苏宇

中国人民公安大学法学院副教授，法学博士

要目

非同质通证是区块链技术与应用的重要创新，技术上主要包括染色方案和“以太坊征求意见提案”标准方案，业务场景丰富。将非同质通证作为物、货币、证券或合同标的处理均存在难以解决的法理难题，应将其视为加密数字凭证。非同质通证可能引发技术安全、网络信息安全、金融安全、知识产权保护等多方面风险，在治理上面临较大挑战。基于加密数字凭证的定性，非同质通证的技术层和应用层可以被有效区分，进而为明确非同质通证的合法性边界、确定监管主体与职权职责结构、完善治理框架与主要法律机制并建立必要的技术标准体系等主要风险治理工作奠定基础。

非同质通证是否为“加密数字凭证”

如果对非同质通证采取上述定性均不可行或困难重重，可以考虑还原其技术本质，将其定性为一种加密数字凭证，将作为载体的标记与其上附加的价值及产品分离，通过独立于数字代币及其他加密资产的法律定位，另建监管制度框架。非同质通证相关的权益结构设计完全取决于智能合约及区块链“标准”，自发和自治性质相当强，甚至一般情况下并不希冀法律的介入。然而，法律又必须介入非同质通证的相关活动，防范经济和社会风险，从安全与秩序的目标维度对其加以调整。对此，重要的是将作为技术载体的加密数字凭证及其附加的价值设定进行切割，每一个加密

数字凭证可以被连接于何种数字文化产品、金融产品、电子文档甚至法律文书，可以由法律规范作出明确地限制。如果在定性上实现了技术载体与连接内容的切割，则以非同质通证的技术特点，完全可以用于支持带有唯一标识或数量有限标识的电子凭证实现可追溯、可验证的流转，在2021年10月中央网信办、中央宣传部、国务院办公厅等18个单位联合发布的《关于组织申报区块链创新应用试点的通知》中提及的“区块链+制造”“区块链+税费服务”“区块链+版权”“区块链+贸易金融”“区块链+股权市场”等多方面有巨大的应用潜力。惟有采取加密数字凭证一类的独立定性，才能实现载体本身与指向内容在合法性层面的切割。

采取加密数字凭证的定性意味着需要建立新的法律关系框架。数字代币的监管框架基本上脱胎于各国的金融监管体制。例如，新加坡政府基于证券与期货法第八章的资本市场产品监管架构对于货币导向的数字通证（代币）采取了分别纳入股份、债券、商业信托单位、证券衍生品合同或集合投资计划（Collective Investment Scheme，简称CIS）单位的分化归类处理的方式，通过《数字代币发行指引》之类的解释性行政规则将数字代币纳入现有的制度框架，进而再细化和完善其具体监管制度。对于非同质通证而言，既然在理论和实践中选择与同质化的数字代币进行切割，并且预计其应用及风险将远不止于金融领域的范围，我们必然需要建立全新的治理框架。对此，有效平衡风险防范与市场创新需求的制度建设仍需要更多积极的探索，尤其是需要首先充分认识非同质通证的潜在风险与治理挑战。

在更深层的意义上，非同质通证的物理本质是机器生成的一组数据，而此类应用广泛的机器生成数据“实质上是一组权利束，它并非一项简单的物权、知识产权或某一种新型财产性权利，而是一种涉及多个主体的权利集合”。尽管此种观点尚可商榷，但亦表明一种新的潜在需求：在非同质通证的未来应用非常广泛的情况下，不应一开始就对其法律性质作方向性的限制。因此，在考察非同质通证的法律定性时，应当尽可能保留其应用上的开放性，这就可以考虑区分技术层面与应用层面，进而创造性地对非同质通证的法律性质进行有限制的界定。

三、非同质通证的潜在风险

技术性安全风险

非同质通证的潜在风险首先来自其自身的安全性。以太坊及比特币现金等公链本身的安全性就不是绝对可靠，所有公链的共识算法都存在不同程度的缺陷。不仅如此，公链的安全性还受到现实条件制约，必须依赖于较强的人性假设。例如，以太坊依托权益证明（POS）的共识算法但持币结构较为集中；比特币现金依托工作量证明（POW）但算力结构过分集中；两者的安全性在理论上均存在缺陷，只能依托理性经济人的假定和硬分叉的保留手段支持其安全性基础。

公链的安全性尚属其次，发行非同质通证的智能合约的安全性是一个更为直接面临考验的问题。在以太坊中，一度有89%的智能合约代码存在安全漏洞或隐患，对各种基于智能合约的应用而言是一个巨大的风险因素。尽管在DAO事件以后以太坊出现了针对智能合约的形式验证机制，但对于越来越多的ERC标准及日益复杂的大型智能合约而言，高度模式化的形式验证机制并不能完全保证相关智能合约不存在安全性漏洞。一旦智能合约本身受到针对性的攻击，整个合约相关的价值流都有可能面临基础性的巨大风险。不仅如此，由于我国区块链行业发展的一些特点，非同质通证的技术安全还有若干需要特别注意之处。例如，“日蚀攻击”一直是区块链安全中一个并未彻底解决的问题。理论上，参与节点越少，越容易遭受日蚀攻击。在我国区块链的发展中，由于政策影响，联盟链将日益占据重要地位，但由于其参与节点相对较少，防范日蚀攻击的风险也将更具挑战性。因此，基于联盟链生成和转移非同质通证时，此种风险亦需纳入技术安全方面的考量。

网络信息安全风险

自2016年网络安全法将“网络信息安全”单列一章以来，网络信息安全风险规制在我国网络治理中一直占据重要地位。区块链可以被用来在全球范围内传输各种各样的数据，且所有节点可以同步存储这些数据，这一特征早已被各界高度关注。我国在区块链领域实施的第一个部门规章《区块链信息服务管理规定》,就是针对区块链信息服务所带来的违法网络信息传播风险而设。非同质通证的网络信息安全风险主要在于交易附加信息。OP_Return附加信息本身就处于《区块链信息服务管理规定》的监管范围内，基于扩容后的OP_Return或ERC-1948等标准发送附加信息时，这些信息与交易记录本身同样不可篡改和删除，这将引发政府极力防范的违法犯罪信息传播风险。基于扩容后的OP_Return或ERC-1948等标准发送信息可能包含较多的非交易类信息，在我国法律制度框架内，更容易触发网络信息安全风险，冲击整个非同质通证的合法性空间。

金融安全风险

非同质通证有可能成为金融领域影响最大的安全风险。非同质通证常以虚拟货币（或数字代币）购买，由于虚拟货币具有去中介化、去国界化、非当面性、匿名性以及交易快捷、全球流动性大等特征，且以非同质通证为载体的数字艺术品容易产生高溢价，因此显然存在利用非同质通证进行洗钱的风险。尤其是以太坊2.0的公链设计增加了比较自由的资产质押功能，在灵活的质押合约加持下，非同质通证极易变为洗钱工具。不仅如此，ERC-1155的出现使非同质通证同样可以被分割和用于支付场景，导致非同质通证在一定程度上可能对金融、外汇及税务体系造成类似于同质化数字代币带来的冲击。不仅如此，对于同质通证项目而言，通过硬分叉恢复被盗资产是一种可用的最后手段。然而，对于单一的非同质通证而言，硬分叉在此可能形成的结果是对于同一标的的权属认定出现重大分歧，甚至意味着某一非同质通

证将永久负担此种权属缺陷，这对于非同质通证的最关键属性—单一或珍稀产品的可靠认证是不利的。当非同质通证如果通过智能合约承载着质押、投资等复杂的金融操作时，硬分叉对金融安全所产生的影响更是难以估量。因此，非同质通证必须慎用硬分叉作为最后手段，这就进一步加剧了其在金融安全方面的隐忧。

知识产权风险

非同质通证目前主要聚焦于文化艺术产品，有引起知识产权风险的可能。尽管非同质通证对于保护知识产权而言有相当积极的价值，但如果最先完成上链的作品本身就存在知识产权缺陷，发行非同质通证将有可能使侵权引起的损害大幅升高。易言之，区块链固然可以通过其防篡改、可追溯的功能固定证据以保护知识产权，但如果从一开始就发生了知识产权纠纷或侵权的情形，损害后果也可能通过公链的金融杠杆效应被不断放大，甚至产生难以精确衡量的严重侵权结果。不仅如此，同一个作品可以用于生成多个非同质通证，一旦各个非同质通证的发行方都声言其为唯一的、原创的来源，对于普通投资者和消费者而言有可能引起颇为棘手的困惑局面；作品的所有权人和著作权人也有可能将不同的权利分别配置于不同的非同质通证中发行（理论上甚至可以分割所有权或著作权的不同权能而发行多种非同质通证），导致更复杂的知识产权冲突。

因此，对非同质通证的华丽想象背后实际上潜藏着多重风险。将其视为一种加密数字凭证，保留其应用层面的多元性与差异性，不仅有利于精准设计非同质通证治理的制度框架，也有利于针对其各种应用风险进行精准的制度化预防。然而，正是由于非同质通证在应用层面的多元性与差异性，相关风险治理与制度完善很难简单套用既有的规制路径，平衡其潜在社会经济价值与风险治理需求需要相当有开拓性和前瞻性的制度方案。

四、非同质通证的风险治理与制度完善

非同质通证在实践中方兴未艾，相关风险治理工作的主体结构、制度框架、主要法律机制、治理精度及相应的技术标准体系等或者未尽明确，或者尚付阙如，对于法治化的风险治理带来了难题。但是，也为新的规制路径与制度方案留下了空间。在制度初创之际，相关法治建设需要聚焦若干基础性的目标：一是界定非同质通证的合法存在空间；二是明确监管主体及其权责结构；三是完善治理框架与主要法律机制；四是建设相应的技术标准体系。此四者可以初步构建非同质通证治理的法律框架，有效回应技术面和应用面的风险治理需求，为探索具体而精准的治理方案奠定基石。

明确非同质通证的合法性边界

非同质通证的合法性边界是未来其面临的最主要问题。将非同质通证定性为加密数字凭证，并不能完全消除其合法性风险。理论上，非同质通证虽然可以与虚拟货币及其他加密资产进行界分，但还需要获得明确的政策认可方能确认其合法性状态与边界。尤其在ERC-1155等可分割技术出现后，非同质通证与普通数字代币之间的界限理论上又有进一步模糊的可能性。对此，如果将非同质通证定性为加密数字凭证，其合法性问题就可以转换为如何生成与使用此种凭证的问题，无论分割与否均不影响载体本身的合法性。由政府、公共事业单位、公有制企业或私主体生成凭证应当均被允许，但利用此种凭证进行非法集资之类的违法活动须被禁止，同时也根据既有的实体法规定限制或禁止部分凭证的交易活动。如此，在相当一段时期内，非同质通证的合法性边界可以采取“线下—线上”直接对应的规则加以界定：相关凭证生成和流转的合法性边界直接取决于其线下原始形态的生成和流转合法性边界。尽管放弃华丽的质押融资、期货交易、复合权益结构设计等金融运作空间可能引起“区块链原教旨主义”支持者的不满。但是，基于风险预防原则，在非同质通证引起复杂金融风险的不确定性尚相当高的情况下，有必要选择较为谨慎的处理方式，待相关技术更为成熟、风险更为清晰、国家与社会对此有更高接受度以后，再稳步扩展合法性空间和允许开展的业务范围。

确定监管主体与职权职责结构

即便非同质通证与此前常见的同质化数字代币能够实现完全切割，在监管架构方面仍可能存在一定的制度惯性。由当前我国数字代币（含虚拟货币）的监管态势观之，非同质通证风险治理的行政主体构成可能颇为复杂。《通知》的联合发文单位包括央行、网信、工信、公安、市场监管、银保监、证监、外汇等八个部门，以及最高人民法院和最高人民检察院，即“两高八部门”。负有监管职责的“八部门”基本上也是非同质通证监管的主要部门，而一旦非同质通证被确认合法，由于其主要涉及文娱产品，宣传、文化、新闻出版、知识产权等部门还很可能需要介入。众多相关部门构成一个复合型的监管主体框架，其中“八部门”的职权职责要划分清楚已非易事，再加上文化领域的各主管部门，监管职权职责结构的具体划分将更为棘手。不过，只要非同质通证的法律性质能够合理确定，仍有可能形成初步的整体性制度安排。总体上，若对非同质通证采取加密数字凭证的定性，即可一定程度上区分技术与应用（业务）层面的规范问题，形成一种层次化的职权职责结构设计：非同质通证自身作为加密数字凭证的技术安全问题由工信部门监管；非同质通证中的信息流、业务流、价值流分别由网信部门、市场监管部门等业务主管部门、央行等金融管理部门监管，相关活动构成犯罪的，移送公安机关处理；以非同质通证名义或利用非同质通证进行的诈骗或传销等违法犯罪活动，由公安机关处理。这样一种层次化的职权职责结构尽管只是一种总体性的构思，但可以最大限度地与各部门当前在综合性监管活动中的职权职责结构相衔接，可以为进一步展开具体的权责清单提供基础性的框架与方向。

完善治理框架与主要法律机制

非同质通证的治理不能仅依靠自上而下的监管。来自市场与社会的治理合力对于实现精准治理、平衡非同质通证的技术发展、应用价值与风险防控需求而言，有着不可替代的作用。鉴于区块链技术和业态发展的高度自发性和充沛的市场活力（知识社区及投资界尤为活跃），非同质通证项目的风险治理可以首先依托区块链自身的治理手段，而来自政府的监管力量则作为治理方向的积极引导者和风险底线的有力保护者，利用“后设规制”的方式完善非同质通证的治理体系。由于我国的非同质通证（数字藏品）主要基于联盟链发行，此种较多依赖企业合规的治理方式即更有可行性。具体而言，政府可以推动建立多种国家标准或行业标准，要求相关企业对非同质通证的发行、使用和流转建立合规体系，尤其强调非同质通证的程序设计必须包含充分的安全保障措施，并一定程度上包含基于区块链的交易追溯、权益证明、纠纷解决、合约审计等机制；在此基础上，政府根据不同标准及合规评估结果确定非同质通证发布平台的“白名单”，在持续全面监测风险的前提下稳步推动非同质通证业务的健康发展。

建立必要的技术标准体系

非同质通证的风险治理需要确定合理的精度，既要充分防控风险，又要避免过度干预区块链自身内生的治理机制和逻辑，人为削弱非同质通证乃至区块链的安全性及可用性，以及限制有益的技术与业态发展。由于非同质通证的风险治理是高度技术化的，精准治理的许多具体安排很有可能将主要通过规范性文件中的政策性要求及技术标准进行。其中，经由法律规范中的授权性条款、准用性条款等连接的技术标准体系，可以在针对非同质通证的专业治理中发挥不可替代的重要作用。技术标准往往并不仅仅承载纯技术性的要求，也包含了较多具有价值内涵的行为规范在内，可以实现贯通非同质通证技术层与应用层的精准治理。

对于非同质通证而言，技术标准体系主要可以解决以下几种问题：一是防控非同质通证自身的技术性安全风险。例如，相关智能合约安全性的形式验证、重要的ERC提案及合约部署平台的安全性要求等，都可以一定程度转化为指引非同质通证技术安全的技术标准。中国电子学会发布的《区块链智能合约形式化表达》（T/CIE095-2020）就是一次典型的探索。二是防控非同质通证所可能引发的金融风险。非同质通证源于公链平台，在法律与政策对其不加限制的情况下，其本身就可以基于智能合约与同质代币及各种虚拟货币联动，构成复杂的金融运作。非同质通证如获认可，在可预见的未来只能以人民币直接或间接交易。一旦非同质通证形式（尤其是可分割的非同质通证形式）的数字文化艺术产品或其他产品需要链接数字人民币的支付通道及智能合约，就需要通过技术标准建立规范的、安全的操作形式和风险监测机制，防止引发金融风险。三是引导非同质通证提供符合社会经济需求的衍生功能和服务。非同质通证如用于开具各类电子证明、单据，则在非同质通证自身的技

术标准以外，证明和单据的内容本身也需要基于一定的标准生成，以便满足相关信息上链乃至进行多种复杂链上操作的要求。

结语

在区块链掀起的数字经济浪潮中，非同质通证是极具想象力的一个新事物。它的特殊标记能力和有限分割机制与区块链的其他功能相结合，就可以在广泛的领域发挥积极作用，有可能成为构建未来数字社会的关键技术之一，甚至直达所谓“元宇宙”。然而，种种有关非同质通证的想象虽有“心游万仞”之意蕴，但切不可演变为“挟山超海”的冲动，而试图跨越一国法律与政策所设定的风险底线。秉持务实的立场，从一开始就对非同质通证进行全方位的风险监测与深度治理，才是对这一新生事物最好地保护与支持。

非同质通证的风险治理是一项极具专业性的工作，不仅在全球范围内并无成熟先例可供借鉴，技术和业态上的不断发展变化也令相关风险的不确定性持续居高不下，在公有链及数字代币遭遇严厉监管政策的环境中探索专门针对非同质通证的精准风险治理框架需要格外谨慎。尽管如此，我们仍然可以未雨绸缪，强化技术与制度层面的基础性研究，通过范围有限、风险可控的渐进式试点，在合法范围内不断探索有益于我国社会经济发展的非同质通证应用与业态，以更丰富和安全的加密凭证技术与应用迎接数字经济和数字社会的繁荣未来。