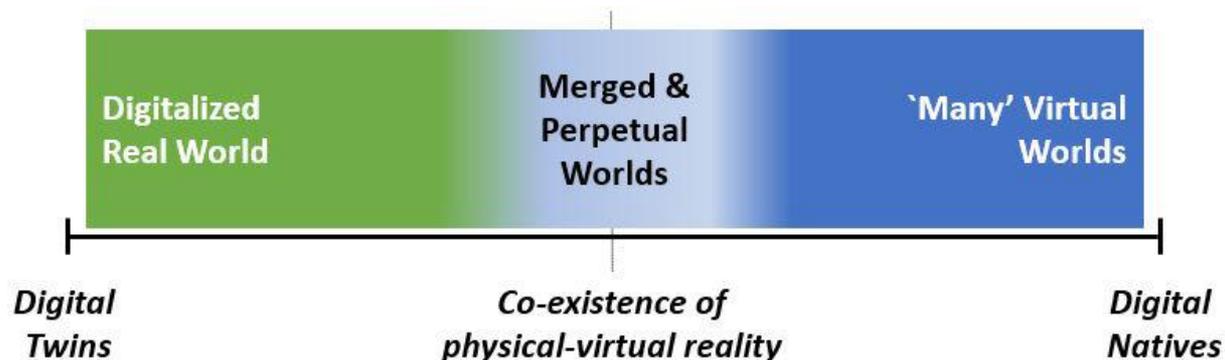


STRATEGIC
PARTNER



INTRODUCTION

- ❑ METAVERSE, combination of the prefix “meta” (implying transcending) with the word “universe”.
- ❑ The word ‘metaverse’ was first coined in a piece of speculative fiction named Snow Crash, written by Neal Stephenson in 1992. In this novel, Stephenson defines the metaverse as a massive virtual environment parallel to the physical world, in which users interact through digital avatars.
- ❑ To achieve such duality, the development of metaverse has to go through three sequential stages, namely:
 - Digital twins,
 - Digital natives and eventually
 - Co-existence of physical-virtual reality or namely the surreality.



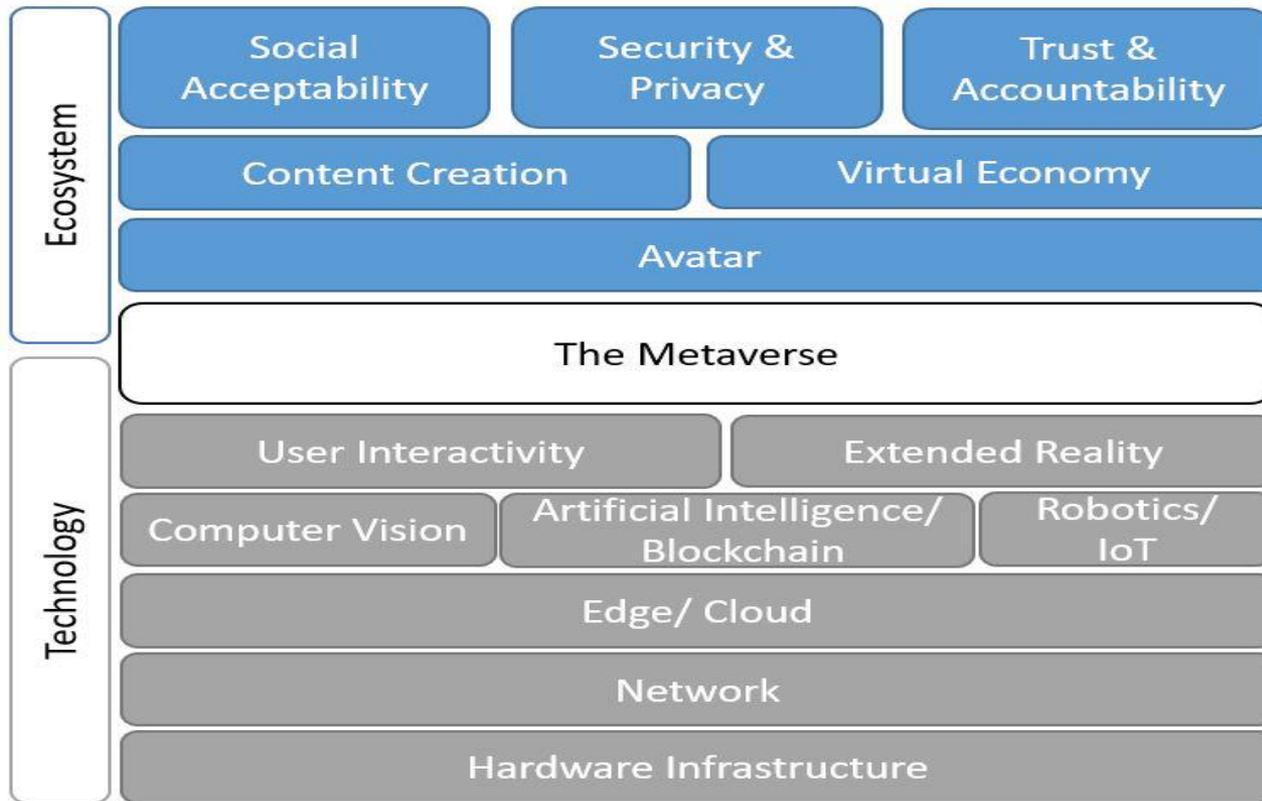
The under-explored cyberspace
(Opportunities of entering the Metaverse)

(RW)(P)(CC)(S)/ Experience- Duality (ED)										
(RW)(P)(CC)/ Social as Community (S)	 Twitter	 Instagram	 Clubhouse	 TikTok	 Animal Crossing	 Second Life	 VR Chat	 XSight	 Pokémon Go	 University
(RW)(P)/ Content Creation (CC)	 Medium	 Pixlr	 Adobe Audition	 YouTube	 Super Mario Maker	 Roblox	 Quill	 Adobe Aero	 BIM	 Soft Clay
(RW)/ Personalisation (P)	 Xanga	 Meitu	 Spotify	 Netflix	 Diablo	 Fortnite	 VR Commerce	 IKEA Place	 Google Map AR	 Shopping
Read & Write (RW)	 SMS	 Camera App	 MMS	 Zoom	 S. Mario Bros	 Simcity	 Beat Saber	 Skype	 AR Translator	 Mah Jong
	Text	Image	Audio	Video	Gaming	Virtual 3D	VR	MR	AR	Physical

Fig.: The cyberspace landscape of real-life applications, where superseding relationships exists in the information richness theory (left-to-right) as well as transience-permanence dimension (bottom-to-top).



“Metaverse = Physical world + Digital world”



➤ Connecting the physical world with its digital twins, and further shifting towards the metaverse:

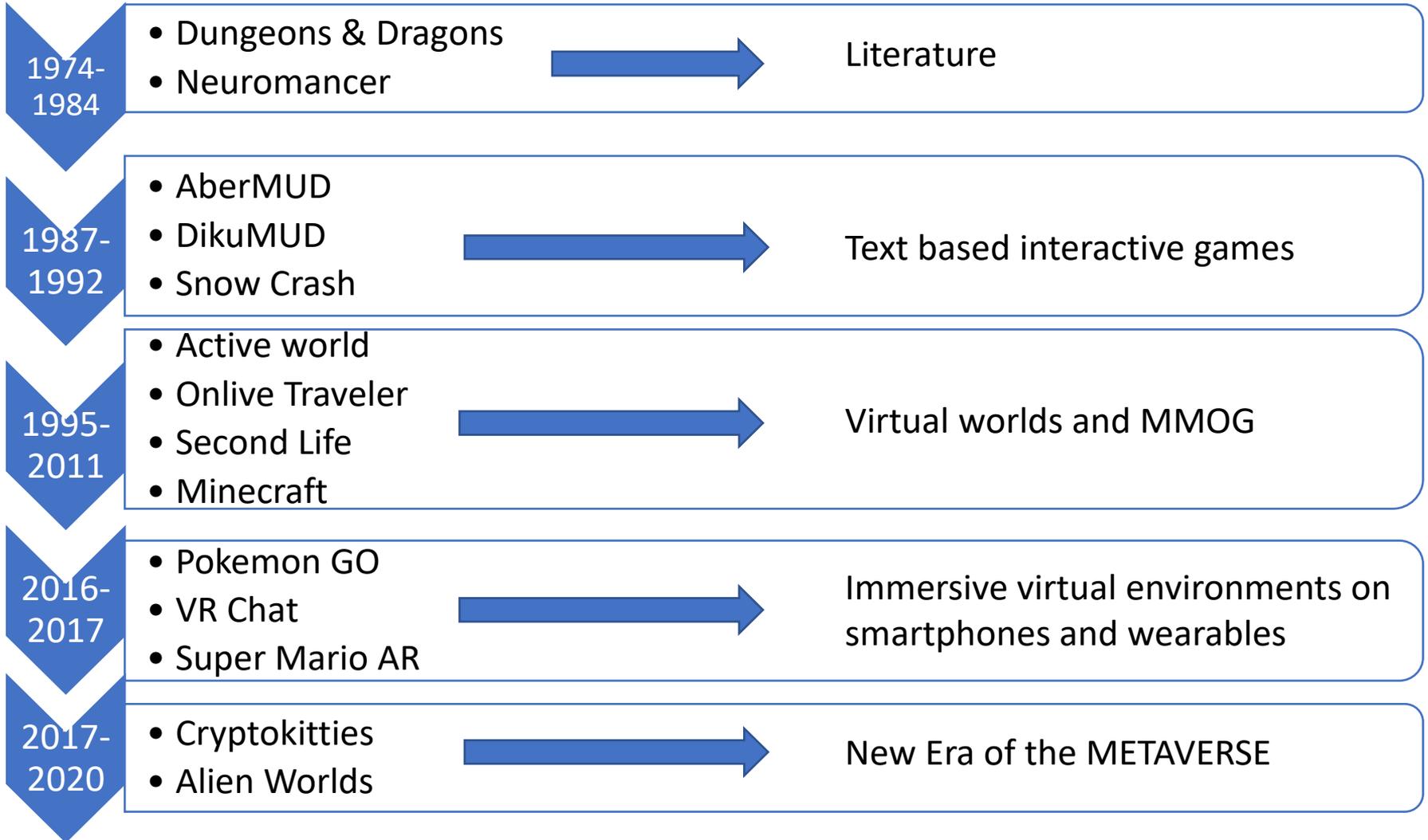
(A) *The key technologies* –

Blockchain, Computer Vision, Distributed Network, Pervasive Computing, Scene Understanding, Ubiquitous Interfaces and

(B) *Ecosystems* –

Avatar, Content Creation, Data Interoperability, Social Acceptability, Security/Privacy, Trust/Accountability.

TIMELINE



RISKS IN METAVERSE

- The metaverse may be used for **cybercrime activities**. These include cyberbullying, impersonation, hacking and others. A criminal can impersonate an actual person or business in the metaverse and cause a lot of reputational damage in the real world.
- The metaverse raises **new legal challenges**. One is the lack of legislation and enforcement. The metaverse has no physical laws and jurisdictions. It is therefore difficult to control and regulate actions that would be deemed illegal.
- Violence and murder may be propagated in an **uncontrolled** metaverse. Warnings have already been issued about some digital games due to their graphic content. The metaverse would pose additional danger as it is a 3D simulated experience.
- The metaverse will make it easier for **intellectual property infringement** to take place. Since there are no laws in the metaverse, then anybody can infringe content in the metaverse. Disclosure of unprotected information on the metaverse can be dangerous for a company. Disclosure of trade secrets by a company can be risky if the competitors access that on the metaverse.
- The metaverse carries a **data privacy risk**. Third parties can monitor activities on the metaverse to study consumer behaviour and engage in uncontrolled data mining.

➤ Risks To People:

- **Physical damages** – People using immersive technologies – such as virtual reality headsets can become disoriented in the real world environment and injure themselves. They may even get used to taking actions that have no consequences in the metaverse, such as jumping off the second floor or walking into traffic, thus making them insensitive to real-world hazards.
- **Mental health** – Because these are new technologies, there are no long-term studies on their physical and mental impacts. Although side effects vary between people, immersive games can lead to depression, isolation, lonely behavior, and even suicide and violence.
- **Digital consent** – There are no laws or legal jurisdiction in the metaverse, as there are no physical boundaries or boundaries. For the same reason, there is no responsibility for actions, although there is progress in the regulation of social networks.

Some Important Risks And Their Mitigation In Metaverse

Copyright Risk:

“Copyright (or author’s right) is a legal term used to describe the rights that creators have over their literary and artistic works. Works covered by copyright range from books, music, paintings, sculpture, and films, to computer programs, databases, advertisements, maps, and technical drawings.”

The metaverse also creates risks for copyright owners. e.g., policing the metaverse for piracy of copyrighted works can be challenging. Additionally, if the use of the copyrighted work is de minimis, the copyright owner may have difficulty proving infringement.

Also, content creators face unique risks. e.g, if they are relying on existing licenses in underlying works to create digital content for the metaverse, they must ensure that those existing licenses cover the use of the copyrighted work within the metaverse.”

Best practices for owners and users of copyrighted works:

Suggested best practices for use of copyrighted works in the metaverse include-

- **Reviewing agreements** for distribution of third-party content for proper licenses to copyrighted works
- **Ensuring** that agreements with customers protect against unintended distribution of copyrighted works
- Promptly **registering** copyrights in metaverse assets and software
- Properly **marking** copyrighted works
- **Implementing technological measures** to protect against unauthorized distribution of the works

Trademark Risk:

“A trademark is a sign capable of distinguishing the goods or services of one enterprise from those of other enterprises. Trademarks are protected by intellectual property rights.”

A case study –

In the United States at least, trademark owners have not always fared well in their efforts to enforce trademarks used in virtual worlds.

An early example of the potential pitfalls of using real-world trademarks in the virtual world played out in *E.S.S. Entertainment 2000, Inc. v. Rock StarVideos, Inc.*, 547 F.3d 1095 (9th Cir. 2008). In *E.S.S.*, the issue was whether a virtual depiction of a real-world strip club in the popular game **Grand Theft Auto: San Andreas** infringed the real strip club’s logo and exterior design trademark rights. The court ultimately held that the depiction of the strip club in the video game did not infringe the strip club owner’s trademark and trade dress rights as the video game was an artistic expression protected by the First Amendment, and it was unlikely that consumers would be confused into believing that the strip club produced the sophisticated video game.

With the proliferation online “virtual world” games such as **Pokémon Go**, **The SIMS**, and **Second Life**, a new set of issues have arisen involving the use of third-party trademarks in virtual worlds. For example, *Second Life*, a large multiplayer role-playing game that also operates as an online economy, allows users to create their own virtual worlds, develop and promote intellectual property, and even sell their own branded creations (or those of others – more on that below) for a profit. However, with these opportunities also come the risks of unauthorized use of third-party trademarks and possible brand dilution.

Best practices for trademark owners:

- **Registration of trademark:** Brand owners are strongly encouraged to register their trademark with the USPTO and foreign equivalents.
- **Subscribing to a trademark watch service:** Trademark watch services allow the trademark owner to monitor relevant markets and Internet content for possible infringing activity.
- **Notification:** Assuming the infringing activity is being conducted by a third-party platform user, brand owners should report this infringement to the platform.
- **Evaluate the nature of use and possible claims:** Once aware of possible infringing activity, consider the nature of the infringing use and how the use affects the overall brand and the market for the goods/services associated with the brand.

Patent Risk:

“A patent is an exclusive right granted for an invention, which is a product or a process that provides, in general, a new way of doing something, or offers a new technical solution to a problem. To get a patent, technical information about the invention must be disclosed to the public in a patent application.”

The risks to owners of metaverse-focused patents include potential invalidation of the patents during litigation to enforce the patent. U.S. courts increasingly have been invalidating software-focused patents as “abstract” and ineligible for patenting under section 101 of the U.S. Patent Code and a landmark U.S. Supreme Court decision titled *Alice Corp. v. CLS Bank International*, 573 U.S. 208 (2014). In 2020, the patent eligibility of 27 software patents was at issue in appeals before the U.S. Court of Appeals for the Federal Circuit (CAFC), which is the U.S. appellate court dedicated to deciding patent law issues. Out of the 27 patents, the CAFC found only four to be partially or fully eligible under section 101.

The law in this area is still developing and is murky at best. This creates uncertainty in the value of patented AR/VR inventions.

Best practices for owners of metaverse related inventions:

- Whether the invention will be useful in more than 20 years. If so, it is worth **exploring trade secret protection** because trade secrets can last longer than the 20-year life of a patent, assuming the trade secret does not become stale due to advances in technology.
- **How difficult it is for other companies to reverse engineer the invention.** The easier it is to reverse engineer an invention, the less likely it will be considered to be a trade secret.
- **How often their employees who have access to the invention change jobs.** It becomes more difficult to protect trade secrets in industries with high attrition rates and in jurisdictions that do not view noncompete restrictions favorably.



Disclaimer

This report has been produced by students of Global Risk Management Institute for their own research, classroom discussions and general information purposes only. While care has been taken in gathering the data and preparing the report, the student's or GRMI does not make any representations or warranties as to its accuracy or completeness and expressly excludes to the maximum extent permitted by law all those that might otherwise be implied. References to the information collected have been given where necessary.

GRMI or it's students accepts no responsibility or liability for any loss or damage of any nature occasioned to any person as a result of acting or refraining from acting as a result of, or in reliance on, any statement, fact, figure or expression of opinion or belief contained in this report. This report does not constitute advice of any kind.

Campus Address :

88, Sector 44,
Gurgaon – 122002

CONTACT US

www.grm.institute

Email :
admissions@grm.institute

Thank you!

