院系：网络空间安全学院

姓名：胡宇

学号：U202112146

**基于区块链实现访问控制**

本人对这区块链和元宇宙十分感兴趣，虽这两个概念联系不大，但我还是想借此机会谈谈我对此的理解。

1. **关于区块链技术**

**1）初识区块链**

接下来我根据自我学习浅谈一下我对区块链技术的理解，从技术层面来看，区块链技术可以说是集多种学科于一身，区块链包含如下多种学科：包括数学、密码学、计算机科学与技术、网络安全技术、互联网相关技术等。从区块链技术的实用价值角度来说，区块链是一个特殊共享账本和数据库，且此账本是分布式的（下文有具体介绍何为分布式）具有去中心化、难以篡改、操作留有陈迹、可以且容易回溯、通过用户集体来维护、公开且透明的特性。而区块链所具有的丰富的应用场景，基本上都来自于区块链能够处理信息不对称的问题，实现用户间统一协作。

区块链是点对点传输（下文简称P2P）共识机制、加密算法、分布式数据存储等多种复杂计算机技术的新型模式。分布式理解起来很简单，其实就可以看作是多台服务器共享一个数据块，而分布式计算的特点就是能把需要巨大算力的问题分解成许多算力需求较小的小问题上，从而较低对硬件设备的需求，以达到节约资源的目的，然后把这些算力较小的问题再让普通计算机逐一解决，而最后的计算结果的总和便是我这个大问题的答案。区块链技术被我们这些普通人熟知一是因为大势所趋，二是因为一个叫比特币的很值钱的东西，区块链与比特币的关系我如是认为，区块链技术是比特币的底层技术，也就是说比特币这种数字货币的交易离不开区块链技术，而比特币的技术基础便是区块链技术，换言之，区块链技术可以有许多的实际应用，而比特币只不过是我们所熟知的第一种应用而已。

本质上应该说是先有了比特币再有了区块链，比特币是一种数字加密货币，区块链技术在1991被提出，当时是在用于给电子文档做标记，来记录这个文档被记录后的每一次改动，从而防止有人去篡改相关信息，然而这个应用并没有被广泛重视，直到2009年一个叫中本聪的日本学者提出了用区块链创建电子货币的构想，并且创造了比特币，他把区块链用成了账本，此时区块链上面存储的信息便是每一笔转账，这样人们就可以把区块链看成是所有人都可以信赖的分布式账本，只要这个转账信息被写道区块中就很难篡改。

区块链技术在具体应用中，具有开放特命性、独立公正性、匿名性和去中心化特点，使得数据信息传输更加安全高效，与新时期数据处理要求相符。在区块链技术的使用过程中，应使用网络空间安全技术，计算机科学技术，以此来避免数据在传输过程中被截获、盗取、修改、和非法使用，为用户提供公开透明安全的信息环境。基于网络空间安全技术应用，数据信息最核心的特点去中心化得以彰显，区块链数据可向所有用户开放，因此系统信息非常安全透明。为增加安全检验和数据高效合理传输，需要对目前应用的安全技术进行综评，来防止有关数据发生修改或被盗取，确保区块链技术应用安全透明值得信赖。

**2）区块链技术的应用**

因为其具有去中心化的特点，区块链技术使数据传输更加可靠，其作用就是更大程度的防止了中心节点（每个区块就是一个节点）被一些不法分子有意攻击所造成的数据被截获或者泄露的风险。

区块链的实际工作流程如下：当前一个节点向另外一个节点进行转账的过程中，产生的交易信息会以区块的形式广播到网络中所有有效节点,以点对点传输（P2P）的方式（也就是说所有区块都会记录下这次转账信息），这时节点就会通过一种特殊共识机制对此区块进行检测和认证，当该区块的正确性和有效性被大于一半节点认可后，这次的转账才能成功完成。由于区块链中的信息得到了网络中大部分节点的一致性认同，因此我们可以认为该信息是无法被攻击者篡改的，且所有节点都可以被人们读取和查询其整个交易记录的信息,退一部讲，就算有人有能力篡改相关数据信息，其成本必远大于其收益（共识机制），故区块链具备优越的安全特性。

区块链相比曾今的网络空间安全防护手段主要具有以下三大特性

第一，这种特殊共识机制代替以往使用的中心认证机制。在区块链这个特殊的共识机制下，无需第三方信任平台（政府，公司，组织），写入的数据需要网络大于等于百分之五十的节点的认可才可以被记录，因此，攻击者需要控制全网络大于一半的节点才能够有可能成功的伪造或者篡改数据，这将大大增加攻击的成本和难度。

第二，数据篡改影响大。区块链采用哈希值当链条的链式区块结构存储数据，为数据的记录增加了时间维度，具有可验证性和可回溯性的特殊性质。即当改变其中一个区块中的任何一个信息，其哈希值（区块的指纹，每个区块不仅有自己的哈希值，还有前一个区块的哈希值，由此形成链条）也会改变，类似我们现在c语言中链表的地址，整个区块链随哈希值的改变就断掉了，故攻击者需要计算出从该区块开始往后的所有区块的哈希值，而由于区块链有特有工作量证明机制，不会因为计算机算力强大而快速算出后面的哈希值，使哈希值的计算时间的难度大大的提高，故篡改数据是很难做到的，可以说是吃力不讨好。

第三，可以轻易抗拒DDOS攻击。区块链的节点分散，每个节点都具备完整账本（也就是整个区块链的信息），而且可以对其他节点的数据有效性和正确性进行验证，由于这特有特性，因此针对区块链的DDOS攻击十分难以开展。退一步说，即便攻击者成功攻破某个节点，剩余节点也可以正常维持整个区块链系统，整体不受影响。 **二.关于访问控制**

**1）元宇宙的出圈与起源**

2021年可以说是元宇宙元年，我也浅谈拙见一二。元宇宙一词来自科幻小说雪崩，这个小说描绘了一个多人在线的虚拟时间（类似《头号玩家》那部电影）其可以说是2021年资本市场最爱谈的概念了，Facebook也将自己公司更名为meta，腾讯、阿里、谷歌也纷纷入局元宇宙。

元宇宙的出圈是因为一家叫Roblox的公司，其和腾讯成立了一家官方名称叫罗布乐思的合资公司，罗布乐思在2021年三月在纽交所上市，市值一路上涨，现在已达到480亿。罗布乐思简单来说是一个游戏平台，平台提供游戏开发工具，而玩家通过此平台开发的游戏可以自由进行买卖，甚至是卖游戏道具，玩家以此就可以盈利。而这个公司上市的时候首次把元宇宙这个概念写到招股书里，资本市场认为其有很好前景，便纷纷购入此公司股票，之后更多的公司就来蹭元宇宙的概念了。资本市场追捧元宇宙，还有一个推动就是疫情，大家宅在家里就需要找寻一个娱乐方式，社会的停摆推动了资本市场对元宇宙的重视。

**2）元宇宙的火爆的原因**

元宇宙就是一个独立于现实世界的虚拟世界，我们可以在里面干任何想干的事，不管是购物还是社交还是看演唱会（2021年Travis Scott和堡垒之夜合作在游戏里开演唱会，全球1200万人参加）。

元宇宙为何如此火爆？依我所见，是因为其是UGC模式（也就是我们熟知的用户生产内容），电视台产出内容的时代是PCG时代，而现在则是典型的UGC时代，每个人都拥有一部手机，都能轻轻松松录制一段短视频放到网上。在互联网发展的近几十年，我们不难看出唯有内容更加平权的UGC产品胜出了，比如淘宝、博客、微信、端视频。PGC的产品质量当然胜于UGC，但高成本，高投入以及产能不足都是制约它发展的原因，UGC质量低，但产能多且丰富多样，你永远能找到你想看的东西。而游戏领域一直都是PGC，不管是3A大作乃至独立游戏，都需要很高的门槛才能制作，而元宇宙则打破了先河，在游戏领域采用UGC，也唯有采用UGC，元宇宙才可能存在。

**3）元宇宙的特点**

去中心化，就和区块链一样。元宇宙也是去中心化的，即没有中央管理机构，是由用户一起自治、共治管理这个虚拟社区，而公司只起到平台的作用。对于元宇宙，我认为特点如下：第一，它和电子游戏高度相关；第二，它和区块链高度相关；第三，它是一个宏大的叙事；第四，它有自己的经济系统，我们每个人都能参加；第五，它是UGC；第六，它是去中心化；第七，它需要高技术支撑，例如5G，云游戏。

元宇宙六大相关技术支柱包括：区块链技术，交互技术，人工智能技术，电子游戏技术，物联网技术，智能网络技术。而构成元宇宙的三要素分别为：身份系统，价值系统和沉浸式体验。

元宇宙的身份系统是去中心化的，所以用户可以选择一个或多个虚拟的数字身份，且不易丢失。而加值系统则是有了独立的数字身份的基础上，用户可以在虚拟时间用NFT进行物品的确权，从而产生价值创造以及市场交易，在此基础上，生存出一套属于元宇宙的经济体系，区块链技术解释了为什么身份系统具有独立性，而NFT为数字货品提供了不可分割，不可复制的交易价值，让用户可以实现创造者经济， 而当用户在虚拟世界有了资产，自然就对它的依赖性更强了。尤其是作为元宇宙的底层技术支持的区块链衍生出来的去中心化金融DEFI将会释放元宇宙的流动性，当然朝着一个方向的演化也将会伴随着金融管控，合规交易，跨市场风险，数字安全等多方面的讨论。

关于NFT我也想浅谈一二，NFT在我看来就是数字产权。在现今社会，对于数字作评的产权保护是极为困难的，而NFT的作用就是在区块链上通过铸币的方式为数字艺术品赋予一个哈希值，使其永久的保存在区块链上。这样的好处是，基于区块链的不可逆和公开透明性，能够使得数字作品正真意义上具备了唯一性，因此，它在区块链上的id是唯一的，且无人能篡改，在这种情况下，任何拥有作品原始哈希值的人，才会被认为是作品的拥有者，由此数字资产的产权问题就得以解决。

**三．元宇宙与区块链的联系**

区块链是一个去中心化的分布式共享账本和数据库。我用QQ空间举例，以此来阐述我所认为的元宇宙和区块链的联系，QQ空间中用户可以花钱买皮肤、权限，在这个体系中，腾讯的Q币系统便是一个中心化的账本，而Q币购买的就是腾讯自己建立的各种二维空间内的虚拟产品和体验，而在元宇宙这样一个三维虚拟空间里，全球各地的程序开发者和设计者会开发出更多更炫酷的产品和体验，全球的用户们也希望能用各国的货币去结算一种可以在元宇宙里共通的货币去购买这些虚拟的产品和体验，并保证他们在元宇宙里的财富交易和结算是安全且隐私的。因此，去中心化的区块链技术几乎可以满足在元宇宙的所有交易和结算的应用场景。但其实这两者并没有绝对的因果关系，它们最多是高度匹配，互相成全的两种技术。