

团体标准

T/GZDFA 001—2025

区块链异常金融交易行为分类及特征指标

Classification and Features of Anomalous Financial Transaction Behaviors in
Blockchain

2025 - 05 - 13 发布

2025 - 06 - 13 实施

广州市数字金融协会 发布

前言

本文件按照GB/T 1.1——2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件发布机构不承担识别这些专利的责任。

本文件由广州金融风险监测防控中心有限责任公司提出。

本文件由广州市数字金融协会归口。

本文件参加起草单位：中山大学、中国质量认证中心广州分中心、广州市数字金融协会、广州金融风险监测防控中心有限责任公司、广州金融科技股份有限公司、广东股权交易股份有限公司、广州鹏聚信息服务有限公司、北京康达（广州）律师事务所、广州赛宝联睿科技有限公司、广州华商职业学院财金学院、中邮消费金融有限公司、中国联合网络通信有限公司广州市分公司、中科汇智（广东）信息科技有限公司。

本文件主要起草人：吴维刚、李宗亮、江映霞、李杰、郑龙哲、邹锦坤、钟瑜、肖飞、何文秀、黄建新、刘琰、陈迪亨、陈利生、朱静贤、余念姿、李安琪、郭桂福。

本文件为首次制定。

区块链异常金融交易行为分类及特征指标

1 范围

本文件规定了五种主要的区块链异常金融交易行为的分类以及特征指标和判定准则。

本文件适用于区块链异常金融交易行为的分类和识别，为相关机构对后续异常金融交易行为判定提供依据。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 42752-2023 《区块链和分布式记账技术 参考架构》

JR/T 0193-2020 《区块链技术金融应用 评估规则》

3 定义和术语

GB/T 42752-2023、JR/T 0193-2020 界定的以及下列术语和定义适用于本文件。

3.1

区块 block

一种包含区块链元数据和交易数据的数据结构。

注：区块是组成区块链的基本结构单元。

[来源：GB/T 42752-2023，3.6]

3.2

共识 consensus

在分布式节点间达成区块数据一致性认可的结果。

[来源：GB/T 42752-2023，3.7]

3.3

共识机制 consensus mechanism

在分布式节点间达成共识的规则和程序。

[来源：GB/T 42752-2023，3.8]

3.4

账本 ledger

按照时序方法组织的事务数据集合。

[来源：GB/T 42752-2023，3.9]

3.5

分布式账本 distributed ledger

在分布式节点间共享并使用共识机制实现具备一致性的账本。

[来源：GB/T 42752-2023，3.10]

3.6

交易 transaction

在区块链上的一次原子性账本数据状态变更及其过程和结果记录。

[来源：JR/T 0193-2020, 3.8]

3.7

区块链 blockchain

使用密码技术链接将共识确认过的区块按顺序追加形成的分布式账本。

[来源：GB/T 42752-2023, 3.12]

3.8

智能合约 smart contract

存储在分布式账本中的计算机程序。

[来源：GB/T 42752-2023, 3.13]

3.9

加密货币 cryptocurrency

一种以数字或虚拟方式存在并使用密码学原理来确保交易安全及控制交易单位创造的交易媒介。

3.10

区块链洗钱 blockchain money laundering

区块链洗钱是指将非法行为所获得的违法收入，通过区块链技术进行非法资金转移和转化，隐瞒其来源与性质的行为。

3.11

区块链庞氏骗局 blockchain Ponzi scheme

区块链庞氏骗局是指一种非法性质的金融诈骗，在本文件中指利用区块链技术的平台，以承诺高额投资回报来吸引投资者，并利用后期投资者的资金向早期投资者支付利息和短期回报，来吸引更多投资者的投资，最后骗取投资者的金额。

3.12

区块链钓鱼诈骗 blockchain phishing scam

区块链技术平台的钓鱼诈骗行为是指通过伪装成合法实体（如交易所、钱包或项目团队）的方式，来欺骗平台用户提供个人敏感信息、钱包密码、私钥等或欺骗用户进行转账，以窃取其加密货币或个人财产的诈骗行为。

3.13

区块链蜜罐诈骗 blockchain honeypot scam

区块链技术的蜜罐诈骗行为是指在区块链技术平台上创建智能合约，诱骗用户向该合约发送任意额度的资金，就能够取出合约中的全部资金，一旦平台用户投入资金参加，平台用户发送的资金将被锁在智能合约中，只有蜜罐合约创建者才能提取出来，从而实现诈骗目的。

3.14

区块链市场操纵 blockchain market manipulation

区块链技术平台的市场操纵行为是指在区块链交易市场中，以非法手段或欺诈行为来人为地操纵市场价格、交易量或其他相关指标，以获取非法利益的行为。

3.15

区块链异常金融交易行为 anomalous financial transaction behaviors

区块链领域中与正常金融交易规则、法律法规或道德标准不符的交易行为，包括但不限于区块链洗钱、区块链庞氏骗局、区块链钓鱼诈骗、区块链蜜罐诈骗、区块链市场操纵和区块链首次代币发行等。

3.16

链下关联风险 off-chain associative risk

链下活动（如中心化服务、第三方数据存储、物理世界交互）中与区块链交易存在关联的风险要素。

3.17

账户 accounts

账户是用于唯一标识用户、实体或资源，并关联其权限、状态、数据及操作记录的逻辑单元。本文中，钱包与账户的含义等同。

3.18

资金来源非法

涉及来自非法活动（如走私、贩毒、恐怖主义、赌博、诈骗等）的资金。

4 区块链异常金融交易行为分类

4.1 区块链洗钱行为

涉及下列行为中的一种或几种都可认定为洗钱：

- 1) 掩盖资金来源：区块链洗钱通常涉及将非法来源的资金转换成加密货币进行交易。通过多次转账和分割交易来增加交易路径的复杂性，或利用混币服务，混合资金和其他用户的资金，以掩盖资金的来源。
- 2) 智能合约洗钱：区块链洗钱利用智能合约功能，在区块链上自动执行洗钱活动，避开银行、第三方支付公司或中介机构。
- 3) 跨境兑换：区块链洗钱利用虚拟货币跨境兑换，将非法所得转换成境外法定货币或者财产。

4.2 区块链庞氏骗局

涉及下列行为中的一种或几种都可认定为区块链庞氏骗局：

- 1) 虚假项目宣传：通过创建虚假的区块链项目，承诺提供远高于市场上其他合法投资的投资回报，吸引更多的用户参与。
- 2) 回报支付策略：承诺用户将获得高额回报，通常以新投资者的资金支付给早期投资者，没有真正的投资或经营产生收益，另外早期投资人成功推荐新投资者进行投资也会获得额外奖励。
- 3) 崩盘和逃逸：在诈骗到足够的资金或者当没有足够的新用户进入无法维持回报支付时，诈骗方卷走投资者的资金，庞氏骗局最终崩盘。

4.3 区块链钓鱼诈骗

涉及下列行为中的一种或几种都可认定为区块链钓鱼诈骗：

- 1) 仿冒合法平台：通过冒用官方标志、名称和品牌伪装成合法的区块链平台或交易所，引诱用户与其交互获取用户的个人身份信息敏感信息。
- 2) 伪造钱包应用：通过开发或发布与真实的钱包应用非常相似的伪造的区块链钱包应用程序，用户在使用这些伪造应用程序时会被要求输入私钥、助记词等敏感信息，因此诈骗者能够访问用户的加密货币钱包并窃取其资产。
- 3) 伪造钓鱼链接：通过发送钓鱼电子邮件，其中包含伪造的链接指向恶意网站，要求用户进行转

账或者输入私钥或其他个人信息。

- 4) 社交媒体欺诈：通过社交媒体平台、聊天应用程序或区块链相关的讨论论坛上冒充知名区块链项目或专家，会发布虚假信息、推广欺诈项目或向用户发送欺诈性消息，诱使用户泄露个人信息或转账资金。

4.4 区块链蜜罐诈骗

智能合约中包含以下一种或几种合约漏洞可以认定为区块链蜜罐诈骗：

- 1) 蜜罐合约余额混乱：蜜罐创建者部署蜜罐智能合约，合约代码的逻辑看起来是调用者使用大于或等于智能合约当前余额的值来调用合约时，合约的余额和转入的金额可以转移到任意地址。然而在实际执行时，合约的余额已经增加了转入的金额，条件不能满足，因此，用户转入的资金被困在合约中。
- 2) 蜜罐合约编译漏洞：蜜罐创建者会在智能合约中部署一些明显的漏洞吸引用户向合约中转移资金，但其中由于编译的问题隐含了更多的漏洞，如果用户不仔细分析智能合约或不在真实环境中进行测试，可能会被忽视智能合约中隐含的问题。

4.5 区块链市场操纵

涉及下列行为中的一种或几种都可认定为区块链市场操纵：

- 1) 虚假交易：操纵通过虚构交易或利用大量交易来操纵市场的交易量，以创造人为的需求或供应压力，从而影响价格。
- 2) 传播虚假消息：操纵通过发布社区虚假或误导性的信息，如虚假新闻、虚假声明或夸大的市场前景，以影响投资者的决策或操纵价格。
- 3) 集中操控：少数机构或个人通过控制大量资产或市场交易活动，来影响市场价格和趋势，从而获得不当的利益。
- 4) 短线交易：操纵通过利用快速买入和卖出的策略，迅速变动市场价格，并从价格波动中获利。

5 区块链异常金融交易行为特征指标

5.1 区块链洗钱

1) 区块链交易特征指标

区块链洗钱行为的风险监测预警应综合考虑以下特征指标及识别规则：

- a) 异常交易量：账户频繁收到其他账号转账，转账账户数量众多。统计当日账户交易笔数和交易对手个人账户数量，账户交易笔数 ≥ 10 （笔），交易对手账户数量 ≥ 30 （个）。
- b) 入账金额为整数或者倍数：账户收款金额特征（用于投资的资金一般为金额较大的整数），当日入账金额为加密货币市值的倍数且有明显的数字规律特征分布。
- c) 集中转入，分散转出：计算当天有转出交易的账户，流出笔数/流入笔数 > 10 （笔）。
- d) 频繁大额交易：期间内超规模交易，当天发生交易的账户，回顾该账户发生的单日单笔或累计交易金额 ≥ 200 万元。
- e) 中转账户“快进快出、频繁收付”：查询该账户3天内的所有交易，当日账户余额 ≤ 1000 元， $0.9 \leq \text{账户累计流入资金} / \text{账户累计流出资金} \leq 1.1$ 。
- f) 以上指标数值仅供参考，具体指标值可根据实际应用调整。

2) 链下关联风险特征指标

- a) 高风险地区参与方：涉及与高风险地区有关的交易参与方，这些地区可能与洗钱、恐怖融资或其他非法活动有关。
- b) 非法交易行业参与方：涉及与非法行业相关的交易参与方，如毒品贩卖、走私、非法

赌博、电信诈骗等。

5.2 区块链庞氏骗局

1) 区块链交易特征指标

区块链庞氏骗局的风险监测预警应综合考虑以下特征指标：

- a) 交易频率特征：短期内（3 个交易日内）该账户频繁收到来自不同账户的转账，不同的账户数量 ≤ 100 （个）。
- b) 交易金额特征：短期内（3 个交易日内）转账给同一账户的单笔金额相等的笔数 > 30 （笔）。
- c) 关联交易特征：短期内（3 个交易日内）与 5 个以上相同账户发生交易。

2) 链下关联风险特征指标

- a) 虚假承诺和宣传：涉及到虚假的宣传和承诺吸引投资者，包括夸大回报、承诺低风险、保证资本安全等的行为。

5.3 区块链钓鱼诈骗

1) 区块链交易特征指标

区块链钓鱼诈骗的风险监测预警应综合考虑以下特征指标：

- a) 频繁交易特征：短期内（3 个交易日内）该账户频繁地接收小额交易，交易的账户数量 ≥ 100 （个）。
- b) 交易对象特征：短期内（3 个交易日内）该账户频繁的转移资产到不相关的账户，或与其他可疑账户之间进行频繁的交易，交易笔数 ≥ 10 （笔）。
- c) 多个接收地址/账户特征：转出资金分散到多个接收账户，账户数量 ≥ 10 （个）。
- d) 频繁小额交易特征：短期内（3 个交易日内）该账户接收到的单笔转账金额不超过 2 万元。
- e) 大额资金流动特征：短期内（3 个交易日内）单笔或多笔转出资金在 10 万元以上，并且转出金额有明显数字规律特征分布。

1) 链下关联风险特征指标

- a) 社交工程手段：涉及电话、短信、电子邮件或社交媒体等渠道，冒充合法机构或个人以获取用户的敏感信息的行为。
- b) 伪造身份或资格证明：涉及伪造身份证明或资格证明来获得用户的信任的行为，例如冒用知名人士、区块链项目方或交易所的身份。

5.4 区块链蜜罐诈骗

1) 区块链交易特征指标

区块链蜜罐诈骗的风险监测预警应综合考虑以下特征指标：

- a) 异常交易量特征：短期内（3 个交易日内）接收到多个账户的转账，账户数量超过 30 个。
- b) 高度集中的交易特征：短期内（3 个交易日内）多笔交易资金流向少数几个账户，交易数量不少于 100 个，接收账户数量不超过 5 个。
- c) 同一账户转账特征：短期内（3 个交易日内）该账户接收到多个账户的金额相同的转账，且同一账户转账次数不少于 5 次。
- d) 相同交易额度特征：短期内（3 个交易日内）该账户接收到多笔金额相同的转账，且金额为加密货币市值的整数倍。

2) 链下关联风险特征指标

- a) 缺乏信息透明度：涉及到部署的智能合约代码提供的信息不清晰或模棱两可，隐含代码漏洞的行为。

- b) 合约创建者匿名：涉及合同的创建者身份未知或匿名，未公开真实身份信息的行为。

5.5 区块链市场操纵

1) 区块链交易特征指标

区块链交易市场操纵的风险监测预警应综合考虑以下特征指标：

- a) 异常交易量特征：短期内（3 个交易日内）快速连续的发生大量的买卖订单，订单数 ≥ 10000 。
- b) 频繁大额交易特征：短期内（3 个交易日内）交易金额在 1000 万元以上。
- c) 异常的交易时机特征：在特定交易时间发生异常交易或大额交易，例如在低流动性时段或市场波动性较高的时候。
- d) 交易对象特征：同一交易账号与异常数量的交易对象之间进行交易，交易对象的数量 ≥ 100 （个），通过在一个交易对象上创造交易来影响另一个交易对象的价格。

2) 链下关联风险特征指标

- a) 虚假的市场信息：涉及到通过传播虚假的市场信息来误导交易者和投资者的行为。
- b) 高压销售策略：涉及利用高压销售策略来推销虚假的投资机会的行为。

附件 1 参考文献

- [1] 中华人民共和国反洗钱法[J]. 中华人民共和国最高人民检察院公报, 2007(03):1-4.
- [2] 金融机构反洗钱规定[J]. 中华人民共和国国务院公报, 2007(29):43-45.
- [3] 中华人民共和国刑法[J]. 中华人民共和国全国人民代表大会常务委员会公报, 2021(S1):1-116.
- [4] 中华人民共和国证券法[J]. 中华人民共和国全国人民代表大会常务委员会公报, 2020(01):4-32.
- [5] 关于进一步规范深圳市非法集资异动交易线索报送工作的通知. 深圳市打击和处置非法集资工作领导小组办公室, 中国人民银行深圳市中心支行, 深圳银监局, 深圳市公安局, 2018: 36-42.