# 背景

面对数量庞大的异常交易数据以及每日不断累积的亟待审核的异常交易数据，工作人员需要在一定时间周期内完成所有被异常交易系统可疑模型判定为疑似参与异常交易活动的客户以及相关交易的数据审查，人工审核工作量巨大。除了审核工作本身繁杂耗时之外，往往需要联系到客户本人或者相关人员对客户进行身份核实以及交易信息核验，因而人工成本高昂、效率难以提高。因此，充分运用大数据和人工智能等新兴技术，对现行的异常交易可疑模型进行迭代升级，已成为交易监测业务发展的必由之路。

当前，异常交易监测大多通过基于规则的方法，即在交易系统里预先设置好相关规则。该规则基于业务专家的实践经验，预先设定了基于客户信息、账户信息和交易信息的相关联系和阈值，根据预先设定好的条件每日捕捉满足的交易。系统生成可疑案例后，需要对所有的案例进行人工甄别，以确认其是否可疑。由于系统内每日生成的可疑案例数量庞大，这给人工甄别带来了极大的工作量。针对该问题，通过将机器学习算法引入异常交易监测中，在系统基于规则的模型生成的案例基础之上，借助已完成人工甄别的案例特征数据为训练数据集，训练出符合要求的模型算法，并对系统生成的还未进行人工甄别的案例进行初步甄别，为异常交易甄别人员提供参考，从而减少人工甄别的工作量，进而在降低人力成本的同时提高异常交易识别效率。

# 异常交易监测智能分析思路

（一）基于主体的目标锁定分析思路

异常交易活动目前来看仍只是少数违法分子的行为，而大多数交易主体的交易都是合法的。异常交易交易属于小概率事件。如果将目标锁定过广，既加大监测成本，也会影响监测的质量。准确定位风险客户主体将是异常交易监测的高效途径，如果账户对应的机构主体本身就涉嫌异常交易，或者其交易行为发生较大变化，则其所有的交易应属于重点观察对象。

1. 数据收集与预处理

数据来源：从数据中台等处获取交易记录，包括但不限于交易金额、时间、地点、交易双方信息等。

特征工程：对原始数据进行清洗、转换和标准化，提取出有助于模型训练的特征，如交易频率、金额分布、地理位置等。

2. 构建客户画像

使用聚类算法（如K-means、DBSCAN）或图神经网络（GNNs）来构建不同客户的交易行为模式，形成每个客户的基础画像。

利用历史交易数据建立客户的行为基线，识别正常交易行为模式。

3. 行为变化检测

应用时序分析技术（如ARIMA、LSTM）监测每个客户交易行为的时间序列变化，捕捉偏离正常模式的异常情况。

引入滑动窗口机制，对比当前窗口内的交易行为与历史基线，评估行为变化程度。

4. 风险评分系统

设计一套综合考虑多种因素的风险评分规则，将交易行为变化、客户画像相似度、交易环境等纳入考量。

使用机器学习算法（如XGBoost、Random Forest）训练风险预测模型，输出每个交易主体的风险分值。

5. 主体关联分析

运用社交网络分析（SNA）或者图数据库技术挖掘主体间的潜在联系，识别出可能存在的团伙作案行为。

对于有直接或间接关联的高风险客户，将其纳入重点观察名单。

6. 模型优化与反馈循环

不断更新和完善模型，根据最新的交易数据调整参数，提高模型准确性和响应速度。

建立反馈机制，确保人工审查的结果能反哺给机器学习模型，进一步优化目标锁定策略。

（二）基于场景的资金网络分析思路

很多的异常交易行为，都会形成一个相对复杂的资金流动场景（网络），表现特征为账户（节点）多、交易（对手方）多，并且会呈现出某种结构性异常。也就是说资金的流动网络越复杂、越有规律，存在问题的可能性就越大。因此构建资金网络模型并对其进行分析监测，是识别重点可疑的一个有效途径。通过对资金网络的各项特征，如交易金额特征，资金的流向、流量、流速特征，渠道，接触方式特征（如代理人）等的分析，可以归纳和抽象出若干异常行为，并将监测从特征环节扩展到场景，从而更加有效地识别异常交易。交易网络分析一般和异常交易检测结合使用。比如上述检测出的异常交易放在交易网络中能帮助我们更好的识别真正的异常交易。交易网络中的节点代表账户，边代表交易。通过图的社区发现的算法，可以识别可疑的交易模式。常用的社区检测算法，例如Louvain方法，可以用来寻找由大量相互交易的账户组成的紧密社区，这些社区发生异常交易活动的可能性就非常大。同时，基于交易图谱，充分结合外部有效数据源，通过运用主体资金交易异常行为监测等方法，可快速挖掘出符合异常交易特征的异常图谱结构（例如，频繁汇入汇出、集中/分散型转入/转出、环状交易等），进而发现并定位出复杂的异常交易路径。

1. 数据收集与预处理

内部数据：首先从金融机构内部系统中收集所有相关的资金交易记录，包括交易时间、金额、来源账户、目标账户等信息。

外部数据：结合外部有效数据源，如公开的黑名单、行业报告、社交媒体信息等，以丰富交易背景信息。

2. 构建资金网络模型

节点定义：将每个银行账户视为图中的一个节点。

边定义：每笔交易则构成连接两个节点的一条边，带有方向（转账方向）和权重（交易金额）。

属性添加：为每个节点和边添加属性，如账户类型、交易频率、渠道等。

3. 特征提取

静态特征：包括账户余额、历史交易模式等不随时间变化的特性。

动态特征：涉及交易量的变化、流速（单位时间内发生的交易次数）、流向（资金的最终目的地）等随时间变化的因素。

4. 异常检测算法应用

统计方法：计算每个节点或边的标准偏差，识别出偏离正常范围较大的异常值。

机器学习模型：训练分类器来区分正常交易和可疑交易，可以使用监督学习（如果有标记的数据集）或者无监督学习（聚类分析、异常点检测等）。

图算法：利用图论算法识别特定的结构模式，例如环状交易、集中/分散型转入转出等。

5. 模型优化与验证

反馈机制：让领域专家能够审查并标注模型发现的潜在异常，从而不断优化模型性能。

持续更新：随着新的交易数据流入，定期重新训练模型，确保其适应最新的市场环境。

（三）基于群组的异常识别特征分析思路

群组分析的思路是将客户按照一定的维度特征分为多个组织，在同一组织中的主体，因其属性的相似，会存在相似的行为特征，即群组的一般行为特征。而与群组的一般行为特征出入较大的主体，则通常是异常的识别突破点。

1. 群组划分

确定分组标准：根据业务需求和数据特点，选择合适的维度（如行业、机构类型、产品等）作为分组依据。

聚类算法：使用聚类算法（如K-means、层次聚类等）将客户分为多个群组。每个群组内的成员具有相似的行为特征。

2. 行为模式建模

建立模型：针对每个群组，训练一个或多个机器学习模型（如决策树、随机森林、神经网络等），用以捕捉该群组的一般行为模式。

行为特征提取：从模型中提取出能代表群组正常行为的关键特征。

3. 异常检测

设定阈值：根据群组的行为模式，设定合理的异常评分阈值。

异常评分：对于每个客户，计算其相对于所属群组行为模式的偏离度得分。

识别异常：得分超过预设阈值的个体被视为潜在异常。

# 异常交易监测关联算法

1. 监督类算法

监督类算法可用于从人工筛选的案例中学习到一些更加清晰或者严格的分类边界，从而对规则筛选的异常交易进行进一步划分，或者提高异常报警的准确性。常见方法如：

决策树：决策树是一种基于树结构的分类算法，其通过一系列的判断规则构建决策树来对数据进行分类。

随机森林：随机森林是一种集成学习的方法，通过组合多个相同分布的决策树作为及分类器，并通过投票机制得出最终结果，降低了决策树的不稳定性。

支持向量机：支持向量机是一种基于间隔最大化的分类算法，通过寻找一个超平面进行数据划分。

朴素贝叶斯：朴素贝叶斯是一种基于概率统计的分类算法，其通过计算数据的先验概率和条件概率来进行分类。

K近邻：K近邻是一种基于距离度量的分类算法，其通过计算测试数据与训练数据之间的距离，然后选择最近的K个邻居来进行分类。

（二）无监督学习

应用无监督学习算法解决异常交易监测问题具有多个优势和必要性，这主要体现在以下几个方面：

无需标注数据：

无监督学习不需要预先标注的数据集。在金融交易环境中，获取大量标记为“正常”或“异常”的交易记录可能是困难且昂贵的。无监督学习能够直接处理未标注的数据，降低了对数据标注的需求。

适应未知模式：

异常交易可能表现出之前未见过的行为模式。由于无监督学习不依赖于已知类别标签，它可以检测出那些与历史行为显著不同的新类型异常。

灵活性和自适应能力：

随着时间推移，正常的交易模式可能会发生变化。无监督模型可以持续学习新的交易特征，并自动调整其决策边界，以适应这些变化，保持较高的检测准确率。

成本效益：

相比之下，构建和维护一个基于规则的系统来捕捉所有可能的异常情况既耗时又昂贵。而无监督学习模型一旦部署，就可以自动化地执行任务，减少了人力成本。

Isolation Forest (孤立森林)：

Isolation Forest是专门为离群点检测设计的一种高效算法。它通过随机选择一个特征和该特征上的一个分割值来递归地划分数据，直到所有数据点都被隔离。由于异常点具有较少的相似性，它们通常比正常点更容易被孤立。对于异常交易监测来说，这种特性使得孤立森林成为一种快速且有效的工具。

Autoencoders (自编码器)：

自编码器是一种基于神经网络的模型，用于学习输入数据的有效压缩表示（编码），然后尝试重构原始输入。经过训练后，对于正常交易，自编码器应该能够很好地重构输入；而对于异常交易，重构误差会相对较大。因此，可以通过设定重构误差的阈值来识别可能的异常交易。

Local Outlier Factor (局部异常因子, LOF)：

LOF是一种基于密度的离群点检测方法，它计算每个点相对于其邻居的局部密度偏差。如果一个点的局部密度显著低于其邻居，则该点被认为是一个离群点或异常点。在交易监测中，LOF可以帮助识别那些与周围正常交易行为差异较大的交易。

DBSCAN (Density-Based Spatial Clustering of Applications with Noise)：

DBSCAN是一种基于密度的空间聚类算法，它能自然地处理噪声数据点（即异常）。对于异常交易监测，DBSCAN可以用来识别那些不隶属于任何明显簇的孤立交易，这些交易可能是潜在的异常行为。

Gaussian Mixture Models (高斯混合模型, GMM)：

GMM假设数据是由多个高斯分布混合而成，并尝试估计每个数据点属于各个潜在分布的概率。低概率的数据点可能是异常点。在金融交易环境中，GMM可以用来建模正常的交易模式，并识别那些不符合这些模式的交易作为异常。

（三）强化学习/集成学习

通过强化学习技术(Reinforcement learning techniques)实现小样本下模型权重优化。由于模型的训练过程受到样本数量限制和分布的影响，传统的异常交易模型往往存在泛化能力不足的问题。强化学习技术为进一步提升模型泛化能力、提高预测结果准确性提供了有效的解决思路。以初期积累的小样本数据作为初始状态构造初始化的模型，通过深度强化学习算法对初始模型进行调整，并利用调整后的模型和环境进行交互，得到交互后的新状态和相应的奖励。如此反复循环，在过程中不断优化，最终生成不同状态下的优化模型，从而尽可能优化对异常交易客户的识别准确率，进一步提升模型的泛化能力。

集成学习通过训练多个弱分类器，将每个弱分类器的结果进行投票，往往能产生优于单一机器学习模型的查准率和查全率。因此，集成学习较传统机器学习模型有更高的坏样本覆盖能力，可有效减少漏报问题。有金融机构采用多数投票规则，将多种机器学习算法构建的模型进行集成融合，对异常交易可疑模型的精准度进行提升。由于在异常交易检测场景下，正常交易和异常交易数量偏差较大，是一个典型的样本不均衡的场景，AUC (Area Under Receiver Operating Characteristic Curve)作为基分类器评价指标ROC曲线下面积，反映了分类器对样本的排序能力，即使在类别不平衡的情况下仍用于反映模型性能好坏，能客观识别出较好的分类器。

此外，一些时序算法也可能会在特定场景中异常交易检测的效率

# 异常交易监测特征维度

金融交易监测场景的搭建往往需要结合具体的风险状况以及相关金融监管要求。在特定场景下，金融机构应结合场景内在属性和历史典型案例，提取出该场景的特征。需要说明的是，场景搭建和特征提取工作仍主要基于专家经验，也可通过一些统计分析模型和基于大数据分析技术的智能辅助分析模型来进行特征探查，但这方面的方法论有待进一步探索。

（一）主体特征

账户ID

电子邮件

联络电话

注册地址

省份

负责人

账户类型

资产规模

账户历史交易总量

账户历史回购余额

账户历史交易总次数

账户交易量统计特征

账户历史异常交易次数

账户历史异常交易统计特征

账户历史异常交易总额

账户历史异常交易总额占比

账户历史异常交易次数占比

账户历史累计头寸

主机构特征

主机构类型

主机构地址

主机构电话

主机构ID

主机构核心一级资本充足率

主机构资产规模

主机构历史回购余额

主机构省份

主体异常账户数

主体异常账户占比

主体历史回购余额

...

1. 交易特征

转出账户主体特征

转入账户主体特征

交易量

交易方式

交易利率

交易产品

交易利率偏离度

市场波动率

同类型平均交易利率

交易时段

转出账户交易员

转入账户交易员

交易日期

1. 网络特征

基于特定产品、交易方式、或者周期构建交易子网。

节点特征：

出度

入度

交易节点主体特征

节点交易总量/最大单笔交易量

节点买卖交易量占比

债券平均持有期限

节点净头寸变化

节点净头寸变化/节点交易总量

Pagerank

中介中心性

传播系数

效率

局部聚集系数

模体分布

边特征：

交易特征

网络特征：

频繁汇入汇出统计

集中/分散型转入/转出统计

环状交易统计

图网络Embedding特征

网络一度、二度关联聚合特征

异常交易占比

异常账户占比

以上所有统计特征的维度可包括最大值，最小值、平均值、方差，并且涵盖不同周期（一天，三天，七天，一月，一年）

# 实施计划

1. 数据收集与预处理

数据来源：从数据中台等处获取交易记录，包括交易数据、机构基础信息、历史异常交易数据和主机构信息等。

特征工程：对原始数据进行清洗、转换和标准化，提取出有助于模型训练的特征，如交易频率、地理位置等，离散数据建议使用ID化和向量化。

1. 异常主体检测模型

根据业务需求和数据特点，选择合适的维度（如市场、产品、时间周期等）作为分组依据。

利用历史交易数据建立客户的用户画像，识别正常交易行为模式。使用机器学习算法（如XGBoost、Random Forest）训练风险预测模型，输出每个交易主体的风险分值，label数据主要使用规则和前期人工累积的案例中所出现的机构。

可使用如下特征：

账户ID

省份

账户类型

账户历史交易总次数

账户交易量统计特征

账户历史异常交易次数

账户历史异常交易统计特征

账户历史异常交易总额

账户历史异常交易总额占比

账户历史异常交易次数占比

主机构特征

主机构类型

主机构ID

通过预测所有机构的风险分值，并基于经验或者数据分布特征划分阈值，选出风险性较高的潜在异常账户。

1. 构建交易子网

基于潜在异常账户、正常账户和分组数据构建潜在异常账户的多跳交易子网络，以作为异常交易检测的潜在范围。

节点定义：将每个交易账户视为图中的一个节点。

节点特征：

出度

入度

节点交易总量/最大单笔交易量

节点买卖交易量占比

节点债券平均持有期限

节点净头寸变化

节点净头寸变化/节点交易总量

模体分布

边定义：每笔交易则构成连接两个节点的一条边，带有方向（买卖方向）。

边特征：

卖出账户主体特征

买入账户主体特征

交易量

交易方式

交易利率

交易利率偏离度

卖出账户交易员

买入账户交易员

净债券流量

网络特征：

频繁汇入汇出统计

集中/分散型转入/转出统计

环状交易统计

图网络Embedding特征

异常交易占比

异常账户占比

网络净头寸变化量/网络交易总量

。

4. 异常子网络检测

使用XGboost或者GNN等算法学习正常主体和异常主体的交易子网络的特征，并预测某个子网络中是否可能存在异常交易，label为用规则和前期人工累积的案例中所出现的机构，如果出现，则为1。通过预测所有机构的风险分值，并基于经验或者数据分布特征划分阈值，选出风险性较高的潜在交易子网络。

5.异常交易链条生成

基于已生成的高风险交易子网络和网络中的节点、边特征，寻找子网络中的等价网络节点。等价网络节点的定义是基于一定的业务规则（非现有简单规则）可以共存于某些异常交易链条或者网络的节点。通过将子网络中所有的可连接等价网络节点连接起来后，即可形成多个等价交易网络（类似于洗钱网络），通过遍历所有等价交易网络周边的潜在匹配交易即可形成所有该子网络中可能的异常交易链条。