Advances in Social Sciences 社会科学前沿, 2023, 12(12), 7080-7086
Published Online December 2023 in Hans. https://www.hanspub.org/journal/ass
https://doi.org/10.12677/ass.2023.1212966

Hans汉斯

区块链技术语境下智能合约犯罪的国际刑法回应

宋佳佳

北京师范大学法学院，北京

收稿日期：2023年7月11日；录用日期：2023年12月5日；发布日期：2023年12月13日

摘　要

区块链作为一种广泛应用的新技术，是智能合约由1.0版本向2.0版本迭代的关键，更是为智能合约解决了数据来源和信任机制两大难题，使得智能合约在社会中广泛运行开来。而新技术的广泛应用与扩张迭代的过程必然会诱发社会行为的形变，进而产生治理的困境和犯罪的风险。本文旨在深入剖析区块链环境下智能合约犯罪产生的原因，揭示其主要的犯罪类型，分析智能合约犯罪带来的刑法挑战，最后从国际刑法的视角出发，寻找切实有效的法律回应策略。希望通过本文的研究，能对如何通过国际刑法手段防控区块链环境下的智能合约犯罪提供一些启示，以期为全球范围内的刑法体系在面对这类新型犯罪时提供一些借鉴和参考。

关键词

区块链，智能合约犯罪，国际刑法回应

Criminal Law Response to Smart Contract Crime in the Context of Blockchain Technology

Jiajia Song

Law School, Beijing Normal University, Beijing

Received: Jul. 11th, 2023; accepted: Dec. 5th, 2023; published: Dec. 13th, 2023

Abstract

Blockchain, as a widely used new technology, is crucial for the iteration of smart contracts from

文章引用: 宋佳佳. 区块链技术语境下智能合约犯罪的国际刑法回应[J]. 社会科学前沿, 2023, 12(12): 7080-7086.
DOI: 10.12677/ass.2023.1212966

version 1.0 to 2.0. It solves two major problems for smart contracts, namely, the source of data and the trust mechanism, enabling smart contracts to operate widely in society. The widespread application and iterative expansion of new technologies will inevitably trigger transformations in social behavior, leading to governance dilemmas and crime risks. This article aims to deeply analyze the reasons for the emergence of smart contract crimes in the blockchain environment, reveal their main crime types, and analyze the criminal law challenges brought by smart contract crimes. Finally, from the perspective of international criminal law, we seek effective legal response strategies. Through this research, we hope to provide some insights on how to prevent and control smart contract crimes in the blockchain environment through international criminal law measures, in the hope of providing some references and lessons for the criminal law systems worldwide when facing such new types of crimes.

Keywords

Blockchain, Smart Contract Crimes, International Criminal Law Responses

1. 引言

区块链技术，以其分布式、去中心化和安全可靠的特性，引领了新一轮的科技革命。智能合约，作为区块链技术的重要组成部分，通过自动执行合约的能力，正在逐步改变商业交易的模式。然而，任何一种新兴技术的出现都是一个双刃剑，智能合约同样面临这样的挑战。尽管它在加速商业活动、提高效率方面显示出显著优势，但其去中心化、匿名性等特性也为犯罪分子提供了新的作案手段和空间，已经观察到恐怖组织资金转移、贩卖儿童、洗黑钱等犯罪活动中智能合约的广泛应用。面对这些新的犯罪模式，从国际刑法的角度研究智能合约犯罪并寻找相应的法律应对策略，显得尤为重要。

2. 区块链智能合约犯罪产生原因

2.1. 区块链智能合约技术概述

智能合约(Smart contract)是指在区块链上嵌入的程序化合约，能够自动化和智能执行程序设定的内容。

其最早是在 1995 年由密码学家尼克·萨博提出的[1]。基本逻辑类似计算机程序 if-then 语句(也即“if X occurs, then Y will be triggered”) [2]。在其 1.0 版本中，执行一方预设程序性协议，签约一方在信任基础上同意协议，最终实现协议的运行[3]。但是这一阶段的智能合约面临着两个问题：一是数据来源问题，由于初期技术网络的局限性，智能合约难以获得大量的数据来源，无法进行多领域的社会扩张；二是信任机制问题，智能合约在制定伊始就天然地更倾向于执行一方，在这种情况下，签约一方能否在进行协定时产生信任就成为了智能合约建立的关键。囿于上述两个问题，智能合约长时期内未能得到充分的发展。但是，区块链技术很好地弥补了上述缺陷。

区块链(Blockchain)作为智能时代的重要技术构成，是指利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算范式[4]。具体而言，其具备了“去中心化”、“不可篡改性”、“匿名性”、“可追溯性”等特征，这使得链上各主体能够免于中心裁决者(第三方)的信任背书[5]，在密码学和计算机算法的加持下获得绝对真实且安全的数据。

换言之，区块链技术在容纳海量数据的同时，建立了相对完善的信任机制，这一举突破了智能合约扩张应用的两大难题，使得其能够在原有金融领域之外的广泛社会实践中发挥调配社会资源的作用[2]。

总之，区块链是智能合约的驱动技术，区块链技术可以解决智能合约难以广泛展开适用的困境，二者之间密不可分。对智能合约犯罪的研究也更加需要深入到区块链语境下来，这样能够使得研究更有意义，而不是在几乎不可能实现或者发生的情况的语境下无谓讨论。

2.2. 区块链语境下的智能合约的犯罪风险

众所周知，新技术能够带来技术红利的同时，也同样会带来相应的风险和挑战。区块链智能合约在社会多领域的广泛应用和发展在提高资源配置效率的同时，也会引起社会中行为人行为的形变，进而衍生出超出现有法律规则边界的犯罪空间。

2.2.1. “去中心化”消除第三方监管

区块链智能合约构建了除第三方监管外的信任机制，这在提高效率的同时也为犯罪分子提供了空间。正如前文所述，区块链上每一个主体都拥有平等的法律地位，对链上数据进行共建共享，这一技术条件下的智能合约也实现了交易双方自由、平等、信任、隐蔽地达成协议。区块链智能合约加强社会资源配置效率的同时，也会进一步消融第三方监管的介入，很容易给不法分子以可趁之机，使得区块链智能合约成为“法外之地”。

2.2.2. “匿名性”阻碍犯罪侦查

区块链智能合约奉行的“假名主义”[6]为犯罪侦查设置了阻碍。区块链语境下的智能合约所设置的匿名保护、域名频繁变更、最小化交互等程序在为交易双方提供安全保障的同时，也使得其相关的非法活动更难被执法部分所察觉、监控、侦查。此外，其所具备的隐蔽性和数据的迭代性使得犯罪行为的取证极为困难，对犯罪证据链的构建与形成带来了极大的挑战。可以说，区块链语境下的智能合约为犯罪提供了绝佳的土壤，使得其突破了常规网络犯罪的打击半径，愈来愈成为犯罪分子牟利的便利工具。

2.2.3. “分布式”削弱管辖权

区块链智能合约全球性节点的“分布式”特征使得管辖权模糊。区块链语境下的智能合约突破了其1.0版本的局限性，可以在全球范围内构建分布式账本[7]，进行远程交易确认，使得智能合约犯罪的管辖权在世界范围内泛化。此外，区块链智能合约又因为其所具备的技术特征，导致传统的网络空间主权管辖所遵循的网络设施“领土原则”[8]、网络主体“国籍原则”[9]、网络行为“效果原则”无法得以适用，这更为智能合约犯罪提供了温床。

3. 智能合约犯罪样态的主要类型

随着智能合约的广泛应用，其已经成为一个全新的犯罪载体。在国际社会实践中，智能合约犯罪呈现出不同的犯罪样态，其形形色色的犯罪样态会给国际社会的犯罪治理格局产生深刻的影响，因为有必要对其进行进一步的思考与研究。总的来说，对于智能合约可能涉及到的犯罪问题，具体可以从以下三个方面概括其类型。

3.1. 以智能合约为犯罪手段的犯罪

智能合约犯罪的重要类型是以其为手段的犯罪。在区块链平台上，任何交易都是没有限制的，任何内容的智能合约都是被允许的。在之前的网络犯罪中，犯罪分子利用网络发布信息，进而招募共同犯罪人，锁定被害人后施行危害行为，这往往需要共同犯罪双方具备一定的信任基础。而在智能合约犯罪中，犯罪分子仅需要提前设置代码程序，当犯罪行为人相应邀约实行犯罪并达到约定条件后，智能合约将会

自动运行给予相应报酬。这就使犯罪行为突破了传统网络犯罪的模式，得以通过更隐蔽、更渐变、更匿名、更难以侦破的方式快速扩散及复制。

在国际范围内，智能合约已经在恐怖组织资金转移、贩卖儿童、洗黑钱等犯罪行为中广泛适用，成为犯罪规模化、智能化、全球化的重要手段。这些犯罪行为的广泛性和严重性，为全球的刑法系统带来了严重的挑战。具体而言，智能合约在恐怖组织资金转移中的应用，既具有迅速性也具有隐秘性。恐怖组织可以利用智能合约快速、无痕地转移大量资金，为其恐怖活动提供了稳定的经济支持。这种资金转移方式的智能化和全球化特点，使得传统的金融监管和反恐措施难以对其进行有效管制，从而给国际社会的安全带来了严重威胁。此外，智能合约在贩卖儿童这种严重的人权犯罪中也得到了应用。犯罪分子可以利用智能合约的匿名性和跨国特性，进行大规模、系统性的贩卖儿童活动。这种犯罪行为的规模化和全球化特点，对国际社会的道德伦理和法律规则构成了严重挑战，同时也对儿童的权益带来了深重的伤害。再者，智能合约在洗黑钱这种经济犯罪中的应用，也是令人警觉的。犯罪分子可以通过智能合约，将非法所得资金转化为合法资产，从而逃避法律的制裁。这种洗钱行为的智能化和全球化特点，使得传统的反洗钱机制难以应对，从而对全球经济秩序和金融安全造成了严重影响。

总的来说，智能合约在各种犯罪行为中的广泛应用，不仅使得这些犯罪行为的规模化、智能化、全球化特点日益明显，也对全球的刑法系统提出了更高的要求。因此，各国需要加强国际刑法合作，共同面对智能合约带来的刑法挑战。

3.2. 以智能合约为犯罪对象的犯罪

智能合约犯罪的另一个主要类型是以其为犯罪对象的犯罪。有国外学者对 100 万份智能合约进行分析后发现：有将近 34,200 份智能合约很容易收到黑客攻击[10]。这意味着全球范围内以智能合约为犯罪的犯罪风险普遍存在。具体而言，在以智能合约为犯罪对象的场景中，犯罪呈现出“技术性犯罪”的倾向，犯罪分子往往利用技术手段针对智能合约本身的算法或程序进行破解、修改、获取信息等操作，进而完成犯罪。这一类型以 2016 年 6 月 17 日出现的“The DAO”事件为典型代表。在这一以太坊历史上最大的代码漏洞实践中，黑客通过技术手段将价值 6000 万美元的以太币进行转移，完成了符合代码逻辑的“完美犯罪”。这一案例也成为了以智能合约为犯罪对象的典型犯罪案例。

3.3. 以智能合约扩张为犯罪主体的犯罪

现阶段，智能合约犯罪的主要类型是以其为手段及对象。但是在智能合约进一步迭代拓展的情况下，在人工智能算法的加持下，智能合约极有可能突破传统“人脑－指令－协议”模式，实现自主决策的 3.0 版本迭代。这意味着智能合约犯罪也有可能会完全突破既有法律理论体系，成为犯罪的主体。此时，智能合约犯罪的新样态将在区块链 + 人工智能的语境下实现新的突破，会对刑法规制点来新的挑战，但这并非当前智能合约犯罪实践的主要类型，也超出了区块链技术语境下智能合约 2.0 版本的技术范畴，因此不加以赘述。

总之，就当前实践而言，区块链语境下的智能合约犯罪主要包括两种类型：一是以智能合约为犯罪手段的犯罪，其仍处于传统罪名体系范围之内，具备传统犯罪的相同特征，但又因为智能合约技术的独特性而有所不同；二是以智能合约为犯罪对象的犯罪，其已经完全突破了传统网络犯罪的语境范畴，成为了一种新的犯罪类型。

4. 智能合约犯罪对刑法的挑战

智能合约犯罪是一个依托于技术数据而辐射至各层次、各方面法益侵害的狭长体系，其更是涉及了刑法分则个账的实体内容，呈现出一种新技术与旧规定错综复杂、相互交叉的实践现状。因此，对智能

合约犯罪的研究需要深入到其对现存刑法之挑战上来，进而探求传统的定罪量刑规则体系与新兴技术革命之间的平衡点。

4.1. 罪与非罪：智能合约犯罪的罪名体系

区块链智能合约犯罪突破了原有刑法分则罪名体系，带来了“罪与非罪”的刑法争议。智能合约履行过程具有一定的封闭性，代码一经启动则强制执行，在执行过程中保持代码自决，没有必要甚至不可能适用法律。换言之，由于智能合约执行过程自动且不可更改，其并没有法律介入的余地。可以说，智能合约的执行是以代码为基准的，符合代码的运行结果符合一般正义。从这个意义上说，智能合约犯罪提出了一个新的问题：符合代码要求的合约操作行为是否构成犯罪？正如 The DAO 案例中，转走以太币的黑客表示其行为完全符合代码的技术逻辑，并不属于严格意义上的盗窃行为。由此引发出了代码和法律关系之争议，更引起了“罪与非罪”的广泛讨论。

4.2. 此罪与彼罪：智能合约犯罪的构成

实践中，智能合约犯罪往往分为两大类型，与传统犯罪有所交叉又有所不同，为各国现行刑法带来了“此罪与彼罪”的挑战。一方面，以智能合约为对象的犯罪已经突破了现行刑法的罪名体系，其具体构成及与传统网络犯罪的区分尚不明晰；另一方面，以智能合约为犯罪手段的犯罪仍然在既有刑法框架之中，但其独特的隐蔽性、技术性特征使得智能合约犯罪情节更加复杂，需要在符合法律逻辑的同时对代码逻辑进行分析，进而区分具体罪名。总之，智能合约犯罪因为其技术的创新性与独特性给现行刑法带来了挑战，刑法需要明确智能合约犯罪之构成以确定是此罪还是彼罪。

4.3. 重罪与轻罪：智能合约犯罪的量刑标准

区块链智能合约技术的突破使得其犯罪行为得以大范围扩展，带来了更大的社会危害性。但是就各国现行刑法而言，其对智能合约犯罪的量刑并未有明确标准。而既有刑法之规定显然未曾考虑到区块链智能合约在全球范围内扩张之现状，导致其部分犯罪刑期与实际的社会危害性并不相符。可以说，智能合约的技术扩张使得其犯罪的影响力和破坏性大幅增加，甚至超越了现行刑法之良性上限。因此，区块链技术语境下的智能合约犯罪之量刑标准亟需研究后明晰。

4.4. 证据链：智能合约犯罪的证据认定

智能合约犯罪由于其去中心化、隐蔽性、匿名性的特征使得侦查机关取证困难。我国法律规定，在民事案件中，电子签名、可信时间戳、哈希值校验、区块链等证据可以作为证据使用[1]。但是就刑事领域，却并未对此进行明晰。而区块链智能合约的不可篡改性和程序封闭性使得其取证较为困难，必须依赖技术手段对代码进行破解后对链上数据进行追溯，进而构建完整的证据链。这一必然需求与现行刑法之间的矛盾必然会导致在实际司法过程中的不适应，无形中给智能合约犯罪取证造成了困难。这也是区块链语境下智能合约犯罪对现行刑法带来的挑战之一。

5. 国际刑法视野下的智能合约犯罪

5.1. 国际刑法对智能合约犯罪的管辖

5.1.1. 全球性的犯罪形态

区块链技术的去中心化和跨国特性，使得智能合约犯罪往往具有全球性。一份智能合约可能在一国

[1]最高人民法院 2018 年 9 月颁布的《关于互联网法院审理案件若干问题的规定》第 11 条第 2 款规定：“当事人提交的电子数据，通过电子签名、可信时间戳、哈希值校验、区块链等证据收集、固定和防篡改的技术手段或者通过电子取证存证平台认证，能够证明其真实性的，互联网法院应当确认。”

编写，通过服务器在另一国执行，最后在第三国产生犯罪效果。这种跨境犯罪的新特性让国际刑法的应用面临挑战。按照传统的领土原则或者国籍原则，都可能无法有效地确定犯罪管辖权，因为这种犯罪行为超越了一个单一的领土或者国籍。因此，需要国际刑法以一种更灵活的方式，如效果原则或者普遍管辖原则，对此类犯罪进行规制。效果原则强调如果犯罪行为在某国家产生了实际效果，那么这个国家就有权对犯罪行为进行管辖。普遍管辖原则则意味着对于某些特定的严重犯罪行为，任何国家都可以进行管辖，而不论犯罪行为是否在该国发生。

5.1.2. 区域性的刑事管辖权

然而，即使在国际刑法的视野下，区域性的刑事管辖权也存在挑战。由于不同国家的法律制度、法律文化和技术监管水平的差异，对于同一种智能合约犯罪可能有着不同的认定和处理方式。这就需要在法律冲突的情况下，通过双边或多边条约来解决，或者遵循最有利于被告的原则。此外，也需要对国际刑法在处理此类问题上的适用性进行深入研究，以确保管辖权的确定既能满足各国的刑事司法要求，又能尊重国际法的原则。

5.2. 国际刑事责任的确定

对犯罪主体的认定：智能合约的匿名性和去中心化特性使得确定犯罪主体在国际刑法下变得困难。传统的犯罪主体通常是清晰可识别的，然而在智能合约的环境下，由于编程、执行和使用可能由不同的实体完成，确定谁应当为犯罪行为负责变得复杂。这就需要我们在解释和应用国际刑法时，充分考虑这些特性。一方面，我们需要通过技术手段来识别并追踪犯罪行为，比如使用网络追踪、数字取证等手段。另一方面，我们也需要在法律上对于此类犯罪行为的主体负责性有明确的规定和解释，这可能包括对编程者、执行者、使用者等不同角色的责任划分。

对犯罪行为的界定：对于涉及多个司法管辖区的智能合约犯罪，可能会存在对同一行为的不同解释和判定。在一些国家，可能会重点考虑行为人的主观恶意，而在另一些国家，可能会更注重行为的客观危害。因此，在国际刑法框架下，需要建立一个更具有通用性和接受度的犯罪行为定义，以避免出现对同一行为的不同判定。这可能涉及对于智能合约犯罪行为的本质、特性、影响等进行深入分析，并尝试寻找一个可以被各国接受的公正且合理的解决方案。

5.3. 国际合作与协调的挑战

5.3.1. 法律协助与引渡

对于跨境的智能合约犯罪，需要国际间建立有效的刑事司法合作机制。这包括在尊重各国主权和法律的前提下，进行有效的法律协助和引渡。例如，一个国家在调查智能合约犯罪时，可能需要另一个国家的协助来获取服务器数据、追踪犯罪行为、甚至将犯罪嫌疑人引渡回自己的国家。然而，由于各国的法律制度、数据保护规定、人权保障等因素的差异，如何进行有效的法律协助和引渡，既能满足调查需要，又能尊重国际法原则和人权保障，是一个重要且复杂的问题。

5.3.2. 对比和学习各国法律经验

由于智能合约技术的新颖性，对其的刑法规制在全球范围内还处于探索阶段。因此，各国可以通过比较和学习不同国家的法律经验和判例，以寻找对智能合约犯罪更有效的刑法回应。例如，一些国家可能已经在智能合约犯罪的规制上取得了一些成功的经验，如在确定犯罪主体、界定犯罪行为、进行法律协助和引渡等方面，都有一些值得参考的做法。通过对这些做法的比较和学习，可以帮助各国在处理智能合约犯罪时，更有效地应用和发展国际刑法。

6. 结语

应当强调，区块链技术语境下的智能合约有许多有前途的、合法的应用，但其在实践中不断拓宽社会资源流动的同时，也蕴含着诸多法律风险。虽然有部分学者认为，当前在我国刑事法律实践范围内，智能合约犯罪仍然是一个“未来想象”[11]。但是就长期而言，对智能合约的禁止是不明智的，也是不可能的。因此，紧迫问题是如何在保障智能合约在社会中强有力适用的同时，寻求监管与自由的平衡，也即第三方监管与去中心化的平衡。在技术层面，需要深刻明晰“法律即代码”的思想，以法律对技术进行内部的及外部的约束。在法律层面，需要从罪名、犯罪构成、量刑、取证等多方面对智能合约犯罪进合理规制，以实现现有规则与未来科技变化的融洽化。归根到底，监管与控制并不是目的，通过包容审慎的监管态度推动法律人更好地了解和认知智能合约，进而使其从陌生的、有潜在危险之物，成为融入人类社会并创造价值的可控之物，才是目的。

参考文献

[1] 袁勇, 王飞跃. 区块链技术发展现状与展望[J]. 自动化学报, 2016(4): 481-494.

[2] 任航, 谢昭宇. 区块链 2.0 时代智能合约的犯罪风险及其应对——以 The DAO 黑客事件为例[J]. 犯罪与改造研究, 2020(3): 2-7.

[3] 赵志华. 区块链技术驱动下智能合约犯罪研究[J]. 中国刑事法杂志, 2019(4): 90-102.

[4] 中华人民共和国工业和信息化部. 中国区块链技术和应用发展白皮书[EB/OL]. http://xxgk.miit.gov.cn/gdnps/wjfbindex.jsp, 2018-11-13.

[5] 常乐. 论区块链技术下金融衍生物的刑事规制[J]. 检察调研与指导, 2019(4): 11-15.

[6] 王延川. 智能合约的构造与风险防治[J]. 法学杂志, 2019(2): 43-51.

[7] 邓建鹏. 元宇宙金融规制理论[J]. 财经法学, 2022(5): 35-53.

[8] 王雪, 石巍. 数据立法域外管辖的全球化及中国的应对[J]. 知识产权, 2022(4): 54-75.

[9] 吴培琦. 破解迷象: 国内法域外管辖的基本形态与衍生路径[J]. 苏州大学学报(法学版), 2022(1): 147-160.

[10] Nikolic, I., Kolluri, A., Sergey, I., *et al*. Finding the Greedy, Prodigal and Suicidal Contracts at Scale. https://arxiv.org/pdf/1802.06038.pdf

[11] 孙道萃. 网络时代的中国刑法发展研究: 回顾与展望[J]. 华南师范大学学报(社会科学版), 2021(1): 157-174+197.