

What is The Metaverse?

Alfraih, Mohammed, Essa, Abdullah

Saudi Aramco

DOI: <https://doi.org/10.5281/zenodo.7064221>

Published Date: 09-September-2022

Abstract: This paper will examine the broad idea of the metaverse, identify key concepts, distinguish between terms used in the metaverse, and discuss the space's implementation, cybersecurity, and historical aspects. Additionally, covered in the paper are Web 3.0's introduction to the metaverse and how blockchain has evolved into a key building block for a successful metaverse project. The paper defined haptics and described its crucial function in the immersive AR/VR experience. It draws attention to contentious cybersecurity concerns with the Metaverse, including identity as the new perimeter and privacy issues there. The study addresses the metaverse's economic implications and how they will change how people live and work globally. Additionally, it highlights the significance of the metaverse and how this technological breakthrough will affect the labor market in the future. The study briefly discusses the metaverse's major phases at this crucial juncture in human history. The best ways to safeguard yourself in the metaverse are also covered in the study.

Keywords: Metaverse FORTNITE MINECRAFT RUNESCAPE SECOND LIFE Web 2.0 Web 3.0.

I. INTRODUCTION

The term "metaverse," which has a wide range of interpretations, originally debuted in the science fiction book Snow Crash in the 1992. The metaverse was created when the plot of the book was created on early Mac OS versions using specialized image-processing software. The phrase refers to a 3D virtual environment where users can communicate with one another using avatars in order to create an immersive virtual reality experience.

II. PAPER PREPARATION GUIDELINES

2.1 What is the Metaverse?

Metaverse is a catchword that can have several meanings but the origin of the word is dating back to the 1992 as part of a fiction novel called Snow Crash. The novel has used custom image-processing software on early versions of Mac OS to write the storyline, hence the metaverse. The word refers to 3D virtual world where people can socialize in an immersive virtual reality setting represented by avatars. Virtual reality (VR) and augmented reality (AR) are the most common terms used in the Metaverse. Both terms have been circulating for around 30 years. The difference is the user experience when technology is put to use. Virtual reality (VR) has emerged in the late 1980s, it is a first person simulated environment that provides a virtual, immersive, interactive experience and gives the user a strong sensation of presence. Augmented reality (AR) has emerged in the early 1990s, AR on the other hand can be experienced in a real world setting with access to a smartphone. It a combination of real and virtual environment. For many years, the main terms used in academia and business were virtual reality and augmented reality, although more terms have recently gained popularity. For instance, extended reality (XR) arose to define the whole range of VR and AR capabilities and has since evolved into a useful umbrella term for numerous immersive media types. Although it has gained popularity, the term mixed reality (MR) is most often used as a synonym for augmented reality. The term was introduced by Microsoft when it introduced HoloLens headset and began using the term "mixed reality" in its marketing materials back in 2010.

Recently, the term "metaverse" has gained enormous popularity. The term wasn't utilized frequently until Facebook (now Meta) backed it with its marketing power. A metaverse is a large number of concurrent users are immersed in a persistent

and immersive virtual environment and feel strongly connected to one another. It is believed that a metaverse to be called a metaverse needs to have a defined code of moral guidelines and a fully operational economy.

Metaverse is newly introduced to Web 3.0 which is often referenced to whether data is stored on the blockchain in a decentralized approach or centralized if a company decided to store data internally in a traditional way. Public Blockchain provides transparency, interoperability and no control over user data. In contrast, if a metaverse project stores user on the cloud or in premise. Then, the said company is in control of everything and it is up to the internal regulations and regulations of the countries hosting the service to deal with user data.

It is often going undetected but a simple action such as phone vibration is a sign that a message or a call is received or a gentle feedback vibration is a sign that a button was touched. The concept is called Haptics, it is derived from a Greek word “haptikos”, the use of haptics provides non-responsive surfaces like touchscreens may simulate the tactile feedback of manipulating buttons and knobs or it can be kinesthetic haptic that produce force sensations on a human body, they mostly affect the muscles and are not typically felt on the skin. The use for Haptics is what actually gives AR & VR the immersive experience. It is interesting to see reactions of people that try the metaverse technologies as everyone thinks of a specific business case related to their area of interest.

2.2 Cybersecurity Issues with the Metaverse:

The current issues with Metaverse can be controversial but privacy concerns are almost in everybody’s mind. In the metaverse, data collection is far more sophisticated compared to existing data collection mechanisms. Data gathered about users present serious issues regarding the volume and nature of data. Using the most recent technologies, marketers are able to gather and analyze behind-the-scenes data about user behavior, very detailed specifics such as the time spent looking at a certain visual item, and which items are preferred. The platform in the metaverse is able to monitor bodily movements and physiological responses. Such data is very critical to be owned and processed by a platform with no regulations to govern the privacy of data. Identities in the metaverse is represented by Avatars, avatar basically represents your personal information, behavior and communication in the platform. The majority of cyberattacks that occur online currently involve social engineering techniques. If the avatar metadata is leaked or hacked, it can be exploited to orchestrate targeted social engineering campaigns to target specific group of people using leaked metadata. The possibility of a successful campaign increases significantly given the fact that the attacker has acquired sensitive data related to victims.

Adversaries typically invest in their resources during reconnaissance phase, and enumeration is quite rich in its context considering the risk at hand. Likelihood increases in the given circumstances of the metaverse and that potentially exposes the risk to the surface. Methods of cyberattacks are also emerging in a non-traditional technique considering the cyberspace prospectus is all digitalized, hence the metaverse. Users’ identity can be spoofed, which ultimately may lead an avatar takeover, which makes a common challenge that a user’s identity of a person in the metaverse is always questionable. Client vulnerabilities such as VR and AR headsets that have software and memory those are ripe targets for malicious inadvertent hacks, location spoofing and device manipulation enables perpetrators to wreak havoc in the metaverse. For example, spying maybe an intrusion that goes undetected with the change of appearance and interacting with subjects without affecting their knowledge.

The need of extreme moderation at scale is critical, because the metaverse experience is all about facilitating user-to-user communications. Trust and commerce are the basis of metaverse relationship is built upon, and it takes one bad actor to cause tremendous damage. In addition, there is no existence of metaverse regulations and the need of data collection for a truly immersive experience will surely invade privacy to some, even though users are aware of the knowledge of data level they are providing. Virtual experiences have no borders, and regulations such as GDPR have regional sovereignty requirements, this presents a challenge of assuring privacy at the mercy of platform and property owner(s). The metaverse owner has a complete control, much like real world where ad banners could be put in front of a physical store, showing virtual ads may not be appreciated by your customers and you have no control over it.

Augment Reality (AR) overlays third party data, so a compromise in the integrity could present a challenge, for example if a location app overlaid onto a headset uses flawed location data that will surely result in incorrect directions given to the user. That also draws physical security, with users typically moving around the real world with AR overlay that makes physical security a concern, with too immersed experience in the virtual world they could bring harm to themselves or those around them.

Identity is considered the new perimeter is not only a cliché for security. In a fully operational economy, individuals can own, sell and do all kinds of trades. The same principle is applied to the metaverse and since Avatar represents individuals in the metaverse. Security of the Avatar account becomes a subject of concern. If an avatar account owns NFTs, which is unique identifiers in the blockchain that refers to ownership of a digital asset, and the account got compromised. Then, it is a target for cyber criminals to steal or if an avatar is stolen, impersonation is a threat to look for in the metaverse. Imagine how phishing may appear in the metaverse. It won't be a phony bank email. It can be a teller avatar requesting your details in a virtual bank lobby or a board director sending an invitation to a malicious virtual conference. This is the reason why identity is a top priority for any meaningful progress in the metaverse.

2.3 Why the Metaverse matters?

The metaverse will be an ecosystem of shared virtual worlds. It is projected to be a \$30 trillion industry. It is an economy where everyone no matter where they are, can still participate. The metaverse will provide unprecedented access to opportunities and foster deep interpersonal connections. Most people are compelled to live close to places of employment, it is hardly ever to visit friends and relatives who reside elsewhere. The metaverse can enable people to determine where we live and how we live. The employer's office location is not a barrier anymore, you can be Los Angeles, USA working for a company in Tokyo, Japan.

2.4 Major stages of metaverse development

Blockchain companies and developers effectively work on a huge open source project, which helps explain why blockchain, DeFi, and cryptocurrency innovation happens so quickly. Development is done on top of development. Development in this manner will allow for exponential growth. There are 4 major stages of metaverse development:

Stage 1: Modern VR technology is currently at stage one and only needs a headset and two hand controllers to deliver a largely lifelike experience in a virtual environment. However, VR can currently only have a limited impact on our senses of touch, hearing, and sight. The level of immersion is just not yet complete.

Stage 2: The availability of reasonably priced haptic bodysuits, omnidirectional treadmills, and shoes that allow your entire body to move and feel in a virtual environment identically to how it would in the actual one would be made available to mass-market consumers in the second stage.

Stage 3: The term "Advanced VR" refers to the third stage. Neurotech is a term used to describe a device that can communicate with the brain directly in the setting of virtual reality in order to faithfully replicate a virtual environment without the need for a user interface. One example is Neuralink, which is currently under development.

Stage 4: There's no longer any way to tell the difference between the physical world and the metaverse. The human mind may now be completely mapped using modern neurotechnology and uploaded to the Metaverse.

III. CONCLUSION

Digital transformation is meant for user's enablement, and objectively is aimed for users' better experience, but that has been always the cost of convenience as opposed to cybersecurity. In such revolutionary domain, risks arise to the surface whenever a new technology is emerging. That promotes the need of an agile vehicle to dynamically accept and cope with the rapid adoption of new technologies. Readiness is a key factor to stay ahead of the curve, that would be at a cost worth of investment though. Structure of governance is called for to ready the adoption and welcome the transformation ahead. Readiness and Extreme moderation on a large scale is necessary since the metaverse experience is all about fostering user-to-user communications. To protect the trust and commerce that are the cornerstones of a metaverse partnership. Even if users consent to the scope of the data they are supplying, legislation for data collection for an immersive experience is necessary to guard against privacy violations.

REFERENCES

- [1] Centieiro, H. (2021). The 4 key stages of the Metaverse. Retrieved 22 August 2022, from <https://medium.com/geekculture/the-4-key-stages-of-the-metaverse-84d34cce6f6f>
- [2] Metaverse - Wikipedia. (2022). Retrieved 22 August 2022, from <https://en.wikipedia.org/wiki/Metaverse#:~:text=The%20term%20%22metaverse%22%20originated%20in,to%20increasing%20demands%20for%20immersion.>
- [3] Louis Rosenberg, U. (2022). Metaverse 101: Defining the key components. Retrieved 22 August 2022, from <https://venturebeat.com/arvr/metaverse-101-defining-the-key-components/>