# 《网络空间安全导论》期末论文

**陈鑫蕾22920202202877**

**目录**

[《网络空间安全导论》期末论文 1](#_Toc19442)

[1．导言 2](#_Toc25098)

[2．对网络空间安全专业的认识 2](#_Toc9988)

[2.1网络空间 2](#_Toc11652)

[2.2网络空间安全 2](#_Toc6188)

[2.3网络空间安全专业 3](#_Toc8810)

[3．网络空间安全的核心技术 3](#_Toc5892)

[3.1区块链技术的历史背景 4](#_Toc26984)

[3.2区块链技术的优势 4](#_Toc25366)

[3.3区块链技术的未来发展 5](#_Toc24362)

[（1）金融领域 6](#_Toc15492)

[（2）物联网领域 6](#_Toc18663)

[（3）大数据领域 6](#_Toc10967)

[4．建议 7](#_Toc21102)

# 1．导言

从21年初大火的NFT概念到22年初全球最大黑客组织(Anonymous)对俄发起网络战争等，这些事件的发生无一不体现着现今网络的边界越来越模糊，安全形势也越来越复杂化。尤其是在当下，虚拟空间与实体空间结合越来越紧密，元宇宙等概念也正在步入应用创新和推广的活跃期，网络空间安全的范畴发生了巨大的变化，同时网络空间安全也就显得格外重要。正好借助这次的导论课，让我对整个网络安全空间有了一定的认识，接下来我将进行一些简单的阐述。

# 2．对网络空间安全专业的认识

下面，我将从网络空间，网络空间安全，网络空间安全专业这三个部分来阐述我的认识。

2.1网络空间

首先，什么是网络空间？追究其发展历史，Cyberspace最早是由William Gibson于一九八二年发表的小说《Burning Chrome》中首次提出的，并在小说《Neuromancer》中被大众所熟知。他将这个空间命名为“Cyberspace”，也就是现在人们所熟知的赛博空间。

而追究其定义，网络空间其实是一个由相关联的基础设施、设备、系统、应用和人等组成的交互网络。也是一个屏幕后的特殊宇宙空间，在这个空间中，物联网使得虚拟世界与物理世界加速融合，云计算使得网络资源与数据资源进一步集中，泛在网保证人、没备和系统通过各种无线或有线手段介入整个网络，各种网络应用、设备、系统和人逐渐融为一体。[1]

而现如今，网络空间已经成为国家主权的第五空间，也是唯一一个边界不清，主权概念存在巨大争议的空间。

2.2网络空间安全

那什么是网络空间安全呢？网络空间安全是通过识别、保护、检测、响应和恢复等环节，以保护信息、设备、系统或网络等的过程。[1]在此过程中，其关键是根据风险管理的理念，动态实施连续协作的五环论，即识别、保护、检测、响应、恢复。其主要包括两个层面的安全问题，即信息层面和物理层面。

2.3网络空间安全专业

**而网络安全的竞争，归根结底是网络安全人才的竞争。因此**网络空间安全专业应运而生。

网络空间安全专业涵盖众多课程，如计算机网络，密码学基础，操作系统，大数据分析与隐私保护等，是计算机，通信，物理，法律等学科的交叉学科。其致力于培养能够支撑国家网络空间安全领域的，具有较强的工程实践能力，系统掌握网络空间安全的基本理论和关键技术，具有社会责任感、使命感、宽广的国际视野、创新精神和实践能力的拔尖创新人才和行业高级工程人才。

党的十八大以来，习近平总书记多次就网络安全发表一些列重要论述，“以安全保发展，以发展促安全”、“没有网络安全就没有国家安全”、“构建网络空间命运共同体”等。这些无一不彰显了网络空间安全的重要性。同时，当前网络空间安全人才缺口较大，因此网络空间安全专业的就业方向十分广泛，就业前景十分广阔。

3．网络空间安全的核心技术

首先，网络空间安全的研究领域主要包括信息安全、信息保密、信息对抗、云的安全、大数据、物联网安全、移动安全、可信计算领域。其中，信息安全是核心和根本，其他领域是信息安全向外的延伸。围绕这8个领域，归纳总结了网络空间安全的4层次模型对应的安全技术[2]



而在这其中我最看好的技术是区块链技术。

下面我将从三个方面来论证我的观点，分别是区块链技术的历史背景，区块链技术的优势，区块链技术的未来发展

3.1区块链技术的历史背景

关于区块链技术的历史元年，网络上有着许多种不同的说法，因此，此处就仅根据我所收集到的资料来叙述。首先，区块链技术背后的核心思想出现在20世纪80年代末和90年代初。1989年，莱斯利·兰波特开发了Paxos协议，并于1990年向ACM计算机系统学报提交了论文《PartTime Parliament》。这篇论文最终发表在1998年的一期杂志上。本文描述了一个共识模型，用于在计算机或网络本身可能不可靠的计算机网络中就结果达成一致。这些概念在2008年时结合并应用于电子现金，并在论文《比特币:一种点对点的电子现金系统》中进行了描述，该论文由中本聪（化名）发表。中本聪希望“允许利用网络支付直接从一方发送到另一方，而不通过金融机构”。因此他提出了一个完美的解决方案：建立一个时间戳的、基于共识的、密码标记交易的分布式数据库，链接成无法改变的记录——区块链。[3]

3.2区块链技术的优势

众所周知，传统的网络安全主要以加密和信任技术为基础，采用的边界防护模式，这样的模式存在网络安全的致命弱点，容易遭受网络的侵害。而区块链技术不同于传统的安全防护模式，它是采用反向链接数据结构和共识机制来保护区块链上的数据，是对边界内进行全盘监视，对监视范围内的数据进行甄别，去伪存真。它是一种按照时间顺序将数据区块以链条的方式组合成特定数据结构，并以密码学方式保证的不可篡改和不可伪造的去中心化共享总账，能够安全存储简单的、有先后关系的、能在系统内验证的数据。区块链可以看作是存储数字记录的数据库，数据库由网络节点共享，节点可以提交新的记录，区块链网络通过共识机制保证节点之间数据的一致性，记录一旦被输入就永远不会被更改或删除。

事实上,区块链并不是一个全新的技术,它不但融合了若干成熟独立的安全技术外,还结合了不少新的安全技术。因此,它具有全新的、特有的安全功能。而与以往的网络空间安全方法比较,区块链技术有着四个显著的优点。

（1）区块链上的信息难以篡改，安全可靠。在不使用区块链技术保存的信息里，安全依赖于层层设防的访问控制。可是如果运用区块链技术的话，我们的交易记录可以让任何人查看，但由于巧妙的设计并辅以密码学和共识机制，区块链的数据记录方式使得修改某一数据需要变更所有的后续数据记录，难度非常大。最典型的例子便是比特币。比特币的所有活动都被记录在开放的互联网上的一个区块链数据库中，它完全暴露于政府、犯罪组织和黑客面前，即使这样，截至目前为止，比特币区块链也从未被黑客入侵过。

（2）区块链采用分布自治的数据管理结构。众所周知，网络中的每个节点都具有一定的安全防护能力，且每个节点之间都以自治的方式，按照一定的规则来执行合约。加入网络中的某个节点遇到故障，如网络问题、硬件故障、被黑客控制等，均不会影响系统以及其他参与节点。区块链中的节点通过点对点的通信协议进行交互，在保证通信协议一致的情况下不同节点可由不同开发者使用不同的编程语言、不同版本的全节点来处理交易。由此构成的软件异构环境确保了即便某个版本的软件出现问题，区块链的整体网络不会受到影响，这也是其高可用的基石所在。

（3）区块链具备智能合约，自动执行。智能合约具有透明可信、自动执行、强制履约的优点。通过智能合约，各方就条款和条件达成一致，并将其输入区块链分类账。当满足协议的所有条款时，交易将自动执行。一旦智能合约在分类账中，它就是不可变的或不可更改的。这意味着买家无法退出或卖家无法提高商品价格。尽管如此，自尼克·萨博1993年提出以来，智能合约始终停留在理念层面。而区块链第一次让智能合约的构想成为现实。

（4）区块链拥有网状直接协作机制，更加透明。区块链提供了不同于传统的方法，以对等的方式把参与方连接起来，由参与方共同维护一个系统，参与方职责明确，无需向第三方机构让渡权利，有利于各方更好的开展协作。作为信任机器，区块链有望成为低成本、高效率的一种全新的协作模式，形成更大范围、更低成本的新协同机制。

3.3区块链技术的未来发展

纵观区块链的发展历史，其形成了三个发展模式——区块链1.0、区块链2.0和区块链3.0。

区块链1.0一般指的是数字货币领域的创新，如支付系统，货币转移等；区块链2.0则是在金融领域的运用，如征信系统，跨国支付，证券登记等金融产品的清算结算，以及所谓的智能合同等；区块链3.0则是致力于将其应用的领域扩展到人类社会生存的方方面面。在各类社会活动中实现信息的共享，解决信任问题，提高整个系统的运转效率。[4]

其实，区块链技术发展到今天，其应用需求已经从最初的数字货币扩展到社会领域的方方面面。正如我上述所说的，区块链显著的技术优势，让区块链在金融、物联网、大数据等领域拥有广泛的应用前景。

（1）金融领域

区块链技术具有极高的成本效益。因为其没有第三方，交易和其他管理费用通常低于传统系统。而对于金融行业的基础体系，如数字货币、征信系统、跨国支付与清算等，这些系统现在都是中心化的，收费高且效率低的。伴随着区块链技术的成熟，当其能完美应用于这些体系时，即使只节省1％的中间费用，其应用前景也是相当吸引人的。

（2）物联网领域

现今，物联网飞速发展。但目前物联网仍面临一些问题，如由于设备之间的互联互通性差，导致连接成本较高、中心化的网络结构导致成本高，效率低以及物联网中用户之间的相互信任和安全问题。而区块链技术的去中心化、匿名性可以很好地解决这些问题。同时，目前已经有一些应用的案例，如IBM开发的Adept项目中使用区块链技术创建一个可行的分布式网络；VISA与DocuSigIl联合推出区块链汽车租赁项目；Slock.it公司致力于通过区块链实现闲置资源的共享等。这些应用都充分证明了区块链在互联网领域的广阔前景。

（3）大数据领域

在大数据领域，一直以来的挑战与难点是如何在保护个人隐私的情况下开放数据。基于区块链的散列处理等加密算法可将一些数据进行脱敏处理．为隐私保护下的数据开放提供了解决方案。对于个人或机构有价值的数据资产，可以利用区块链对其进行注册，交易记录是全网认可的、透明的、可追溯的，明确了大数据资产来源、所有权、使用权和流通路径，对数据资产交易具有很大价值。区块链的可信任性、安全性和不可篡改性．保障了大数据的安全性、隐私性及不可篡改性．非常符合大数据的核心需求，将来必会在大数据领域广泛应用。

综上所述，区块链技术的优势显著，未来发展是丰富多样的，潜力巨大。所以我最看好的技术就是区块链技术。

4．建议

（1）保持趣味性的同时增加实践。实践动手与理论课并行，增加知识理解。比如，在计算机网络专题部分，可以适当布置简单有趣的实验作业。因为数字媒体技术专业本学期也刚好学习了计算机网络这个专业。在做计算机网络的实验时，我大部分都觉得十分的新奇有趣。所以如果在上课的时，布置一些比如抓包，路由配置等，诸如此类的不需要过多代码量，上手简单的实验，应该能吸引同学们的兴趣，同时对计算机网络有一个较为初步的认知。

（2）以当下时事热点引入，吸引大家的兴趣，然后在逐步解释其背后包含的网络安全技术等，课堂效果可能会更好。由于大部分的同学都才大学二年级，所以对很多专业知识可能并不了解。若是以典型例子或代码片段开篇，再对专业技术开始阐述，可能会因为有些枯燥难懂而劝退大家。所以可以在讲解的过程中适当添加许多时事热点，比如吸引同学兴趣。进而一步步阐述背后的原理等。

（3）在进行实验室方向介绍的时候，可以采取视频的形式来进行介绍。单纯的文字形式同学们可能无法完全了解具体的研究方向。个人认为，视频的形式会更加吸引人，同时也能更好地解释自己的研究方向，让同学们更好地进行选择。

参考文献

1. 冯登国.网络空间安全——理解与思考[J].网络安全技术与应用,2021(01):1-4.
2. 方滨兴.从层次角度看网络空间安全技术的覆盖领域[J].网络与信息安全学报,2015,1(01):2-7.
3. 中本聪. 比特币:一种点对点的电子现金系统[EB/OL]. <https://bitcoin.org/bitcoin.>, 2009.
4. 伍旭川,王鹏.区块链技术应用及展望[J].清华金融评论,2016(10):23-25.DOI:10.19409/j.cnki.thf-review.2016.10.007.
5. 董慧,张成岩,严斌峰.区块链技术应用研究与展望[J].互联网天地,2016(11):14-19.