从跨链桥Multichain被抓说起：做跨链项目，要注意哪些法律风险？

作者：刘红林、金鉴智

华人跨链桥项目 Multichain 因涉及刑事犯罪，首席执行官等人被中国警方带走调查，一夜之间代币暴跌。旨在解决不同区块链之间价值互通的跨链技术，在中国真的不能创业吗？

### 创始人被抓，项目被迫停止运营

2023 年 5 月 21 日，知名的跨链项目 Multichain 首席执行官 Zhao Jun 被国内警方从家中带走，并与全球 Multichain 团队失去了联系。团队联系了 MPC 节点运营商，得知他们对 MPC 节点服务器的操作访问密钥已被撤销。

随后，专案组与 Zhao Jun 的家人取得了联系，并了解到 Zhao Jun 的所有电脑、手机、硬件钱包和助记词都被没收。自项目启动以来，所有运营资金和投资者的投资都由 Zhao Jun 掌控。

6 月 4 日，Zhao Jun 的家人成功登录了云服务器平台上的家用电脑，并只允许 Multichain 团队工程师物理访问家庭计算机来修复 Router2 和 Router5 的技术问题。

7 月 9 日，Zhao Jun 的姐姐转移了路由器池中剩余的用户资产，并随后通知了团队和多个项目方。这些资金被转移到了 Zhao Jun 姐姐控制的 EOA 地址。

7 月 13 日，根据 Zhao Jun 家属提供的情况，警方将 Zhao Jun 的姐姐带走。

据慢雾监测，自 7 月 7 日以来，从 Multichain 流出的资金总额高达 2.65 亿美元，分布在 Ethereum、BNB Chain、Polygon、Avalanche、Arbitrum、Optimism、Fantom、Cronos、Moonbeam 链。其中 6582 万美元已经被 Circle 和 Tether 冻结，1,296,990.99 ICE（约 162 万美元）被 Token 发行方 Burn。

据公开信息，Multichain 成立于 2020 年 7 月，并在 2021 年 12 月获得了 6000 万美元的融资。投资机构包括 Binance Labs、Sequoia Capital、IDG Capital、三箭资本、DeFiance Capital、TRON Foundation、Hashkey Capital、Circle、Hypersphere Ventures、Primitive Ventures 和 Magic Ventures。

### 区块链跨链是什么？

公链的快速发展与区块链技术的日益普及和创新密不可分。根据夸张数据，目前存在的公链可能高达数百条，不同的区块链之间存在不同的通信协议、共识规则和治理模型。知名公链包括比特币、以太坊、Solana、币安智能链（BSC）等，除此之外，还存在许多其他基于不同共识机制和技术架构的公链项目。每条公链都有其独特的特点、优势和应用场景。因此不同区块链之间的互操作性，让用户在链与链之间实现资产和信息转移的跨链技术成为必然产物。

跨链技术是区块链行业中的一项关键技术，旨在解决不同区块链之间的数据流通、资产转移和价值互通问题。跨链技术的底层技术比较复杂。非技术人员可以用一个简单的例子来理解跨链技术。多数情况下，当用户要把资产从 A 链跨到 B 链时，需要先把资产存到跨链技术在 A 链的指定地址中，接下来，当桥的检测者收到这一信息时，会在链 B 铸造等量的封装资产（wrapped token），或者通过在目标链建立资金池把跨链资产转换成目标链的原生资产，最后把钱打到用户在链 B 的账户中。

跨链技术最受关注的问题是安全问题。对于跨链的创业者来说，除了项目要安全，人身也要安全。

### 项目被攻击的法律风险

跨链技术领域的安全事故并不少见。2021 年 7 月 3 日，Chainswap 跨链项目的合约遭到攻击，部分用户代币被从与 ChainSwap 交互的钱包中取出，总损失约为 80 万美元。2021 年 7 月 12 日，Anyswap 新推出的 V3 跨链流动性池也遭到黑客攻击，总计损失超过 787 万美元。2021 年 8 月，Poly Network 宣布主网被黑客攻击，用户在 BSC、以太坊和 Polygon 三条区块链上的资产总计被转移 6.1 亿美元，成为迄今金额最大的 DeFi 安全事件。

由于区块链技术本质上是去中心化的，在智能合约出现缺陷或漏洞导致损失时，确定责任方可能非常困难。在出现用户资产丢失的情况下，跨链的项目方是否要承担相关责任是个比较复杂的问题。

对此，项目方可以提前做的有两件事：

1.智能合约安全审计。确保智能合约经过安全审计，从技术上以防止漏洞和攻击。大部分跨链技术本身是跟金融直接打交道的，关乎用户的资金，所以跨链技术协议的设计和实现需要从一开始就将安全考虑进去，而且无论多严谨都不为过。另外，协议最好通过至少两家安全审计公司进行审计，从而减少安全风险。不引入非必要的管理员身份，同时限制协议部署者和管理员的权限，防止因为单个账户泄露而导致整个协议的全部资金陷入安全隐患。

2.写好合同。确保项目方与合作伙伴、投资者和用户之间的用户协议、合同条款清晰明确，尽量在文本中规定在出现安全事故时各方的责任和义务，以及用户资产丢失情况下的赔偿机制。

### 项目发币的法律风险

绝大多数的跨链项目会有自己的项目代币。跨链创业者必须了解的是，不同国家和地区对于区块链和加密货币的法律框架差异巨大。例如，美国证券交易委员会（SEC）可能将某些代币视为证券，而欧盟则可能有完全不同的分类。这意味着，在设计和实施跨链解决方案时，必须考虑到各种法律要求和监管框架。

发币在中国更是敏感的问题。2017 年 9 月 4 日，央行等七部委发布《关于防范代币发行融资风险的公告》，明确指出代币发行融资本质上是一种未经批准非法公开融资的行为，涉嫌非法发售代币票券、非法发行证券以及非法集资、金融诈骗、传销等违法犯罪活动，要求自公告发布之日起，各类代币发行融资活动应当立即停止，已完成代币发行融资的组织和个人应当做出清退等安排。

如果项目方面向中国内地用户发行代币，属于监管的高压线。

### KYC、KYT 和 AML

引言中的 Multichain 被抓，据公开媒体报道，其涉及为犯罪集团洗钱，金额巨大。由于跨链技术本身的一些特性如匿名性和难以追踪，使得其容易被犯罪集团盯上成为洗钱的工具。

具体而言，跨链技术因为涉及多个不同的区块链网络之间的资产转移，其中一些网络可能具有更高的匿名性和隐私保护功能，如零知识证明或隐私币，这使得洗钱者可以更轻松地隐藏其资金流动的来源和去向。同时，跨链涉及多个区块链网络之间的资产转移，追踪和监视这些交易变得更加复杂。一些跨链协议设计还使得交易记录更难以被追踪或监视，从而为洗钱活动提供了更多的机会。

欧科云链研究院统计数据显示，洗钱、诈骗、传销、赌博是 2022 年最常见的四种虚拟货币犯罪形式，其中 54.72% 的虚拟货币犯罪与洗钱相关，21.13% 与诈骗相关。

各国政府不喜欢虚拟货币，很重要的原因是它被坏人们给用坏了。一旦犯罪团伙被监管部门盯上，为犯罪集团的犯罪资产提供帮助的跨链项目自然也无法脱离干系。而跨链项目肯定无法以技术中立为自己辩护。2022 年 8 月，美国财政部外国资产控制办公室 (OFAC) 曾制裁混币器 Tornado Cash，据制裁文件显示，Tornado 自 2019 年创建以来已用于清洗价值超过 70 亿美元的加密资产，其中包括朝鲜黑客组织 Lazarus Group 从两个区块链应用中窃取的超过 4.55 亿美元的加密资产。

而做好 KYC 和 AML 可以有效降低前述风险。

KYC（了解你的客户）：设计和实施有效的 KYC 流程是确保业务合规的第一步。这包括收集和验证用户的身份信息，如姓名、地址、身份证件和其他相关资料。确保 KYC 流程符合当地法律法规的要求，并进行持续的更新和审查。需要注意的是，在收集、处理前述个人数据时，需要确保遵守隐私法规，明确告知用户数据收集和使用方式。KYC 更适合法币世界，而 KYT 更适合区块链世界。

KYT（Know Your Transaction）：KYT 是一种金融机构用来监控和跟踪金融交易是否存在欺诈或可疑活动的过程，KYT 可以帮助金融机构识别每笔交易的来源和去向，评估交易风险，采取相应的措施，以及向监管部门报告可疑交易。KYT 与传统金融领域常用的 KYC 有所不同。KYC 主要关注客户的身份信息，更关注特定个体 / 机构的静态身份，而 KYT 主要关注客户的动态交易过程。如果说在传统金融领域，KYT 现阶段是加分项，但在虚拟资产交易中，KYT 或许将成为应对风险的必需品。

原因在于，在区块链世界中，类似去银行开户需要提供一大堆身份认证材料的环节是没有的，币圈人在账号开通上的原则是万事不求人，自己随便开，而且可以匿名创建无数个链上地址，这种情况下，通过一串乱码似的钱包地址你很难知道对方的真实身份到底是哪个人，更别提反洗钱防范了。KYT 将帮助区块链的使用者识别哪些地址和交易存在风险，找到可疑非法交易的黑地址，并能顺着黑地址追溯到交易的起点和终点。可疑的交易行为、暗网中的交易地址、它的关联地址们、某个地址在交易所的 KYC 记录等信息可以将链上地址与对应的实体联系起来，从而将匿名的链上世界和实名的线下身份进行链接。

AML（反洗钱）：实施有效的交易监控机制，以识别和报告任何可疑或异常交易活动。利用技术工具和系统来监测客户的交易模式、资金流动和风险行为，并及时采取必要的措施进行调查和报告。

有效的 KYC、KYT 和 AML 措施可以降低与洗钱、恐怖主义融资和其他金融犯罪相关的风险，并建立信任和声誉，在保障项目方安全的基础上，为业务和用户提供更安全和可靠的环境。

### 小结

随着越来越多的国家和地区将虚拟资产反洗钱纳入监管范围，涉及到虚拟资产发行和流转的机构们都不可避免地需要通过 KYT 来补充 KYC 的尽调工作，以满足监管部门对合规要求。

跨链创业者在追求技术创新和商业模式探索的同时，必须将法律风险管理作为重中之重。只有这样，才能确保自己的安全，只有在自己安全的基础上，才有项目的长期发展和用户资产的安全。