标题：

买卖usdt违法吗？BTC比特币、以太坊等虚拟数字货币诈骗、洗钱、掩饰隐瞒违法所得罪、非法经营罪、帮助信息网络犯罪活动罪怎么判刑

本文分两部分：

一：买卖或帮助别人买卖数字货币的犯罪风险及定罪量刑标准。

二：如何化解数字货币交易犯罪风险--如何争取到最轻的处罚。

第二部分：如何化解数字货币交易风险--争取到无罪和最轻处罚

我们要想预防、化解数字货币交易的刑事犯罪风险，争取到最轻的处罚，就必须掌握区块链、数字货币、网络支付、网络黑灰产、电子取证等专业知识，这对我们律师提出了更高的专业要求，有些犯罪嫌疑人被拘留了，需要律师提供辩护，结果和律师说了半天案情，律师听不懂或者一知半解，不知道钱包地址、冷钱包、热钱包、私钥、公钥、混币，不知道VPN、Tor、代币控制器，不知道暗网等，自然也就找不到案件的辩护的空间在哪里，导致有些案件的处理结果不理想。公安机关为了打击网络犯罪，成立了专门的网警部门进行侦查取证，如果我们律师不加强研究和学习，不具有专业的知识，以不专业辩护专业，又如何能取得好的辩护效果呢，这就是我多次提到的专业化的原因，处理网络犯罪的律师必须具有专业知识和经验。

这就是我一直提到的专业化的原因。

数字货币系统非常复杂，没有互联网技术背景的办案人员即使在专业人员的指点下，也很难明白系统工作方式及运行原理，很多律师不了解虚拟货币发行、交易的基本规律，掌握不了数字货币的追溯性在证据当中的体现，不懂得数字货币交易的伪匿名性以及如何增强交易的匿名性，未能敏锐洞察此类新型犯罪的共性与差异，从而在处理案件时陷入被动与滞后。

律师处理比特币BTC、泰达币USDT等虚拟币犯罪案件，首先要明晰运用虚拟货币犯罪的主要手段，对数字货币关键技术、发行运算框架、流通环境以及各大交易网站的特点要有所了解，熟练掌握相关电子证据的取证以及质证技巧。 除此之外，我们还要掌握数字货币犯罪案件的特殊程序要求，数字货币犯罪案件在立案、侦查取证、审查逮捕、起诉、审判涉及的问题十分复杂，包括刑事管辖、立案条件和标准、证据的调取、收集、固定、证据的采信等，由于相关程序性规定的不完善，办案人员缺乏经验，程序违法事项时有发生，甚至一些费劲周折获取的证据，因程序严重违法而被作为非法证据予以排除。只有掌握这些基本的知识，才能在争取无罪和罪轻时找到必策略和方法。

一、 化解数字货币交易风险的方法和策略。

（一）从证据上化解。

由于该类犯罪主要是在网络虚拟空间进行，所以在收集证据方面多是以电子证据为主，同其他网络犯罪所表现出的电子证据具有一定的共性，即具有易毁性、易篡改性，而且由于是虚拟空间内的犯罪很难留下足够的痕迹线索，再加上网络黑产从业人员一般都具有一定的反侦察能力，留下的网络痕迹证据很多是虚假的，例如使用tor或挂梯发起交易、租用人头户在火币等交易网站注册虚假账户、直接通过U盘等移动存储，以现金支付的方式场外进行的数字货币交易等，要从虚假的痕迹中找到确凿的定罪的证据是很难的。

网络黑产从业人员对网络及计算机的掌握程度远高于普通人，其对电子证据的销毁删除会更彻底，而且大部分会涉及原始性的电子数据，在加上网络黑产从业人员一般在被捉获后多有抵触情绪拒绝如实交代，这就导致数字货币交易的交易行为、交易网络、资金流向证据链在很多案件中难以形成，在加上网上证据与网下证据衔接难，很难形成完整的证据链，容易导致事实不清、证据不足，最后定不了罪。

数字货币网络犯罪案件中，证据一般都是围绕资金流和网络痕迹，我们律师要做的

工作就是从资金流和网络痕迹的证据中入手，充分利用数字货币用户匿名性、智能合约“内部交易”的隐蔽性、电子证据的易篡改性毁灭性的特点，通过审查证据，看能否找到证据中存在的问题，审查是否形成指控犯罪的闭合证据链，如果能切断证据链，就有可能从证据上切断数字货币
交易网络、交易行为
以及资金流向与被告人的对应或关联关系
，就有可能争取到不批捕、不公诉或者无罪的可能。在毕某、王某、杨某等人网络犯罪案件中，就是因为切断了资金流证据和痕迹证据，才最终让检察院不公诉让他们无罪释放。

我们在办理此类案件时，要想从证据上化解刑事犯罪风险，首先要熟悉区块链取证内容、取证流程、规范以及暗网中的取证手段，要掌握此类案件的证据体系。

1、审查区块链取证的内容是否完整。如果取证不完整，则可能不能形成指控犯罪的闭合证据链，可能存在证据瑕疵和漏洞，容易找到辩护的突破口，我们要审查是否包括以下几个方面的取证：

●账户地址 / 钱包地址；

●区块链客户端 ；

●交易信息；

●智能合约地址；

●用户调用智能合约情况。

2、审查区块链取证的证据是否与证据体系中的其他证据相互印证。如何证据不能相互印证，则不能形成指控犯罪的闭合证据链，就有可能争取到罪名不成立。其他证据包括：

●火币网、OKEX平台调取的账户注册信息、充币交易信息、提币交易信息以及内部交易信息，

●被诈骗资金的流转情况以及银行卡交易记录和明细；

●取款记录、凭证；

●通过提币地址对被告人数字货币进行追踪服务报告；

●通过计算机、手机及云取证方式获取以及分析的钱包地址关联的用户信息，例如邮箱名称、微博账户、qq登录ip等；

●犯罪嫌疑人的口供、同案犯的口供、上家或下家的证言；

●微信、qq以及蝙蝠、纸飞机等境外聊天软件的聊天记录。

●从扣押的电脑、手机、移动硬盘等硬盘中提取恢复的电子数据以及分析鉴定报告；犯罪嫌疑人其所控制的数字货币地址、密钥以及利用犯罪嫌疑人的交易记录进行交易人员的虚拟地址分析。

●针对第三方交易平台、客户端、相关移动设备以及所采用的资金流动的相关支付行为等的目标性电子数据。

我总结的“两审查策略”，
是从证据上化解数字货币交易刑事犯罪风险的有效思路方法，这里介绍一下“两审查策略”。

1、审查资金流证据：是否形成指向犯罪嫌疑人的闭合证据链。

资金流是破案的关键证据，很多案件就是因为找到在变现过程的证据才抓获犯罪嫌疑人，我们必须掌握数字货币变现的风险点以及审查资金流相关证据的思维和方法，这是我们能争取到撤案、不公诉或无罪的关键一环。

由于数字货币的匿名性以及黑产从业人员具有一定的反侦察能力，在资金的流转过程中多使用他人的银行卡、支付宝账户、黑卡、地下钱庄、赌博网站或者混币、暗网，并且买卖银行卡已经成为一条产业链，要想将每一笔资金都形成指向犯罪嫌疑人的证据链是有难度的。

在陕西毛某掩饰隐瞒犯罪所得罪一案，第三级收款账户的钱如何转出，以及尾号为TH5Y提币地址如何变现都未查清，警方在补充侦查报告中，称查清难度大，无法查清，便草草结案。

我去年在河南处理了一起案件，王某、李某为电信网络诈骗团伙提供洗钱服务，他们购买了大量的银行卡黑卡提供给诈骗团伙，然后将银行卡里的钱全部通过火币网购买了比特币，他们为了逃避侦查采取线下现金的方式交易比特币，增加了匿名性，使用黑卡账户进行资金流转、采取线下现金的方式交易，使得幕后主犯的身份一直没法确认，只是知道微信名称叫xxx。到案件结案时，因无法查清资金来源和幕后老板身份，警方只是对此作了一个说明，说各部门在继续侦查，一旦确定xxx的真实身份就立刻实施抓捕。

还有我在2017年处理的一起网络诈骗案中，他们将客户的入金全部从境外网站上购买了比特币，公安机关认定的涉案金额是2000多万，但我们在辩护时发现，这2000多万的诈骗金额中有很大一部分的资金是没法形成资金流转的证据链的，最终检察院在公诉时认定的涉案金额改为700多万，在我办理的网络犯罪案件中，降低金额最多的一起案件是发生在浙江的一起案件，诈骗金额由一开始的1.9亿降低为1.2亿，足足降低了七千万左右的金额。

我们律师在办理网络犯罪案件时要重点审查：

（1）操作赃款的的支付宝、网银或其他网络支付账户是否是犯罪嫌疑人持有和操作。在很多案中，赃款会流入多个支付宝、网银等网络支付账户，我们律师在办理案件时，要重点审查是否有证据证明这些账户都是由犯罪嫌疑人所有或操作。

我们需要注意的是IP轨迹吻合问题，在很多案件中，都会出现这个问题，我们律师要注意的是，根据多个支付账号的IP地址轨迹吻合就来认定一个人是犯罪嫌疑人是一种推定，在租借虚拟专用服务器（VPS）和虚拟专用网络（VPN）的情况下，在同一个公共网络中多台计算机的IP地址是相同的，如果没有其他证据印证，是不能形成资金流向闭合证据链的。

例如在王某案中，赃款被转入5个支付宝账户，之后全都流入网络赌博平台，没有任何证据证明这5个支付宝账户由王某操作，那公安机关为何将王某抓获呢？原因就是网安侦查总队分析这5个支付宝账户的登录IP地址轨迹，发现王某的QQ号和邮箱以及支付宝账号IP轨迹在不同时间点与这5个支付宝账号多次吻合，以此来证明涉案的5个支付宝账号使用者是王某。

（2）赃款流入的银行卡是否是犯罪嫌疑人所有或持有。要重点注意在赃款流转的过程中那些黑卡的问题，要看这些黑卡是否为犯罪嫌疑人持有，要审查证据中，是否有黑卡的扣押证据；还要注意取款人方面的证据问题，是否抓到取款人，是否有证据证明取款人与犯罪嫌疑人有关联。对于采取线下现金交易的，还要注意与言词证据以及证人证言的吻合度进行审查。

2、审查数字货币账户与被告人的关联性证据：是否形成指向被告人的闭合证据链。

警方在破案时，先根据黑钱的资金流向，找出可疑的数字货币账户地址，然后想办法破解匿名性，与嫌疑人的个人信息关联。一旦有嫌疑的数字货币地址与犯罪嫌疑人产生了关联，就有可能被调查甚至被冻结账户被拘留。

我们律师在办理案件时需要注意，由于数字货币具有具有强匿名特点，持有者信息则为公钥与私钥字符串，系统生成的不同账户、地址不存在关联性。在这种特性之下，用户的真实身份很难去追踪和验证。尽管用户在区块链网络中的行为都是公开透明的，凭借这些交易行为确实可以利用大数据分析技术来对交易双方的真实身份进行推断，但这种方式的推断具有很大的主观性,容易找到辩护的空间。

我们还需要注意一种情况就是在一些案件中，犯罪嫌疑人可能会使用混币器、联合币（共享发送）、暗钱包、隐形地址等方式混币，分离交易中的输入和输出地址，即割裂输入地址和输出地址之间的关系，目的是提高加密货币的隐私性和匿名性，使其更难追踪加密货币的用途以及它属于谁。

我们在辩护时，在对证据进行审查与质证时，要有专业的思维，来审查数字货币账户与犯罪嫌疑人之间的关联性证据。从以下三个方面入手:

（1）能否阻断钱包地址与犯罪嫌疑人（被告人）的身份信息对应关联关系的证据链。

（2）能否阻断断钱包地址与犯罪嫌疑人的IP地址以及设备的MAC地址对应关联关系的证据链。

（3）能否阻断比特币交易过程与犯罪嫌疑人的其他网络信息、网络痕迹形成对应或关联关系的证据链。

关于这三个方面的内容我已经说过多次，这里就不在重复。

（二）从性质和罪名上化解。

买卖比特币、泰达币等数字货币，做数字货币交易并不违法，之所以会被冻结账户甚至构成诈骗罪、洗钱罪、掩饰隐瞒犯罪所得罪，帮助信息网络犯罪活动罪，最主要的原因就是明知道买币的客户是诈骗分子，明知道客户的购币款是黑钱赃款，仍

然将数字货币卖给他们，为他们提供资金洗白和掩饰的通道。

所以，要想化解数字货币交易的刑事犯罪风险，就要将数字货币交易的性质回归到单纯的“交易和买卖”，单纯的搬砖套利赚取差价，而不是为了诈骗和为黑钱提供资金洗白和掩饰的通道。

要想从性质上化解掉诈骗罪、洗钱罪、掩饰隐瞒犯罪所得罪、帮助信息网络犯罪活动罪，就要审查是否有充分证据证明被告人明知道购币者是诈骗分子，明知道购币款是黑钱赃款。

此类案件中，被告人与同案犯一般都互不认识，可能只是网友，互相之间连真实名字都不知道，网络犯罪中行为人之间意思联络形式多样化、联络主体虚拟化、共同行为模糊化，有时候要形成指向被告人“明知”证据链是有难度的。例如陕西某案中，被告人通过“社工库机器人CCTV认证群”中，认识有购买USDT需求的客户A,最终经过侦查，无法查明A的具体身份，最终无法认定被告人存在与诈骗分子合谋的诈骗目的，最终法院认定检察院指控的诈骗罪罪名不成立。还有李某等人诈骗案中，李某在QQ上搜索QQ群‘电信洗白’“专业洗白”，加入群，在群里为客户“小蜻蜓”（化名）提供比特币洗钱通道，最终小蜻蜓的身份也未查明。

随着网络黑产从业者反侦察能力的提高，公安机关在取证时要找到“由人到人”的证据链来证明“明知”越来越困难，我处理的网络犯罪案件中，犯罪团伙使用的聊天软件主要有：蝙蝠聊天软件和台湾的聊天软件whatsapp，还有毛某等人案件中，使用的聊天软件是SKYPE，还有纸飞机等，这些聊天软件是端到端的加密，服务器不留痕迹，直接用ID登录，不需要绑定任何身份信息，极致安全私密、信息可以看后即焚、双向撤回、删除聊天信息，这些都是我们从证据上审查“由人到人”“明知”的证据链时需要注意的地方。

我们律师在办理此类案件时，要具有专业的思维和方法，审查“明知”的证据，包括聊天记录、
转款记录、通话记录等，看
是否有充分证据证明被告人
“明知”购币款是黑
钱赃款、“明知”购币客户是诈骗分子，
看“由人到人”、“明知”的证据链是否闭合。

除此之外，我们还要特别注意“推定明知”的情况，什么叫“推定明知”，就是司法机关根据一些证据来推定卖币者明知客户的购币款是黑钱。在我遇到的案件中，办案机关推定“推定明知”主要有以下几种情况：

1、被告人与买家的聊天记录中，被告人提到，现在黑钱较多，要求买币者进行kyc实名认证，但被告人最终未与“买币者”进行实名认证。

2、被告人在每笔资金转入交易银行卡账户前，通过转入、转出小额资金测试银行账户是否被冻结。

3、被告人明知用于“某某平台”买卖usdt币的银行账户遭到公安机关和司法机关的冻结，其资金来源可能是犯罪所得，仍然指使员工及时将到账的资金全部及时转到火币网上购买usdt币，防止被冻结。

4、在使用的账户被冻结后更换账户继续与该买家进行交易。

5、价格明显高于市场价格。

《最高人民法院关于审理洗钱等刑事案件具体应用法律若干问题的解释》中，细化了洗钱犯罪中“明知”的司法认定。《解释》列举了六种推定“明知”的具体情形，即，（1）知道他人从事犯罪活动，协助转换或者转移财物的；（2）没有正当理由，通过非法途径协助转换或者转移财物的；（3）没有正当理由，以明显低于市场的价格收购财物的；（4）没有正当理由，协助转换或者转移财物，收取明显高于市场的“手续费”的；（5）没有正当理由，协助他人将巨额现金散存于多个银行账户或者在不同银行账户之间频繁划转的；（6）协助近亲属或者其他关系密切的人转换或者转移与其职业或者财产状况明显不符的财物的。

“推定明知”本身就是一种推定，与疑罪从无的刑法精神相悖，我们在办理案件时遇到“推定明知”的情况，就要从整个案件的综合证据入手，用专业的思维技巧据理力争。我今年处理的刘某网络诈骗案，整个案件的涉案诈骗金额为1.2亿，经过两次补充侦查，最终潍坊某县检察院采纳了我们的辩护意见，认定刘某“明知”的证据不足，对刘某做不起诉撤案处理。

只要没有充分证据证明被告人“明知”，那被告人买卖数字货币的行为就不构成诈骗罪、洗钱罪、掩饰隐瞒违法所得罪、帮助信息网络犯罪活动罪。

（三）从情节和主从关系上化解。

1、从情节上化解。对交易次数少，涉案金额低的案件，可以考虑自首、立功、坦白，退赃、认罪认罚、预缴罚金等，努力争取取保候审、检察院不起诉、法院免予刑事处罚，或适用缓刑。我们处理的沈阳张某、莱芜李某案件，就是从情节上争取到取保候审的。

2、从主从犯关系上化解。争取认定为从犯，即使不能完全化解刑事责任，一旦认定为从犯也会大幅度的降低刑期。

由于司法办案人员对于此类犯罪产业链的分工比较陌生，有时对某一个环节的被告人所起到的作用可能拿捏不准，所以会出现主从犯认定标准不一的情况，这都需要我们律师根据专业的知识和思维进行辩护，一旦争取到从犯，就能大幅度的降低刑期。

可以从以下三方面审查论证，争取被告人是从犯：

①从被告人的身份、地位上看，是否属于决策层的人员或者属于团队运营的主要出资人或者实际控制人；是否处于被管理、被分配、或者上命下达的作用，在团队中有无管理、组织职责或管理、组织职责是否明显等。

②从被告人的职责上看，仅仅接受老板命令帮助操作银行账户或数字货币账户的，或者帮助取钱送钱的、开发和联络上下游客户等非核心业务的，在实践中要争取认定为从犯。

③从被告人获利来看，是拿固定工资还是参与分红。

最后，再说一下，此类案件中电子证据和口供问题，这是网络犯罪中老生常谈的问题。

1、虚拟货币犯罪案件最终罪名能否成立，很大一部分取决于收集、分析、质证电子证据的能力，大多数证据都以电子证据形式呈现，专业性强，未经专业培训的人员难以辨别和鉴定，从当前的司法实践上看,对电子证据证明力如何进行认定,即电子证据的证明力如何?往往成为法庭争论的焦点, 亦成为法官认定电子证据的棘手之处，同时这也是我们律师在辩护时要重点关注的地方。我们在办理此类案件时需要掌握对电子证据的质证技巧，从形式审查和实质审查两方面入手，看能否找到电子证据的的问题。关于这方面的内容我已经说过多次了，这里就不在重复。

2、关于口供言辞证据问题。

在这类案件中，犯罪嫌疑人（被告人）自己的口供非常重要，由于数字货币的去中心化和匿名性特点，电子证据容易被窜改和灭失，很难形成完整的证据链，所以严重依赖被告人的口供。

在很多案件中犯罪嫌疑人会自信自己的技术高超，或者自信侦查人员听不懂一些专业术语，在被讯问时，故意说一些区块链、数字货币以及网络黑产方面专业术语，

以求蒙混过关，所以经常出现口供来回翻供或者与同伙之间口供不一的情况，对于每一种情况该怎么处理，包括我们律师会见时如何在不违法的前提下提供最明确的法律咨询，这些都考验着我们律师的办案能力。

张洪强律师经验总结，禁止一切形式的转载复制剽窃。