《924通知后，涉虚拟货币案件民事救济路径分析》系列文章对于民事领域审判涉虚拟货币案件情况进行了梳理，其实在刑事领域，也存在大量涉虚拟货币案件同案不同判情形。

刑法理论与实务界对虚拟货币的财产属性以及窃取虚拟货币行为的定性存在较大分歧。

对于虚拟货币的财产属性存在“否定说”“肯定说”“区分说”不同观点，对于窃取虚拟货币行为的定性问题，也存在“盗窃说”“计算机信息系统犯罪说”“想象竞合说”“牵连犯说”等多种观点。

本文系笔者原创，转载请注明出处。

文 | 王菲 律师

三、安装软件型

方式八：在电脑植入挖矿程序，电脑开机即自动运行挖矿程序，在后台挖取虚拟货币

如(2018)粤0113刑初2876号案中，2018年2月至2018年8月15日期间，被告人成某利用在被害人江某所有的5间网吧任职技术员的便利，私自将“挖矿程序”通过网吧服务器植入网吧的616台电脑，电脑开机即自动运行“挖矿程序”在后台为被告人成某“挖取”虚拟货币。

方式九：在已经安装挖矿软件的电脑上安装外挂进行双挖

如（2018）湘0422刑初327号案中，被告人罗某某经营一家电脑维修店，平时亦使用电脑进行网上虚拟货币运算挖矿赚钱。被害人唐某某从毛某某处了解到网上挖矿可以赚钱，便通过毛某某介绍认识了被告人罗某某。2017年6月，被害人唐某某从被告人罗某某处购买了10台专门配置的电脑用于网上虚拟货币“以太币”挖矿，被告人罗某某组装好电脑，并帮其安装了“长沙-矿工”的挖矿件和申请了“以太币”电子钱包。同年8月，被害人唐某某又自行购买了30台电脑用于网上挖矿，并雇请被告人罗某某帮其安装电脑和下载挖矿软件。2017年9月的一天，被告人罗某某帮被害人唐某某维修电脑，在被害人唐某某不知情的情况下，通过远程操控在被害人唐某某的40台电脑内安装了一个代号为“eth.exe”的隐藏、自动运行“双挖”（即1台电脑同时运算挖取两种虚拟货币）程序的外挂软件，并帮定其本人的电子钱包，使得被害人唐某某的40台电脑在为被害人唐某某挖取“以太币”的同时，还自动运行“双挖”程序挖取“SC币”存入到被告人罗某某的电子钱包。2017年12月，被害人唐某某在其电脑里发现该外挂软件，被告人罗某某遂将通过上述外挂程序挖取的40万个“SC币”全部返还给了被害人唐某某，并取得其谅解。

方式十：修改添加软件代码，下载软件时自动上传私钥

如(2019)苏0111刑初1078号案中，被告人杜某在上海某信息科技有限公司担任安卓开发工程师。同年6月期间，被告人杜某在负责该公司的某软件安卓系统维护的过程中，私自添加代码，使使用该版本的安卓手机用户的账号私钥自动上传至自己私人的腾讯bugly账号内，并筛选出有ACG虚拟货币的八个账号。同年9月27日，杜某使用自己的手机登陆八个账户，将3473009个ACG虚拟货币合计人民币约五十余万元，转至自己控制的账户内。

四、系统漏洞型

方式十一：利用系统自身漏洞窃取虚拟货币

如（2020）闽0305刑初82号案中，被告人许某通过手机微信广告群获取了某数字货币交易软件的下载链接，并用自己的身份信息在平台上注册账户，其在交易过程中发现了该平台上存在交易漏洞，该漏洞表现为：该平台进行数字货币交易前需要用户将自己的USDT充值进平台方可交易，当用户向该平台充值USDT后，平台入账

会出现延迟，该平台在延迟过程会显示用户的转账成功已到账平台，同时，该平台会将USDT入账到用户账户内，用户可非法利用延迟漏洞将充值的USDT再提取出来，从而出现用户未充值，该平台却入账USDT给用户，造成平台遭受经济损失。后被告人许忆航发现该交易平台漏洞后，为了非法获取更多的USDT，便利用冯某、韩某、郑某、蔡某、同案人许某等五人的身份证信息进行注册账户，后利用自己的账户以及上述五个账户分别在数字货币交易平台上，利用漏洞采取虚假输入充值USDT的手段，从该交易平台非法获取了大约116932.515个左右USDT。

后记

虚拟货币具有去中心化、匿名性、跨国性以及交易快捷、不可撤销等特点，存在着被滥用于从事洗钱、传销、非法集资、盗窃等犯罪活动的风险。由于对虚拟货币犯罪进行监测存在较大的技术难度，涉虚拟货币犯罪手段层出不穷，本文针对已经接受法律制裁的部分窃取方式加以总结，后续文章将对窃取行为的定性及裁判观点进行分析。