可以自动触发清算逻辑，按照约定的优先级与比例，实时自动分配给全球范围内的投资者。这种机制不仅消除了传统金融中介的冗长流程与高昂费用，更使得资产在全球范围内的快速流动成为可能。

四、信任闭环与未来展望

数据归人与现实世界资产数字化的实践，最终指向的是一个构建在数智技术之上的全新信用体系。在这一体系中，数据的真实性验证与闭环管理是基石。

为了确保上链数据的真实可信，未来的数据基础设施将普遍采用双签或多签机制。即在每一次数据交互或交易发生时，不仅需要数据生成方的数字签名，还需要交易对手方如支付方、物流方的同步签名确认。这种基于交易闭环的交叉验证机制，能够有效防止单方面的数据造假，构建起类似于区块链共识机制的社会化信任网络。

当海量的数据通过数据归人机制汇聚于个体，并通过资产数字化模式实现价值转化时，我们实际上正在构建一个数字与物理深度融合的新世界。在这个世界中，数据不再是静止的记录，而是流动的黄金；个体不再是数据的被动贡献者，而是价值的主动创造者。

从数据要素的供给侧改革到数据服务行的基础设施建设，再到实体资产的金融创新，这一演进逻辑清晰地描绘了数字经济的未来方向。这不仅是一场技术的变革，更是一场涉及产权制度、生产关系与治理模式的深刻革命。随着相关法律法规的完善与技术生态的成熟，数据归人与价值共创将成为推动经济高质量发展的核心引擎，引领我们迈向一个更加公平、高效且充满活力的数智时代。

黄科满：面向数据社会化的智能数据空间与治理防线

一、数据社会化的演进逻辑与跨域壁垒

在国家大力推进数据基础设施建设与数据要素市场化的宏观背景下，我们对数据的理解正在经历一场深刻的范式转变。数据战略的核心议题已经从早期的要素化探索，逐渐聚焦于如何构建全国一体化的技术与数据市场。这不仅需要基础设施层面的巨额投入，更预示着下一代信息高速公路的雏形正在形成。

我们需要从理论层面审视这一变革的本质。数据的价值释放实际上是一个社会再生产的过程。历史上，无论是政府机构还是企业主体，早已在内部业务中广泛使用数据，数据库技术也已成熟多年。今天我们之所以重新强调数据的价值，是因为我们试图推动数据走出单一主体的内部循环，进入社会化大生产的广阔天地。这种从私域使用向社会化流通的跨越，意味着数据将在生产、消费、交换和分配的各个环节引发效率的质变。

然而，数据一旦尝试突破原有的边界，就会面临多重复杂的挑战。我们将这种挑战总结为三个层面的跨域难题。

首先是物理层面的跨地域连接。这不仅仅指光纤与网络的铺设，更涉及到异构系统之间的物理互联，是数据流通的物质基础。

其次是更为棘手的管辖域突破。这是数据社会化面临的最大制度性障碍。在单一主体内部，管理者可以通过行政命令强制要求所有员工和系统遵循统一的数据标准与操作

规范。然而，当数据流转跨越了组织边界，进入社会公共空间时，不同的主体往往遵循着各自的标准体系与管理规范。这种各说各话的局面，使得数据在跨越管辖边界时面临着巨大的协同成本。如何让不同管理体制下的数据系统实现对话，是技术架构必须解决的核心问题。

最后是跨越信任域的挑战。当数据离开生产者的控制范围，流向外部需求方时，接收方难以验证数据的真实性与完整性。这就是所谓的承诺数据与交付数据之间可能存在的偏差。在缺乏有效信用背书的情况下，跨主体的数据协作往往因为信任赤字而难以达成。

因此，数据社会化的核心目标，就是通过技术与制度的创新，打通物理域、管辖域与信任域的壁垒，建立一套能够支撑数据在不同主体间自由、安全、可信流转的全新体系。

二、数据空间：自治与互联的数据网络架构

为了应对上述跨域挑战，学界与产业界正在探索基于数据空间的新型数据基础设施架构。不同于传统的大数据中心或集中式数据湖，数据空间本质上是一个由众多独立自治的数据域所组成的动态连接网络。

在这个网络中，每一个节点，无论是大型医院、金融机构还是政府部门，都保留了对自己数据的完整控制权和管理权。数据空间并不试图将所有数据物理汇聚到一处，而是通过一套标准化的协议与连接器，将这些分散的节点串联起来，形成一张价值共创的动态自适应网络。这种架构类似于电力网格，每个电厂独立发电，但通过统一的电网进行调度与输送。

构建这样一个高效的数据空间，需要经历三个关键的演进步骤，这同时也定义了数据空间所需具备的基础能力。

第一步是组织内部的数据准备与汇聚。这是数据社会化的基石。每个主体首先需要在内部建立一套高质量、可动态更新的数据目录。这与过去为了应对审计而建立的静态资产目录有着本质区别。动态目录需要实时反映业务系统中数据的变化状态，确保对外展示的数据资源是鲜活且可用的。这背后需要强大的自动化元数据管理技术作为支撑，仅依靠人工维护在规模化场景下是不可持续的。

第二步是建立对外开放的流通通道。通道的建立看似简单，实则包含了复杂的形态选择。根据数据敏感度和应用场景的不同，流通的内容可以是原始数据，可以是经过脱敏处理的脱敏数据甚至是合成数据，也可以是计算模型本身。特别是在涉及隐私计算的场景中，如医疗科研数据的共享，往往采用数据不动模型动的策略。例如，在多中心医疗研究中，各家医院的数据不出本地，而是让科研模型在不同医院的节点间流转训练，最终聚合出具有全样本特征的智能模型。这种通道技术的多元化，使得数据空间能够在保障安全的前提下实现价值的最大化流通。

第三步是面向需求的动态网络协同。当外部的业务需求产生时，系统需要具备智能化的调度能力，自动在数据域网络中检索匹配的通道，并将它们动态串联起来形成服务链条。例如，当一个智慧城市的防汛决策需要调用气象数据、交通数据和水务数据时，数据空间能够迅速识别分布在不同部门的数据服务，并将其组合成一个综合性的决策支持产品。

这种从内部准备到通道开放再到动态网络协同的过程，构成了数据空间的典型的价值释放过程。特别注意的是，数据空间的建设，不追求一步到位，而是强调在具体的业务循环中持续迭代，逐步形成覆盖全社会的数据基础设施体系。

三、智能治理：跨越自然语言与机器规则的语义鸿沟

如何高效治理数据空间中的数据访问行为，确保数据在合规的框架下流通，是一个关键命题。在数据流通中，我们需要明确界定谁在什么时间、什么条件下可以访问哪些数据。这涉及到复杂的访问控制策略与法律合规审查。

目前，国际上广泛采用开放数字权利语言ODRL（开放数字权利语言）作为数据空间及其策略描述的标准。ODRL基于资源描述框架（RDF）来描述数据的使用规则。然而，这种严谨的机器语言对于人类管理者而言存在着巨大的认知门槛。现实世界中的法律法规、企业隐私政策以及合作协议，通常是以自然语言的形式存在的。让法务人员或数据管理者直接编写复杂的ODRL代码，不仅效率低下，而且极易出错。

为了解决这一人机交互的痛点，我们引入了大语言模型作为治理体系的翻译官。我们致力于构建一个智能化的转换系统，其核心任务是将非结构化的自然语言规则，自动、准确地转化为机器可读的ODRL策略代码。

这项工作面临着巨大的挑战，因为人类的语言习惯与机器的逻辑结构存在显著差异。为了训练这一系统，我们收集整理了涵盖欧盟GDPR、国内数据安全法以及各类行业规范在内的700多个典型规则样例。通过对这些样例进行深度的结构化拆解与重写，我们构建了一个高质量的任务数据集。

在技术实现上，我们构建了一种多阶段的处理流程。首先，利用大模型对复杂的自然语言政策进行语义理解与逻辑重构，将其拆解为若干个原子的规则意图；随后，将这些原子意图映射到ODRL的词汇表中；最后，生成符合语法规范的策略代码。

实验结果令人振奋。基于我们的框架，以及设计的提示工程与微调策略，该系统在规则转换的准确率上达到了95%以上。这意味着，在未来的数据空间治理中，管理者只需用自然语言表达管控意图，例如该医疗数据仅允许在工作日的9点至17点被认证的科研机构访问，系统即可自动生成并部署相应的数据使用规则。这种智能化的治理手段，有效地填补了上层管理意图与底层技术实现之间的语义鸿沟，为数据空间的落地进一步铺平道路。

四、多智能体协同下的数据供应链安全防线

数据空间作为一种智能化的数据服务生态，大量的智能体Agent被引入系统中，它们不仅负责数据的检索与匹配，还能够自动执行复杂的数据分析与任务调度。这种多智能体协同的工作模式，极大地提升了系统的运行效率，但也引入了全新的安全风险。

在多智能体系统中，我们面临着一种新型威胁。一个复杂的数据处理任务往往由多个智能体协作完成，它们之间形成了紧密的依赖关系。这种结构使得系统对于单点故障极为敏感。如果攻击者成功攻破了链条中的某一个智能体，向其植入恶意逻辑，或者诱导其产生错误的输出，这种危害就会沿着协作链条迅速扩散，最终导致整个系统的输出结果被篡改，甚至引发敏感数据的隐蔽泄露。

为了量化这种风险，我们设计了一系列攻防演练实验。在实验中，我们模拟了两种典型的攻击场景：一种是针对输入的恶意诱导，即通过精心构造的提示词诱骗智能体执行违规操作；另一种是针对智能体本身的供应链投毒，即模拟某个开源智能体在版本更新中被植入了恶意代码。

实验结果揭示了一个反直觉且令人警惕的现象：越是参数量巨大、推理能力先进的大模型，在面对此类精心设计的供应链攻击时，往往表现出更高的脆弱性。这是因为先进模型具备更强的指令遵循能力，一旦攻击者成功绕过其安全对齐机制，模型就会更

高效地执行恶意指令。而绕过其安全对齐机制，当前所需成本非常低。

基于此，我们提出了一种基于安全围栏的防御策略。这种策略的核心思想在于为系统输入和进入数据空间的智能体进行安全加固，以此提升整个系统的安全韧性，有效提升数据空间整体的安全水平。

此外，传统的防御思路往往倾向于对每一个智能体进行全方位的加固。然而，在动辄包含数百个智能体的复杂系统中，这种全面防御的策略不仅资源消耗巨大，且边际效益递减。更加重要的是，并非全面防御就能够得到更好的安全水平。相反，对关键交互节点的安全加固，将有限的安全资源集中在了最关键的控制点上，往往能够以最小的成本换取了系统整体安全水位的显著提升。

总之，在数据社会化的深水区，智能数据空间的安全治理需要从分散的单点防御走向体系化的架构防御，为数据的自由流通构建起一道坚实的智能防线。

五、结语

数据社会化不仅是技术架构的革新，更是生产关系的重构。从突破物理、管辖与信任的三重边界，到构建自治互联的数据空间；从利用大模型实现自然语言到机器规则的智能转换，到建立应对多智能体安全风险的安全防线，这一系列探索不断完善保障数据要素价值释放的治理体系。随着相关技术的不断成熟与落地，我们有理由相信，一个高效、可信、智能的智能化数据空间将逐步形成和成熟，提速数据社会化进程，为数字经济的高质量发展提供源源不断的动力。

王清：以“十五五”规划引领创新方向，筑牢成果转化制度根基

一、“十五五”规划下创新与转化的核心逻辑

“十五五”规划的出台标志着我国创新发展进入全新阶段，国家创新战略从“规模化布局”正式转向“精度化赋能”。这一转型的核心要义在于推动科技创新与产业创新深度融合，将创新资源集中投向国家战略急需领域、产业卡脖子环节以及民生关键问题，为创新创业活动提供坚实的制度保障与清晰的方向指引。

在这一政策框架下，创新创业与成果转化形成了“选拔赛”与“团体赛”的协同关系。政策为创新划定了明确的赛道边界，创新创业需要紧密依托国家政策导向，聚焦核心领域开展探索；而成果转化则是创新价值的最终落地环节，需要政府、高校、企业、资本等多方力量协同发力，共同将创新创意转化为现实生产力。二者相辅相成，缺一不可，构成了“十五五”时期创新发展的核心逻辑。

精度化赋能作为“十五五”规划创新战略的核心内涵，主要体现在三个维度：其一，目标精准，摒弃“大水漫灌式”的资源投放，将创新力量集中于国家战略急需、产业发展瓶颈、民生改善关键等核心领域，确保创新方向不偏离实际需求；其二，资源靶向，打通基础研究、应用研究到成果转化的全链条资源供给，针对不同创新阶段的特点提供精准支持，解决创新链条中的断点与堵点问题；其三，生态协同，打破部门之间、院校与产业之间的壁垒，构建政策、市场、主体联动的一体化创新生态，让创新资源自由流动，最大化提升创新效率。