AI & Metaverse - How to trust our digital twin?

Zaïda Rivai, zaida.rivai@danubetech.com

1 Introduction

The next generation successor Artificial Intelligence (AI) & Metaverse has recently attracted a lot of attention in both academia and industry [1]. On one side, metaverse is mostly known to serve the purpose of video games or social platforms such as Fortnite, Second Life or Pokémon Go, however it could likewise be extended to the fields of manufacturing, education, entertainment, and many others [2, 3]. In its core idea, metaverse integrates the physical world with the virtual one, allowing digital avatars to carry out activities, like attending concerts, virtual exhibitions or meetings without the necessity to travel [1]. So, besides serving the corporate interests, the metaverse offers the potential to function as a decentralised platform for many kinds of users.

1.1 AI and Metaverse

Since the breakthrough of AI in fields such as computer vision, decision-making and natural language processing, developers have been motivated to realise AI in metaverse [1]. Machine learning-based methods allow to exceed the level of human's learning by providing technical support for all systems in metaverse, thereby, effecting the operational efficiency and intelligence. As an example, one could use AI for building intelligent voice services that could provide technical support such as voice recognition and communication for metaverse users.

1.2 Digital Twins

To enforce the transition towards a symbiotic AI-metaverse approach, industries are working on building so called digital twins (DT) that create virtual models for physical objects in the digital way to simulate their behaviours [4]. DT have the ultimate goal to be used not only during prototyping and testing, but also during the operational phase. The metaverse generates a huge amount of big data from all different kinds and structures. In order to make use of big data, deep learning-based algorithms are essential [5].

2 Problem

Technological developments in AI resulted in great progress in the automatic operation and design in the metaverse and perform better than conventional approaches [1]. However, with the advances in AI- and metaverse related technologies, critical ethical issues regarding trust over the internet, harm prevention, bullying protocols, fairness, privacy and accountability raise. How should these technologies be used and how should these not be used? Several known issues are:

- *Bullying or sexual harassment* [6]

  A women's avatar was sexually harassed on one of Meta's virtual-reality (VR) platforms, Horizon Worlds. With the current problems of cyberbullying, how do we also solve bullying and harassment in the metaverse?

- *The Metaverse of Intellectual property (IP)*

  In the ultimate vision, the metaverse seamlessly integrates interoperable and decentralised worlds and merges the virtual world with the reality. However, currently the reality is that these worlds are centralised controlled by single entities, raising many IP issues. In order for IP owners to not lose their brand, clear IP licensing arrangements should be established. As with any IP licence, typical terms such as territory, and royalty rates are important. With these IP issues, we should ask ourselves what the scope of these licenses are.

- *Bias in the AI algorithms*

  Flaws in the algorithms are a direct result of the data that is fed into the AI systems. As real world data is likely to be biased in certain or maybe all fields, AI systems build their algorithms incorporating this bias. How can we make sure algorithms are built transparent, explainable, bias-free and accountable?

The intersection between trust and AI are of great importance and relevance to AI ethics and harm prevention. It is possible, however, that the combination of metaverse and AI will fundamentally alter the boundaries between the real world and the digital world or even dissolve them. An individual's face will remain its identity which, with the current technologies, anyone could theoretically (re)-create without having the owner's permission or knowledge. Once it is in a system it has a life of its own.

Solution

Due to the advances in AI and metaverse, it is critical to identify and prevent upcoming problems as soon as possible. The Trust over IP (ToIP) foundation is a project hosted by the Linux Foundation to enable the trustworthy exchange and verification of data between any two parties on the Internet. ToIP technology-stack working group recently launched a new task force called AI & Metaverse Technology Task Force (AIM-TF). The goal of this task force is to complete a ToIP Recommendation for the ToIP community to address opportunities and challenges brought on by advances in AI, Metaverse and related technologies, in relation to ToIP's mission of creating interoperable trust over the Internet. The task force aims to identify the issues brought on by these developments and provide a recommendation for a roadmap of future work in ToIP.

To elaborate on this topic, it is essential to discuss and identify the most important issues regarding trust and identity as AI and metaverse develop. Some

examples of topics that could be discussed during the workshop are:

- What will be the main problem regarding trust as AI and metaverse will be the main platform for social media, trading or collaboration and how could we solve it?
- What complications could we think of when AI is used to build your digital identical self, e.g.: your Digital Twin? What institutions are involved?
- How do we define IP of Meta users and how do we protect it?

Conclusion

With the advancing technologies in AI and metaverse, critical ethical issues raise. We might not even be aware of the scope of these problems yet. Not only should we consider the current problems of AI and internet like cyberbullying or algorithms based on biased data, but many other problems regarding identity, trust, AI and metaverse should be discussed. Identifying these problems before they develop or emerge is crucial and therefore discussing this topic with experts is necessary.

In times where visiting a concert, collaboration with your colleagues or having lunch with your family might soon all happen in the metaverse, it is important that we should focus on *rather than digitalising the human world for machine, machines should learn to live in the human world.*

Acknowledgements

Part of Danube Tech's work on DIDs, SSI, etc. has been supported by eSSIF-Lab.

References

[1] Qinglin Yang, Yetong Zhao, Huawei Huang, Zehui Xiong, Jiawen Kang, and Zibin Zheng. Fusing blockchain and ai with metaverse: A survey. IEEE Open Journal of the Computer Society, 2022.

[2] Pragya Soni. 6 use cases of ai in metaverse, 2022.

[3] Yuhei Ando, Ruck Thawonmas, and Frank Rinaldo. Level of interest in observed exhibits in metaverse museums. Proceedings of the innovations in information and communication science and technology IICST, pages 62–66, 2012.

[4] Jacob Hochhalter, William P Leser, John A Newman, Vipul K Gupta, Vesselin Yamakov, Stephen R Cornell, Scott A Willard, and Gerd Heber. Coupling damage-sensing particles to the digitial twin concept. Technical report, 2014.

[5] Qinglin Qi and Fei Tao. Digital twin and big data towards smart manufacturing and industry 4.0: 360 degree comparison. Ieee Access, 6:3585–3593, 2018.

[6] BBC. Female avatar sexually assaulted in meta vr platform, campaigners say, 2022.