

虚拟货币分为可兑换和不可兑换两种类型，可兑换的虚拟货币具有真实货币的价值，可与法定货币、其他虚拟货币进行自由兑换，例如比特币；不可兑换的虚拟货币仅在特定的虚拟世界使用，根据其使用规则兑换法定货币或其他虚拟货币。例如：Q币、魔兽世界金币。

其中可兑换的虚拟货币又可分为中心化和去中心化货币，如Q币等有具体网络游戏运营商或平台作为发行方的为中心化虚拟货币，而比特币等无专门发行方，不依赖中央银行、政府机构以及网络运行平台担保，需要通过用户“挖矿”获得的货币为去中心化虚拟货币。

对于虚拟币，存在的风险有：

（一）交易隐匿性

传统意义上的普通货币交易是在指定账户间进行，账户开通和交易需先通过实名认证。虚拟货币基于网络数据产生和交易，打破了传统货币交易限制，仅通过数字秘钥等方式进行流通，部分虚拟货币交易平台和运营商虽要求客户进行实名登记注册，但缺乏对用户身份信息真实性、准确性进行核实的必要手段，客户真实身份信息难以追溯和辨别，特别是去中心化虚拟货币的产生，整个交易过程可以完全隐藏交易者身份。

以比特币为例，通过私钥技术保证交易信息只有用户本人可以获取，外界只能看到交易产生的一串数字，无法分辨交易详细信息，加大追踪难度，从而成为洗钱等违法犯罪活动的帮凶。



（二）加强沟通协作，建立机构和区域间协作机制

虚拟货币的发行和交易往往涉及多个机构和国家，仅靠一个部门或一国监管难度较大，在政策制定和实施环节加强各部门和国家的密切配合，及时了解虚拟货币的洗钱和恐怖融资风险。积极响应FATF关于虚拟货币反洗钱反恐怖融资监管方面的应对建议，吸取各国先进的监管经验，建立机构和区域间协作机制，推动决策者、监管机构、金融情报中心、执法机关形成监管合力，以风险为本原则识别、评估虚拟资产的洗钱和恐怖融资风险，采取有效措施降低我国被虚拟资产利用的洗钱风险。

（三）加强技术开发，提高虚拟货币反洗钱监测能力

虚拟货币交易本身具有去中心化、匿名性、跨国性等特点，这也是吸引犯罪分子通过虚拟货币洗钱的主要原因。一方面，虚拟资产交易的平台应完善客户身份信息实名制，了解、核实客户真实身份，完整、准确登记客户身份基本信息，加强IP地址追踪能力，对超过规定金额以上的交易或异常交易进行可疑交易分析与报送；另一方面，反洗钱情报部门应以加大技术投入，提高反洗钱情报部门监测分析异常交易的能力，使反洗钱监管部门能够在必要时完整查看加密信息，获取客户身份和交易信息，开展洗钱犯罪调查活动。

本文由蜡笔聊最炫科技原创，欢迎关注，带你一起长知识！