区块链与加密货币相关的有害行为识别

区块链的概念伴随着加密货币比特币而诞生，随着第一笔使用10000个比特币购买两个披萨的交易后，比特币被赋予了现实中的价值。随着加密货币的总价值不断变大，利用加密货币的欺诈行为随之出现。利用区块链进行有害行为的情况，可能会对区块链社区造成损害，对加密货币的投资者也有可能造成恐慌或实际的资金损失，因此对于这类行为的尽早识别并给出警告或漏洞修补，对于促进区块链技术的持续发展有着重要的意义。

在 Understanding Ethereum via Graph Analysis一文中，提出了对收集的交易数据进行分析的一种方法，其过程是从数据中构建图来识别交易的特征并获得更多的信息。在图的构建中需要构建资金流动图（MFG），智能合约的创建图（CCG）以及调用图（CIG）。对于智能合约的内部交易信息的获取方法是通过修改以太坊客户端，使之记录以太坊虚拟机中执行的对合约的创建及调用。通过 MFG，可以识别出交易所账户(节点的度较大)，并且 MFG 中大部分的节点间存在着相互的有向路径，意味着交易所的节点的存在，其特征是对大量的账户进行发送或接收的交易。通过 CCG，可观察到较小的一部分节点创建了较多的智能合约，因为智能合约数量大于合约开发者的数量，而且在所有合约中存在着大量的无用合约，独特合约仅占了小部分。对 CIG 的分析可观察到仅有小部分合约被较多地使用；包括交易所在内的金融性应用在资金转移、合约创建与合约调用中都占有最大的比重。通过构建图的方法，可以找出区块链中存在的占用硬盘或网络资源的无用合约，文中给出了一个通过构建的三个图搜寻无用的合约的算法，通过算法可以检测出创建大量合约的潜在攻击者同时排除有创建大量合约需求的交易所。

类似于上文的方法Market Manipulation of Bitcoin: Evidence from Mining the Mt. Gox Transaction Network 一文中采用对图进行分析的方法对门头沟交易所（Mt. Gox）操纵比特币市场价格的证据进行挖掘。通过对 Mt. Gox的交易数据根据账户对币价的影响程度进行图的构建，观察到部分账户在交易中使用的价格过高或过低，这些异常交易与交易所的价格变动有着较大的关系；根据数据可认为这些账户被交易所控制；在异常交易间存在着部分正常正常交易，可能是由交易所构造的虚假交易额；而且发现的异常账户有着被某一组织控制的可能，存在着异常的交易模式。由此认为 Mt. Gox很可能存在操纵比价的情况。为了维持加密货币市场的稳定性与投资者的信心，通过文中提出的方法对交易所行为进行监督是有必要的。

在以太坊为代表的二代加密货币出现后，利用以太坊上的智能合约进行欺诈的行为也出现，Detecting Ponzi Schemes on Ethereum: Towards Healthier Blockchain Technology 一文中提出了使用 XGBoost 机器学习算法来实现准确的对智能庞氏骗局合约进行识别。识别中使用的合约特征为合约交互的账户特征和合约指令码特征，无需获取合约的源代码。结合两个特征进行合约的分类可以取得较高的准确率。

在区块链和加密货币中出现的诈骗或其他的非法行为会对区块链的整体生态带来不良的影响，部分组织对信息的造假或交易量的操纵可能会造成不必要的恐慌和对用户的误导，对区块链去中心化的特点造成破坏。以上论文中提到的构建区块链中交易或账户相关的图，或者使用机器学习构建分类器的方法，可以应用在更多场景下，对区块链中存在的有害行为进行自动的识别。对这些有害行为的尽早发现，可以防止利用区块链对用户造成损失的行为，这是对区块链推广发展的前提保证。