

Doi: 10. 11835/j. issn. 1008-5831. fx. 2025. 05. 003

欢迎按以下格式引用:王德政. 区块链向度下盗窃数字货币行为的刑法审视:实证解读与逻辑定位——基于2014—2024年38份刑事判决书的考察[J]. 重庆大学学报(社会科学版),2025(3):257-271. Doi:10. 11835/j. issn. 1008-5831. fx. 2025. 05. 003.



**Citation Format:** WANG Dezheng. The scrutinize about criminal law of stealing digital currency in the perspective of blockchain: Empirical interpretation and logical orientation[J]. Journal of Chongqing University (Social Science Edition) ,2025 (3):257-271. Doi:10. 11835/j. issn. 1008-5831. fx. 2025. 05. 003.

# 区块链向度下盗窃数字货币行为的 刑法审视:实证解读与逻辑定位 ——基于2014—2024年38份刑事判决书的考察

王德政

(西南石油大学 法学院,四川 成都 610500)

**摘要:**通过考察我国法院作出的关于盗窃数字货币案件的刑事判决书,不仅可发现我国盗窃数字货币案件的特点并由此可得出许多对司法实践有用的启示,还可发现我国法院对于盗窃数字货币行为以盗窃罪定性的占一半比例,紧随其后的是非法获取计算机信息系统数据罪,想象竞合犯和破坏计算机信息系统罪仅属极为小众的定性结论。在我国法院的实践中,盗窃数字货币的行为定性呈现出极为不同的现象,衍生出在刑法理论上对该问题进行深入研究的必要性。数字货币是一种作为财产性利益的数据。应将数字货币这种无体物纳入所有权的对象,盗窃罪的行为客体“财物”由此包含数字货币。数字货币属于限定违禁品,如果盗窃数字货币行为构成盗窃罪或含盗窃罪的数罪,应对行为人从宽处罚。在司法实践中处理盗窃数字货币案件时应先排除假性盗窃数字货币案件。如果行为人实施的是针对“矿机”和电力的盗窃行为,以及利用自己和他人的计算机制造数字货币的“挖矿”行为,这类案件并非真正的盗窃数字货币案件,对前者情形应回到盗窃普通财物的轨道进行处理,对后者情形应判断非法侵入计算机信息系统罪和非法控制计算机信息系统罪是否成立。再分别审查盗窃数字货币行为是否构成盗窃罪和非法获取计算机信息系统数据罪,审查的重点是该行为是否满足盗窃罪中数额较大的要求和非法获取计算机信息系统数据罪中情节恶劣的要求。如果行为人的行为不满足数额较大的要求但满足情节恶劣的要求,则构成非法获取计算机信息系统数据罪。如果行为人的行为不满足情节恶劣的要求但满足数额较大的要求,则构成盗窃罪。如果上述要求均不满足,行为人的行为不构成二罪。如果行为人的盗窃数字货币行为同时构成盗窃罪和非法获取计算机信息系统数据罪,二罪的关系为想象竞合犯,该行为应被认定为盗窃罪。另外还应审查行为人除了实施盗窃数字货币行为,是否还伴随、独立地实施了非

**基金项目:**司法部法治建设与法学理论研究部级科研项目“人工智能时代自动驾驶汽车涉及的刑法问题研究”(21SFB4036)

**作者简介:**王德政,西南石油大学法学院讲师,法学博士,Email:182402257@qq.com。

法侵入计算机信息系统行为和非法控制计算机信息系统行为,如果实施了上述行为,应将行为人的整体行为认定为盗窃罪、非法侵入计算机信息系统罪、非法控制计算机信息系统罪并进行数罪并罚。

**关键词:**区块链;数字货币;比特币;盗窃罪;非法获取计算机信息系统数据罪

**中图分类号:**D923.4   **文献标志码:**A   **文章编号:**1008-5831(2025)03-0257-15

## 一、问题的提出

当前,随着区块链技术在全球和我国的迅猛发展和广泛应用,数字货币(或称加密货币、“比特币”)的发行和运用所导致的刑法问题呈现在我国社会面前,其解决方案的研讨值得我国学界重视。数字货币中最为知名的当为比特币(Bitcoin)。2009年2月11日,一个网络署名为“中本聪”的人在P2P基金委网站上声称自己开发出一种叫比特币的电子现金系统<sup>[1]</sup>。不同于传统货币的是,底层技术为区块链的比特币在发行和交易上不依赖于国家、政府和中央银行的信用担保,而依赖于对等式网络中种子文件达成的网络协议,实现单个节点与其他节点的直接交互以及地址之间的价值互换<sup>[2]</sup>。比特币具有以下特性:无实体性、数字化存储和支付性、无集中发行主体性、数量有限性、适用范围有限性、匿名性、无法追踪性<sup>[3]</sup>。比特币诞生时一文不值<sup>[4]</sup>,但之后不断经历价格的巨幅波动。2013年4月20日,四川芦山地震后,我国基金会接受了235个比特币的公益捐赠,比特币由此走入我国公众的视野。然而,比特币仅属于当前全球2 000多种数字货币中的一种<sup>[5]</sup>,还有泰达币、以太币、瑞波币、莱特币等,以及我国正在进行试点的数字人民币。

行为人对于上述数字货币所实施的行为可分为两类:一是制造行为(所谓的“挖矿”)<sup>[6]</sup>,即通过在计算机(所谓的“矿机”)上使用软件制造数字货币的行为。该行为本身不是盗窃行为。如果行为人未经他人同意,在他人的计算机上使用软件制造数字货币后取得该数字货币(如河北王某等非法控制计算机信息系统案)<sup>①</sup>,此时,行为人利用他人计算机“挖矿”的“借鸡生蛋”行为原始取得了对数字货币的所有权和占有,这决定了行为人随后实施的对该数字货币的取得行为不是盗窃行为。详言之,虽然数字货币的制造由使用软件行为和计算机运行共同完成,并且数字货币被行为人取得之前存储于计算机内,但该数字货币的所有权人和占有人都是使用软件的行为人而非计算机所有人,理由在于:第一,行为人取得数字货币对计算机所有人并未造成根本性的损害;第二,行为人取得的数字货币并非软件运行之前计算机固有的数据;第三,软件积极主动地驱动计算机制造数字货币,而计算机仅被动地参与制造,这决定了使用软件的行为人而非计算机所有人对制造数字货币起到了重大作用。因此,使用软件的行为人并未转移对数字货币的占有,这不符合盗窃行为的核心定义——排除他人对财物的占有并对该财物取得占有<sup>[7]</sup>,行为人的取得行为由此不构成盗窃罪;二是转移行为,即在不同主体之间实现数字货币占有转移的行为。行为人如果未取得数字货币占有者的同意而对该数字货币实施转移占有行为,则该转移占有行为系盗窃行为。此时,盗窃行为的客体是数字货币本身,该情形不同于司法实践中频发的为了“挖矿”而针对“矿机”(如四川梁某等盗窃案)<sup>②</sup>,及电力(如辽宁贺某某等盗窃案)的盗窃行为<sup>③</sup>。但有学者认为,针对数字货币,行为人无法为

① 河北省保定市莲池区人民法院(2018)冀0606刑初65号刑事判决书。

② 四川省康定市人民法院(2020)川3301刑初11号刑事判决书。

③ 辽宁省锦州市古塔区人民法院(2018)辽0702刑初47号刑事判决书。

自己或他人建立新占有<sup>[8]</sup>。这属于对数字货币具有可转移占有性的误解。

在我国当前司法实践中，时常发生针对数字货币的盗窃行为，即：行为人通过某种手段（在数字货币中插入代码等），排除他人对数字货币的占有并取得对该数字货币的占有，此时，如何定性行为人的行为，我国法院的审判结论并不一致。以比特币为例，有法院将盗窃比特币行为定为盗窃罪，如浙江武某盗窃案<sup>④</sup>。也有法院将之定为非法获取计算机信息系统数据罪，如江苏陈某非法获取计算机信息系统数据案<sup>⑤</sup>。这些定性结论上的明显差异产生了以下问题：第一，就实证解读而言，我国相关刑事判决书中的盗窃数字货币案件有哪些特点，法院的定性结论在罪名的种类和比例上呈现出何种状态，可从中得出何种启示？第二，就逻辑定位而言，针对盗窃数字货币行为，如何根据《中华人民共和国刑法》（以下简称《刑法》）规定和刑法原理，通过论证推导出合理、具备可操作性的定性结论，为司法实践工作者提供一个类型化的解决方案？笔者拟于下文中依次讨论上述问题、得出结论并以此求教于学界同仁。

## 二、盗窃数字货币案件的特点和罪名状况

笔者在中国裁判文书网上，以比特币等多种数字货币为关键词进行搜索，获取2014—2024年我国法院作出的所有关于盗窃数字货币案件的刑事判决书共计38份，对这些判决书进行分析后，可以小见大发现我国盗窃数字货币案件所具备的某些特点，以及法院的定性结论在罪名上的种类和比例分布。

### （一）特点

第一，从案件发生的地区看，在河北发生的案件为5件，上海、浙江、河南、广东均为4件，北京、湖南为3件，江苏、四川、辽宁为2件，天津、重庆、湖北、河南、海南为1件。这说明河北、上海、浙江、河南、广东属于盗窃数字货币案件相对较为频发的省份，关于盗窃数字货币行为定性的研究结论对这些地区的法院更为实用，该地区的司法机关亦应当更加重视对盗窃数字货币行为定性的研究和运用。

第二，从不同年份的案件数量看，从2014年到2024年，案件数量分别为1、2、1、2、8、7、8、3、1、2、3件。这说明，盗窃数字货币案件的数量在2018—2020年达到高峰以后迅速回落，但目前又有上升趋势，意味着当前盗窃数字货币行为定性的理论和实践价值仍较大。

第三，从不同种类被盗数字货币的数量看（同一案件涉及多种数字货币则重复计算），涉及比特币的案件为15件，其余由多至少分别为：泰达币11件，以太币5件，瑞波币4件，莱特币、阿希币2件，门罗币、浩德币、“双子新约”、数字人民币、柚子币、小蚁币、LRC、DDV均为1件。这说明，一方面，比特币、泰达币依然是我国数字货币监管工作的重点，也是司法实践工作者在刑事办案实践中最应关注的数字货币；另一方面，全国首发盗窃数字人民币案件是2024年在江苏，这是盗窃数字货币案件的最新动态，应当密切重视和加强对数字人民币试点的安全监管，细化数字人民币的监管措施<sup>[9]</sup>。

第四，从盗窃行为的实施前提看，获取被害人数字货币账户和密码信息的案件为27件，其中合法获取该信息的案件为4件，非法获取该信息的案件为23件，其中不通过技术手段直接向被害人获取该信息的案件为12件，通过对被害人的计算机设置病毒程序并实施远程操作获取该信息的案件

<sup>④</sup> 浙江省天台县人民法院（2016）浙1023刑初384号刑事判决书。

<sup>⑤</sup> 江苏省金湖县人民法院（2015）金刑初00090号刑事判决书。

为5件,通过对被害人的计算机实施远程操作获取该信息的案件为3件,通过黑客等技术手段获取该信息的案件为1件,在非法网站获取该信息的案件为1件,在非法网站获取大量公民个人信息为信息库并使用黑客等技术手段从中查明该信息的案件为1件;利用数字货币服务平台漏洞的案件为6件;在数字货币服务平台修改被害人数字货币账户和密码信息的案件为4件;在被害人的计算机上设置病毒程序的案件为1件。这说明:其一,公民个人信息保护对防范盗窃数字货币案件的发生极为关键。数字货币服务提供者应加强对数字货币账户和密码信息的安全性的管理,根据变动的客观情况不断提升服务平台的安全技术层级;数字货币占有人应提高警惕,不轻易让他人获取自己的数字货币账户和密码信息,并在他人知晓该信息后及时进行修改,同时应严格防范他人对自己的计算机实施远程操作;网络监管部门应加大力度查处非法网站(尤其是暗网)并及时清理其中的公民个人信息。其二,计算机病毒程序的传播对盗窃数字货币案件的发生推波助澜。网络监管部门应加强对计算机病毒程序的防控和清除,数字货币占有人应通过安装和及时更新功能强大的计算机反病毒软件等措施,防止其计算机感染病毒程序。其三,数字货币服务平台的技术先进性程度与盗窃数字货币案件的发生直接相关。数字货币服务提供者应在技术提升上增加资金和人力投入,防范服务平台可能存在的漏洞,以先进的技术保障服务平台正常运行。

第五,从犯罪所得数额看,达到盗窃罪数额较大标准(1 000元至3 000元以上)的案件为7件,达到数额巨大标准(3万元至10万元以上)的案件为15件,达到数额特别巨大标准(30万元至50万元以上)的案件为12件,另有4个案件数额不明。这说明,达到数额巨大和特别巨大标准的案件占绝大多数,这意味着盗窃数字货币案件对财产法益的侵害一般较为严重。

## (二)罪名的种类和比例

在上述刑事判决书中,法院判处行为人所犯罪名为盗窃罪的案件为19件,罪名为非法获取计算机信息系统数据罪的案件为17件,罪名为非法获取计算机信息系统数据罪和盗窃罪的想象竞合犯的案件为1件,罪名为破坏计算机信息系统罪的案件为1件,其比例见图1。

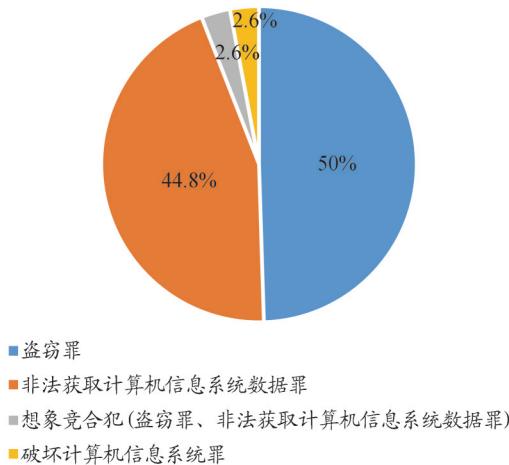


图1 罪名的比例分布

由此可知,我国法院对于盗窃数字货币行为以盗窃罪定性占一半比例,紧随其后的是非法获取计算机信息系统数据罪,想象竞合犯和破坏计算机信息系统罪仅属极为小众的定性结论。这说明:第一,我国法院对于盗窃数字货币行为定性的认知从传统、保守逐渐转为开放、灵活,对数字货币这

种虚拟商品是否属于盗窃罪的行为客体——财物不再持过度谨慎的态度,因而将盗窃数字货币行为定性为盗窃罪的结论在数量上已超越非法获取计算机信息系统数据罪。同时,二罪在定罪比例上的微弱差距说明盗窃数字货币案件在司法实践中呈现出严重的同案不同判现象<sup>[10]</sup>。第二,以想象竞合犯定性盗窃数字货币行为较为新颖而合理(合理性论证见下文),但该定性结论极低的比例不仅意味着我国法院应当充分重视盗窃数字货币行为的定性在刑法理论上的复杂性,还意味着我国刑法学界应加强对该问题的研究,以提出多样、合理的定性结论为司法实践工作者提供办案参考。第三,以破坏计算机信息系统罪定性盗窃数字货币行为在刑法理论上存在疑问(理由见下文),但该定性结论占比极低并不意味着我国法院对该问题在整体上存在定性上的缺陷。

### 三、盗窃数字货币行为的应然定性

盗窃数字货币行为在刑法理论上可否构成盗窃罪或非法获取计算机信息系统数据罪,二罪又属于何种犯罪竞合,应依次予以讨论。

#### (一) 盗窃罪可否成立的判断

对于盗窃数字货币行为可否构成盗窃罪,我国学界的争点主要集中在数字货币是否属于盗窃罪的行为客体——财物、盗窃数字货币是否侵害所有权、数字货币是否属于违禁品及其是否值得刑法保护3个方面。

##### 1. 数字货币的属性

数字货币是否属于财物首先涉及对数字货币的属性进行界定。对此,我国学界有货币说和非货币说两种观点。货币说可具体分为普通货币说、特殊货币说和虚拟货币说。普通货币说基于数字货币符合货币的五大特征:价值尺度、流通手段、贮藏手段、支付手段和世界货币,认为数字货币属于货币<sup>[11]</sup>。特殊货币说认为数字货币是互联网时代货币理念的革新,属于一种特殊的电子货币<sup>[12]</sup>。虚拟货币说认为数字货币是基于互联网和算法生成的、体现商业信用的新型货币<sup>[13]</sup>。非货币说分为虚拟资产说、支付手段说和虚拟商品说。虚拟资产说否认数字货币是货币,但承认其为虚拟的投机资产<sup>[14]</sup>。支付手段说认为应将数字货币界定为支付手段<sup>[15]</sup>。虚拟商品说来源于2013年《关于防范比特币风险的通知》(以下简称《通知》),其明确将比特币界定为虚拟商品,由此可推知我国有关部门将数字货币的属性界定为虚拟商品。

如果赞同货币说中的普通货币说,数字货币当然可以被界定为等同于人民币现金的财物,但这引发的疑问是:人民币现金具有实体,如何等同于虚拟的数字货币?普通货币说对此显然无法自圆其说。货币说中的特殊货币说和虚拟货币说虽然承认数字货币的虚拟性,但无法据此直接得出数字货币属于财物的结论,并且将引发“虚拟财产”是否属于财产这一问题,使判断过程更复杂。由此可见,货币说无法在法学上为数字货币是否属于财物提供直接、合理的判断标准。非货币说回避了从货币角度界定数字货币属性的路径,但其中的支付手段说认为数字货币属于行为方式而非财物,将导致盗窃数字货币行为一概不可罚的结论,同时未提供任何有说服力的理论根据;其中的虚拟资产说和虚拟商品说着眼于数字货币的虚拟性,同样无法直接回答数字货币是否属于财物的问题。上述理论的本质都是从经济学角度对数字货币的属性进行界定,未直接面对法学意义上数字货币是否属于财物这一问题,自然无法对该问题提供针对性的结论及理由。由此可见,要解决数字货币是否属于财物的问题,应当回避学界既定的研究路径,围绕数字货币的本质从法学角度进行论证。

从本质上讲,数字货币是一种作为财产性利益的数据,具备双重属性:既属于数据又属于财产性利益,这两个属性同时决定了数字货币属于财物。

一方面,数字货币系计算机通过算法产生,属于数据自无疑问,无法以其具有经济价值为理由否定其在技术层面上的数据属性,这导致数字货币具备不同于一般财物的虚拟性<sup>[16]</sup>,类似于游戏装备等虚拟财产<sup>[17]</sup>。对于虚拟财产是否属于财物,我国学界有肯定说、否定说和区分说之争<sup>[18]</sup>。肯定说值得赞同,数字货币虽然具备虚拟性,但仍属于财物,理由如下:第一,《刑法》第263条对盗窃罪的行为客体使用“财物”的用语是出于时代的局限,不应在当前将财物机械地解释为有体物。盗窃罪作为一种汉代就被刑法惩治的行为由来已久<sup>[19]</sup>,但近几十年来计算机技术的突飞猛进是人类有史以来从未有过的变局,由此产生的数据在属性上的定位及其保护问题,是立法者在制定1979年《刑法》和1997年《刑法》时始料未及的。在当时的立法背景下,行为人一般针对有体物实施盗窃行为,立法者据此使用明显具备有体物特征的财物一词。但在当前我国社会中,不仅数据可以成为财产性利益,而且盗窃数据的现象频繁发生,继续沿用当时立法者对财物充满时代局限性的理解,将其解释为有体物将导致数据无法得到刑法保护,显然无法解决新时代提出的新问题。第二,将数据解释为财物不违反罪刑法定原则。有学者认为将数据解释为财物属于类推解释从而违反罪刑法定原则<sup>[20]</sup>。诚然,不利于行为人的类推解释由于违反罪刑法定原则应当受到禁止<sup>[21]</sup>。但根据刑法通说,判断某种刑法解释是否属于类推解释的标准在于该刑法解释是否符合可能的语词含义<sup>[22]</sup>。正如移动支付已成为当前我国公民主要使用的支付方式,将移动支付所转移的债权解释为财物不会引发理解上的难题,计算机和网络同样在我国受到大规模运用,在我国公民的观念里,数据已悄然符合财物可能的语词含义。将数据解释为财物不会超越我国公民对财物的理解,由此不是类推解释而无违反罪刑法定原则之虞。第三,认为数字货币属于财物符合《通知》对数字货币属性界定的内在精神。《通知》通过将比特币界定为“虚拟商品”承认了数字货币内在的经济价值,而财物也具备经济价值,这意味着数字货币在本质上等同于财物。因此,认为数字货币属于财物非但不与我国有关部门的意思相悖,相反,二者一脉相承。

另一方面,数字货币属于可界定为财物的财产性利益,理由如下:第一,数字货币在本质上属于可以满足人类需要的经济利益,属于财产性利益。虽然从规范角度看,《通知》禁止特定机构从事有关数字货币的业务并禁止其作为货币流通使用,但从现实角度看,行为人通过数字货币购买产品、服务或转让数字货币以获利的现象时常发生,数字货币由此具备事实上的经济利益性,这意味着其成为类似于债权、知识产权的财产性利益。有学者通过将数字货币视为无记名的有价证券将其认定为财产性利益<sup>[23]</sup>。但即使不将数字货币认定为证券,仍然可以直接肯定其为财产性利益。第二,财产性利益可被解释为财物。从比较法的视角看,德国《刑法》第242条将盗窃罪的行为客体限定为“可移动的物”<sup>[24]</sup>,不包括电力等无体物<sup>[25]</sup>,数据由于没有形体、易被复制和远距离传输、欠缺单件性和固定位置也被排除在外<sup>[26]</sup>。我国台湾地区“刑法”也完全沿用此做法,将盗窃罪的行为客体限定于有体物<sup>[27]</sup>。但既然当前在我国社会中以债权替代现金的移动支付方式大行其道,并且数据具备经济利益性也是有目共睹的事实,将财物限制解释为有体物的传统理论显然无法照搬于我国刑法学中,否则将导致债权、数据等财产性利益完全无法受到刑法保护,从而导致他人受到财产损害,以及阻碍社会经济的有序运行。相反,可参考日本刑法学的做法,将财物界定为他人的物和财产性利益<sup>[28]</sup>,由此在我国刑法学中建立对财物的周延保护体系。对此,我国有法院在盗窃数字货币案件的

判决说理中支持该做法<sup>⑥</sup>。

## 2. 所有权被侵害与否

所有权涉及盗窃罪的法益。有学者以“数字货币并非有体物”为理由认为数字货币占有人对该数字货币不具有所有权，行为人实施的盗窃数字货币行为据此不构成盗窃罪<sup>[29]</sup>。该观点存在以下疑问。

第一，以法益的有无直接判断犯罪的成立与否将架空犯罪论体系在判断犯罪成立与否上的核心作用。以法益直接判断犯罪成立与否的观点来源于日本刑法学并深刻影响着我国刑法学界。在日本刑法学中，盗窃罪的法益有本权说、占有说、平稳占有说等多种理论<sup>[30]</sup>。本权说认为盗窃罪的法益是所有权和抵押权、质权等其他本权<sup>[31]</sup>。如果行为人实施的盗窃行为没有侵犯所有权，该盗窃行为则不构成盗窃罪。该观点正是沿袭了本权说的论证方式，才得出盗窃数字货币行为不构成盗窃罪的结论。但根据刑法学通说，行为人的行为是否构成某种犯罪的必要充分条件是该行为能否通过该罪犯罪论体系的检验，如果能通过，该行为则构成该罪<sup>[32]</sup>。而犯罪论体系的第一个阶层是构成要件，其中的构成要件要素属于判断犯罪成立与否的核心<sup>[33]</sup>。刑法诚然有保护法益的任务<sup>[34]</sup>，但法益本身无法替代构成要件要素来判断行为人的行为是否构成犯罪，否则将导致犯罪论体系本有的功能遭到破坏，还导致法益将承载本不该有的功能，以致混淆刑法的逻辑和理论体系。

第二，属于“倒果为因”的论证方式。即使以“数字货币并非有体物”否定盗窃数字货币行为构成盗窃罪，也不应遵循从构成要件要素推导出法益，再从法益推导出犯罪成立与否的逻辑思路，相反，应当颠倒上述顺序，先根据法益推导出构成要件要素，再根据构成要件要素推导出犯罪成立与否。简言之，应以法益为“因”、构成要件要素为“果”。这是因为，法益有解释构成要件要素的功能<sup>[35]</sup>，而构成要件要素没有反向推导法益的功能。

第三，不符合当前我国社会中推广数据运用的需求。该观点的逻辑前提是，所有权的对象只能是有体物，这是传统民法学的观点<sup>[36]</sup>，肇始于1896年德国《民法典》第90条的立法例。但德国立法者之所以将所有权的对象限定为有体物，是因为在当时知识产权勃兴的时代背景中，为了在社会上促进知识产权的运用，只能将知识产权从所有权的对象中驱离，防止过度保护知识产权而阻碍其在社会上的充分运用<sup>[37]</sup>。但早在2007年我国《物权法》出台以前，我国已有学者呼吁将网络环境产生的虚拟物纳入所有权的对象<sup>[38]</sup>。相比2007年，当前我国社会的网络化和信息化程度不可同日而语，无体物的对象事实上早已突破知识产权的局限而纳入了数据，数据的广泛运用和财产化成为既定事实，对数据提供刑法保护亦是迫在眉睫。正如德国学者戈拉所言：“在21世纪，数据如同石油一样宝贵。保护数据犹如保护环境一样重要。”<sup>[39]</sup>在此新时代背景下，如果恪守19世纪末德国《民法典》创立的旧理论，以数字货币是无体物为理由将其排除在所有权的对象以外，从而得出盗窃数字货币行为一概无罪的结论，显然不利于推广数据在我国社会中的运用。相反，应采取与当时德国立法者相反的做法，在理论上使数据这种无体物回归到所有权的对象中，以对数据的刑法保护来实现对其运用的推广。

由此可见，从法益角度直接定性盗窃数字货币行为非但没有必要，反而将衍生更多的问题。一个较为合理的论证路径是，为了满足当前我国社会中保护数据运用的需求，应将数字货币这种无体

<sup>⑥</sup> 河南省平顶山市中级人民法院(2021)豫04刑终483号刑事判决书。

物纳入所有权的对象,盗窃罪的行为客体——财物则必然包含数字货币,这就无法得出行为人实施的盗窃数字货币行为不构成盗窃罪的结论。

### 3. 违禁品及其刑法保护性

违禁品及其刑法保护性涉及两个问题:(1)数字货币是否属于违禁品?这是事实判断问题。(2)违禁品是否值得刑法保护而成为盗窃罪的行为客体——财物?这是规范判断问题。

关于数字货币是否属于违禁品,应先考察我国有关部门依次出台的5个规范性文件:《通知》《关于防范代币发行融资风险的公告》(以下简称2017年《公告》)、《关于防范虚拟货币交易炒作风险的公告》(以下简称2021年《公告》)、《关于进一步防范和处置虚拟货币交易炒作风险的通知》(以下简称2021年《通知》)、《关于加强数字货币监管的通知》(以下简称2023年《通知》)。《通知》对数字货币的关键性限制体现为:禁止金融机构和支付机构从事关于比特币的营利性业务。2017年《公告》对数字货币的关键性限制体现为:禁止融资主体向投资者筹集数字货币、禁止代币融资交易平台提供关于数字货币的营利性业务。2021年《公告》除了重复强调上述文件的内容,还设定了以下限制:其一,禁止互联网平台企业会员单位从事关于数字货币的营利性业务。其二,禁止任何机构和个人从事关于数字货币的营利性业务。其三,禁止消费者从事数字货币账户的充值和提现、购买和出售充值码、划转资金等活动。可见,上述规范性文件对数字货币的禁止力度不断增强,在2021年《公告》中达到巅峰,表现为:其一,将数字货币的范围从比特币扩展到所有种类的数字货币。其二,被禁止实施特定行为的主体从金融机构等扩展到我国所有的机构和个人。其三,被禁止实施的行为从筹集数字货币等扩展到所有的营利和流通行为。2021年《通知》除了重复前述规定的内容以外,将特定境外虚拟货币交易所纳入实施特定行为的主体。2023年《通知》除了首次采用数字货币这一提法以外,增加了加强对数字货币交易平台监管力度等内容。

但这仍然无法说明数字货币达到了诸如毒品、枪支等违禁品的限制程度,相反,数字货币并非标准意义上的违禁品,属于一种限定违禁品,理由如下:第一,并非所有关于数字货币的行为都受到禁止,制造数字货币的“挖矿”行为和持有数字货币的行为未被禁止。这低于制造毒品行为构成犯罪的限制力度,也低于非法持有枪支行为构成犯罪的限制力度。第二,法律渊源的层级较低。限制数字货币的5个规范性文件在法律渊源上均属于“其他规范性文件”,而限制枪支这一违禁品的规范性文件系我国《治安管理处罚法》,其在法律渊源的种类上属于法律。很明显,限制数字货币的法律渊源层级较低。第三,规范制定机关的层级较低。限制毒品这一违禁品的规范性文件系《刑法》,其制定机关是全国人民代表大会,但限制数字货币的规范性文件的制定机构为中国互联网金融协会等自律组织,就规范制定机构的层级而言,显然后者低于前者。当然,可以建立一种动态性的界定机制,如果将来我国出台法律,将含制造和持有在内的所有关于数字货币的行为都予以禁止,使数字货币达到毒品等违禁品的限制程度,数字货币将变成违禁品。

数字货币是否值得刑法保护而成为财物,直接关系到盗窃数字行为可否构成盗窃罪。首先应讨论的是违禁品是否值得刑法保护。对此,有肯定说和否定说之争。肯定说提出:“非法财物可能具有重大价值,体现重大法益,值得刑法予以保护。”<sup>[40]</sup>该说存在的问题是,将违反法秩序一致性原则<sup>[41]</sup>。如果肯定违禁品值得刑法保护,将导致否定违禁品合法性的法律规范与刑法产生冲突,造成法秩序发生内在矛盾,这是肯定说无法逻辑自洽的。否定说认为财物必须具备合法性,违禁品因而不值得刑法保护<sup>[42]</sup>。该说维护了法秩序一致性原则,但无法解决以下问题:如果据此不处罚盗窃违

禁品行为，社会秩序将遭受严重的违反。正因为肯定说和否定说都不具备相对彻底的合理性，导致学界对该问题争论不休。

具体到数字货币而言，亦有处罚说和不处罚说之争。处罚说认为数字货币属于违禁品从而不属于我国刑法保护的财物，但为了维护社会秩序，仍应将盗窃数字货币行为认定为盗窃罪<sup>[43]</sup>。该说不仅违反法秩序统一原则，还有以下问题：第一，事实认定有误。前文已述，数字货币属于限定违禁品而非标准意义上的违禁品。第二，架空了犯罪论体系在判断犯罪成立与否上的核心作用。既然数字货币并非财物，盗窃数字货币行为在构成要件上便无法既遂，这导致犯罪论体系的阶层性受到破坏。第三，违反了法益保护原则。入罪时完全以秩序来替代构成要件要素的适用，造成刑法保护的是秩序而非构成要件要素背后的法益，以致法益保护原则被违反。不处罚说认为，数字货币由于在我国受到规范性文件的限制而不是财物，盗窃数字货币行为不构成盗窃罪<sup>[44]</sup>。该说和处罚说一样，都误将数字货币认定为违禁品，还无法满足司法实践中对秩序维护的要求，皆不可取。

对此，一种较为合理而可行的处理方案是限定处罚说，其将数字货币认定为刑法限定保护的财物，盗窃数字货币行为可构成盗窃罪，但应对行为人从宽处罚，理由如下：第一，应采取与数字货币的限定违禁品定位相匹配的处罚力度。不加限定地处罚盗窃数字货币行为是将数字货币置于违禁品地位，完全不处罚盗窃数字货币行为是将数字货币置于合法地位，都不符合数字货币属于限定违禁品的定位。第二，与刑法基本理论不冲突。限定处罚盗窃数字货币行为不仅通过对该行为的否定维护了法秩序统一原则，还通过对财物这一构成要件要素的适用维护了犯罪论体系在判断犯罪成立与否上的核心作用，并且不以秩序来替代构成要件要素从而间接维护了法益保护原则。第三，回应了司法实践中对秩序维护的要求。秩序维护的要求必然禁止行为人针对任何财物（含数字货币）实施盗窃行为，盗窃数字货币行为构成盗窃罪的处理方案蕴含着禁止盗窃数字货币这一规范要求，从而维护了财产秩序和社会秩序。第四，凸显了对数字货币的有限保护性。数字货币既然属于限定违禁品，对盗窃数字货币行为的行为人从宽处罚从反面角度起到了警示作用——刑法对数字货币的保护是有限的，这与既定规范性文件在立法态度上是一致的，有助于限制数字货币在市场上的流通。

综上所述，盗窃数字货币行为可构成盗窃罪。但值得注意的是，盗窃罪是数额犯，其成立须具备数额较大这一客观处罚条件<sup>[45]</sup>。审查盗窃数字货币行为是否构成该罪时，被盗数字货币的价值必须经鉴定达到数额较大的要求，应根据全国各省、自治区、直辖市的具体数额标准进行判断。

## （二）非法获取计算机信息系统数据罪可否成立的判断

非法获取计算机信息系统数据罪是1997年《刑法》为了应对当时社会上新出现的计算机犯罪现象而设立的新罪名<sup>[46]</sup>。我国台湾地区“刑法”中有类似罪名为“非法取得电磁记录罪”，同样将盗窃数据的行为入罪<sup>[47]</sup>。德国《刑法》第202a条规定了非法获取数据罪，其构成要件为：未经同意获取他人的数据或者为了防止被他人非法获取而进行了特殊安全处理的数据<sup>[48]</sup>。根据德国刑法通说，该罪的行为客体不局限于计算机信息系统数据，而与一般意义上的信息同义<sup>[49]</sup>，保护法益为数据持有人对该数据形式上的处分权<sup>[50]</sup>。由此可见，该罪的设立并非我国独创，设立该罪在当前全球信息时代具备普适性和必要性。

对于盗窃数字货币行为可否构成该罪有肯定说和否定说之争。肯定说以数字货币的法律属性是计算机信息系统数据为理由，认为盗窃数字货币行为构成该罪<sup>[51]</sup>。但否定说认为，由于非法获取

计算机信息系统数据罪的法益是计算机信息系统的安全,属于社会法益,而盗窃数字货币行为侵犯的是个人法益,这种区别决定了盗窃数字货币行为不构成该罪<sup>[52]</sup>。

对比上述二说可知,肯定说通过将数字货币认定为计算机信息系统数据,从而将盗窃数字货币行为认定为该罪,维护了构成要件要素在判断犯罪成立与否上的核心作用,在方法论上值得肯定。因此,问题的核心在于数字货币是否为计算机信息系统数据。前文已述,数字货币属于作为财产性利益的数据,并且该数据并非抽象意义上的信息,而是一种严重依赖于计算机的数据,其制造、持有、转移和消除均依赖于在计算机上的操作,无法脱离计算机而单独存在。因此,将数字货币认定为计算机信息系统数据自无疑问,盗窃数字货币行为自然可构成该罪。而否定说的问题在于,不仅回避承认数字货币属于计算机信息系统数据这一事实,还以法益替代构成要件要素的适用,导致犯罪论体系在判断犯罪成立与否上的核心作用遭到破坏,此外,认为非法获取计算机信息系统数据罪只能是社会法益,盗窃数字货币行为只能侵害个人法益,这种观点亦不符合事实,因为盗窃数字货币行为既侵害了数字货币占有人的财产法益,还可能侵害计算机信息系统的安全,二者并不冲突。

综上所述,肯定说较为合理,行为人的盗窃数字货币行为可构成非法获取计算机信息系统数据罪。但值得注意的是,该罪的成立有情节严重这一客观处罚条件<sup>[53]</sup>。审查盗窃数字货币行为是否成立该罪时,必须满足情节严重的要求,具体认定标准为最高人民法院、最高人民检察院制定的《关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》第1条。

### (三)犯罪竞合的判断

通过上述论证可知,盗窃数字货币行为可同时构成盗窃罪和非法获取计算机信息系统数据罪,但二罪存在何种犯罪竞合关系直接影响对行为人的量刑,因而值得进一步讨论。对此,我国学界有法条竞合的特别关系说、牵连犯说和想象竞合犯说3种观点。

法条竞合的特别关系说认为:盗窃罪属于一般法条,非法获取计算机信息系统数据罪属于特别法条,二者属于法条竞合中的特别关系,根据特别法条优先于一般法条的适用规则,盗窃数字货币行为应被认定为非法获取计算机信息系统数据罪<sup>[54]</sup>。但该说与刑法通说相悖。刑法通说将特别关系界定为:如果一个法条的构成要件包含另一个法条中构成要件的所有要素,同时至少还有一个后者不具备的特别要素,则前者属于特别法条,后者属于一般法条<sup>[55]</sup>。可见,特别关系的本质是逻辑上的包容关系<sup>[56]</sup>。但非法获取计算机信息系统数据罪的构成要件显然不完全包含盗窃罪的所有要素。具体而言,虽然非法获取计算机信息系统数据罪的实行行为——非法获取行为包含盗窃罪的实行行为——盗窃行为<sup>[57]</sup>,但前罪并不包含后罪构成要件中独有的非法占有目的要素,也不包含后罪构成要件中的财物要素,相反,财物包含了计算机信息系统数据。因此,非法获取计算机信息系统数据罪并非盗窃罪的特别法条,二罪之间并非法条竞合的特别关系。此外,如果赞同该说,将导致对行为人量刑失衡,无法充分保护数字货币占有人的财产法益。具体而言,如果将盗窃数字货币行为认定为非法获取计算机信息系统数据罪,无论行为人盗窃的数字货币价值多少,受该罪法定刑的限制,行为人最高只能被判处3~7年有期徒刑。但从前文中对相关刑事判决书的实证考察结论可知,达到盗窃罪数额巨大和特别巨大标准的案件占盗窃数字货币案件的绝大多数。如果定盗窃罪,行为人将被判3~10年有期徒刑、10年有期徒刑或无期徒刑,这就通过与犯罪所得数额相匹配的宽广的量刑幅度,恰当地保护了数字货币占有人的财产法益,但如果定非法获取计算机信息系统数据罪,对行为人所适用的3~7年有期徒刑这一量刑幅度显然无法充分保护数字货币占有人的财

产法益。

牵连犯说认为：侵入他人计算机信息系统获取数据仅是手段行为，目的行为是非法获取他人持有的数字货币。根据牵连犯的处断规则，应将行为人的行为定为盗窃罪<sup>[58]</sup>。但问题在于：一方面，该说并未解决非法获取计算机信息系统数据罪与盗窃罪之间的犯罪竞合关系。行为人实施非法侵入计算机信息系统行为后实施的盗窃数字货币行为既属于非法获取计算机信息系统数据行为，又属于盗窃行为，二者之间的犯罪竞合关系并未得到解决，该说仅解决了非法侵入计算机信息系统罪与盗窃罪的关系；另一方面，牵连犯说本身存在固有和现实弊端而不可取。该说并非源自德国刑法学<sup>[59]</sup>，是日本刑法学的独有理论<sup>[60]</sup>，并被我国刑法学沿用<sup>[61]</sup>。该说的立论根据是复数行为之间手段与目的的关系<sup>[62]</sup>。但手段与目的的关系既无法降低复数行为的不法内涵，也无法降低行为人的罪责程度，对行为人从一重罪处断的规则还可能导致被侵害的复数法益无法受到充分保护。这是该说的固有弊端，其现实弊端为：在盗窃数字货币的场合，手段行为侵害的是计算机相关法益，当前我国社会中计算机在各个领域被广泛运用，其重大性和应保护性不言而喻，运用该说的结果是非法侵入计算机信息系统行为无法得到评价，显然不满足我国当前充分保护计算机安全、平稳运行的现实需求。

想象竞合犯说认为盗窃数字货币行为同时侵害了盗窃罪和非法获取计算机信息系统数据罪的法益，二罪属于想象竞合犯。该说较为合理，但论证思路需要调整。盗窃数字货币行为之所以属于二罪的想象竞合犯，并非由于侵害了二罪的法益，而是因为符合二罪的构成要件。想象竞合犯是指，行为人故意实施了一个实行行为（亦即行为单数），符合复数构成要件的情形<sup>[63]</sup>。想象竞合犯在犯罪竞合中的体系性定位属于真正竞合，系指行为人的行为真正触犯复数罪名，这与法条竞合中行为人的行为仅在形式上（假性）触犯复数罪名存在本质区别<sup>[64]</sup>。因此，想象竞合犯具备法条竞合所欠缺的“厘清功能”（Klarstellungsfunction）<sup>[65]</sup>，即法官在判决书中必须将行为人所犯复数罪名逐一列明，以此表明对复数法益的充分保护。但犯罪竞合的功能是对行为人的行为进行适当（充分且不过度）的评价<sup>[66]</sup>，由于行为人仅实施了一个实行行为，应遵循禁止双重评价原则<sup>[67]</sup>，对行为人适用从一重罪处罚而非数罪并罚的规则，以起到防止过度处罚行为人的效果。

行为人实施的盗窃数字货币行为显然是一个实行行为，如果该行为同时符合非法获取计算机信息系统罪和盗窃罪的构成要件，则构成二罪的想象竞合犯，应从一重罪——盗窃罪处罚。此外，从实质角度看，采取想象竞合犯说可充分保护数字货币承载的法益：财产法益和信息自决权。这是由数字货币作为财产性利益的数据这一双重属性决定的。值得注意的是，司法实践中已出现以下特殊情况：行为人的盗窃数字货币行为可能同时构成盗窃罪、非法获取计算机信息系统数据罪、破坏计算机信息系统罪的想象竞合犯。比如，行为人在他人的计算机中增加数据（如上海吴某某破坏计算机信息系统案）<sup>⑦</sup>，起到虚假充值的作用并由此自动获取他人的数字货币。此时，增加数据行为必然导致数字货币占有的转移，这意味着增加数据行为等同于盗窃数字货币行为，应根据想象竞合犯说将行为人的行为认定为盗窃罪。

将盗窃数字货币行为根据想象竞合犯说最终认定为盗窃罪后，根据个案中情形的不同，行为人的行为可能同时构成非法侵入计算机信息系统罪、非法控制计算机信息系统罪。比如，行为人先在

<sup>⑦</sup> 上海市奉贤区人民法院（2019）沪0120刑初435号刑事判决书。

他人的计算机中设置病毒程序,或实施远程操作侵入甚至控制他人的计算机(如河南张某某非法控制计算机信息系统数据案)<sup>⑧</sup>,再单独实施了盗窃数字货币行为。由于上述分别被实施的行为属于行为复数,显然不符合想象竞合犯中行为单数的要求,无法从想象竞合犯的角度来处理。但前文已述,以牵连犯说认定上述行为之间的关系,将行为人所实施的所有行为认定为盗窃罪,显然无法保护计算机相关法益,以致无法满足我国当前充分保护计算机安全、平稳运行的现实需要。因此,应回到实质竞合的理论立场<sup>[68]</sup>,将行为人实施的上述行为认定为盗窃罪、非法侵入计算机信息系统罪、非法控制计算机信息系统罪,将这三罪进行数罪并罚,通过对行为人判处更重的刑罚来保护计算机相关法益。

综上所述,在司法实践中,处理盗窃数字货币案件时可采取以下5个步骤:第一,排除假性盗窃数字货币案件。如果行为人实施的是针对“矿机”和电力的盗窃行为,以及利用自己和他人的计算机制造数字货币的“挖矿”行为,这类案件并非真正的盗窃数字货币案件,对前者情形应回到盗窃普通财物的轨道进行处理,对后者情形应判断非法侵入计算机信息系统罪和非法控制计算机信息系统罪是否成立。第二,分别审查盗窃数字货币行为是否构成盗窃罪和非法获取计算机信息系统数据罪,审查的重点是该行为是否满足盗窃罪中数额较大的要求和非法获取计算机信息系统数据罪中情节恶劣的要求。如果行为人的行为不满足数额较大的要求但满足情节恶劣的要求,则构成非法获取计算机信息系统数据罪。如果行为人的行为不满足情节恶劣的要求但满足数额较大的要求,则构成盗窃罪。如果上述要求均不满足,行为人的行为不构成二罪。第三,如果行为人盗窃数字货币行为同时构成盗窃罪和非法获取计算机信息系统数据罪,二罪的关系为想象竞合犯,该行为应被认定为盗窃罪。第四,审查行为人除了实施盗窃数字货币行为,是否还伴随、独立地实施了非法侵入计算机信息系统行为和非法控制计算机信息系统行为,如果实施了上述行为,应将行为人的整体行为认定为盗窃罪、非法侵入计算机信息系统罪、非法控制计算机信息系统罪并进行数罪并罚。第五,如果行为人的行为构成盗窃罪一罪或含盗窃罪的数罪,应考虑数字货币属于限定违禁品,量刑时应对行为人从宽处罚。

## 结论

盗窃数字货币行为的定性在我国法院的审判实践中呈现严重不同的现象,这衍生出对该问题在刑法理论上进行深入研究的必要性。通过考察我国法院作出的关于盗窃数字货币案件的刑事判决书,可发现我国盗窃数字货币案件所具备的诸多特点,以及法院所判罪名在种类和比例上的现状,并由此得出许多对司法实践有用的启示。数字货币在属性上是一种作为财产性利益的数据。应将数字货币这种无体物纳入所有权的对象,盗窃罪的行为客体——财物则必然包含数字货币。数字货币属于限定违禁品,如果盗窃数字货币行为构成盗窃罪,应对行为人从宽处罚。如果行为人的盗窃数字货币行为同时构成盗窃罪和非法获取计算机信息系统数据罪,二罪的关系为想象竞合犯,该行为应被认定为盗窃罪。如果行为人除了实施盗窃数字货币行为,还伴随、独立地实施了非法侵入计算机信息系统行为和非法控制计算机信息系统行为,应将行为人的整体行为认定为盗窃罪、非法侵入计算机信息系统罪、非法控制计算机信息系统罪并进行数罪并罚。以此方式,可在

<sup>⑧</sup> 河南省南阳市卧龙区人民法院(2018)豫1303刑初364号刑事判决书。

国未来的司法实践中，在不违反刑法基本原理的前提下，通过对行为人恰当地定罪量刑来合理地处理盗窃数字货币案件，并全面保护数字货币所代表的财产法益、信息自决权和计算机相关法益，有效应对数字时代提出的刑法挑战。

#### 参考文献：

- [1] 高卫民. 对新型货币比特币的观察与瞻望[J]. 对外经贸实务, 2013(10): 17-20.
- [2] 谢杰. 区块链技术背景下金融刑法的风险与应对：以比特币交易对外汇犯罪刑法规制的冲击为视角[J]. 人民检察, 2017(8): 63-65.
- [3] 盛松成, 张璇. 虚拟货币本质上不是货币：以比特币为例[J]. 中国金融, 2014(1): 35-37.
- [4] 夏建邦. 比特币的“罪与罚”：对比特币等虚拟资产须设置监管底线[J]. 银行家, 2017(4): 131-132.
- [5] 廖晓琼, 赵华伟, 苏志伟, 等. 数字货币币值的动态特征分析：以比特币、以太币和瑞波币为例[J]. 2021(2): 11-18.
- [6] 袁秋梅. 比特币究竟是不是货币：基于货币与财富关系的探析[J]. 南方金融, 2018(6): 28-32.
- [7] JOHANNES W, THOMAS H. Strafrecht Besonderer Teil[M]. Heidelberg: C. F. Müller, 2016: 92.
- [8] 李立丰, 张鑫蕾. 盗窃法定数字货币行为的刑法认定[J]. 武汉大学学报(哲学社会科学版), 2024(3): 29-39.
- [9] 汤睿阳. 大数据背景下数字货币犯罪治理对策研究[J]. 网络安全技术与应用, 2025(1): 140-142.
- [10] 叶良芳. 数据抑或财物：以虚拟货币为犯罪对象的案件之定性分析[J]. 中国应用法学, 2023(3): 65-73.
- [11] 曲磊, 郭宏波. 比特币等虚拟货币金融犯罪风险前瞻[J]. 经济研究参考, 2014(68): 60-63, 72.
- [12] 姜立文, 胡玥. 比特币对传统货币理念的挑战[J]. 南方金融, 2013(10): 31-35, 92.
- [13] 戴飞. 论比特币的法律问题：以Faiella案为视角[J]. 武汉金融, 2020(10): 81-84.
- [14] 李翀. 比特币会成为货币吗？[J]. 当代经济研究, 2015(4): 60-65, 2, 97.
- [15] 樊云慧, 栗耀鑫. 以比特币为例探讨数字货币的法律监管[J]. 法律适用, 2014(7): 48-52.
- [16] 刘宪权, 肖宸彰. 非法获取加密数字货币行为的刑法规制[J/OL]. 河南财经政法大学学报, 1-13 [2025-05-14]. <http://kns.cnki.net/kcms/detail/41.1420.Z.20250408.1421.016.html>.
- [17] 宋路明. 非法获取虚拟货币行为之刑法定性：基于“权利束”理论的展开[J]. 河南财经政法大学学报, 2024(5): 58-68.
- [18] 李佩遥. 侵犯网络虚拟财产行为之定性研究：以73份判决书为样本的分析[J]. 大连理工大学学报(社会科学版), 2020(4): 84-91.
- [19] 全国人大常委会法制工作委员会刑法室. 中华人民共和国刑法条文说明、立法理由及相关规定[M]. 北京：北京大学出版社, 2009: 549.
- [20] 欧阳本祺. 论虚拟财产的刑法保护[J]. 政治与法律, 2019(9): 39-54.
- [21] HANS W. Das Deutsche Strafrecht[M]. Berlin: Walter De Gruyter, 1969: 19.
- [22] CLAUS R. Strafrecht Allgemeiner Teil[M]. München: Verlag C. H. Beck, 2006: 149.
- [23] 王熠珏.“区块链+”时代比特币侵权犯罪研究[J]. 东方法学, 2019(3): 149-160.
- [24] WOLFGANG M. Strafrecht Besonderer Teil[M]. Berlin: Springer, 2015: 5.
- [25] URS K. Strafrecht Besondere Teil[M]. Baden-Baden: Nomos, 2015: 38.
- [26] TOBIAS S. Ausufernd und fehlplatziert: Der Tatbestand der Datenhehlerei (§ 202d StGB) im System des strafrechtlichen Daten-und Informationsschutzes[J]. Zeitschrift für Internationale Strafrechtsdogmatik, 2016, 7: 433-439.
- [27] 卢映洁. 刑法分则新论[M]. 10版. 台北：新学林出版股份有限公司, 2015: 631.
- [28] 前田雅英. 日本刑法各论[M]. 董藩舆,译. 台北：五南图书出版股份有限公司, 2000: 147.
- [29] 赵天书. 比特币法律属性探析：从广义货币法的角度[J]. 中国政法大学学报, 2017(5): 77-88, 159.
- [30] 大谷实. 刑法讲义各论[M]. 黎宏,译. 北京：中国人民大学出版社, 2008: 309.
- [31] 大塚仁. 刑法概说(各论)[M]. 冯军,译. 北京：中国人民大学出版社, 2003: 182.
- [32] REINHART M, HEINZ Z. Strafrecht Allgemeiner Teil[M]. Heidelberg: C. F. Müller, 1992: 181.

- [33] EDMUND M. Strafrecht[M]. Berlin: Verlag von Duncker & Humblot, 1949: 89.
- [34] HANS-HEINRICH J, THOMAS W. Lehrbuch des Strafrechts Allgemeiner Teil [M]. Berlin: Duncker & Humblot, 1996: 7.
- [35] 王皇玉. 刑法总则[M]. 3版. 台北: 新学林出版股份有限公司, 2017: 23.
- [36] 王利明, 杨立新, 王轶, 等. 民法学[M]. 北京: 法律出版社, 2005: 259.
- [37] 克尼佩尔. 法律与历史[M]. 北京: 法律出版社, 2003: 251.
- [38] 杨建斌. 论无体物权与知识产权的关系[J]. 求是学刊, 2006(6): 73-76.
- [39] SEBASTIAN G. Papiertiger gegen Datenkraken: Zum Schutz der informationellen Selbstbestimmung durch das Strafrecht [J]. Zeitschrift für Internationale Strafrechtsdogmatik, 2016, 3: 192-198.
- [40] 盛豪杰, 行江. 类型化认定: 窃取比特币行为的刑法适用[J]. 西北民族大学学报(哲学社会科学版), 2021(2): 106-113.
- [41] BERND R. Rechtstheorie[M]. München: Verlag C. H. Beck, 2002: 320.
- [42] 黄祥青. 谈定罪中的犯罪对象梳理方法[J]. 人民司法, 2012(3): 26-30.
- [43] 郭旨龙. 侵犯虚拟货币刑法定性的三层秩序观: 从司法秩序、法秩序到数字经济秩序[J]. 政治与法律, 2023(5): 49-68.
- [44] 储陈城, 马世理. 比特币的刑法保护方式: 从教义学到国家政策的分析[J]. 重庆大学学报(社会科学版), 2022(5): 235-248.
- [45] 陈兴良. 规范刑法学[M]. 3版. 北京: 中国人民大学出版社, 2013: 840.
- [46] 高铭暄. 中华人民共和国刑法的孕育诞生和发展完善[M]. 北京: 北京大学出版社, 2012: 513.
- [47] 林山田. 刑法各罪论-上册: 修订五版[M]. 北京: 北京大学出版社, 2012: 392.
- [48] URS K. Strafgesetzbuch Lehr-und Praxiskommentar[M]. Baden-Baden: Nomos, 2010: 723.
- [49] THOMAS F. Strafgesetzbuch[M]. München: Verlag C. H. BECK, 2018: 1400.
- [50] ADOLF S, Horst S. Strafgesetzbuch Kommentar[M]. München: C. H. BECK, 2014: 1943.
- [51] 胡云腾, 周加海, 周海洋. 《关于办理盗窃刑事案件适用法律若干问题的解释》的理解与适用[J]. 人民司法, 2014(15): 18-25.
- [52] 王卫, 南庆贺. 论盗窃比特币的行为性质[J]. 西部法学评论, 2018(5): 83-90.
- [53] 周光权. 刑法各论[M]. 2版. 北京: 中国人民大学出版社, 2011: 311.
- [54] 任彦君. 网络中财产性利益的刑法保护模式探析[J]. 法商研究, 2017(5): 112-120.
- [55] REINHART M, KARL G, HEINZ Z. Strafrecht Allgemeiner Teil[M]. Heidelberg: C. F. Müller, 2014: 659.
- [56] JÜRGEN B, ULRICH W, WOLFGANG M, et al. Strafrecht Allgemeiner Teil Lehrbuch[M]. Bielefeld: Verlag Ernst und Werner Giesecking, 2016: 866.
- [57] 周铭川. 盗窃比特币行为的定性分析[J]. 南通大学学报(社会科学版), 2020(3): 103-109.
- [58] 张明楷. 刑法学[M]. 5版. 北京: 法律出版社, 2016: 1047.
- [59] 柯耀程. 刑法竞合论[M]. 北京: 中国人民大学出版社, 2008: 195.
- [60] 黎宏. 日本刑法精义[M]. 2版. 北京: 法律出版社, 2008: 316.
- [61] 高铭暄, 马克昌. 刑法学[M]. 5版. 北京: 北京大学出版社, 高等教育出版社, 2013: 194.
- [62] 松宫孝明. 刑法总论讲义[M]. 钱叶六, 译. 北京: 中国人民大学出版社, 2013: 250.
- [63] HELMUT F. Strafrecht Allgemeiner Teil[M]. München: Verlag C. H. Beck, 2015: 465.
- [64] KRISTIAN K. Strafrecht Allgemeiner Teil[M]. München: Vahlen, 2017: 905.
- [65] CLAUS R. Strafrecht Allgemeiner Teil[M]. München: Verlag C. H. Beck, 2003: 831.
- [66] 林书楷. 刑法总则[M]. 4版. 台北: 五南图书出版股份有限公司, 2018.
- [67] INGEBORG P. Strafrecht Allgemeiner Teil[M]. Baden-Baden: Nomos, 2016: 391.
- [68] GEORG F. Strafrecht Allgemeiner Teil[M]. Berlin: Springer, 2009: 450.

# The scrutinize about criminal law of stealing digital currency in the perspective of blockchain: Empirical interpretation and logical orientation Based on the investigation of 38 Chinese criminal judicial verdicts from 2014 to 2024

WANG Dezheng

(Law School, Southwest Petroleum University, Chengdu 610500, P. R. China)

**Abstract:** By investigating the criminal judgments about the cases of stealing digital currency made by Chinese courts, not only can be found that the characteristics of the cases of stealing digital currency in China and many useful revelations for the judicial practice, can also be found that the proportion that Chinese courts consider the conduct of stealing digital currency as the crime of stealing is a half, the followed is the crime of illegally obtaining data of computer information system. Imaginative joinder of offences and the crime of destroying computer information system are very rare conclusions. The phenomenon that the conclusions of judging the conduct of stealing digital currency are very different with each other in the trial practice of Chinese courts results in the necessity of in-depth research on this issue in the theory of criminal law. Digital currency as a property benefit is a kind of data. Digital currency as incorporeal things should be included as the object of ownership. The conduct object of the crime of stealing “property” consequently includes digital currency. Digital currency is a restricted contraband. If the conduct of stealing of digital currency constitutes the crime of stealing or several crimes including this crime, the conductor should be given a lenient punishment. In judicial practice, we should firstly exclude pseudo cases of stealing digital currency. If the conductor implemented the conduct of “mining machines” and electricity, as well as the conduct of “mining” through using his or others’ computers to create digital currency, such cases are not real cases of digital currency, and the former case should be returned to the track of stealing ordinary property. In the latter case, we should judge whether the crime of illegally invading into computer information system and the crime of illegally controlling computer information system are established. Then we should examine whether the conduct of stealing digital currency constitutes the crime of stealing and the crime of illegally obtaining computer information system data. The focus of the examination is whether the conduct of conductor meets the requirement of large amount in the crime of stealing and bad circumstances in the crime of illegally obtaining computer information system data. If the conduct of conductor does not meet the requirement of large amount but meet the requirement of bad circumstances, it constitutes the crime of illegally obtaining computer information system data. If the conduct of the conductor does not meet the requirement of bad circumstances but meet the requirement of large amount, it constitutes the crime of stealing. If the above requirements are not met, the conduct of the conductor does not constitute the two crimes. If the conduct of stealing digital currency of the conductor constitutes the crime of stealing and the crime of illegally obtaining computer information system data at the same time, the relationship between the two crimes is imaginative joinder of offences, and his conduct should be judged as the crime of stealing. In addition, we should also examine whether the conductor concomitantly and independently implemented the conduct of illegally invading into computer information system and the conduct of illegally controlling computer information system beside the conduct of stealing digital currency, if the above conducts are implemented, the whole conducts of the conductor should be considered as the crime of stealing, the crime of illegally invading into computer information system and the crime of illegally controlling computer information system, and the conductor should be given concurrent punishment for these several crimes.

**Key words:** blockchain; digital currency; bitcoin; crime of stealing; crime of illegally obtaining computer information system data

(责任编辑 刘 琦)