1. 区块链可扩展性

a)研究导向：

当前，比特币以太坊等为代表的传统公链，每笔交易都需要全网验证和存储，可扩展性受到很大的限制，导致目前的区块链底层平台上很难支撑大规模的应用。目前，对区块链可扩展性的研究主要从解决交易的吞吐量和增加交易的速度入手。现有技术实现的角度来说，可以通过侧链、分片、DAG 等技术解决区块链的可扩展性。请参考相关论文提出自己对区块链可扩展性的理解，并分析基于这些技术的区块链与传统区块链相比有什么优劣。（参考资料 https://github.com/decrypto-org/blockchain-papers#general）

b) 工程导向：（参考网络搭建思想，下同）

以下部分为基本要求：

区块链可被视作一个去中心化的账本，账本内容由所有节点共同维护。这其中涉及了网络共识协议、对等式网络传输等技术。

现假设如下场景：n 个节点（n 大于等于 3）希望创建区块链网络，这些节点希望区块链系统具备如下功能：1）维护一条具有不可篡改性的区块链；2）允许加入新交易与新区块；3）允许新节点的加入。请基于上述要求，搭建区块链网络（包括共识机制、网络传播机制等），可以使用不同机器（或使用同一台机器的不同端口）启动不同的节点。

以下部分为附加题：

当节点的数量相当大、且区块链主链较长时，若所有节点均保存区块链的全部信息，将不可避免的导致数据的冗余。请结合计算机网络课程中学习到的知识，通过以下方式避免数据的冗余：a)数据的分布式存储；b)节点间网络传播机制的优化.

参考资料：https://github.com/dvf/blockchain

2. 工作量证明区块链的安全性

工作量证明（Proof of Work）区块链系统具有公开透明、难以篡改、可靠加密等优点。因此被比特币等数字加密货币采用。然而，它的安全性仍然受到其共识机制设计等因素制约。现实中，不少基于工作量证明共识机制的数字加密货币都遭受过不同程度的攻击。在先前的研究中，提出了 51%攻击，Selfish mining, Block Withholding Attack 等攻击。 请参考相关论文，分析现有的攻击方式，并提出对这些攻击方式的改进或防御措施。（参考资料 https://github.com/decrypto-org/blockchain-papers#general）

3. 区块链智能合约技术

a)研究导向：智能合约是区块链最为吸引商业界广泛关注的一个发展方向，请参考相关资料，搭建公链或联盟链平台，部署并运行智能合约，了解智能合约的发展趋势。（联盟链的搭建可参考：https://hyperledger-fabric.readthedocs.io/en/release-1.4/whatis.html；智能合约的相关研究可参考 https://github.com/decrypto-org/blockchain-papers#general）

b) 工程导向：智能合约可自动在区块链上执行，但其应用并不局限于处理交易。目前，智能合约也被用于实现安全多方计算、实现简单的区块链小游戏等方向。请基于以太坊或联盟链平台，编写智能合约，并利用该智能合约实现除处理交易以外的功能（例如：简单的智能合约小游戏）。（联盟链的搭建可参考：https://hyperledger-fabric.readthedocs.io/en/release-1.4/whatis.html ，以太坊的使用请参考：https://ethereum.org/）。

4. 区块链的隐私与监管

区块链的去中心化、去中介和匿名性等特性与传统的企业管理和政府监管体系不协调。一方面普通用户在区块链上的交易隐私应该得到保护，现目前的匿名化技术也还不能完美地保证匿名（例如 Zero Cash）；另一方面又应该防止恶意用户将区块链用作非法交易的平台。请参考相关资料，搭建公链或私有链平台，说明如何实现区块链中的隐私保护或如何实现区块链的监管。（联盟链的搭建可参考：https://hyperledger-fabric.readthedocs.io/en/release-1.4/whatis.html；区块链隐私/监管的相关研究可参考 https://github.com/decrypto-org/blockchain-papers#general）

5. 对抗学习在金融风控中的研究

在金融风控场景中存在许多用户攻击、欺诈行为。近年来兴起的"褥羊毛"的用户也给公司带来了巨大的经济损失。从海量数据中寻找出这些欺诈用户是个急需解决的问题。与此同时，数据具有数量巨大、数据维度高、特征缺失严重、人力标签成本大等等问题。本研究旨在结合对抗学习解决金融风控中的上述问题。大家可以结合所学知识，阅读相关论文，在大规模数据处理、无监督或半监督模型、模型可解释性、模型增量挖掘等等方面提出自己的方法。(对抗自编码器：Adversarial autoencoders https://arxiv.org/abs/1511.05644；应用方向可参考 Generative adversarial network based telecom fraud detection at the receiving bank 等)

这个题目起源的项目介绍见于 https://www.chainnews.com/articles/062638888819.htm，我们可提供的数据介绍见于 https://www.pkbigdata.com/common/cmpt/2018%E5%B9%B4%E7%94%9C%E6%A9%99%E9%87%91%E8%9E%8D%E6%9D%AF%E5%A4%A7%E6%95%B0%E6%8D%AE%E5%BB%BA%E6%A8%A1%E5%A4%A7%E8%B5%9B_%E8%B5%9B%E4%BD%93%E4%B8%8E%E6%95%B0%E6%8D%AE.html。当然这个题目数据不限于这个数据集，场景也不限于金融风控薅羊毛。

6. 联邦学习

联邦学习（Federated Learning）是一种新兴的人工智能基础技术，在 2016 年由谷歌最先提出，原本用于解决安卓手机终端用户在本地更新模型的问题，其设计目标是在保障大数据交换时的信息安全、保护终端数据和个人数据隐私、保证合法合规的前提下，在多参与方或多计算结点之间开展高效率的机器学习。其中，联邦学习可使用的机器学习算法不局限于神经网络，还包括随机森林等重要算法。联邦学习有望成为下一代人工智能协同算法和协作网络的基础。作为这几年新提出的技术，本研究大家可以了解联邦学习的具体框架，实现，落地情况。有两个方向可供同学们选择：

a. 研究导向：去探究联邦学习还存在哪些问题，目前的存在的难点(例如每次参数如何更新，各方数据分布问题等)；展望联邦学习的未来发展。

b. 工程导向：模拟一个联邦学习的任务。假设这样一个场景，多个参与方（数量自定，越多越好）加入一个联邦学习。他们有一个需要共同维护的模型（相当于一个公共的服务器），其中每一方需要不断通过下载这个公共的模型的参数到本地进行训练，再将本地训练后的参数更新传回公共的模型。请考虑这样一个机制下可能存在的问题，并设计方案，做出实验模拟。这个方向同样适用于问题七。

（可能存在的问题有需要公共服务器的布置，各个参与方之间的同步问题，海量参数传递的问题，以及一些异常情况的处理。在这里可以简化本地对训练中参数更新的过程）

（联邦学习相关学习资料可参考 https://federated.withgoogle.com/#learn）

7. 协同训练下的隐私保护

在深度学习中，由于数据往往分布在不同的地方。当数据分布在不同的拥有者手中时，隐私问题常常成为阻挡数据流通的壁垒。传统的将数据直接加密具有数据隐私依赖加密手段、加密后的数据丧失原本数据的特征等缺点。而近年来同态加密与深度学习的结合也取得了一定的成果，然而同态加密在效率上难以达到实际应用的需求。本项目将聚焦在如何在协同训练中保障数据的隐私性，让数据拥有方放心将数据相互流通。大家可以调研相关研究，比较已有的方法之间的优劣；有能力的同学可以提出自己的算法。除此之外，同学们也可做工程向的实现，参考第六个课题中的工程导向。

（相关文章参考：deep learning on private data http://aceslab.org/sites/default/files/DLoPD.pdf 还有一些从数据分享的角度保护隐私，例如 Adversarial Learning of Privacy-Preserving Text Representations for De-Identification of Medical Records.）

8. Deepfakes 技术

近年来，基于深度学习技术的生成模型的发展十分迅速，这导致人工合成内容诸如图像、视频、音频得以更加逼真。这其中 Deepfakes 就是一种典型的基于自编码器的视频换脸技术。由于名人明星等公众人物在社交网络上存在着大量的图片、视频信息，使得这类人更容易成为换脸的目标。而最近 Deepfakes 技术被用于制造一些虚假内容来达到某种不正当的目的，如色情影片中的脸部替换，篡改公众人物的演讲视频等，可能导致肖像侵犯、信息混淆乃至舆论恐慌等一系列严重的问题。本项目中大家可以调研相关资料和论文，了解并尝试实现 Deepfakes 换脸，有能力的同学可以对现有的 Deepfakes 技术提出自己的改进方案。也可以对现有的 Deepfakes 合成视频的检测方法进行调研，或提出自己的检测方法。(相关文章参考：Deep Learning for Deepfakes Creation and Detection)

9. 网络 车联网 物联网/