Metaverse, Zero Trust

"Metaverse" and "Zero Trust", these are the two most hot words now on the Internet, but the author is definitely not to join in the fun, but the author thinks that we must add something new to the hot "metaverse", because we need a secure metaverse.

The author checked the English Wikipedia, Chinese Wikipedia and Baidu Encyclopedia, and believed that Baidu Encyclopedia's explanation of the "Metaverse" is relatively complete. The Metaverse is a virtual world that is linked and created by technological means and is a virtual world that maps and interacts with the real world, a digital living space with a new social system. The Metaverse is essentially the process of virtualizing and digitizing the real world, which requires a lot of transformations in content production, economic systems, user experience, and physical world content. It provides an immersive experience based on extended reality technology, generates a mirror image of the real world based on digital twin technology, builds an economic system based on blockchain technology, and closely integrates the virtual world and the real world in the economic system, social system, and identity system, and allows every user can produce content and edit content.

The author does not have time to deeply understand and study the Metaverse but based on the author's 30 years of experience in the Internet industry and 17 years of experience in the cryptographic industry,

the author boldly predicts what the Metaverse needs, it is "Metaverse needs zero trust" and "Metaverse needs cryptography".

First, the Metaverse needs trusted digital identities. How to prove the true identities of individuals (people and things) in the virtual world must give each individual a digital identity certificate. We should zero trust on virtual people and things without a trusted digital identity certificate, and only in this way, can ensure the security of people in the virtual world.

The second is that all communication connections in the Metaverse require HTTPS encryption. Whether it is from people, things to the cloud or from the cloud to the cloud, encrypted connections must be used to effectively protect the exchange of confidential information between people in the virtual world and the real world, which is a zero-trust security guarantee for network traffic, which effectively guarantees the connection security of all applications in Metaverse.

The third is the code security of Metaverse. The realization of Metaverse is inseparable from the realization of software codes. These codes must have digital signatures to prove their trusted identities. Zero trust in the codes that realize Metaverse is to ensure Metaverse base security in virtual worlds. Never trust and never running code without trusted digital signatures can effectively ensure the security and reliable operation of all systems in Metaverse, including remote upgrades of virtual reality devices that only install the upgrade code with trusted digital signature.

The fourth is the electronic documents in Metaverse. How to prove that the identity of the publishers of these electronic documents is authentic and trusted? It must be guaranteed by digital signatures, never trust electronic documents without digital signatures. This is one of the important elements to ensure the safety of people in Metaverse. For document security, of course, timestamps are indispensable. How to prove the trust of time related applications in Metaverse, it must be guaranteed by timestamp signatures, which can not only ensure the trust of the document time and the signing time of electronic contracts, but also it can ensure the trust, non-tampering, and non-repudiation of Metaverse data production time and usage time.

The fifth is the data security in Metaverse. Each data producer must digitally sign the data with its trusted digital certificate to prove that the source of the data is authentic and encrypt it with the public key of the recipient to ensure that only the recipient can decrypt this data with its private key, this is a powerful technical means to secure the usage and exchange of important data in Metaverse.

Metaverse is an advanced stage of digitalization. The production, circulation, transaction, consumption, etc. of elements of Metaverse are inseparable from cryptography and zero trust. Zero trust plus cryptographic technology can effectively protect the digital security of Metaverse.

In this article, the author boldly proposes several new terms: meta-certificate, meta-CA, meta-PKI, and meta-cipher. PKI and digital certificate are the core technologies for securing the digital world, and of course they become the core technologies for securing the Metaverse. Therefore, the author firmly believes that cryptography will be widely used in Metaverse, and coupled with the concept of zero trust, the security of the metaverse will be guaranteed. It is hoped that this article can serve as a guide, so that cryptography and zero trust can be widely used in the Metaverse and provide a strong security guarantee for the Metaverse.

Richard Wang

Dec. 29, 2021
In Shenzhen, China