元宇宙，零信任

“元宇宙”和“零信任”，这是目前网上最火的两个名词，但是笔者绝对不是凑热闹，而是笔者认为必须为火热的“元宇宙”再添点新意，因为我们需要安全的元宇宙。

笔者查了一下英文维基百科、中文维基百科和百度百科，认为还是百度百科对元宇宙的解释比较完整。元宇宙（Metaverse）是利用科技手段进行链接与创造的，与现实世界映射与交互的虚拟世界，具备新型社会体系的数字生活空间。元宇宙本质上是对现实世界的虚拟化、数字化过程，需要对内容生产、经济系统、用户体验以及实体世界内容等进行大量改造。它基于扩展现实技术提供沉浸式体验，基于数字孪生技术生成现实世界的镜像，基于区块链技术搭建经济体系，将虚拟世界与现实世界在经济系统、社交系统、身份系统上密切融合，并且允许每个用户进行内容生产和编辑。

笔者并没有时间去深入了解和研究元宇宙，但是基于笔者在互联网从业三十年和密码行业 17 年的经历，笔者还是大胆地预测一下元宇宙还需要什么，总结一句话就是“元宇宙需要零信任”，“元宇宙需要密码”。

首先，元宇宙需要可信数字身份，如何证明虚拟世界的个体(人和物)的真实身份，必须给每个个体一个数字身份证书，我们应该对没有可信数字身份证书的虚拟人和物零信任，只有这样，才能保障人们在虚拟世界的安全。

其次就是元宇宙的所有通信连接需要 https 加密，无论是从人、物到云端还是云端到云端

之间的连接，必须采用加密连接，从而有效保护人们在虚拟世界与现实世界各种机密信息交换安全，这是一个对网络流量的零信任安全保障，有力保障元宇宙的各种应用连接安全。

再就是元宇宙的代码安全，元宇宙的实现离不开各种软件代码的实现，这些代码都必须有数字签名来证明其可信身份，对实现元宇宙的代码的零信任就是为了保障元宇宙虚拟世界的基础安全。不信任和不运行没有可信数字签名的代码，能有力保障元宇宙的各种系统的安全可靠运行，包括各种虚拟现实设备的远程升级，都必须验证有可信数字签名的代码才能运行。

还有云宇宙中的电子文档，如何证明这些电子文档的发布者的身份是真实可信的，必须有数字签名来保障，不信任没有数字签名的电子文档，这是保障人们在元宇宙的安全的重要元素之一。对于文档安全，当然也少不了时间戳，如何证明元宇宙中的各种时间应用的可信，必须有时间戳签名来保障，不仅能保证文档的时间可信，电子合约的签署时间可信，而且能保证各种数据生产时间和使用时间的可信、不可篡改和不可否认。

最后就是元宇宙中的数据安全，每一个数据的生产者都必须用其可信数字证书数字签名此数据来证明数据的来源真实可信，并用数据的接收者的公钥加密确保只有接收者才能用其私钥解密此数据，这是保障元宇宙中各种重要数据使用和交换的有力技术手段。

也就是说，元宇宙是数字化的高级阶段，元宇宙的各种元素的生产、流通、交易、消费等等都离不了密码技术，离不开零信任安全，零信任加密码技术能有效保障元宇宙的数字安全。

笔者就在本文大胆地提出几个新名词：元证书、元 CA、元 PKI 和元密码，PKI 和数字证书是保障数字世界的核心技术，当然也就成为了保障元宇宙安全的核心技术。所以，笔者坚信：密码技术将在元宇宙中得到广泛应用，再加上零信任理念，则元宇宙的安全就有了保障。希望本文能起到抛砖引玉的作用，使得密码和零信任在元宇宙得到广泛应用，为元宇宙提供有力的安全保障。

王高华

2021 年 12 月 29 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。